Achieve Easier Device Management at Scale in the Smart World

Discover how you can improve the security and manageability of your estate of devices by enabling remote access and management with Intel® Active Management Technology

Introduction

Across industries, the IT function needs to take on an increasingly diverse range of operational technology (OT) devices, such as connected point of sale (POS), vending systems, ATM machines and digital signage. At the same time, the IT used by today’s knowledge workers needs to be secure, easy to use and mobile. The challenge is to secure and manage an increasingly diverse and dispersed estate of devices, without starting over. Organizations want an approach that works within their existing processes and protocols for managing their device fleets, based on IT Infrastructure Library (ITIL) and other industry standards. To keep costs down and tackle the complexity, IT organizations need automated and scalable processes and tools.

Intel Active Management Technology, or Intel® AMT, is a feature of Intel® Core™ vPro™ processor-based devices and workstation platforms based on select Intel® Xeon® processors, which has been available for over a decade.

It can be used, for example, to:
- Provide remote access to a device to reduce maintenance and support costs and avoid desk-side visits;
- Improve system deployment, rebuild and upgrade processes;
- Keep devices updated with the latest patches and avoid working hours reboots, even for remote employees; and
- Provide a secure and effective decommissioning process for lost or retired devices, including quickly removing sensitive stored data with technologies such as Intel® Remote Secure Erase, available on Intel® SSD Pro drives.
Solution Overview

Intel Active Management Technology is a standard component of Intel® vPro™ platforms that provides remote access to a device for security, diagnostic and management functions, even if it is powered down, the operating system is unavailable or the drive has failed.

The only requirements are that the system is connected to a power supply and has a wired (LAN) and/or wireless (WLAN) network connection.

Intel Active Management Technology operates independently of the CPU and the firmware and is delivered in an unconfigured state. There are three main elements to the solution:

- **On-device components**: Intel Active Management Technology is comprised of multiple hardware and software components. The software includes the Intel® Management Engine (Intel® ME) firmware, the Intel® Management Engine BIOS Extension (Intel® MEBx), the Intel® Management Engine Interface (Intel® MEI) driver, the Intel Active Management Technology Serial-Over-LAN (SOL) device driver, the Intel® Local Manageability Service (LMS.exe), and the Intel® Management and Security Status (IMSS). Some of these software components are not present in a standard Windows* OS installation and may need to be downloaded from your system manufacturer.

- **Activation solutions**: To enable Intel Active Management Technology to remotely manage Intel vPro platforms Out of Band, you can configure it using Intel® Setup and Configuration Software (Intel® SCS) tools and utilities; manually configure Intel Active Management Technology through the Intel MEBx or configure with a USB key on the device.

- **Management solutions**: After activation, you can manage your estate of Intel Active Management Technology enabled devices with Intel® Manageability Commander, both standalone and integrated with Microsoft System Center Configuration Manager* (Microsoft SCCM), and third-party solutions such as Microsoft PowerShell* and RealVNC VNC Viewer Plus*.

Two Ways to Use Intel Active Management Technology

This document outlines two main approaches to using Intel Active Management Technology. They are:

- **Client Control Mode (CCM)**: CCM can be very simple to deploy—no more complex than pushing out a new driver. There are a number of limitations in CCM, in particular the need for user consent for a redirection operation or change to the boot process.

- **Admin Control Mode (ACM)**: ACM deployment is a little more involved and requires a PKI infrastructure (certificates) to establish trust between the provisioning server and client. In ACM, all the supported Intel Active Management Technology capabilities are available.
Solution and System Requirements

These guidelines assume that your organization has an existing estate of Intel Core vPro processor-based devices, which may span several generations of Intel Active Management Technology. Before you begin, you don’t need to know how many Intel vPro platforms you have, or where they are. Intel SCS can be used to discover the devices prior to activation of the Intel Active Management Technology capabilities.

