



Intel® vPro™ Technology Reference Guide

Updated for Intel AMT 7.0

Revision 3.0

March, 2011

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.

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 by visiting Intel's Web Site.

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

Systems using Client Initiated Remote Access require wired LAN connectivity and may not be available in public hot spots or "click to accept" locations. For more information on Fast Call for Help go to: <http://www.intel.com/products/centrino2/vpro>

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.

Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain computer system software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses. For more information, see [here](#)

Intel® Anti-Theft Technology—PC Protection (Intel® AT-p). No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT-p) requires the computer system to have an Intel® AT-enabled chipset, BIOS, firmware release, software and an Intel® AT-capable Service Provider/ISV application and service subscription. The detection (triggers), response (actions), and recovery mechanisms only work after the Intel® AT functionality has been activated and configured. Certain functionality may not be offered by some ISVs or service providers and may not be available in all countries. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof.

Enabling Execute Disable Bit functionality requires a PC with a processor with Execute Disable Bit capability and a supporting operating system. Check with your PC manufacturer on whether your system delivers Execute Disable Bit functionality.

Intel® Identity Protection Technology (Intel® IPT)— No system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, firmware and software and a website that uses an Intel® IPT Service Provider's Intel IPT solution. Consult your system manufacturer and Service Provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or or any other damages resulting thereof. For more information, visit <http://ipt.intel.com/>

Intel, the Intel logo, Intel® Core, Intel® Centrino, and Intel® vPro are trademarks or registered trademarks of Intel Corporation in the United States and other countries.

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

Copyright © 2009, 2010, 2011 Intel Corporation. All rights reserved.

Contents

Introduction	1
What's New?.....	1
What is Intel® vPro™ Technology?.....	2
Use Cases	4
Introduction	4
Use Case 1: Platform Auditing.....	4
Use Case 2: Software Inventory.....	4
Use Case 3: Hardware Inventory.....	5
Use Case 4: Remote Diagnosis and Repair.....	5
Use Case 5: Remote Diagnosis and Local Repair	6
Use Case 6: Software Version Compliance.....	7
Use Case 7: System Defense	7
Use Case 8: Agent Presence	8
Use Case 9: End Point Access Control	9
Use Case 10: One-Touch Configuration	10
Use Case 11: Remote Configuration.....	11
Use Case 12: Fast Call for Help	12
Use Case 13: Intel® Anti-Theft Technology (Intel® AT).....	13
Use Case 14: Access Monitor	16
Use Case 15: Remote Power Control.....	17
Use Case 16: PC Alarm Clock.....	17
Use Case 17: KVM Remote Control	18
Use Case 18: Remote Encryption Management	19
Use Case 19: Unattended Software Updates	20
Use Case 20: Host Based Configuration.....	20
Use Case 21: Intel® Identity Protection Technology (Intel® IPT).....	21
Selected Intel® vPro™ Technology Features	23
Compliance with Industry Standards.....	23
Alert Standard Format Support.....	23
WS-MAN Compliance.....	23
DASH Compliance.....	23
IPv6 Support.....	24
AES-NI Support	24
Cisco* Self-Defending Network Architecture (SDN).....	25
Microsoft* Network Access Protection (NAP)	25
Software Tools	27
Intel® Anti-Theft Status Utility	27
Intel® Remote Configuration Certificate Utility	27
Intel® Remote Configuration Scout	27
Intel® AMT Scan.....	27
Intel® Client Manageability Add-on for Microsoft* SMS 2003.....	28
Intel® WS-Management Translator	28
Intel® AMT USB Key Provisioning Utility	28
Intel® AMT SCSDiag Utility	28

