Intel® Management and Security Status Application

User's Guide

July 16, 2008
Revision Version: 0.96

Intel Confidential

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

Revision History

Version	Modification
June 05	Initial version received from PAE (bschrei), legal disclaimer modification
June 12	Revision History table addition
June 15	.NET framework installation (section 3.1) addition, with first differences between 4.x and 5.x
June 16	Added Troubleshooting section with the loading time and the error message descriptions
June 22	Corrected sections suggested by hyitzhak
June 22	Corrected section suggested by nradian
June 26	Added version numbering, and general corrections by nradian
version 0.9	Corrected text, formatting and troubleshooting section.
version 0.95	Added information about the time between polls and the refresh of data in the application
Version 0.96	Fixed chapter 3.1 (On installing the framework) according to bschrei comments.

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) and Intel® Trusted Platform Module (Intel® TPM) services.

The Intel® Management and Security Status icon indicates whether Intel® AMT and Intel® TPM are running on the platform. The icon is located in the notification area. By default, the notification icon is displayed every time Windows* starts.

Note: The Intel® Management and Security Status icon will be loaded to the notification area only if Intel® AMT or Intel® TPM is enabled in the platform.

Note: The information displayed in the Intel® Management and Security Status is not shown in real time. The data is refreshed every 10 seconds.

2 System Requirements

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

- Intel® AMT versions 4.x or 5.x.
- Windows* XP or Windows Vista* 32/64
- Microsoft* .NET Framework 2.0 or 3.5
- The Intel® MEI driver. Instructions on installing Intel® MEI can be found in the Bring Up Guide document.
- The LMS/SOL or Intel® TPM drivers. The Intel® Management and Security Status Application is bundled with these drivers. Installing either of these drivers also installs the application.

3 Installing the LMS/SOL or Intel® TPM Drivers

The Intel® Management and Security Status Application is automatically installed and invoked when either the LMS/SOL driver or the Intel® TPM driver is installed. This section describes how to install these drivers.

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

Note: Intel® AMT versions 4.x install the appropriate .NET framework automatically as part of the software package installation. For Intel® AMT versions 4.x, skip to section 3.2.

3.1 Installing Microsoft* .NET Framework 3.5

1. Download Microsoft .NET Framework 3.5 (**dotnetfx35.exe**) from the same location where the Intel® AMT kit is obtained. Installing the version available in that location ensures that you are using the latest version required by the software package.
   The installation 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.

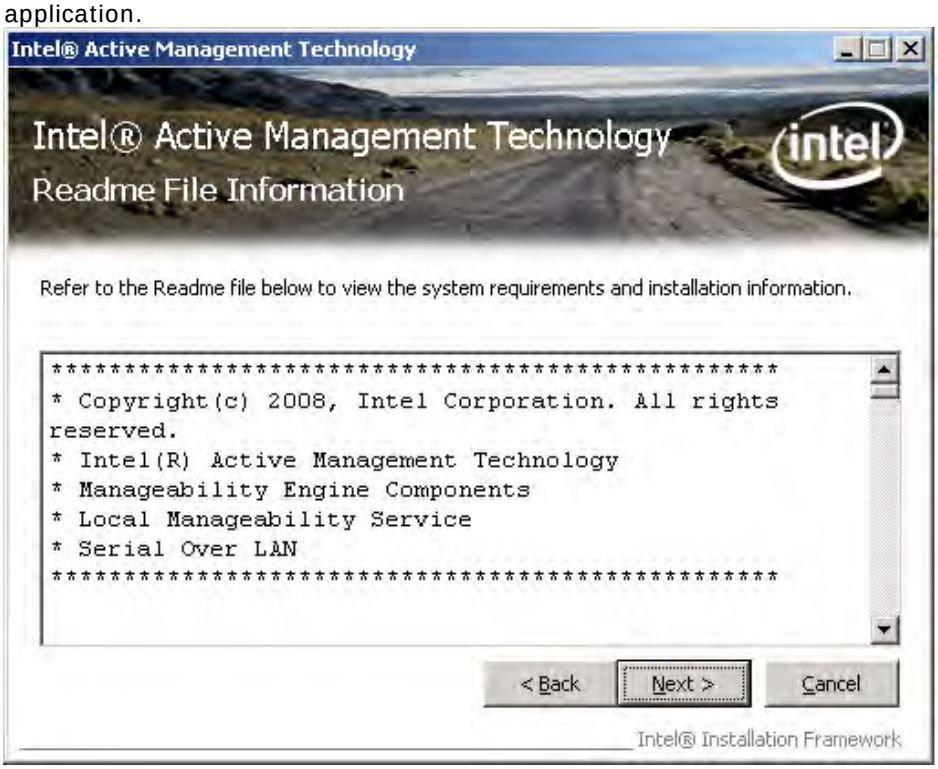
4. When the installer finishes, press the **Finish** button.