Client Software Components

The Intel ME software is a requirement on all Intel Active Management Technology systems. This is either pre-installed or available via the OEM’s support site and consists of the following components:

- The Intel ME firmware enables the hardware components.
- The Intel MEBx is a BIOS menu extension used to view and manually configure some of the Intel Active Management Technology settings.
- The Intel MEI driver provides the software interface to the Intel Active Management Technology device and is installed as a system device.
- The Intel Active Management Technology SOL device driver installs as a COM port to allow text/keyboard redirection.
- The Intel Local Manageability Service (LMS.exe) is a Windows service installed on an Intel Active Management Technology system that has Intel Active Management Technology Release 9.0 or greater. LMS enables local applications to send requests and receive responses to and from the Intel ME, via the Intel MEI. LMS is required for host-based configuration (HBC) but not for remote provisioning.
- The Intel Management and Security Status (IMSS) provides status information to the local user about Intel Active Management Technology including messages and an indication that Intel Active Management Technology is configured.

This software and the OEM drivers for Intel Active Management Technology must be installed on the device before Intel Active Management Technology can be enabled. The only exception is when devices are enabled using a USB key, in which case the software and device drivers can be installed as part of the same process.

System Requirements for Intel SCS

Intel SCS has been successfully deployed and used by several organizations that have more than 100,000 Intel Active Management Technology systems. Although Intel SCS does not specify any specific hardware requirements, you should carefully select the server or servers that will run the Intel® SCS Remote Configuration Service (RCS). The RCS will obviously benefit from having a strong CPU configuration and a large amount of RAM. For its scalability testing of up to 100,000 virtual Intel Active Management Technology devices, Intel used the architecture shown in Table 1. Similar architecture is recommended as a minimum.

<table>
<thead>
<tr>
<th>Component</th>
<th>CPU Cores</th>
<th>RAM (GB)</th>
<th>Hard Drive (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RCS</td>
<td>8 logical processors</td>
<td>16</td>
<td>136</td>
</tr>
<tr>
<td></td>
<td>(Two Intel® Xeon® E5345 processors)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL Server (if installing the RCS in Database Mode)</td>
<td>2 logical processors</td>
<td>4</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>(Two Intel® Xeon® E5420 processors)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Recommended hardware requirements for Intel SCS.
Solution and System Setup and Configuration

By default, Intel Active Management Technology is delivered in an unconfigured state. The main objectives of the setup and configuration process are to:

- Deliver an encrypted profile to the target Intel Active Management Technology firmware;
- Enable Intel Active Management Technology features and specify behavior; and
- Ensure that only authenticated and authorized users can access the device.

A number of different configuration options are available in the Intel SCS collection of software components and utilities:

- **Intel Active Management Technology Configuration Utility (ACUConfig) Command Line Interface:** Using profiles, it is possible to apply a common configuration to multiple Intel Active Management Technology systems with this tool.

- **Remote configuration with Intel SCS.** This provides access to the full range of Intel Active Management Technology features. Requirements for this configuration method include a domain provisioning certificate and DHCP Option 15 to be enabled on the target device. See the Operating and Utilization section of this document for more information.

- **Manual configuration of multiple systems:** Manual configuration requires a touch of the device, but allows you to enable Admin Control Mode, which provides access to the full range of features offered by Intel Active Management Technology. Configuring a system using a USB key enables Intel Active Management Technology on the device. For a full discussion of CCM and ACM, see the Operating and Utilization section of this document.

- **Intel Active Management Technology Configuration Utility Wizard (ACUWizard):** This is a GUI application that can be used to configure Intel Active Management Technology systems individually or create profiles for use with ACUConfig.

Intel SCS and Infrastructure Best Practices for Distribution of Intel Active Management Technology Configuration and Management Commands

Whichever deployment method or management console you use, the goal is to avoid sending out mass configuration/maintenance commands to all your systems at the same time.

For example, task sequences of Microsoft SCCM are sent out almost simultaneously (within approximately 15 minutes) to all target systems. Therefore, it is recommended to spread out the deployment time by targeting the task sequences on smaller collections, or using batch files with randomized delays.

By default, the number of simultaneous operations on the server is limited to 200. It should only be increased if the computers running the RCS, Active Directory and Certificate Authority can handle a higher number. See the Intel SCS Scalability Guidelines section 4.4.1.

Using Database or Non-database Mode

The Remote Configuration Service (RCS) in Intel SCS can operate in one of two different modes (defined during installation):

- **Non-Database Mode** – In this mode, the RCS does not store any data about Intel Active Management Technology systems.

