



Intel[®] Management and Security Status Application

User Guide

Supporting Intel[®] CSME Firmware Version 10 and above

October 2023

Revision 2.0



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.

This document contains information on products in the design phase of development.

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 are dependent upon hardware, setup and configuration. For more information, visit <http://www.intel.com/technology/platform-technology/intel-amt>.

Client Initiated Remote Access may not be available in public hot spots or "click to accept" locations. For more information on CIRA, visit <http://software.intel.com/en-us/articles/fast-call-for-help-overview>

KVM Remote Control (Keyboard, Video, Mouse) is only available with Intel® Core™ i5 vPro and Core™ i7 vPro processors with Intel® Active Management technology activated and configured and with integrated graphics active. Discrete graphics are not supported.

No system can provide absolute security under all conditions. Intel® Anti-Theft Technology 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. 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>

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 © 2023 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 various license files in the firmware kit.

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 | 7 |
| 2 | System Requirements | 8 |
| 3 | Using Intel® Management and Security Status Application and Icon | 9 |
| 3.1 | General Tab | 10 |
| 3.2 | Intel® Active Management Technology Tab | 12 |
| 3.2.1 | Fast Call for Help | 14 |
| 3.2.2 | Support Session Status | 14 |
| 3.2.3 | System Defense | 15 |
| 3.3 | Intel® Standard Manageability Tab | 16 |
| 3.3.1 | Fast Call for Help | 17 |
| 3.3.2 | Support Session Status | 17 |
| 3.3.3 | System Defense | 17 |
| 3.4 | Advanced Tab | 18 |
| 3.4.1 | Intel® Management Engine | 18 |
| 3.4.2 | Secure Output Window Settings | 19 |
| 3.4.3 | Network Information | 19 |
| 3.4.4 | Extended System Details | 21 |
| 3.4.5 | Access Monitor | 23 |
| 3.5 | Intel® Unique Platform ID Tab | 24 |
| 3.5.1 | Intel® UPID Status | 24 |
| 3.5.2 | Intel® Platform Service Record (Intel® PSR) | 25 |
| 3.6 | Shutting Down the Intel Management and Security Status Application | 26 |
| 3.7 | Windows* 10 | 27 |
| 4 | Troubleshooting Intel® Management and Security Status | 28 |
| 4.1 | Error Message Appears Upon Application Load | 28 |
| 5 | Intel® Management and Security Status Application Error Codes | 30 |
| 5.1 | Partial Firmware Update Failures | 30 |



Revision History

| Revision# | Description | Revision Date |
|-----------|---|----------------|
| 0.7 | <ul style="list-style-type: none">• Initial Release | June 2020 |
| 0.8 | <ul style="list-style-type: none">• Update revision to 0.8 | August 2020 |
| 0.9 | <ul style="list-style-type: none">• Update copyright year to 2021• Update supported OS in section 2 | January 2021 |
| 1.0 | <ul style="list-style-type: none">• Updated revision to 1.0 for Beta | January 2021 |
| 1.1 | <ul style="list-style-type: none">• Add Fast Call for Help in Intel® Standard Manageability tab | June 2021 |
| 1.2 | <ul style="list-style-type: none">• Remove Anti-Theft Technology | July 2021 |
| 1.3 | <ul style="list-style-type: none">• Add note for MEBx description in section 3.4.4 | September 2021 |
| 1.4 | <ul style="list-style-type: none">• Update copyright year to 2022• Add Windows* 11 in system requirements | February 2022 |
| 1.5 | <ul style="list-style-type: none">• Add disclaimer for Windows* 11 support in system requirement | February 2022 |
| 1.6 | <ul style="list-style-type: none">• Update .NET framework requirement to 4.8 | June 2022 |
| 1.7 | <ul style="list-style-type: none">• Update description about the option "Intel® Management and Security Status application will be available next time I log on to Windows*" in General Tab | November 2022 |
| 1.8 | <ul style="list-style-type: none">• Update copyright year to 2023• Update the description about the startup option | January 2023 |
| 1.9 | <ul style="list-style-type: none">• Update description of Intel® UPID tab | April 2023 |
| 2.0 | <ul style="list-style-type: none">• General cleanup• Update UPID status section | October 2023 |





1 ***Introduction***

This User Guide describes how to use the Intel® Management and Security Status (Intel® MSS) application. The application's tabs display information about a platform's support for Intel® Active Management Technology (Intel® AMT) and Intel® Standard Manageability. These technologies are built on the Intel® Management Engine (Intel® ME), a feature provided within the platform hardware.

The Intel MSS icon indicates whether Intel Active Management Technology or Intel Standard Manageability are running on the platform. The icon is displayed in the taskbar's notification area. By default, each time Windows* starts, the Intel MSS starts and the notification icon is displayed.

If the Intel MSS starts automatically as a result of the user logging on to Windows*, the icon is loaded to the notification area only if a supported combination of Intel Active Management Technology or Intel Standard Manageability is present on the platform. If the Intel MSS is started manually via the Start button, the icon is loaded even if neither of these technologies is enabled.





2 *System Requirements*

The Intel MSS has the following requirements:

- Supported operating systems:
 - Windows 10*
 - Windows 11* (Note**)
 - Windows Server 2019*
- Platform running Intel Management Engine firmware.
- Intel Management Engine software installed.
- Microsoft* .NET Framework: version 4.8 or above


Note: Some Intel systems can be upgraded to Windows 11* but Windows 11* is not POR for those systems. These include (but are not limited to): Raptor Lake, Alder Lake, Rocket Lake, Tiger Lake, Comet Lake, Whiskey Lake, Coffee Lake, Kaby Lake, Sky Lake, Purley, Purley Refresh, Basin Falls, Glacier Falls and older systems. Intel has not validated execution of the Intel MSS on these systems.





3 *Using Intel® Management and Security Status Application and Icon*

Whenever Intel Active Management Technology or Intel Standard Manageability is enabled, the Intel MSS icon is loaded into the notification area when Windows* starts. The Intel MSS can also be started by clicking **Start> All Programs\Intel\Intel® Management and Security Status\ Intel® Management and Security Status**.


The Intel MSS icon is displayed in the notification area while the Intel MSS is running.  The icon is blue if Intel AMT or Intel Standard Manageability are enabled on the computer.

Note: The icon is gray if the Intel MSS User Notification Service is not running or the Intel® Management Engine Interface (Intel® MEI) driver is disabled or unavailable.

To view the Intel MSS:

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

Note: In the classic Start menu, the path includes Programs instead of All Programs.

