



Intel[®] Management and Security Status Application

User's Guide

June 5, 2008

Revision 0.8

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.

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/

The original equipment manufacturer must provide TPM functionality, which requires a TPM-supported BIOS. TPM functionality must be initialized and may not be available in all countries.

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 © 2008, 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	Installing and Running the LMS/SOL or Intel® TPM Drivers.....	8
3.1	Using the Intel® Management and Security Status Application	11
3.1.1	General Tab.....	12
3.1.2	Intel® AMT Tab	13
3.1.3	Intel® TPM Tab	17
3.2	Exiting the Application	18



Revision History

Revision Number	Description	Revision Date
0.8	Initial release.	June 2008

§



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

Note: The Intel® Management and Security Status Application icon is displayed only if Intel® AMT or Intel® TPM is enabled in the platform.



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.
- 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.
- The Intel® MEI driver.
- Windows * XP or Windows Vista* 32/64
- .NET Framework 2.0



3 *Installing and Running 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.

To install 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.





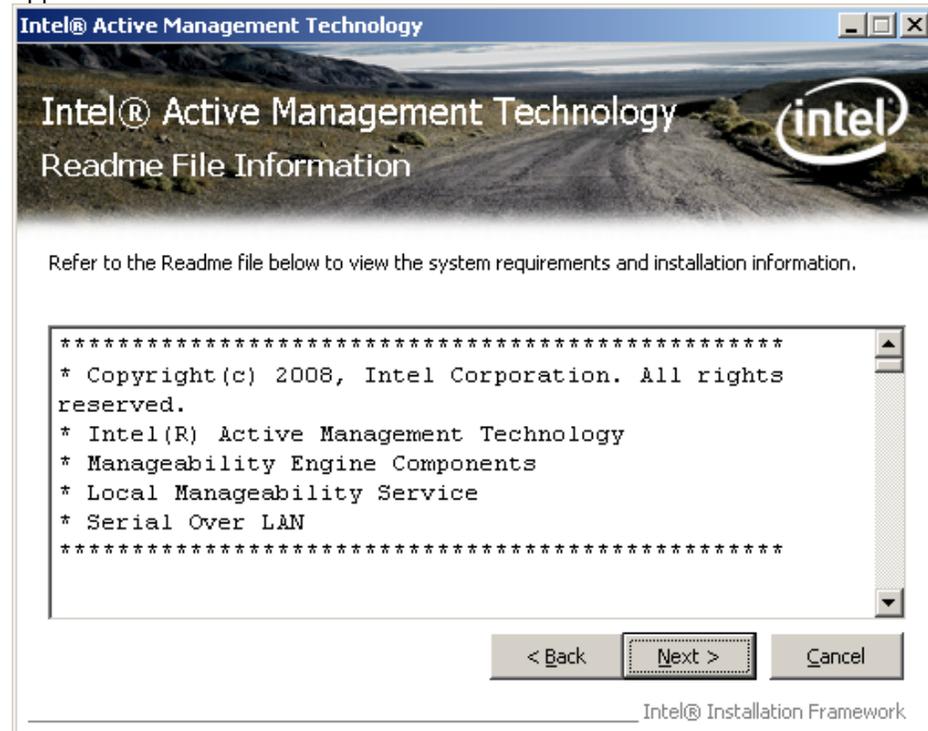
2. Click **Next**. The License window opens.