Intel® vPro™ Activator Wizard	28
Intel® vPro™ Activator on LiveCD	29
Intel® Remote Power Control Utility	29
Intel® AMT Unprovision Utility	29
Intel® AMT Reflector	29
Intel® System Defense Utility	29
Intel® IT Director	30
Microsoft* ConfigMgr Bare-metal Provisioning Script.....	30
Intel® SCS to ConfigMgr Migration Utility.....	30
Microsoft* ConfigMgr Log Parser Script	30
Microsoft* ConfigMgr OOB Settings Update Script	31
Microsoft* ConfigMgr Console VBScript	31
Intel® Remote Encryption Management Software Development Kit (SDK).....	31
Intel® vPro™ Packet Decoder	31
Intel® Manageability Developer's Toolkit (DTK)	32
Manageability Network Connection Reflection Tool.....	32
Manageability Monitor Tool	33
Manageability Network Connection Reflection Tool.....	33
Manageability Flash Drive Tool	33
Manageability Terminal Tool	33
Manageability Net Traffic Tool	33
Manageability Net Status Tool.....	33
Manageability Network Defense Tool.....	34
Manageability Director Tool	34
Manageability Outpost Service Control Panel Tool.....	34
Manageability Outpost Tool	34
Manageability Commander Tool	35
Intel® AMT Software Development Toolkit (SDK).....	35
Intel® AMT Embedded Tools Suite	36
Intel® Power Manager (Plug-in for SpiceWorks).....	36
Intel® Management and Security Status Tool	36
Intel® Setup and Configuration Setup Wizard.....	37
Intel® Setup and Configuration Server (Intel SCS)	37
Third-party Software Vendors	37
Appendix A: Intel® vPro™ Brand Ingredients.....	41
Appendix B: Feature Support Matrix (by Release)	42
Glossary	45
Index.....	49

Introduction

This document is intended for Information Technology (IT) professionals who need to be aware of new features of the Intel® vPro™ Technology platform. This *Reference Guide* provides a high-level overview of how this technology can be used, a short discussion of the key features, and a high level list of tools and software.

This guide provides links to several key web sites for additional information and support:

- [Intel Software Network](#)—this site provides development tools, documentation, and resources to the community of programmers and developers of manageability solutions using Intel Active Management Technology and Intel vPro Technology.
- [Intel vPro Expert Center](#)—a community resource for IT professionals focused on Intel vPro Technology. This site features use case examples that show you how to unlock the value of Intel vPro Technology. This site also has sub-communities for embedded manageability, small business users, and users of manageability software from Microsoft, Symantec, LANDesk, HP, and others.
- [Intel vPro Alliance](#)—this site provides contact information so you can get the help you need to activate your Intel vPro technology.
- [Intel vPro Activation](#)—this site will help new users get started with Intel vPro Technology. The site includes an Activation Wizard that helps users select the activation methods the best meets their needs.

What's New?

The 2nd Generation Intel® Core™ processors with vPro™ Technology add the following new features:

- Intel® Anti-Theft Technology 3.0 with new 3G wireless support and improved resume from S3 sleep state capabilities
- Host-Based Configuration for easier setup and configuration of Intel AMT
- Intel® Management Engine firmware update roll-back capability to help IT professionals synchronize firmware versions in their enterprise environment
- Intel Active Management Technology 7.0
- Intel® Identity Protection Technology for two-factor authentication that eliminates the need for separate one-time password hardware tokens
- Up to 1920 x 1080 screen resolution for KVM Remote Control
- Support for desktop wireless manageability when Intel AMT is used with certain Intel network cards
- DASH 1.1 capable

What is Intel® vPro™ Technology?

Notebook and desktop PCs with Intel vPro technology enable IT departments to take advantage of hardware-assisted security and manageability capabilities that enhance their ability to maintain, manage, and protect their business PCs. With the latest IT management consoles from third-party software vendors, your IT department can now take advantage of enhanced features to manage notebooks over a wired or corporate wireless network—or even outside the corporate firewall through a wired LAN connection.

PCs with Intel vPro technology integrate robust hardware-based security and enhanced maintenance and management capabilities that work seamlessly with third-party management consoles. Because these capabilities are built into the hardware, Intel vPro technology provides IT with the industry's first solution for operating system-absent manageability and down-the-wire security even when the PC is off, the operating system is unresponsive, or software agents are disabled.

Security Features

The hardware-based capabilities of Intel vPro technology improves network traffic filtering and isolates clients under attack. Automatic security agents' verification and immediate remote restoration enhances your preventive security efforts. And with reliable remote power-up functionality, you can deploy off-hours patches faster, speeding up patch saturation. Additionally, the hardware-assisted antivirus protection of Execute Disable Bit protects your PCs from certain viruses that use buffer overflow attacks.

Protecting virtual environments against rootkit and other attacks, Intel Trusted Execution Technology (Intel TXT) offers extra protection on PCs with Intel vPro technology and built in Intel Virtualization Technology (Intel VT). Including an industry-standard TPM 1.2 which can be used by third-party software to store keys and other protected data, Intel TXT enables the PC to boot software into a trusted state and also helps protect the integrity of the virtual machine.