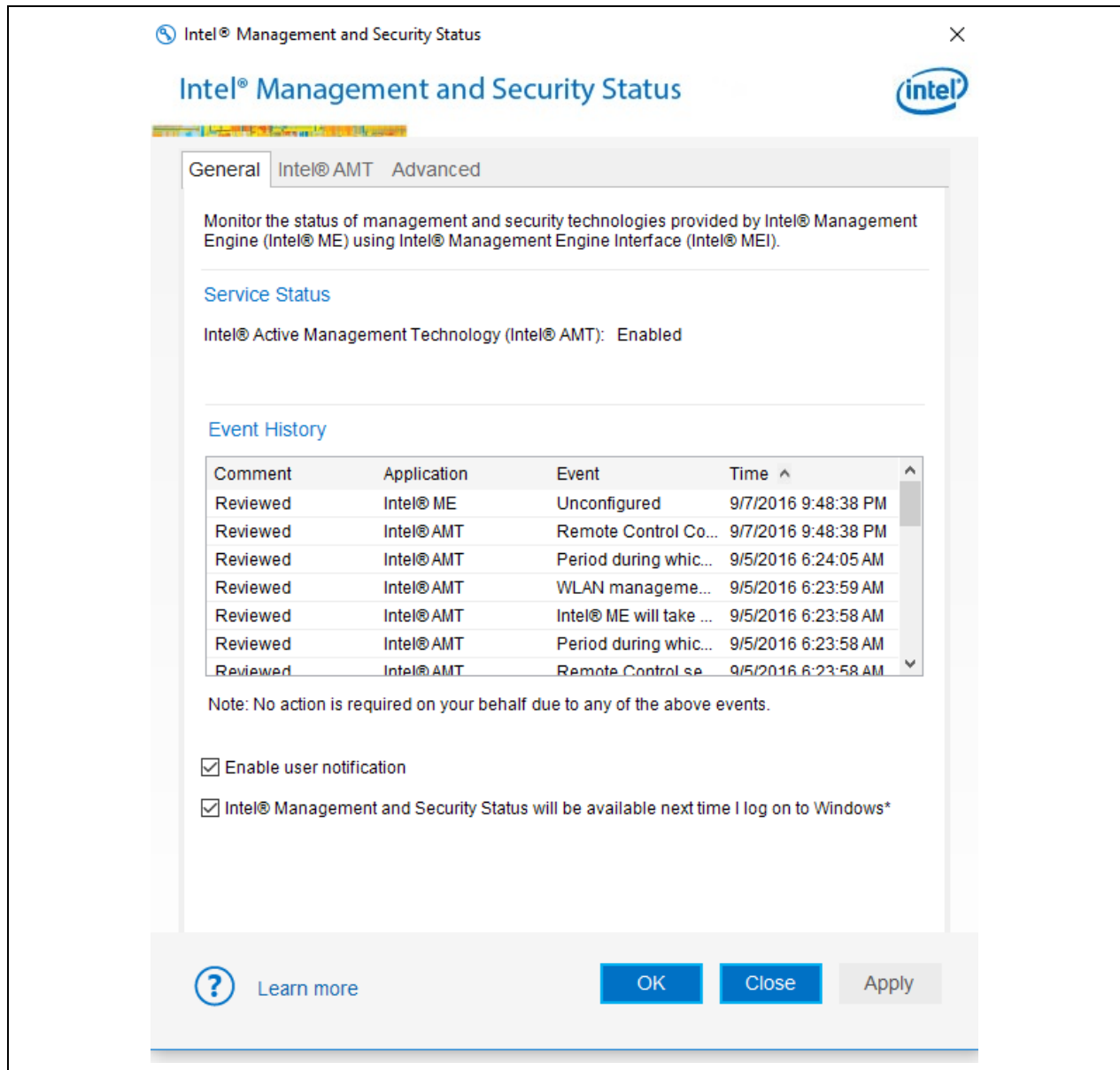
The following sections describe the information available in the application's tabs. Information about the application is available also by clicking the **Learn more** link or the question mark button ().

Note: The application dynamically hides tabs that are not relevant. For example, the Intel UPID tab does not appear if the platform does not support Intel UPID.



3.1 General Tab

The **General** tab provides status information about Intel AMT, Intel Standard Manageability, and events related to these technologies.





The **Event History** section displays events and some of their. These can be sorted by clicking on the relevant column header.

The status of Intel Active Management Technology or Intel Standard Manageability is displayed in the **Service Status** section, depending on which technology is operational on the system. The status can be one of the following:

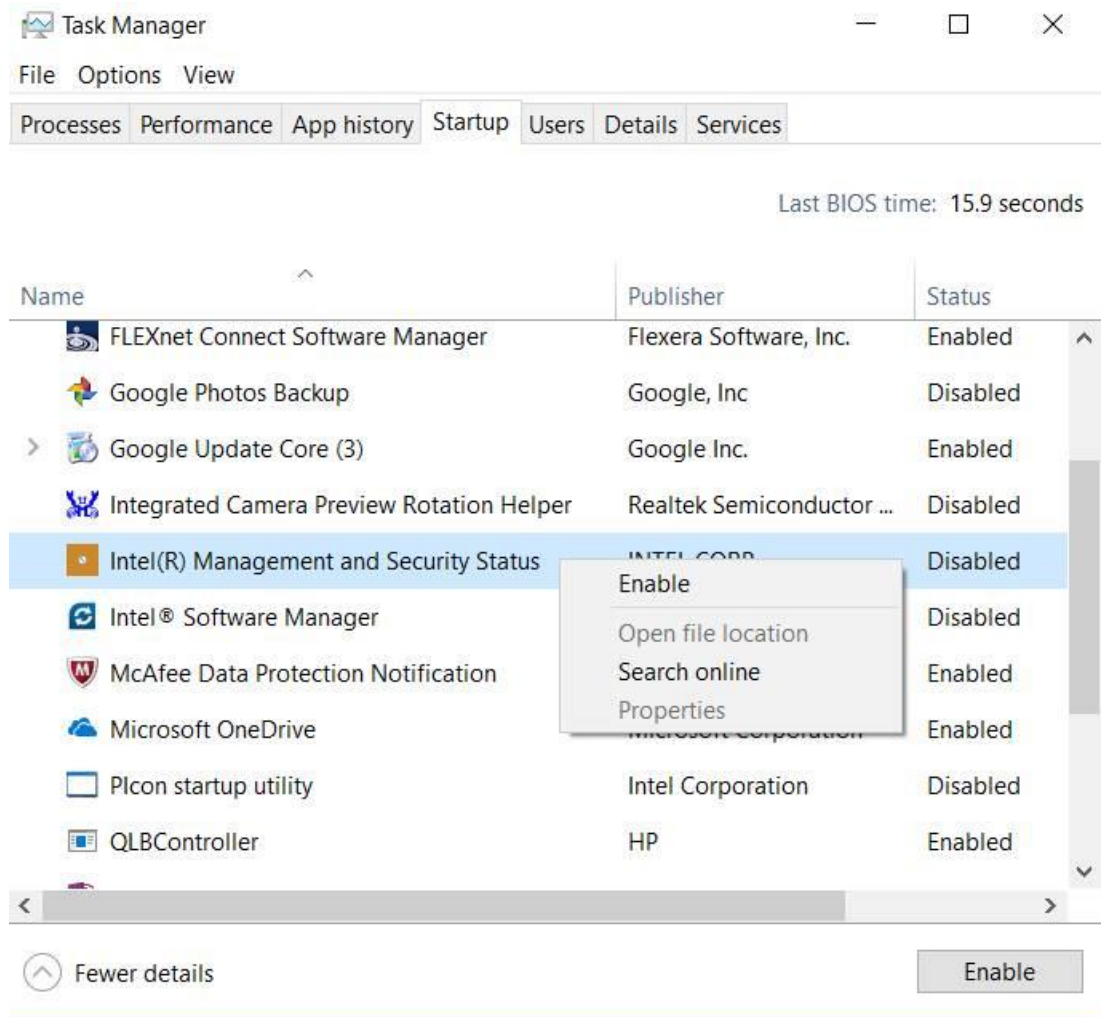
- **Intel® AMT:** Enabled / Disabled / Information unavailable
 - **Enabled:** Intel AMT is supported on the system. The Intel ME status in the Advanced Tab provides information on whether the Intel ME is configured (thereby causing Intel AMT to be functional).
 - **Disabled:** Intel AMT is not enabled on the system or has been disabled by the IT administrator.
 - **Information unavailable:** Not known whether Intel AMT is supported on the system. No Intel AMT information is available. This can be for one of the following reasons: the LMS service has stopped, or the Intel MEI driver is disabled.
- **Intel® Standard Manageability:** Enabled / Disabled / Information unavailable
 - **Enabled:** Intel Standard Manageability technology is supported on the system. The Intel ME status in the Advanced Tab provides information on whether the Intel ME is configured (thereby causing Intel AMT to be functional).
 - **Disabled:** Intel Standard Manageability technology is not enabled on the system or has been disabled by the IT administrator.
 - **Information unavailable:** 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: the LMS service has stopped, or the Intel MEI driver is disabled.