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



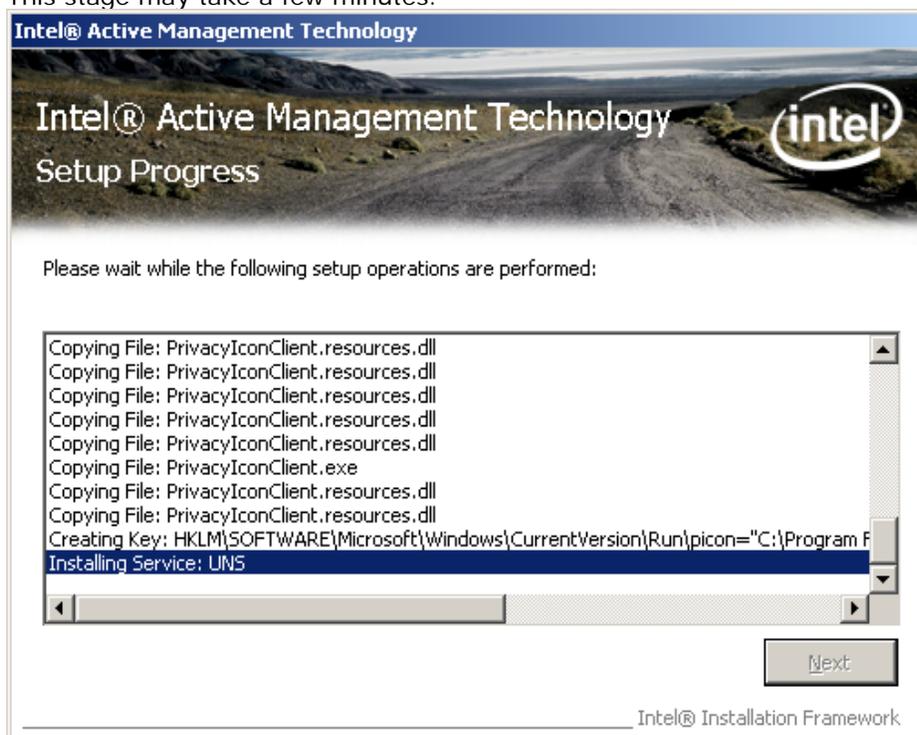
application.





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

Note: 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.
6. To run the application, choose **Start > All Programs > Intel Management and Security > Intel Management and Security Status**. Alternatively, in the \LMS_SOL\PICON or TPM\PICON directory, double-click the **PrivacyIconClient.exe** file to run the application.

3.1 Using the Intel® Management and Security Status Application

When the Intel® Management and Security Status Application is running, the Intel® Management and Security Status Application icon is visible on the status bar. 

To view the Intel® Management and Security Status Application information:

Double-click the icon, or right-click the icon and choose **Open**.