- **Database Mode** – In this mode, data about each Intel Active Management Technology system is stored in a SQL database. This includes data that can be used to connect to the system and the admin password that was configured in the Intel Active Management Technology device.

These different modes do not have any impact on the time that it takes the RCS to configure or maintain Intel Active Management Technology. But there are differences between the two modes that you should take into consideration.

In both modes, the RCS keeps a log file that records all actions done by the RCS. The main purpose of this log file is for debugging problems with the RCS. It is not easy to use this log file to investigate the success or failure of configuration/maintenance commands on the systems. In non-database mode, no other data is available to help you with debugging. Analysis or investigation of the return status codes
from configuration/maintenance commands must be done on the host platforms. But in database mode, the RCS stores an operations log in the database for each system. You can use the Console component of Intel SCS to view these operation logs per system.

In database mode, the admin password configured in Intel Active Management Technology is stored in the database for each system. This means that the password configured for each system is always accessible (you can use the Console to view the admin password of each system). Having access to this password is even more important if you are using the option to create a random admin password for each system; if the passwords are not stored in the database, they will be unknown to you or any application. Using database mode will increase the traffic to your SQL Server. But database mode also includes several other options that can help you to monitor and maintain your systems. For example, you can use the console to define and run maintenance “Jobs” on multiple systems and view discovery data collected from your systems.

Operation and Utilization of the Intel® Solutions

This paper covers two different approaches available when using Intel Active Management Technology. A good approach is to enable Client Control Mode with host-based configuration; and the best approach is to use Intel SCS to enable Admin Control Mode with fewer infrastructure dependencies. Devices enabled with Intel Active Management Technology can also be managed using tools including Microsoft SCCM.

Good: Using Client Control Mode (CCM)

Client Control Mode (CCM) is a good fit for applications that require 1:1 communications, such as a support desk, where the user and the agent requiring access will be communicating with each other in real time. User Consent can also be used to offer an additional level of protection to highly sensitive devices that are enabled for Intel Active Management Technology, such as those used for finance, HR or other business critical or sensitive functions.

In Client Control Mode, there are a number of restrictions:

• User consent is required for all redirection operations (including KVM) and changes to the boot process. When a remote connection to the computer starts, a message shows on the computer of the user. The message contains a code (see Figure 1) that the user must give to the person who wants to connect to their computer. The remote user cannot continue the operation until this code has been provided. Whether consent is required or not, several visual mechanisms on the user’s device indicate when the device is being remotely accessed using Intel Active Management Technology.

• To help ensure that untrusted users cannot take control of the system, some Intel Active Management Technology configuration functions are blocked.

• During configuration, the password for Intel® Management Engine BIOS Extension (Intel® MEBx) is not changed in Client Control Mode. In Admin Control Mode, the password is replaced during Intel Active Management Technology configuration if the password is set to the default (usually “admin”).

Because user consent is required for redirection operations and changes to the boot process, Client Control Mode does not enable procedures such as operating system upgrades at scale.

![Remote Assistance Session](image)

**Figure 1.** Client Control Mode requires user consent for redirection operations and changes to the boot process.
CCM can be enabled on a device using host-based configuration (from Intel Active Management Technology 6.2 and higher), which enables an application running locally on the device to configure its own Intel Active Management Technology functionalities. The application can be based on a GUI or command line interface, and can be distributed like a software upgrade using Microsoft SCCM or other management tools.

Host-based configuration does not require a provisioning certificate, so it can be easier to implement than the other approaches in this document, both technically and organizationally. Used together with Intel® Manageability Commander, Microsoft PowerShell or RealVNC VNC Viewer Plus, it provides a lightweight and low-cost way to manage the estate of Intel Active Management Technology devices. Use cases supported by Intel Manageability Commander, PowerShell and RealVNC VNC Viewer Plus include power control, hardware inventory, boot to alternative OS, boot to BIOS, wake and rebuild, and scheduled wake. Intel Manageability Commander and RealVNC VNC Viewer Plus additionally add support for full KVM remote control. See Table 2 for details of the use cases supported by different solutions.