Note: The information in this field shows the state of the platform at the last platform boot.

Enable User Notification: Checking this box causes the Intel MSS icon to display important notifications in the notification area (for example, notification will be sent whenever one of the technologies is enabled or disabled). Affects the Intel MSS setting for the current user account only.

Intel® Management and Security Status application will be available next time I log on to Windows*: This option is only available in Intel® Management and Security Status application legacy version (non-APPx). Checking this box causes the Intel MSS to be invoked, and the icon to be displayed, whenever you log on to Windows*. Affects Intel® Management and Security Status application's behavior for the current user account only.

This option does not appear in the Intel MSS APPx. If users of the Intel MSS APPx want the Intel MSS to load automatically with Windows* log-on, they need to enable this feature from both the Startup tab in the task manager and the checkbox in the General tab. If the Intel MSS status from the task manager's Startup tab is disabled or the checkbox is unchecked, the feature will not be enabled.

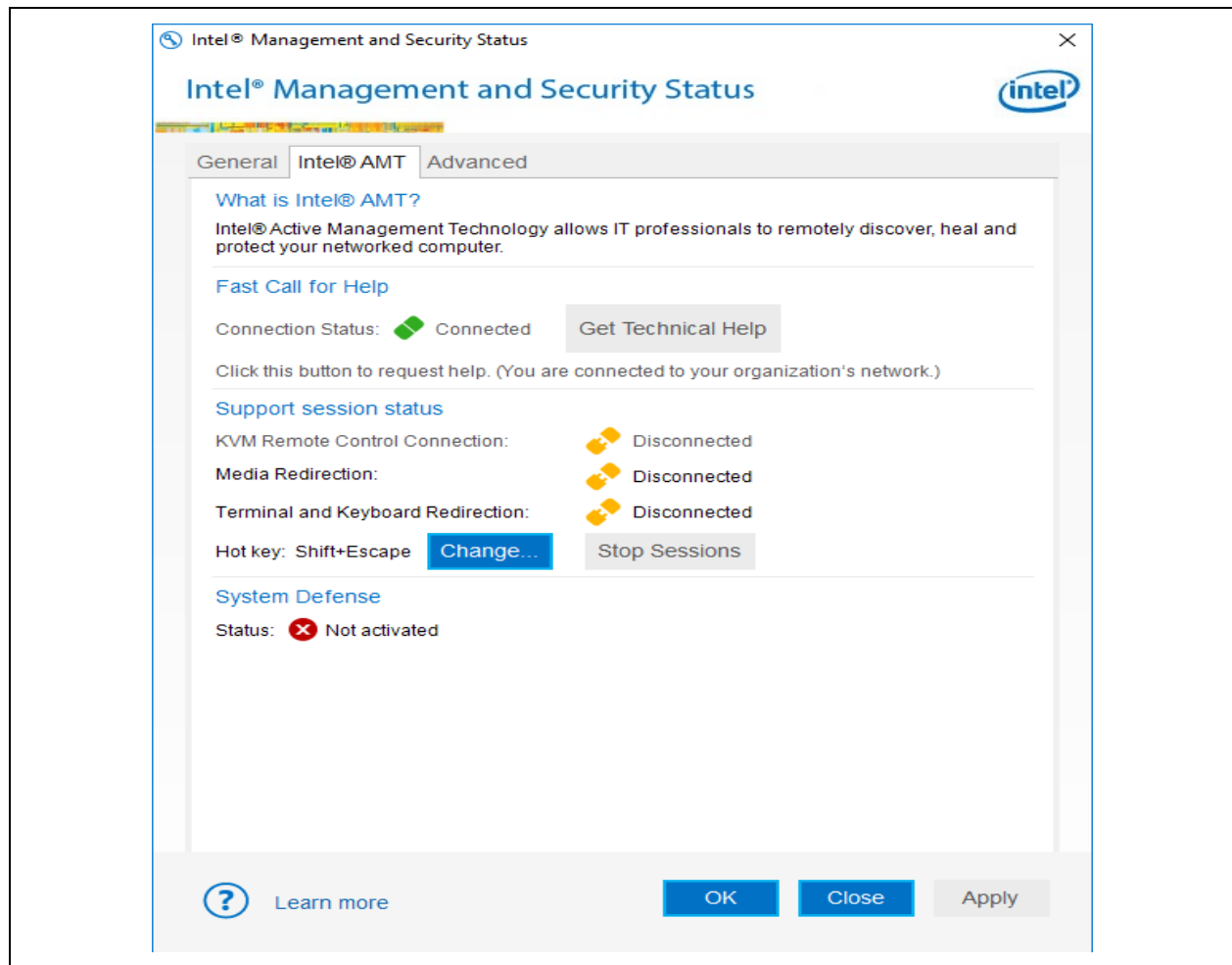


If neither Intel AMT or IntelStandard Manageability is supported on the platform, the Intel MSS does not load automatically with Windows* log-on. If one of the technologies is supported, the Intel MSS will load automatically even if both technologies are disabled.

3.2 Intel® Active Management Technology Tab

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

Click the Intel AMT tab to display Intel AMT information.





3.2.1 Fast Call for Help

The Fast Call for Help section provides Client Initiated Local Access (CILA) or Client Initiated Remote Access (CIRA) capabilities, depending on whether the system is connected to the corporate network or not, respectively. The Fast Call for Help section is available for the CIRA and CILA use cases if the system has been configured for these functions, as well as for a case in which the user's system did not receive an IP address while the wireless network was available for a support session. In other cases, the Fast Call for Help section is grayed out.

CIRA allows a user to connect the Intel AMT system to the company's Information Technology network via an external internet connection.

CILA allows a user connected to the internal corporate network to send a support request to the IT administrator.

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

Note: For CIRA or CILA to work, the machine needs to be configured correctly, and to support the technology. These settings are typically configured by management software. Refer to the [Intel AMT SDK Implementation and Reference Guide](#) for configuration instructions.

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 occurs.

Note: When the user is connected as a Guest account (in Windows*) the "Fast Call for Help" section is grayed out, to prevent users outside the organization from influencing the organization's network.

3.2.2 Support Session Status

The Intel MSS displays the following information about the support session:

- **KVM Remote Control Connection**

Indicates whether a KVM (Keyboard, Video & Mouse) Remote Control session is alive. Possible values: **Connected** / **Disconnected** / **Information unavailable**.

The KVM Remote Control Connection section is grayed out if the feature is disabled on the system.

- **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**.



- **Stop Sessions**

Click **Stop Sessions** to close any open KVM Remote Control, media redirection, or terminal/keyboard redirection sessions. If opening a session requires user consent, re-establishing the session requires renewal of the user consent after clicking this button.