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

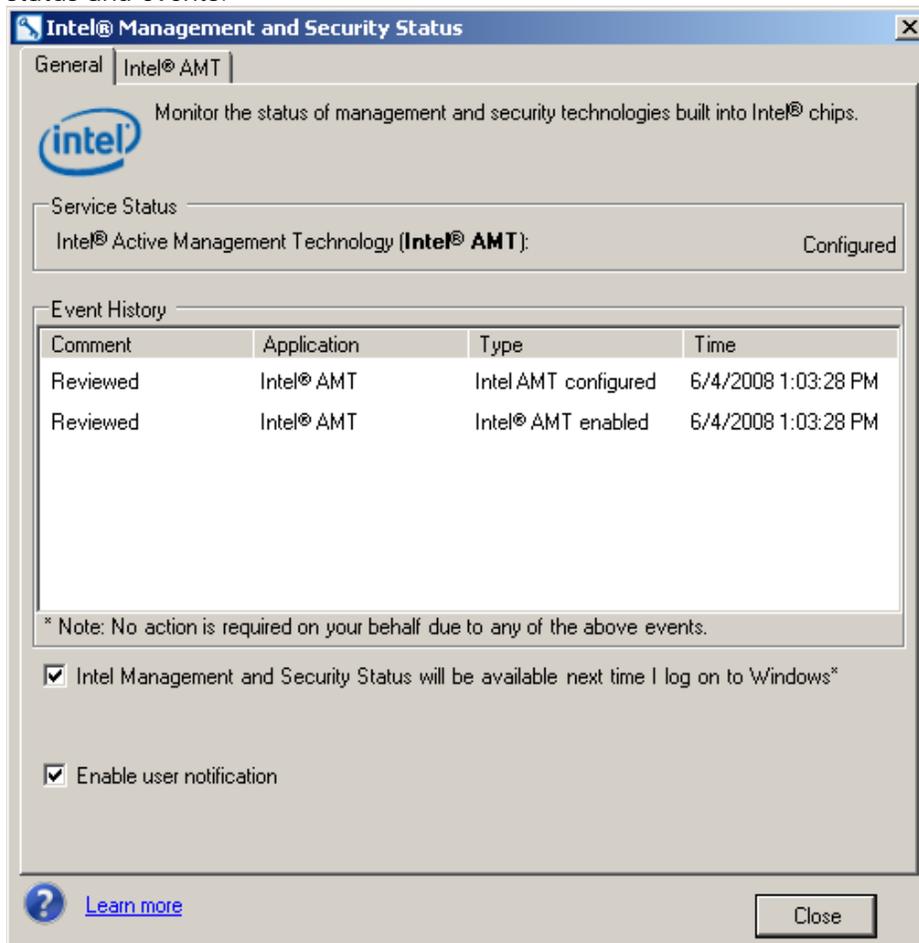


To stop the Intel® Management and Security Status Application:

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

3.1.1 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/Unavailable.
- Intel® TPM: Operational/Not detected.

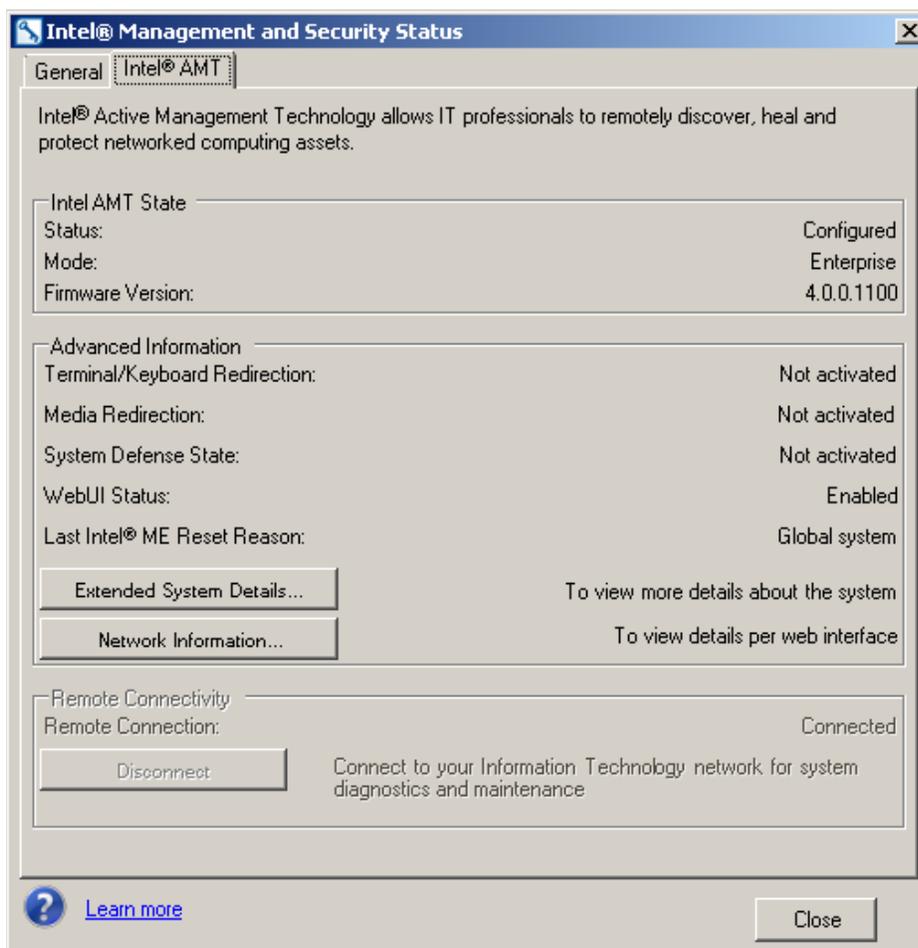


Intel Management and Security Status will be available next time I log on to Windows: Checking this box causes the Intel® Management and Security Status Application to be invoked, and the icon to be displayed, whenever you log on to Windows*.