**Better: Using Intel Setup and Configuration Software to Enable Admin Control Mode (ACM)**

Intel SCS is well documented and updated by Intel in line with each generation of Intel vPro platforms. It is considered the system of record for Intel Active Management Technology activations and has proven scalability to discover, configure and maintain tens of thousands of Intel Active Management Technology devices.

Admin Control Mode (ACM) can enable all Intel Active Management Technology features that are available on the client hardware. In this mode, user consent for redirection operations and changes to the boot process is optional. As a result, ACM makes it possible to carry out processes such as operating system upgrades at scale, without dependence on user availability or intervention.

Using Intel SCS to enable ACM is the best solution when you want to remotely configure a large estate of devices, and when you want to take advantage of the full capabilities of Intel Active Management Technology without the user consent constraint.

Intel SCS is a free suite of tools that provides functionalities for setting up and configuring Intel Active Management Technology, including some integration with the environment, such as Active Directory, the Certificate Authority, and the wireless LAN. It offers command line and GUI interfaces and can run on a physical or virtual server. A database back-end can optionally be used for configuration information, storing the profiles used for activation and information received about the devices.

<table>
<thead>
<tr>
<th>Solution / Use Case</th>
<th>Intel® Manageability Commander</th>
<th>Intel® vPro™ Technology Windows® PowerShell module</th>
<th>RealVNC VNC Viewer Plus*</th>
<th>Microsoft SCCM (Build 1511 and later)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Control</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Intel Manageability Commander</td>
</tr>
<tr>
<td>Hardware Inventory</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Intel SCS Add-On for SCCM</td>
</tr>
<tr>
<td>Boot to Alternate OS</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Intel Manageability Commander or Intel® vPro™ PowerShell</td>
</tr>
<tr>
<td>Boot to BIOS</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Intel Manageability Commander or Intel vPro PowerShell</td>
</tr>
<tr>
<td>Wake and Reimage</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>Intel Manageability Commander</td>
</tr>
<tr>
<td>KVM Remote Control</td>
<td>YES</td>
<td></td>
<td>YES</td>
<td>Intel Manageability Commander</td>
</tr>
<tr>
<td>Intel AMT Alarm Clock</td>
<td>YES</td>
<td></td>
<td></td>
<td>Intel vPro PowerShell</td>
</tr>
<tr>
<td>Wake and Patch</td>
<td>Wake Only</td>
<td>Wake Only</td>
<td>Wake Only</td>
<td>Intel Manageability Commander</td>
</tr>
</tbody>
</table>

Table 2. Standard Intel® Active Management Technology use cases and solutions.
Components within Intel SCS can play a valuable role in a feasibility study because they enable you to discover how many Intel vPro devices your organization has and what capabilities they support. Although Intel Active Management Technology activation is not necessarily a numbers game (some organizations use it to provide an enhanced level of service to a select number of high value assets), the discovery phase can help an organization to establish whether it has the critical mass of Intel vPro devices required for its use case.

Although the Intel SCS console offers a single pane to view the estate of devices, it is not recommended for advanced monitoring of devices. Intel SCS is able to do carry out basic monitoring functions, using a query to the configuration database or the end point for the specific Intel Active Management Technology object information required.

Intel SCS requires a domain provisioning certificate in order to establish a root of trust for remote activation at scale. It also requires DHCP option 15 to be enabled, so that the devices can establish a fully qualified domain name (FQDN) and identify their home network.

Dependent upon Intel Active Management Technology release, the firmware contains root certificate hashes from a number of commercial certificate authorities including GoDaddy, Symantec, Comodo, and Entrust. You can also add your own root certificate hash into the Intel MEBx. To support Intel Active Management Technology remote configuration, an SSL certificate from one of these embedded hashed root certificates must be purchased from a commercial SSL certificate provider.

Alternative Management Solutions

Following configuration using one of the previously mentioned solutions, an estate of Intel Active Management Technology devices can be managed by or integrated with third-party solutions including Microsoft SCCM, RealVNC VNC Viewer Plus, and products from Bomgar, Ivanti, and Accenture.