- **Hot Key**

Indicates the hot key used for closing any open KVM Remote Control, media redirection, or terminal/keyboard redirection sessions. Pressing this key has the same effect as clicking **Stop Sessions**.

Click **Change** to choose a different hot key for this purpose.

- **Prevent Access**

This button appears if user consent is required for opening a remote support session. In such cases, after the user provides the required approval to the remote administrator the Prevent Access button is displayed until the healing session starts. This button enables the user to change their mind, as clicking on it cancels user consent and prevents the IT administrator from beginning the remote session. During this time, the hot key also serves to cancel user consent. Once a remote support session has begun, the Stop Sessions button is displayed instead of the Prevent Access button.

Note: When user consent is required, it is granted to the administrator per session, by the user giving the administrator a one-time pass code which is displayed on the user's screen in the Secure Output Window. See section 3.4.2, Secure Output Window Settings.

Note: During a support session conducted over the wireless interface, a notice is displayed warning not to change the wireless connection until the remote support session has completed.

Intel Management and Security Status Application Icon during support session

- The Intel MSS icon in the system tray icon is animated if user consent or a support session is active.
- **Stop Sessions** is available also by clicking the Intel MSS icon in the system tray.

3.2.3 System Defense

- **System Defense Status**

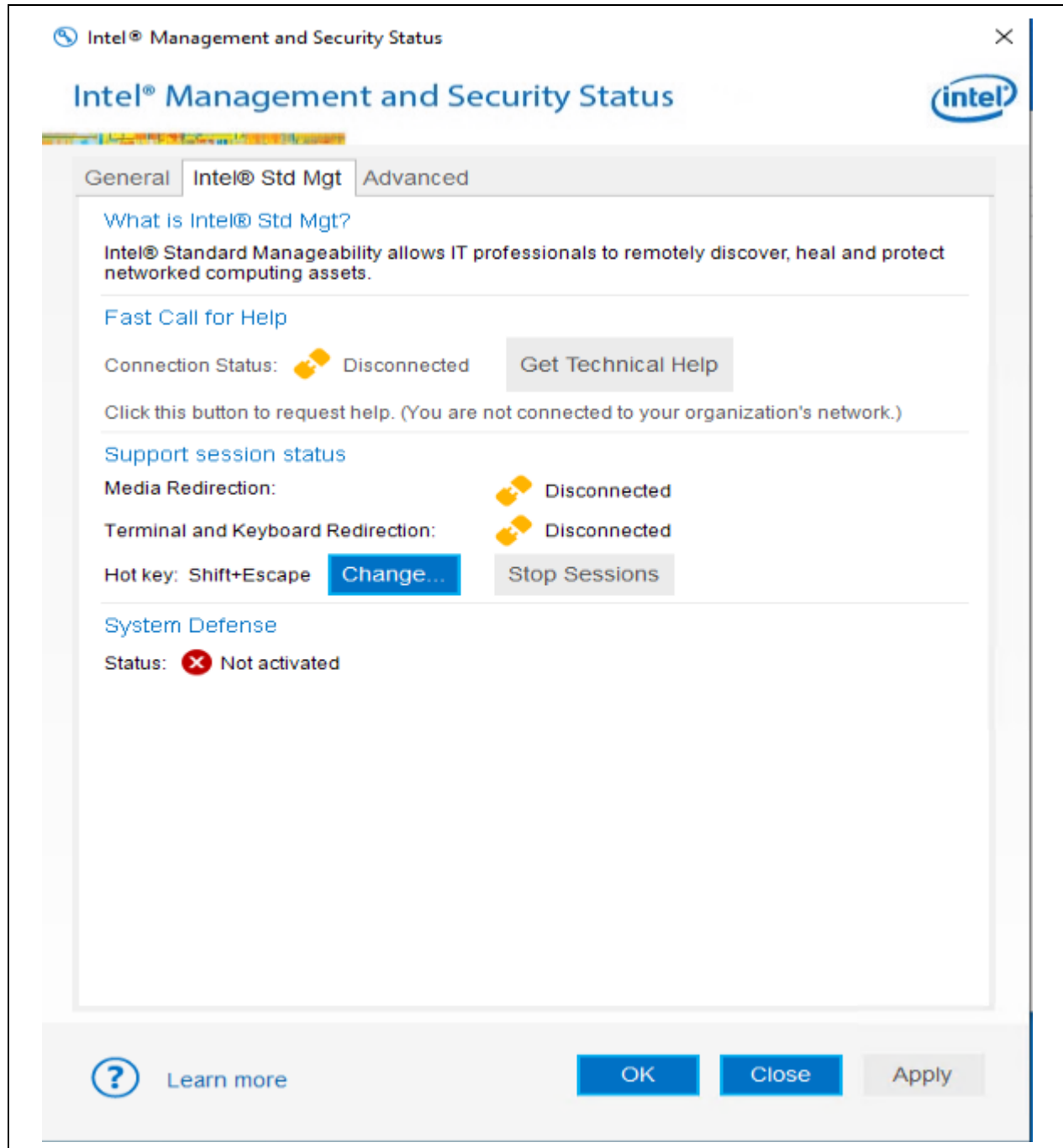
Indicates whether System Defense policies are currently active. Possible values: **Activated** / **Not activated** / **Information unavailable**.



3.3 Intel® Standard Manageability 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.





3.3.1 Fast Call for Help

This feature has the same functionality as the one in the Intel® AMT tab. See section 3.3.1, Fast Call for Help, for details.

Note: This feature is displayed only on Alder Lake platforms (running Intel CSME 16 firmware) or later.