3.2 Installing the LMS/SOL or Intel® TPM driver

1. Double-click **LMS_SOL\setup.exe** or **TPM\setup.exe** to install the LMS/SOL driver or Intel® TPM driver, respectively. The Welcome window opens.

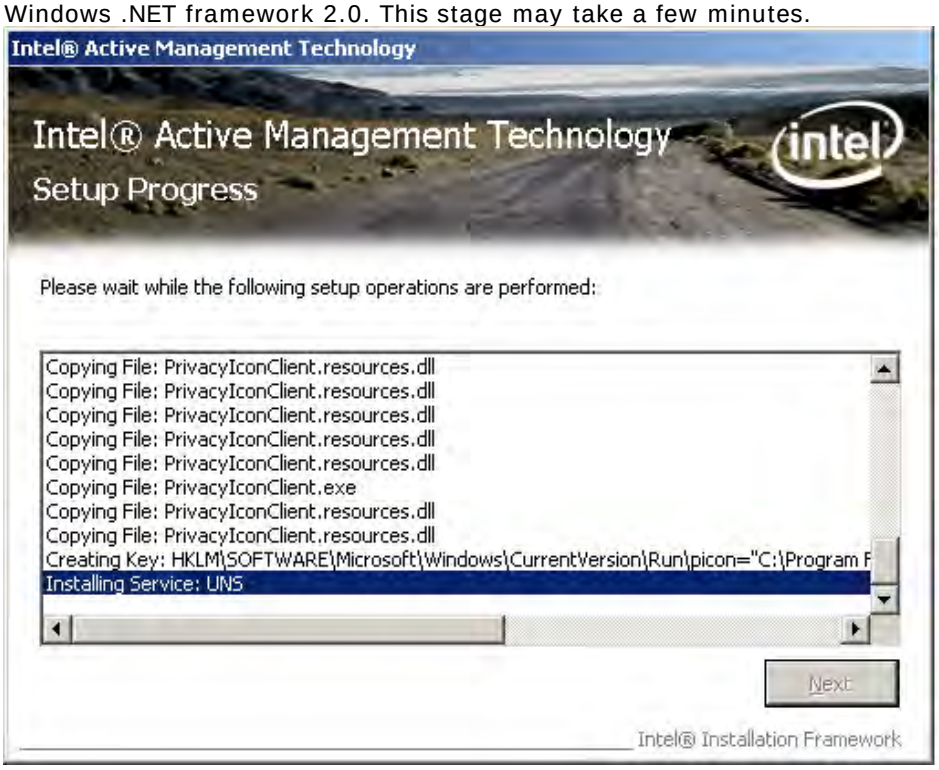
2. Click **Next**. The License window opens.

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



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

Note: In Intel® AMT versions 4.x the installation process also installs Microsoft* Windows .NET framework 2.0. This stage may take a few minutes.



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 or Intel® TPM is enabled, Intel® Management and Security Status icon is loaded into the notification area when Windows* start. It can also be started using the shortcut located in **'All Programs\ Intel® Management and Security Status'** in the Windows* start menu.

While the Intel® Management and Security Status 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.

To view the Intel® Management and Security Status Application:

- Double-click the Intel® Management and Security Status icon, or
- Right-click the icon and choose **Open**, or
- Use the shortcut located in **'All Programs\ Intel® Management and Security Status'** in the Windows* start menu.