Intel Manageability Commander is a lightweight software console that allows IT professionals to administer Intel Active Management Technology PCs to perform functions such as power control, remote management and troubleshooting of PCs, and hardware inventory. User PC and operating system issues can be viewed and solved via the integrated KVM (keyboard, video, mouse) remote control.

To help with integration and enable the development of new applications based on Intel Active Management Technology capabilities, Intel provides the free Intel® Active Management Technology Software Development Kit (SDK). It provides the low-level programming capabilities to enable developers to build manageability applications that take full advantage of Intel Active Management Technology. The Intel Active Management Technology SDK provides sample code and a set of APIs that let developers easily and quickly incorporate Intel Active Management Technology support into their applications. The SDK also has a full set of documentation. The SDK supports C++ and C# on Microsoft Windows and Linux operating systems. The SDK could be used, for example, to create an online self-help application that enables users to request a temporary boot image, an operating system rebuild or an operating system upgrade. The Intel Active Management Technology SDK is updated and maintained by Intel for each platform release.

PowerShell cmdlets can also be used to remotely access and manage Intel Active Management Technology devices.

**Figure 2. Using Intel® Remote Secure Erase to remotely sanitize an SSD.**
Use Case Examples

The solution can be used for a wide range of use cases that take advantage of Intel Active Management Technology's ability to help a device authenticate its network, and the ability to connect remotely to the device.

Remote Secure Erase

When a PC is retired or repurposed, information security policies often require data be sanitized from the drive, which can be difficult, time consuming, and costly if outsourced to a third party. Intel® Remote Secure Erase can provide a solution to all of these issues (see Figure 2).

With this solution, if an employee leaves a job, is terminated, or is moving to a new PC, IT is able to initiate a remote secure erase to sanitize the SSD, eliminating the need to remove or shred it. This solution also allows a drive to be erased prior to shipping to another location, thus eliminating risk of data being lost or stolen during transit.

When Intel Remote Secure Erase is executed, the drive's controller sanitizes all existing data, and the encryption key is destroyed thus no data is recoverable. It effectively wipes all data within seconds—individually of power state, OS state or management agent—while providing an authenticated, logged action.

This solution requires a compatible 6th Generation or newer Intel vPro Platform with an Intel® SSD Professional Family drive. The Remote Secure Erase command can be issued using Intel Manageability Commander or Windows PowerShell and from third-party solutions from Sprinxle, Ivanti, and Kaseya.

Control, Initiate and Monitor Microsoft Windows 10 deployments

Intel Active Management Technology can help streamline deployments of, and in-place upgrades to, Microsoft Windows 10 (see Figure 3). You can use Intel Active Management Technology to control, initiate and monitor the entire build process and it plays a particularly important role in enabling existing hardware features that are supported for the first time in Windows 10, without needing to visit every machine.

Figure 3. Intel® Active Management Technology plays an important role in enabling a smooth operating system upgrade or rebuild
For example:

- The Universal Extensible Firmware Interface (UEFI) Secure Boot protocol validates firmware images before they execute to reduce the risk of boot loader attacks and ensure the operating system starts before anything else.

- The Trusted Platform Module (TPM) 2.0 provides cryptographic and system integrity capabilities implemented in either Trusted Computing Group (TCG)-compliant UEFI firmware or Intel’s Platform Trust Technology (PTT) a TPM 2.0 implementation available as a firmware application within the Intel ME. These technologies can be used by BitLocker for disk encryption and for device health attestation services.

- CPU virtualization extensions are required to support Windows 10 virtualization based security capabilities, including Credential Guard and Device Guard.

Although capabilities such as these have been available on systems for a number of years, a lack of support in the operating system has meant that they have often not been enabled. In order to take advantage of the new security features in Windows 10, it is necessary to enable these features on devices. Intel Active Management Technology enables you to do this remotely, at scale, and as part of a workflow that ultimately leads to the operating system install or upgrade.