3.3.2 Support Session Status

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**

3.3.3 System Defense

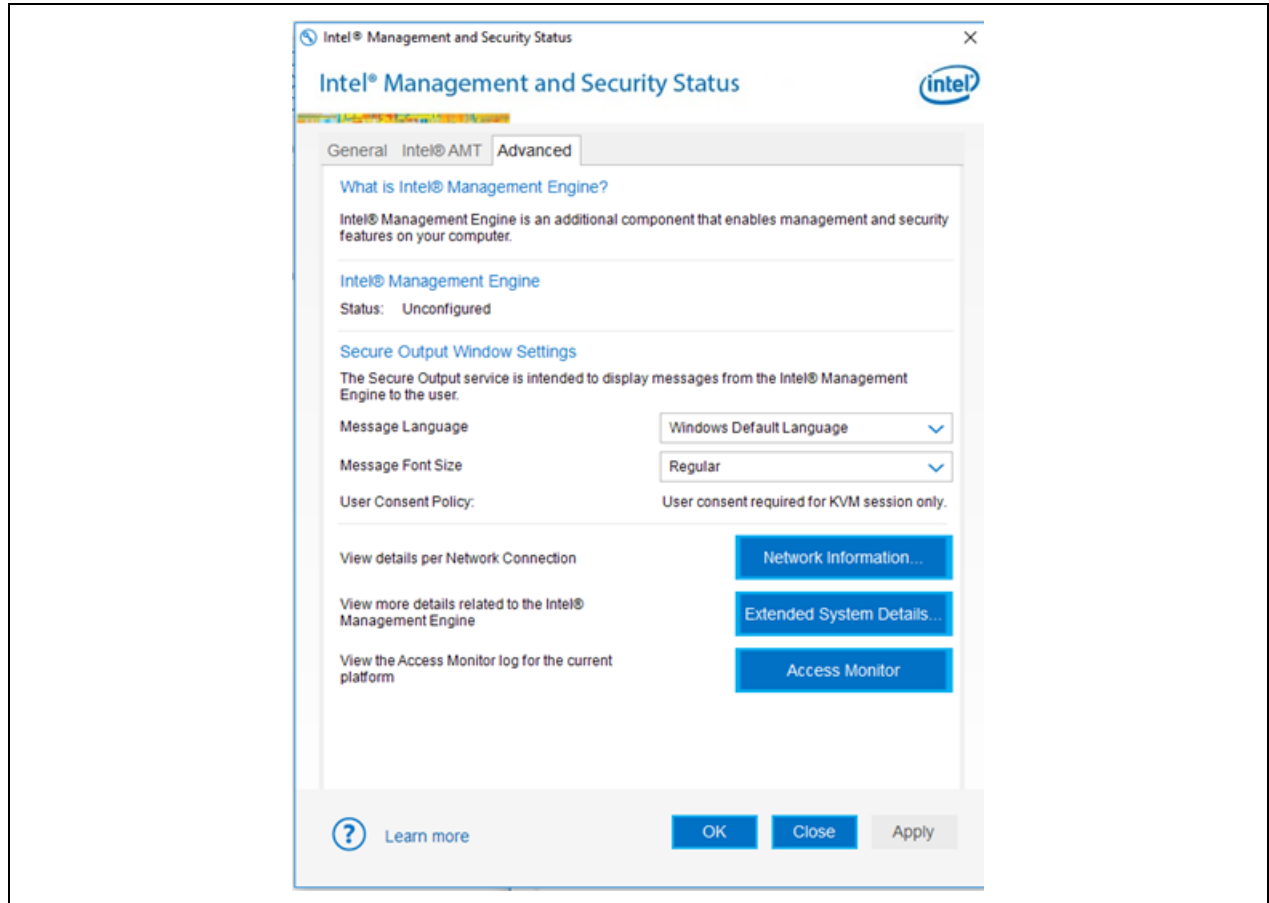
- **System Defense Status**

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



3.4 Advanced Tab

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



Note: The image shows all the buttons and information that can be displayed in the Advanced Tab. However, not everything is always displayed, as this depends on the specific technologies that are enabled and active on the platform: Intel® Active Management Technology (Intel® AMT) or Intel® Standard Manageability.

3.4.1 Intel® Management Engine

The following information is provided:

- **Status**

The operational status of the Intel® ME.

Possible values: Configured / Unconfigured / Information unavailable.

If the status is Configured, the configuration date and time are displayed.

- **Control Mode**

Intel ME can be configured in two modes: Client Control Mode and Admin Control Mode. If the status is Configured, the relevant Control Mode is displayed.



3.4.2 Secure Output Window Settings

The following information is provided for the Secure Output feature, used in KVM (keyboard/video/mouse) redirection. If the machine was configured in Client Control Mode, the information is provided for IDE redirection and remote power operations as well.

- **Message Language**

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

When the Intel MSS is installed, the consent language is set according to the Windows* System Locale language. (Note that this may be different from the Windows* Display language). Selecting a different message language in the Advanced Tab overrides this initial setting. Selecting Windows Default Language reverts the setting to the Windows* System Locale language.

- **Message Font Size**

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

- **User Consent Policy**

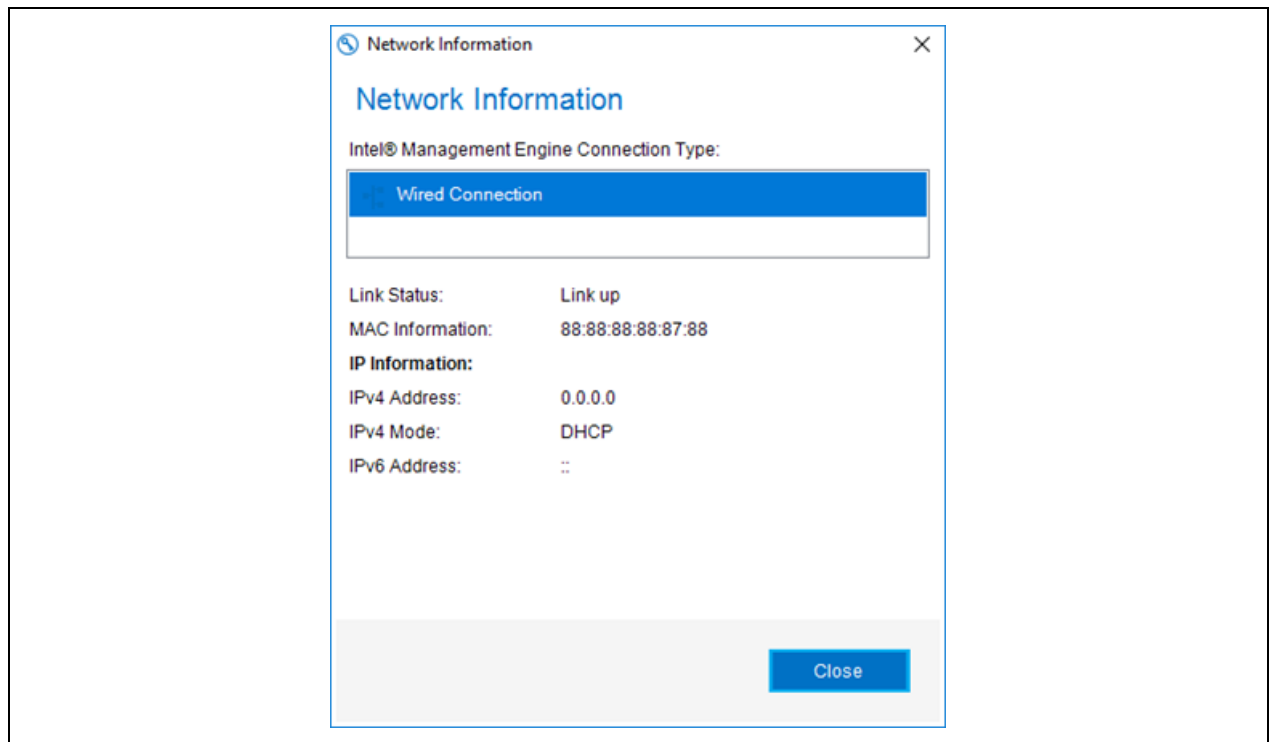
Specifies the policy for when the user's approval will be required to establish a remote support session by an IT administrator. User Consent is granted to the administrator for the duration of a session, by the user giving the administrator a one-time pass code that will appear on the Secure Output Window displayed on the user's screen.

Possible Policies are:

- User consent not required for any remote session (i.e., KVM, IDE redirection, and remote power operations)
- User consent required for KVM session only
- User consent required for all remote sessions

3.4.3 Network Information

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



In the **Connection Type** section, choose the interface (**Wireless Connection** or **Wired Connection**) whose information you want to display. The following information is displayed:

- **Link Status**

Whether the link is currently active.