Manageability Features

PCs with Intel vPro technology can help IT professionals diagnose and repair both wired and wireless systems remotely, cut downtime, and reduce the average in-person IT support time. Intel vPro technology helps perform remote asset tracking and checks the presence of management agents virtually anytime.

Intel Technologies

Intel vPro technology is a collection of platform capabilities that support enhanced manageability, security, virtualization, and power efficiency. The key platform capabilities include the following Intel technologies:

- Intel Turbo Boost Technology for increased performance and power efficiency
- Intel Virtualization Technology (Intel VT) for Dynamic Virtual Client support and other operating system or application streaming techniques using virtualization
- Intel Hyper-Threading Technology (Intel HT) for higher performance
- Intel Active Management Technology (Intel AMT) for greater manageability
- Intel Anti-Theft Technology (Intel AT) for greater security

- Intel Trusted Execution Technology (Intel TXT) for greater security
- Intel Identity Protection Technology (Intel IPT) for enhanced web security

For more information:

- [Intel vPro Technology](#)
- [Demo](#): Get inside notebook and desktop PC's with Intel vPro technology

For information on planning and using Intel vPro technology, we recommend the following book from Intel Press:

- Arvind Kumar, Purushottam Goel, and Ylian Saint-Hilaire. 2009. *Active Platform Management Demystified, Unleashing the power of Intel vPro Technology, IT Best Practices*. Santa Clara: Intel Press. ([link](#))

Use Cases

Introduction

With Intel vPro technology, IT departments can discover, protect, and heal their networked PC assets. The following *use cases* illustrate some of the many ways IT departments can use Intel vPro technology to save time, save money, and reduce power consumption. Each use case requires that all the managed PCs are Intel vPro technology enabled, and, in most cases, that the IT management console is using a third-party management software application.

For more information:

- [Technology Brief: Intel Active Management Technology](#)
- [Intel Active Management Technology Use Cases](#)
- [Architecture Guide: Intel Active Management Technology](#)
- [Fast Facts on Intel Active Management Technology \(Intel AMT\)](#)
- [ROI Analysis - Realizing The Cost Saving Benefits of Activating Intel vPro Technology](#)
- [Intel vPro Technology - Technical Use Cases](#)

Use Case 1: Platform Auditing

In this use case, the IT administrator can identify each PC using a Universally Unique Identifier (UUID). Platform auditing reduces or eliminates manual inventory audits by being able to locate systems regardless of their power states or the health of the PC's operating system. This Intel vPro technology use case improves IT asset management.

For more information:

- [Intel Active Management Technology Use Case #1: Platform Auditing \(Discover\)](#)

Use Case 2: Software Inventory

This use case helps IT departments improve the software inventory process, optimize maintenance contracts, licensing, and configurations inventory through firmware-resident software information.

Using a third-party software inventory management application that supports Intel AMT, an IT professional discovers platforms remotely down-the-wire, regardless of operating system or power state. Intel AMT makes that possible via out-of-band (OOB) remote access to the platform's persistent, tamper-resistant asset IDs.

In a typical situation, the IT administrator uses third-party management software with in-band tools or agents to inventory the system, or write inventory information to Intel

AMT's *third-party data store* (a secure data storage area in flash memory). The management software can then be used to access the stored software inventory when the client systems are powered-off (but connected to the AC power and network), or when the operating system is down and the system is powered-on.

Because a system is found using Intel AMT, the IT professional is able to gather information accurately, quickly, and remotely, so the enterprise can more efficiently and effectively manage its software licenses, as well as optimizing utilization of maintenance and service contracts.

In addition, accurate and timely inventory information enables the IT department to better manage software updates.

Software inventory management is supported by all leading management software packages (Microsoft*, LANDesk*, Semantec*, Hewlett-Packard*, and others).

For more information:

- [Intel Active Management Technology Use Case #2: Software Inventory Management \(Discover\)](#)

Use Case 3: Hardware Inventory

Intel vPro Technology improves the visibility of enterprise hardware platforms, dramatically improving the completeness of hardware inventories. Capabilities of Intel AMT help to reduce the impact of software-agent removals, powered-down machines, non-functioning operating systems, and other system failures during hardware inventories. These problems make as many as 15%-20% of all systems not visible down-the-wire at any given time. Wireless environments and laptops make this even more challenging since at any point in time, laptops may be connected over the wireless network (Mobile mode) or remotely connected to a corporate LAN via VPN (Remote mode) or may not be connected to an AC power source.