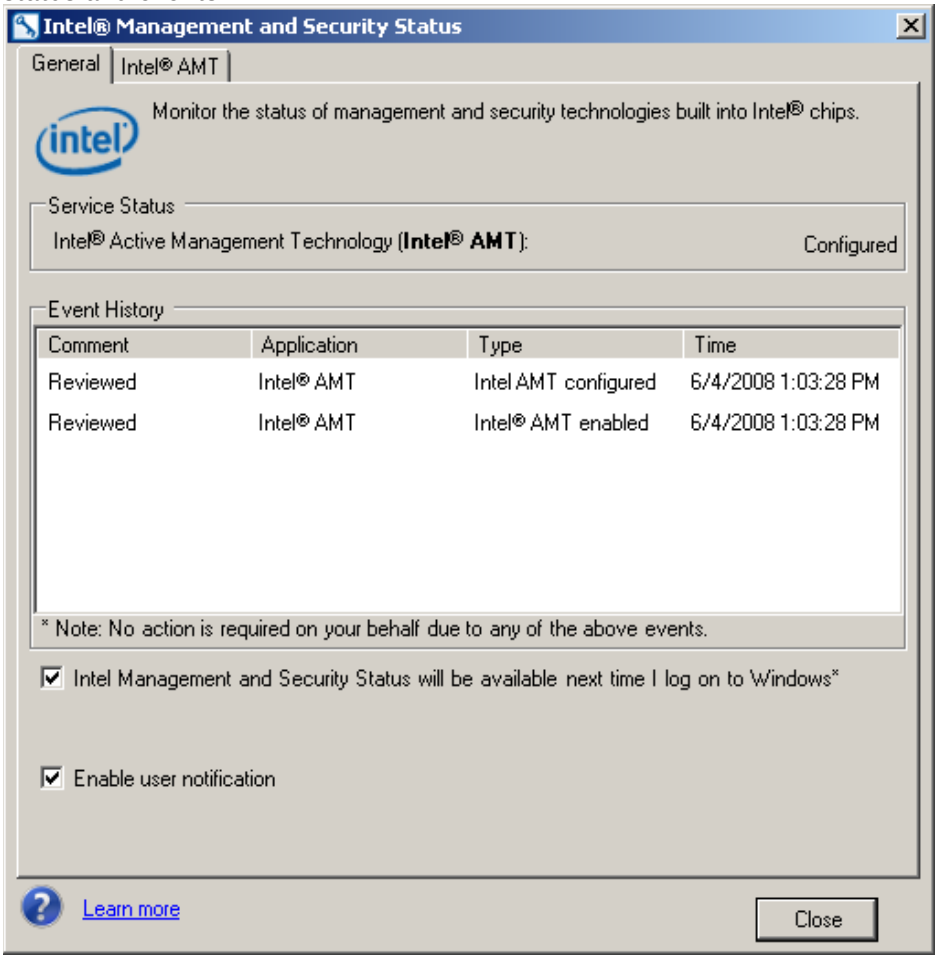
To close the Intel® Management and Security Status icon and application:

Right-click the icon and choose **Exit**.

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

4.1.1 General Tab

The **General** tab provides basic information about the Intel® AMT and Intel® TPM status and events.



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

The status of Intel® AMT and Intel® TPM is displayed in the **Service Status** group box. The status may be one of the following:

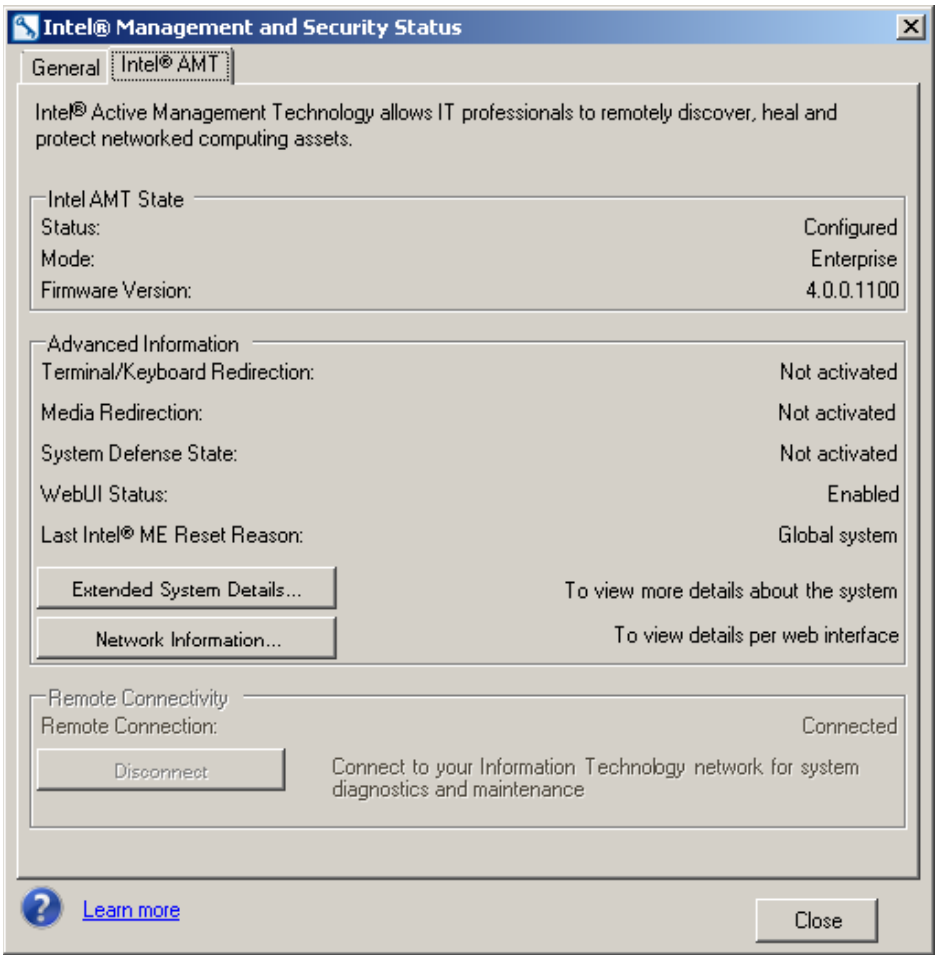
- Intel® AMT: Configured / Unconfigured / Not detected / Information unavailable.
- Intel® TPM: Operational / Not detected.

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*.

Enable user notification: Allow the Intel® Management and Security Status icon to display notifications in the notification area when one of the technologies is enabled or disabled.

4.1.2 Intel® AMT Tab

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



4.1.2.1 Intel AMT State

The following information is provided:

- **Status**

  The operational status of Intel® AMT.
  Possible values: Configured / Unconfigured / Not detected / Information unavailable.

- **Mode**

  The operational mode of Intel® AMT.
  Possible values: Enterprise / Small business / Awaiting configuration / Disabled / Not detected.

- **Firmware Version**

  The Intel® AMT firmware version.

4.1.2.2 Advanced Information

The following information is provided:

- **Terminal/Keyboard Redirection**

  Indicates whether there are any open terminal/keyboard redirection sessions.
  Possible values: SOL activated / Not activated.

- **Media Redirection**

  Indicates whether there are any open IDE redirection sessions.
  Possible values: IDER activated / Not activated.

- **System Defense State**

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

- **WebUI Status**

  Indicates whether a remote user can view or change Intel® AMT information via the Web UI.

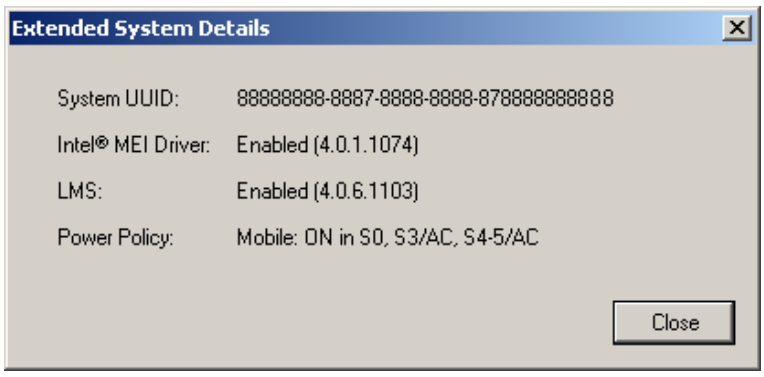
  Possible values: Enabled on TLS / Enabled / Not enabled.