Possible values: Link up / Link down / Information unavailable

- **MAC Information**

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

- **IPv4 Address**

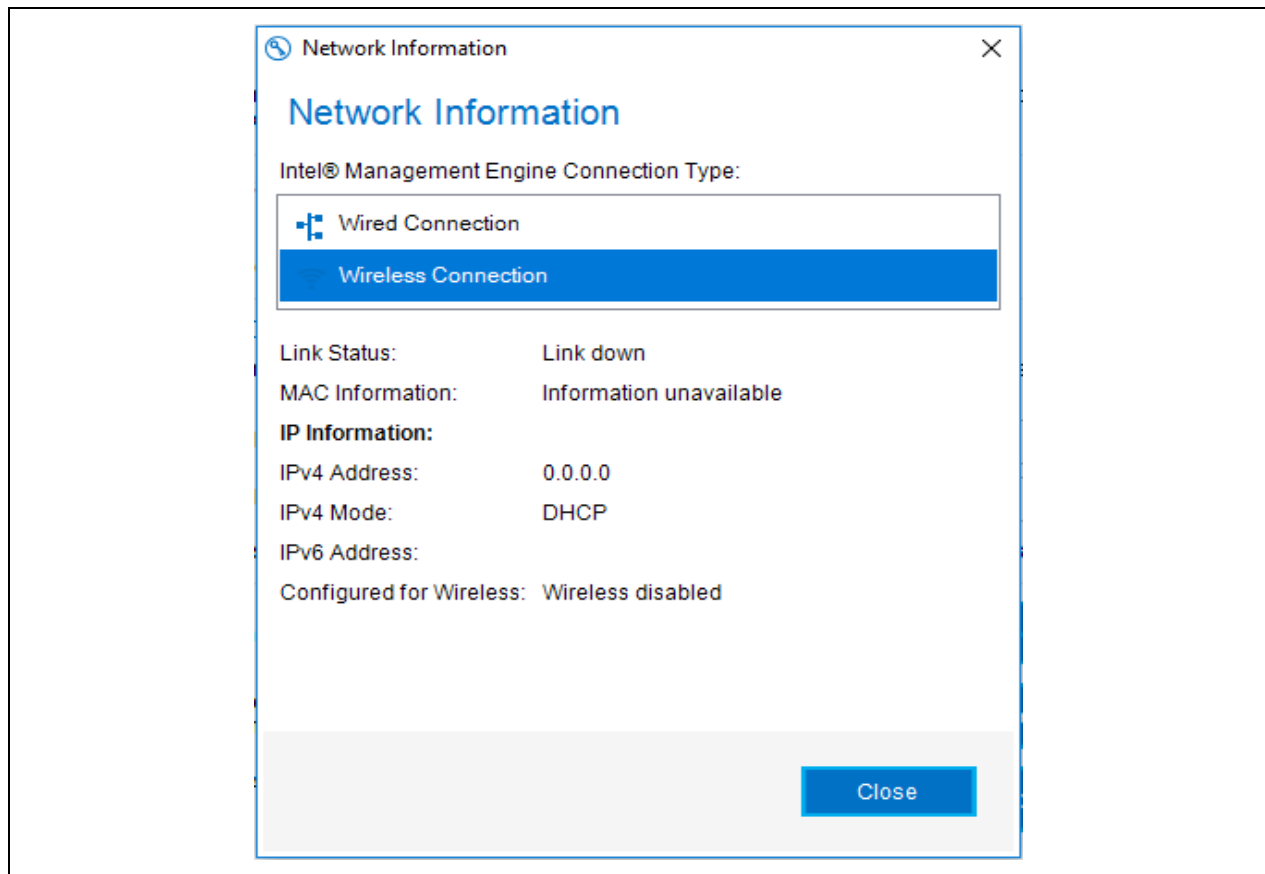
XXX.XXX.XXX.XXX – e.g., 208.77.188.166

- **IPv4 Mode**

Possible values: Static / DHCP / Information unavailable

- **IPv6 address**

If IPv6 addressing is enabled for the Intel ME, the Intel MSS displays up to 6 IPv6 IP addresses configured for an Intel ME network interface with wired connection, and up to 5 IPv6 IP addresses for wireless connection.



The following data appears only for wireless connections:

- **Configured for Wireless**

Possible values: Wireless enabled / Wireless disabled / Information unavailable

3.4.4 Extended System Details

Clicking **Extended System Details** opens a Windows* System Information window, providing an extensive report about the system components and configuration.

The report includes both general information regarding the system (Host Information) and specific Intel Management Engine information (Intel® ME Information).

To save the system report to a file:

- Click **File ➔ Export** in the System Information Window.

Following are explanations of some of the details displayed in Extended System Details:



Host Information:

- Operating System Name: The Windows* operating system that the application is running on.
- Operating System Version: Version of the operating system
- System Manufacturer: Hardware manufacturer
- System Name: Computer name as recognized by the operating system
- System Model: Hardware platform name
- Processor: Processor's full brand name
- BIOS Version: BIOS manufacturer's name and BIOS version number
- LAN DeviceID: LAN device's PCI Device ID
- LAN Driver – LAN device's driver version
- WLAN DeviceID: Wireless LAN device's PCI Device ID
- WLAN Driver: Wireless LAN device's driver version number

Intel® ME Information:

- Intel® ME Control Mode: Configuration mode (Client Control or Admin Control)
- Provisioning Mode: Intel ME configuration state (Pre / In / Post)
- BIOS boot: BIOS boot state (should be Post Boot)
- Last Intel® ME reset reason: Cause of the last Intel ME reset (Global System Reset / FW Reset / Power Up / Unknown cause/ Information unavailable)
- System UUID: Computer's Universal Unique Identifier. Standard System UUID presentation, e.g., 03000200-0400-0500-0006-000700080009
- Local FWUpdate: Local firmware update policy (Enabled / Disabled)
- Power Policy: Power modes in which Intel ME is available (Intel ME ON in S0/S4/S5/DC). **Note:** S0 = Power is on, S4 = Hibernate, S5 = System is shut down though the power cable is connected, DC = Battery Power
- Cryptography Support: Whether Intel ME can work in TLS/SSL mode (Enabled/Disabled)

FW Capabilities:

This section indicates whether the following technologies are present on the platform and enabled:

- Intel Active Management Technology / Intel Standard Manageability
- Intel® TPM Provisioning Service, formerly known as Intel® Capability Licensing Service (iCLS)
- Intel® Dynamic Application Loader
- Protected Audio Video Path (PAVP)

Intel® Active Management Technology / Intel® Standard Manageability

- Intel(R) AMT State (Enabled / Disabled).



- Intel(R) AMT Status (Configured / Not Configured).
- CIRA Connection Status – Client Initiated Remote Access Connected / Not connected (not available for Intel Standard Manageability)

Components Information

Present versions for the following components:

- MEBx Version: Intel ME BIOS Extension version
Note: If MEBX is integrated in BIOS, the MEBX version will show 0.0.0.0000.
- FW Version: Firmware version
- LMS Version: Local Management Service software version
- MEI Driver Version: Intel® Management Engine Interface (Intel® MEI) driver version
- MEI DeviceID: Intel Management Engine Interface PCI Device identification
- SOL Driver Version: Serial Over LAN driver version
- SOL DeviceID: Serial Over LAN PCI Device identification
- PMC Version: Power Management Controller version

Network Information:

- LAN MAC Address: Media Access Control address for the LAN device
- LAN Configuration state: DHCP or static mode for LAN
- LAN Link Status: LAN link up or down
- LAN IPv4 Address: IPv4 address assigned to LAN
- LAN IPv6 Enablement: IPv6 enabled or disabled for LAN
- WLAN MAC Address: Media Access Control address for the Wireless LAN device
- WLAN Configuration state: Only DHCP mode supported for Wireless LAN
- WLAN Link Status: Wireless LAN link up or down
- WLAN IPv4 Address: IPv4 address assigned to Wireless LAN
- WLAN IPv6 Enablement: IPv6 enabled or disabled for Wireless LAN

Note: When the user is connected as a Guest account (in Windows*), some system information is unavailable. In such a case, all the Host Information and some of the Intel ME Information (such as Software Versions) appears as "NA".