With Intel vPro technology, hardware inventories are more efficient to conduct, thus greatly assisting compliance with government regulations, as well as management of recalls, warranties, and configurations. This use case includes hardware inventory to determine the type and quantity of hardware in the environment, and the state of the hardware's warranty.

Hardware inventory management is supported by all leading management software packages (Microsoft*, LANDesk*, Symantec*, Hewlett-Packard*, and others).

For more information:

- [Intel Active Management Technology Use Case #3: Hardware Inventory Management \(Discover\)](#)

Use Case 4: Remote Diagnosis and Repair

Intel vPro technology (with Intel AMT technology) can help to reduce the support overhead associated with repairing platform boot failures. By enabling remote resolution of a greater proportion of such failures, costly, reactive repair processes can be avoided. Additionally, both the end-user and IT technicians save valuable time through the elimination of time-consuming diagnostics.

An example of this use case might be an end-user platform that will not boot due to a missing or corrupt DLL. Intel AMT can be used to facilitate remote diagnosis and repair of the end-user's platform.

In another example, an alert could be sent to a management console identifying a soon-to-fail hardware unit before the fail-to-boot problem occurs. If the system failed without warning and refuses to boot, then, as in the example above, the end-user could contact the help desk directly by phone or by using Fast Call for Help (page 12). The IT technician could use Intel AMT IDE Redirection (IDE-R) to redirect the platform to a known good boot image and then monitor and control the platform remotely (with Serial-Over-LAN or KVM remote control). Using these tools, the IT help desk technician can diagnose the problem and perform remote remediation (utilizing third-party management software) if hardware replacement is not necessary. Furthermore, the technician can perform these operations without the end-user being present and even if the end-user's platform is powered-off.

For more information:

- [Intel Active Management Technology Use Case #4: Remote Diagnosis, Remote Repair \(Heal\)](#)

Use Case 5: Remote Diagnosis and Local Repair

Intel vPro technology can help to reduce the support overhead associated with repairing system-boot failures, even when the issues that underlie those failures cannot be repaired remotely (*for example*, hard drive corruption or memory errors). By enabling problem diagnosis on a down-the-wire basis, Intel AMT platforms can reduce the need for time-consuming technician visits to diagnose the platform, which otherwise increase user downtime, as well as consuming IT resources.

In this use case, an event from the user's machine may be received on a management console operated by the support organization to indicate inoperable or malfunctioning hardware. Policies configured on the console evaluate the event to determine whether an alert to the help desk is needed.

In addition, the user may also contact the help desk directly.

The help desk then diagnoses the problem down-the-wire using Intel AMT's Serial-over-LAN (SOL)/IDE-R remote boot capability and third-party diagnostics. While the help desk is unable to repair the system remotely, it is able to remotely identify the correct field-replaceable unit (FRU) to perform the repair, so that the field technician has the part with them when they are first dispatched to the end-user's location, and they are able to perform the repair at desk-side on their first visit.

In this Intel AMT-enhanced scenario, only one desk-side visit is required to repair the system, potentially saving one desk-side visit.

For more information:

- [Intel Active Management Technology Use Case #5: Remote Diagnosis, Local Repair \(Heal\)](#)

Use Case 6: Software Version Compliance

In addition to simply taking an inventory of the software, Intel AMT can be used to ensure that all platforms in an enterprise are compliant with corporate requirements to have up-to-date software versions. Out-of-band (OOB) polling helps to address the issue that 15% to 20% of all platforms are typically not visible on an in-band, down-the-wire basis, which traditionally complicates efforts to avoid risks associated with outdated software such as runtime errors, viruses, and malware attacks.

Intel AMT also helps to remove issues associated with user non-compliance with your IT policies (for example, user removal of software agents).

One example of this use case is to use Intel AMT to verify that client systems have the latest virus signature files. In this use case example, platforms that are powered-off can be audited OOB and turned-on, if necessary, using Intel AMT to install virus signature files and anti-virus engine updates. If the virus scan software agents are missing, software updates can be installed onto platforms during off-hours to eliminate interruptions to the users, and to decrease the peak network traffic.

For more information:

- [Intel Active Management Technology Use Case #6: Software Version Compliance \(Protect\)](#)

Use Case 7: System Defense

Intel vPro technology can be used to decrease the enterprise vulnerability to network attacks. Outbreak containment filters help to detect suspicious activity. This example examines the case where a zero-day virus (such as Slammer) attacks a network. Note that greater connectivity options, including public wireless hotspots, hotels, and home networks increase vulnerabilities. The example includes efforts to reduce network exposure once platforms infected with the virus begin propagating the infection across the network.