- **Last Intel® ME Reset Reason**

  Displays the reason that the Intel® AMT was last reset.
  Possible values: Global System / FW reset

- **Extended System Details button**

  Click the **Extended System Details** button to show additional Intel® AMT information:



  - **System UUID**

    The current System Unique Universal Identification. Standard System UUID presentation, such as, 03000200-0400-05AA-0006-000700080009

  - **Intel® MEI Driver**

    The version of the Intel® Manageability Engine Interface driver.
    States are: Enabled(x.x.x.x) / Disabled(x.x.x.x) / Uninstalled

  - **LMS Driver**

    The version of the LMS service.
    States are: Enabled(x.x.x.x) / Disabled(x.x.x.x) / Uninstalled

  - **Power Policy**

    The power policy which is currently in effect.
    States are: ON in S0, or any other power policy supported by the system.

Click **Close** to return to the **Intel® AMT** tab.

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

Under **Interface Type**, click either **Wireless Connection** or **Wired Connection** to display information on the following items for the selected interface (only wired information is available in Intel® AMT 5.x):

- **Mode**

  Possible values: Static / DHCP

- **MAC Information**

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

- **Link Status**

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

- **IP Information**

  X.X.X.X – e.g. 10.102.0.1

- **Configured for Wireless**

  Possible values: Wireless disabled / Wireless enabled

4.1.2.3 Remote Connectivity

The Remote Connectivity section provides CIRA (Client Initiated Remote Access) capabilities, which allow a user to connect the Intel® AMT system to the company's Information Technology network from an external internet connection.

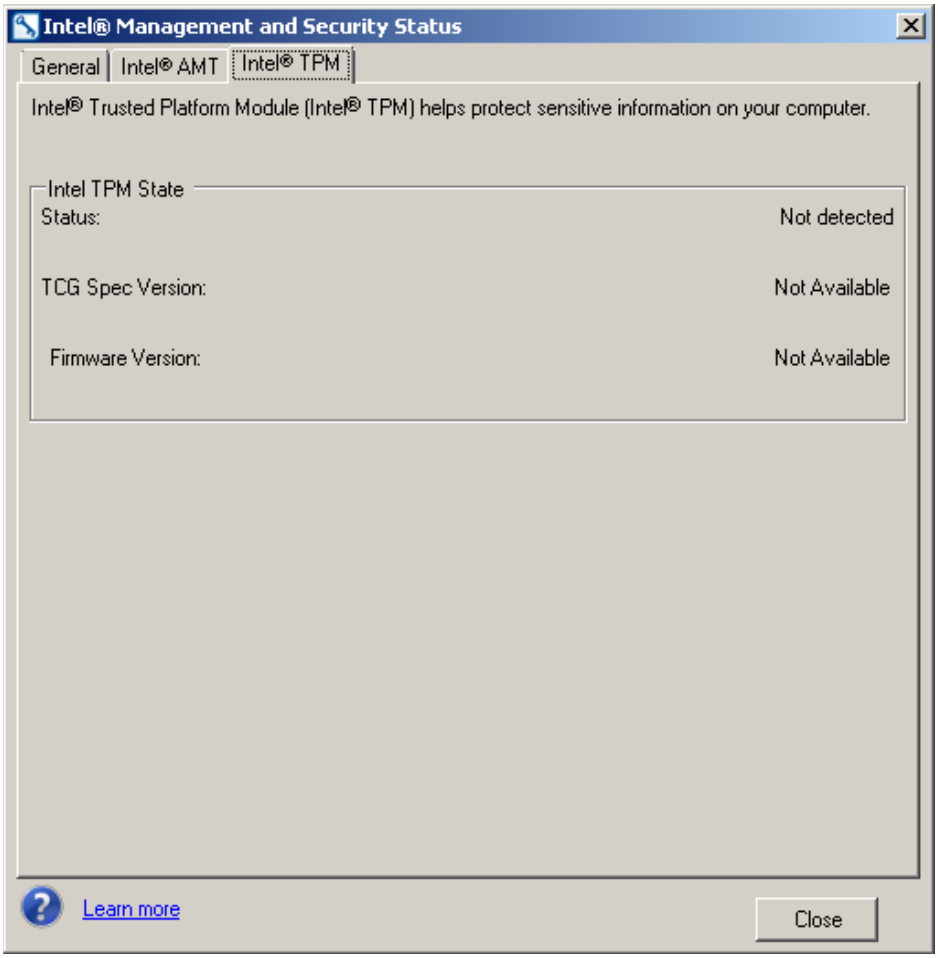
Click the **Connect** button to connect to your Information Technology network for system diagnostics and maintenance. The current connection status is displayed in the Remote Connectivity section.