Enable user notification: Allow the Intel® Management and Security Status Application to display notification balloons in the notification area.

3.1.2 Intel® AMT Tab

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



3.1.2.1 Intel AMT State

The following information is provided:

- **Status**

The operational status of Intel® AMT.

Possible values: Configured/Unconfigured/Not detected/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.

3.1.2.2 **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.

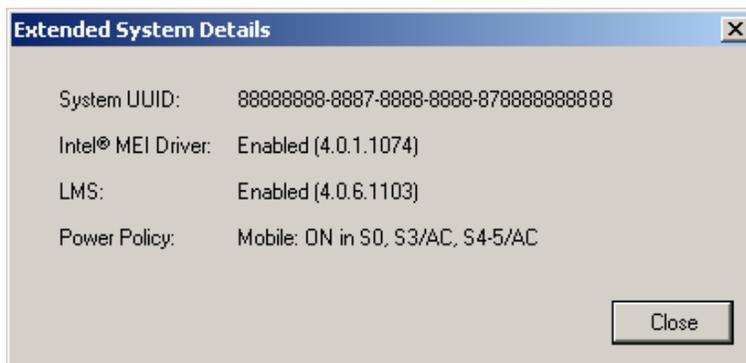
- **Last Intel ME Reset Reason**

Displays the reason that the Intel® AMT was last reset.
Possible values: Intel AMT remote boot/Normal reboot.



- **Extended System Details button**

Clicking this button shows the following additional information about system functions.



- **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 HECI driver.
States are: Enabled(x.x.x.x)/Disabled(x.x.x.x)/Uninstalled

- **LMS Driver**

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

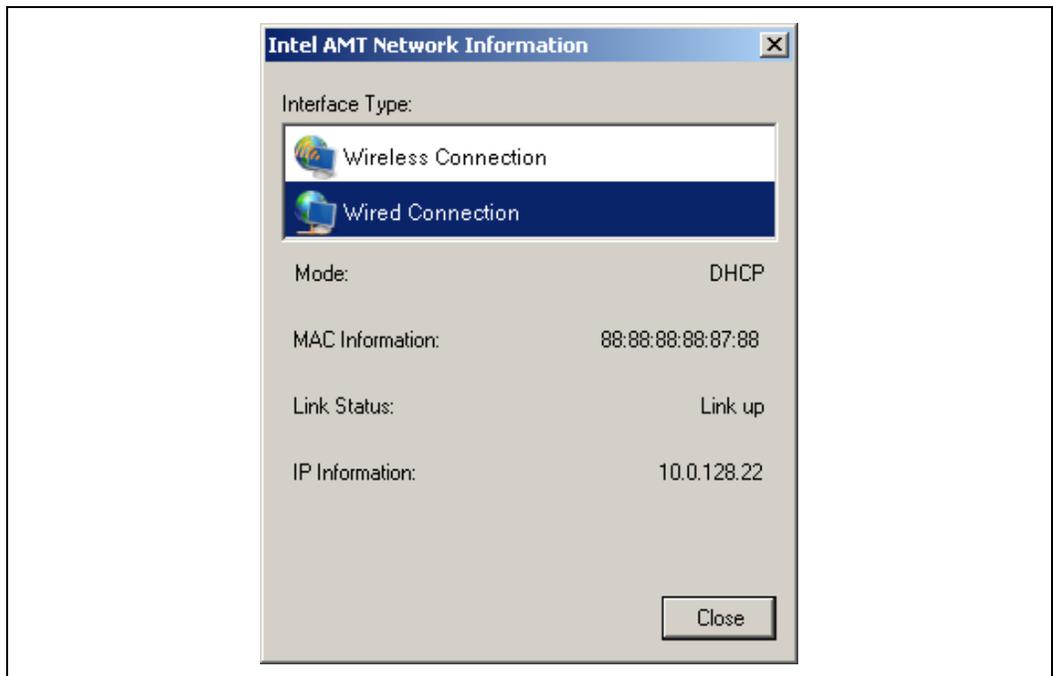
- **Power Policy**

The power policies currently in place.
States are: Mobile: ON in S0, or any other power policy

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



Click the **Network Information** button to display details regarding either wireless or wired connections present in the computer.