3.4.5 Access Monitor

If the Access Monitor feature is enabled on the platform, clicking the Access Monitor button opens a Windows* System Information window with the relevant content. Access Monitor content includes descriptions of system events that may be of interest to the user from a privacy and security perspective, such as network administration, storage administration, remote control operations and more.



Note: Events that occur before Intel AMT is provisioned for the first time are displayed with incorrect time and date.

3.5 Intel® Unique Platform ID Tab

Note: This tab is displayed only if the platform supports Intel® Unique Platform ID (Intel® UPID).

3.5.1 Intel® UPID Status

Intel UPID can be enabled or disabled by clicking the Enabled or Disabled radio buttons in the Intel Unique Platform ID tab, respectively.

If Intel UPID is disabled, Intel® Platform Service Record (Intel® PSR) continues logging (collecting events, counting power transitions, etc.), but its log cannot be retrieved from the OS or from BIOS.

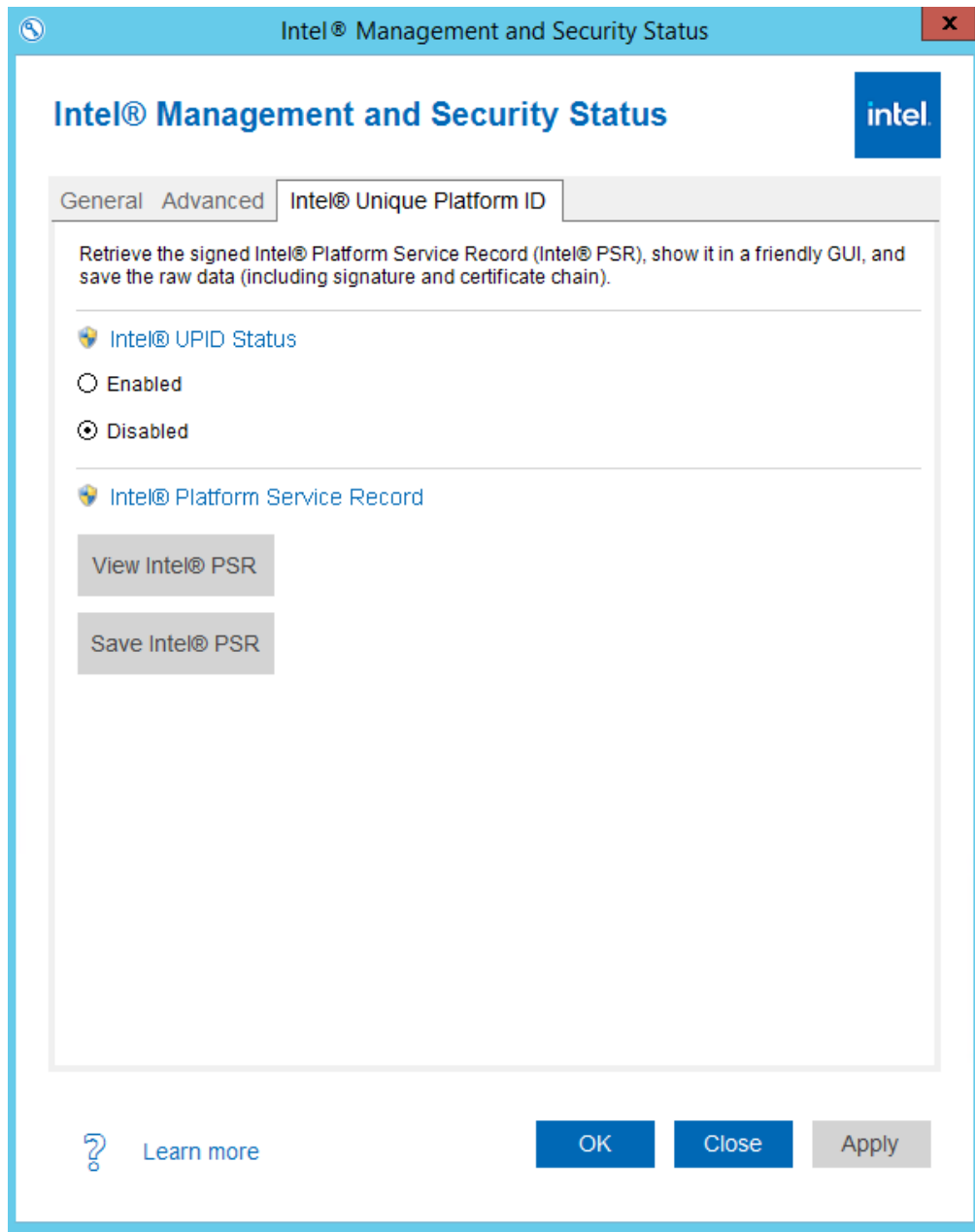
The following table shows what Intel MSS displays, and what functions it makes available, depending on whether Intel UPID and Intel PSR are enabled and supported:

| UPID Supported | UPID Enabled | PSR Supported | Intel MSS Behavior |
|----------------|--------------|---------------|--|
| No | | | Intel UPID tab not shown |
| Yes | Yes | Yes | Intel UPID tab shown Intel PSR buttons available |
| Yes | Yes | No | Intel UPID tab shown Intel PSR buttons grayed out |
| Yes | No | Yes | Intel UPID tab shown Intel PSR buttons greyed out |
| Yes | No | No | Intel UPID tab shown Intel PSR buttons greyed out |



3.5.2 Intel® Platform Service Record (Intel® PSR)

You can view or save the Intel PSR to a file by clicking the View Intel® PSR and Save Intel® PSR radio buttons, respectively.



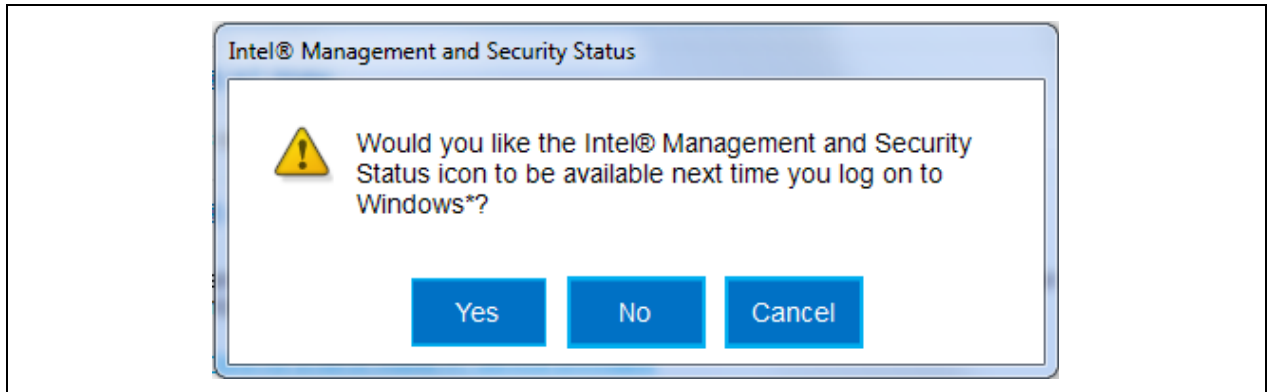


3.6 Shutting Down the Intel Management and Security Status Application

To shut down the Intel MSS, click the Intel MSS icon in the system tray notification area and choose **Exit**.