Note: The information displayed in the Intel® Management and Security Status, including in the remote connectivity section, is not shown in real time. The data is refreshed every 10 seconds.

4.1.3 Intel® TPM Tab

Note: The Intel® TPM tab is visible only if Intel® TPM is supported by the platform.

Click the **Intel® TPM** tab to view Intel® TPM information.



In the **Intel TPM State** section, the following information is displayed:

- **Status –** The operational status of the Intel® TPM, comprising up to 3 parameters**.**

  The displayed status is one of the following combinations:

  - Operational - Active ; Enabled ; Owned
  - Operational - Active ; Enabled ; Not Owned
  - Operational - Active ; Not Enabled; Owned
  - Operational - Active ; Not Enabled ; Not Owned
  - Operational - Not active ; Enabled ; Owned
  - Operational - Not active ; Enabled ; Not Owned
  - Operational - Not active ; Not Enabled; Owned
  - Operational - Not active ; Not Enabled ; Not Owned

- Failed - Flash corrupted
- Failed - HW failure
- Failed - ME reset
- Failed - Unknown
- Not detected

- **TCG Spec Version**

  The Trusted Computing Group version with which this Intel® TPM is compliant.

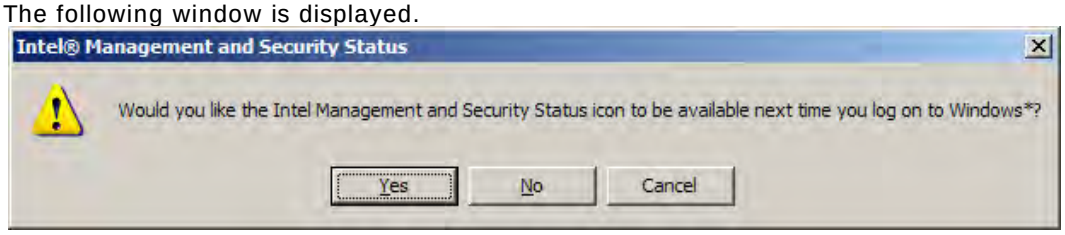
- **Firmware Version**

  The firmware version of the Intel® TPM.

4.2 Exiting the Application

To exit the application, right click on the Intel® Management and Security Status Application 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 Troubleshooting Intel® Management and Security Status

5.1 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 will display the following error message if no .NET framework is present in the system:

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

5.2 Application takes a long time to load

In Intel® AMT 4.x, if the machine is connected to a network, but without internet access, the status application may take up to 2 minutes to load while the system retrieves the Digital Signature Certificate information (it will not prevent other software from loading or stop the operating system from being operational).

To avoid this situation, please follow one of the options below:

1. Internet Access – Provide Access to the revocation list at VeriSign site by granting an open Internet connection with firewall permissions to access the Verisign query (located at **http://CSC3-2004-crl.verisign.com/CSC3-2004.crl**).

2. Changing Internet explorer settings – This will disable the certificate revocation checking for the entire system: Navigate to **IE -> Tools ->**

Internet Options-> Advanced and uncheck the **Check for publisher's certificate revocation** box.

Note: Modifying this Internet Explorer option will disable the certificate revocation checking for the entire system.

3. Unsigned application – use the unsigned version of the executable, available in the kit under the **unsigned_IMSS** folder (just replace one file by the other).

4. .Net framework 3.5 - Install the .Net framework 3.5 and create a file named **PrivacyIconClient.exe.config** alongside the **PrivacyIconClient.exe** with the following content:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <runtime>
   <generatePublisherEvidence enabled="false"/>
  </runtime>
</configuration>
```

5. Manual download of the revocation list – Manually download the Certificate Revocation List from VeriSign at **http://crl.verisign.com** and install it on the system. The CRL is valid for 10-15 days, so this step must be repeated in a frequent base.

5.3 '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, 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 Intel® MEI driver is installed, enabled and functioning properly. Please review the Bring Up Guide document for more information concerning this driver.

5.4 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.