Under **Interface Type**, click either **Wireless Connection** or **Wired Connection** and information on the following items for the selected interface type is displayed:

- **Mode**

Possible values: Static/DHCP

- **MAC Information**

XX:XX:XX:XX:XX:XX – 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 – 10.102.0.1

- **Configured for Wireless**

Possible values: Wireless disabled/Wireless enabled



3.1.2.3 Remote Connectivity

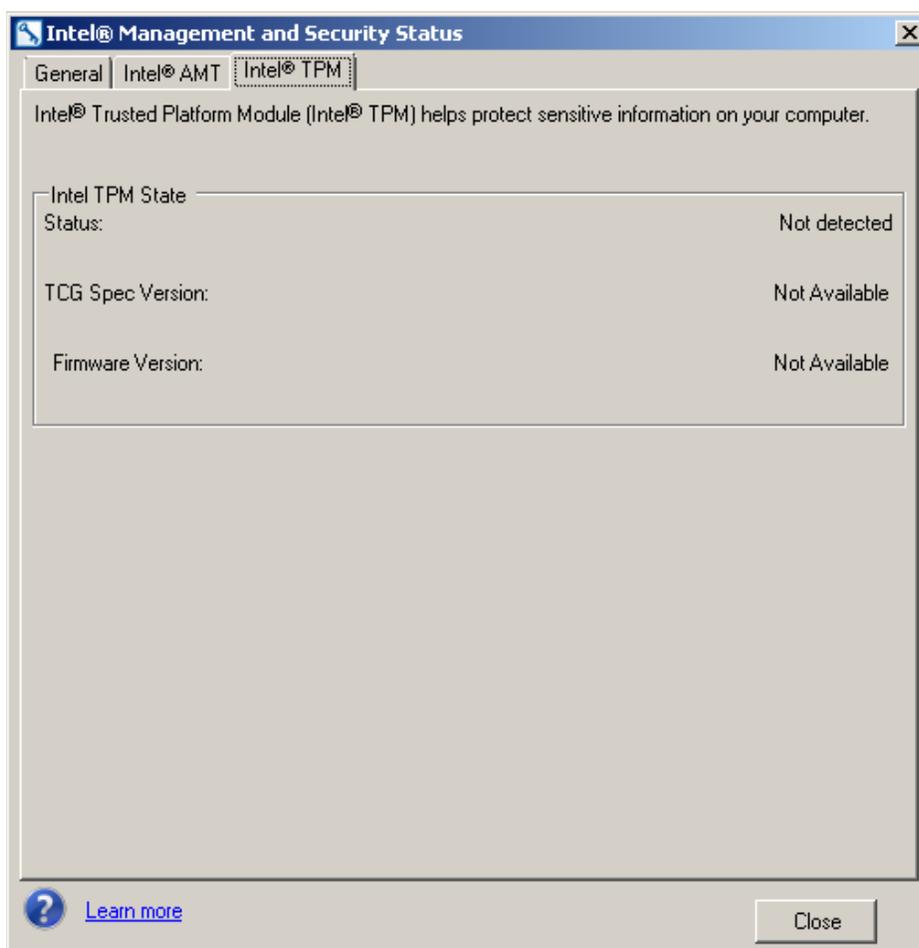
The remote Connectivity section deals with CIRA (Client Initiated Remote Access), which allows a user to connect the Intel® AMT system to the company's information technology network from an external internet connection.

Click the **Connect** button to create a tunnel from outside the network to a management console to enable remote diagnostics and repair.

3.1.3 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** group box, 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 ; Enabled ; Not Owned**
 - **Operational - Not active ; Enabled ; Owned**
 - **Operational - Not active ; Enabled ; Not Owned**
 - **Operational - Not active ; Not Enabled; Owned**
 - **Operational - Not active ; 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.

3.2 Exiting the Application

To exit the application, right click on the Intel® Management and Security Status Application icon in the System tray 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.