The operating system build process using Microsoft PowerShell and Intel Active Management Technology is as follows:

1. Initiate Intel Active Management Technology KVM to ensure that the platform update and operating system build process can be remotely controlled and monitored.
2. Update BIOS, firmware and CPU microcode to a known good level.
   a. Use USB-R/IDE-R to remotely load WinPE disk image.
   b. Identify OEM platform components and versions using the Intel Active Management Technology hardware asset information.
   c. Select OEM specific tools to perform updates i.e. OEM BIOS and firmware upgrade binaries.
3. Configure and enable platform BIOS settings including UEFI Secure Boot, VT-x, VT-d, TPM, Device Guard etc. This can be performed using Intel Active Management Technology Serial Over LAN (SOL) capabilities to automatically navigate the menu system using a VT100 interface, simulated keystrokes, escape codes, etc.
4. Alternatively use OEM specific tools and utilities:
   a. Use USB-R/IDE-R to load WinPE disk image.
   b. Identify OEM platform components and versions using the Intel Active Management Technology hardware asset information.
   c. Select OEM specific tools to perform updates, i.e., Dell Command* | PowerShell Provider.
5. Configure Intel Active Management Technology network interface to Static IP for corporate access and configure OS network interface for PXE using DHCP on the build network.
6. Reboot system to PXE using Intel Active Management Technology Power Control to begin the operating system build process.
7. Reset Intel Active Management Technology interface to DHCP, synchronize hostname and update DNS.
Validation

Users can validate the solution and troubleshoot problems by using a range of tools to check the available functionality. See Figure 4 for a guide.

Validate that Intel® Active Management Technology is enabled
- Check output from command line and GUI logs i.e. “Exit with code 0 - Success”
- If Intel® SCS has been used then use the console to validate success

Validate access control (Authentication and Authorization)
- Connect to Intel Active Management Technology using defined credentials by using a standard internet browser to visit http://hostname.fqdn:16992 (no TLS) or https://hostname.fqdn:16993 (TLS). This enables you to access and log on to an Intel Active Management Technology-enabled device.

Validate Intel Active Management Technology interface functionality
- Use Intel Manageability Commander or RealVNC VNC Viewer Plus for remote KVM.

Figure 4. Workflow for validating Intel Active Management Technology has been successfully configured

Summary

Faced with an increasingly diverse and disparate estate of devices, organizations need a consistent way to manage them that works within their existing processes and protocols.

Intel Active Management Technology enables remote access to a device for security, diagnostic and management functions, even if it is powered down, the operating system is unavailable, or there is a disk failure. It can also be used for securing devices by adding home network authentication features. It is supported by free and commercial tools from Intel for activation and management, and can be integrated with existing management tools and platforms.

Using Intel Active Management Technology enables an organization to cut many of the costs associated with managing and securing their devices. Remote access means that they can offer proactive and reactive maintenance without requiring a site visit, and the ability to wake up and patch a machine helps to keep the entire estate of devices secure. The solution can be used to enable operations such as operating system upgrades to be carried out at scale, across devices worldwide. Intel Active Management Technology can help organizations to cut the cost of functions such as service desk, improve the security of their end point devices, and remain agile in the face of an increasingly complex IT landscape.
References

- Intel® Setup and Configuration Software (Intel® SCS) User Guide
  intel.com/go/SCS

- Intel® Setup and Configuration Software (Intel® SCS) Scalability Guidelines
  intel.com/content/www/us/en/support/articles/000020783/software/manageability

- Intel® Setup and Configuration Software (Intel® SCS) Deployment Guide
  intel.com/content/www/us/en/support/articles/000020917/software/manageability-products.html

- Intel® vPro™ Technology Module for Microsoft® Windows® PowerShell®
  downloadcenter.intel.com/download/25891/Intel-vPro-Technology-Module-for-Windows-PowerShell

- Intel® Active Management Technology SDK
  software.intel.com/en-us/amt-sdk/download

- Intel Business Support
  intel.com/content/www/us/en/support/intel-business-support.html

Learn More

This implementation guide should complement product documentation and is part of an entire solution kit of content that is full of key insights and learnings:

- Reference Architecture: “Streamline Device Management in a Smart, Connected World”

You may also find the following resources useful:

- Intel® Manageability Commander
  downloadcenter.intel.com/download/26375/Intel-Manageability-Commander
- Intel vPro Platform
  intel.com/vPro

Solution Provided By:

Intel®

© 2018 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Core, and Intel vPro are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.