The following window is displayed (only in legacy version):



Click **Yes** to automatically start the Intel MSS when you next log on, or **No** to prevent the Intel MSS from starting automatically. **Note:** This change affects the Intel MSS behavior for the current user account only.

Note: This user selection will affect the **Intel® Management and Security Status application will be available next time I log on to Windows*** checkbox in the General Tab of the legacy version of Intel MSS.

3.7 Windows* 10

When the application is installed on a Windows* 10 operating system, a tile is placed on the Start window. This allows the application to send toast notifications to the Windows UI. If the tile is deleted, no toast notifications can be posted.

Provisioning Intel® Active Management Technology on the system recreates the missing tile.

§

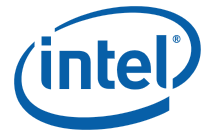
4 *Troubleshooting Intel® Management and Security Status*

4.1 **Error Message Appears Upon Application Load**

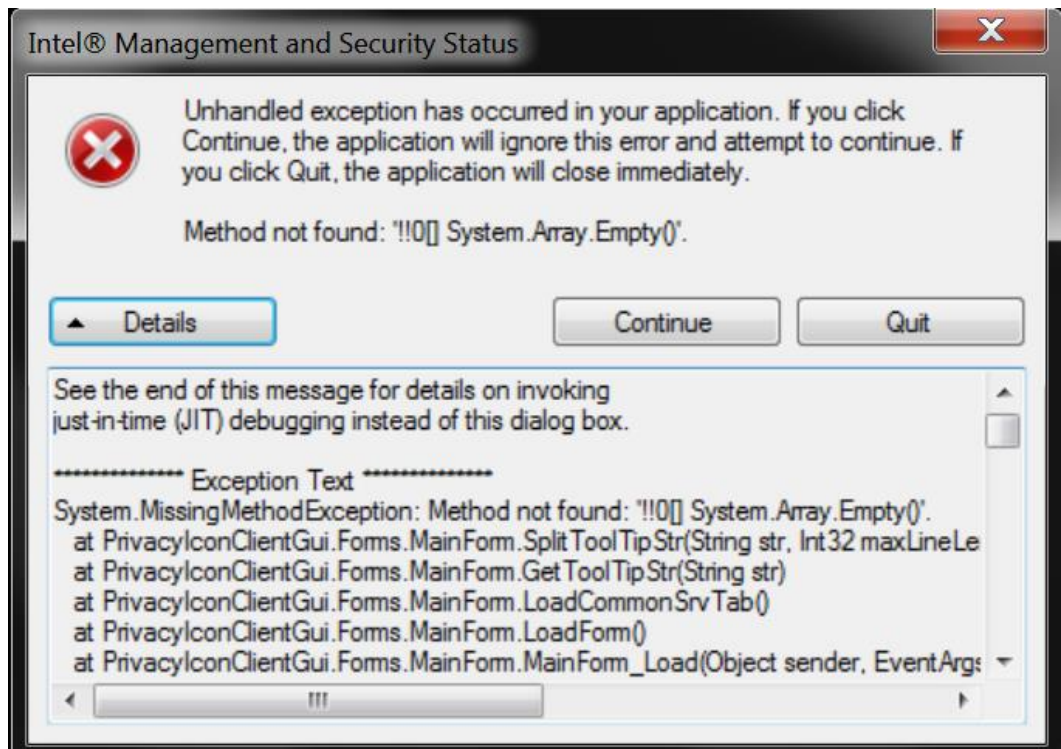
.NET applications fail when they are executed in an environment that has no Microsoft* .NET Framework installed. Microsoft* does not provide a safeguard mechanism in such conditions.

If no Microsoft* .NET Framework is present in the system, the Intel MSS displays the following error message:





The following message may also be displayed:



To resolve these issues, install Microsoft* .NET Framework version 4.8 or above and then re-open the Intel MSS.

§



5 *Intel® Management and Security Status Application Error Codes*

5.1 Partial Firmware Update Failures

Intel ME Wireless LAN updates and User Consent language updates both utilize the Partial Firmware Update feature of Intel MSS. If Partial Firmware Update fails, the user is notified via a balloon. The Windows* Event Log includes an error code signifying the cause of the failure. The possible causes are listed below:

| Code | Meaning |
|------|--|
| 8193 | Intel® ME Interface : Cannot locate Intel ME device driver |
| 8703 | PLEASE REBOOT YOUR SYSTEM. Firmware update cannot be initiated without a reboot |
| 8704 | Firmware update operation not initiated due to a SKU mismatch |
| 8705 | Firmware update not initiated due to version mismatch |
| 8706 | Firmware update not initiated due to integrity failure or invalid FW image |
| 8707 | Firmware update failed due to an internal error |
| 8708 | Firmware Update operation not initiated because a firmware update is already in progress |
| 8710 | Firmware update tool failed due to insufficient memory |
| 8713 | Firmware update not initiated due to an invalid FW image or header |
| 8714 | Firmware update not initiated due to file open or read failure |
| 8716 | Invalid usage |
| 8718 | Update operation timed-out; cannot determine if the operation succeeded |



| Code | Meaning |
|------|--|
| 8719 | Firmware update cannot be initiated because Local Firmware update is disabled |
| 8722 | Intel ME Interface: Unsupported message type |
| 8723 | No firmware update is happening. |
| 8724 | Platform did not respond to update request. |
| 8725 | Failed to receive last update status from the firmware. |
| 8727 | Firmware update tool failed to get the firmware parameters. |
| 8728 | This version of the Intel® Firmware Update Tool is not compatible with the current platform. |
| 8741 | FW Update Failed. |
| 8744 | OEM ID verification failed. |
| 8745 | Firmware update cannot be initiated because the OEM ID provided is incorrect. |
| 8746 | Firmware update not initiated due to invalid image length. |
| 8747 | Firmware update not initiated due to an unavailable global buffer. |
| 8748 | Firmware update not initiated due to invalid firmware parameters. |
| 8754 | Encountered error writing to file. |
| 8757 | Display FW Version failed. |
| 8758 | The image provided is not supported by the platform. |
| 8759 | Internal Error. |
| 8760 | Update downgrade vetoed. |
| 8761 | Firmware write file failure. |
| 8762 | Firmware read file failure. |
| 8763 | Firmware delete file failure. |



| Code | Meaning |
|------|---|
| 8764 | Partition layout not compatible. |
| 8765 | Downgrade not allowed, data mismatched. |
| 8766 | Password did not match. |
| 8768 | Password not provided when required. |
| 8769 | Polling for FW Update Failed. |
| 8771 | Invalid File. |
| 8772 | Invalid usage, -allows v switch required to update the same version firmware. |
| 8776 | Get Partition Attribute Failure. |
| 8777 | Update Info Status Failure. |
| 8778 | Unable to read FW version from file. Please verify the update image used. |
| 8780 | Buffer Copy Failure. |
| 8787 | Password exceeded maximum number of retries. |
| 8793 | FW Update/Downgrade is not allowed to the supplied FW image. |
| 8794 | FW downgrade is not allowed due to SVN restriction. |

§