Conventional Virus-Recovery Limitations

In a typical zero-day inbound virus attack, infected platforms propagate the virus through the network. In many cases, manual IT intervention is required to prevent the spread of the attack.

Traditional environments facing malware attacks must scramble to reduce network exposure. Compromised software firewall agents leave platforms vulnerable to malware attacks. Network threats (once successful) can spread quickly throughout the network. Distributed methods for detecting malware activity across multiple managed end nodes are limited. During an event, network managers have little recourse if a software firewall patch or update is not available. These patches can take a day or more for the software firewall vendors to create, leaving networks vulnerable unless entire subnets are brought down. Productivity is halted until the threat can be contained.

Using Intel vPro Technology to Overcome Limitations

In an Intel vPro enabled environment, zero-day inbound and outbound virus protection benefits from System Defense filters that scan incoming and outgoing network traffic,

regardless of operating system or virus protection agent state. Scans for suspicious behavior compare five points of data (source and destination IP addresses and port numbers, as well as protocol type) against preset rules.

Additionally, heuristics-based network traffic filters monitor the outbound network traffic for IP scans and port scans. Each node is able to compare a time slice of network traffic against the heuristics filters defined in the system defense engine. Based on time and number of occurrences of thresholds set in the filters, suspicious behavior is detected.

These filters are configurable via third-party console applications, which govern whether traffic identified as suspicious is dropped, alerted to the IT organization, or passed through (no action). Depending on the IT policy setup, filters can be programmed to protect the system from receiving or transmitting malware, resulting in reduced support calls and increased user productivity.

In order to reduce network exposure, the IT organization can detect suspicious activity at a node or series of nodes via alerts sent to a central control console. It can send real-time updates via the out-of-band (OOB) channel to suspected nodes to block the suspicious traffic (allowing the user to remain connected and active with only the malware blocked) and update unaffected nodes with additional filter criteria. While a platform is in quarantine, console software can clean the system of malware, viruses, etc., using either a specific dedicated port or Serial-over-LAN (SOL)/IDE-R to boot the system to a known good image for remediation.

For more information:

- [Intel Active Management Technology Use Case #7: Hardware-Based Isolation and Recovery \(Protect\)](#)
- Intel AMT System Defense Use Cases ([video](#))

Use Case 8: Agent Presence

Intel vPro Technology can virtually eliminate the ability of users or malware to circumvent virus protection. If the user disables the virus scan agents, that action triggers alerts, quarantines the system, and re-initializes agent.

Intel Active Management Technology (Intel AMT) helps to safeguard the operation of critical manageability functions by helping to remove the threat associated with critical software agents being removed without detection. In this use case example, malware attacks and infects a platform, disabling software agents. The platform now is vulnerable to malware and is capable of mounting attacks on the network. Additionally, software agents can be intentionally or unintentionally disabled or removed by users, negating the value of the manageability and security software.

Conventional Limitations of Software Agents

In a traditional environment, management consoles poll platform-resident software agents to ensure that they are present. This activity takes up network bandwidth and only works if the platform is powered on, the operating system is present and operational, and the platform is attached to the corporate LAN. Many systems typically cannot be polled, including mobile client systems, those that are powered off, those

that are non-responsive, etc., leading to time-consuming issues that may yield inaccurate results.

Using Intel AMT to Overcome Limitations

Intel AMT enabled third-party software agents register with the Intel AMT firmware. Once they are registered, third-party management-console software configures how often it will poll for agent presence. The polling is performed locally and does not impact network performance. For example, the Intel AMT firmware can check to see if the agents are present every 10 seconds. If agents don't respond to the poll, an alert is sent to the management console.

If configured to do so, the system will take immediate action based on the policy that was preconfigured, such as isolating the system from network access, while leaving a port open to allow the console to force a reinstall of the disabled agent. In other configurations, the management console will determine the action to take upon receiving an alert from the system. Both mechanisms can reduce the number of support calls received to remedy the affects of agent removal and reduce the amount of time the system remains vulnerable.

For more information:

- [Intel Active Management Technology Use Case #8: Agent Presence Checking \(Protect\)](#)

Use Case 9: End Point Access Control

Intel vPro Technology can limit network access by visitor, rogue systems, and systems that do not conform to company policies for virus protection, and operating system patches. The outcome will force systems that do not meet corporate policy onto a remediation network.

Endpoint Access Control: Using Intel AMT with Network Access Control (Cisco SDN or Microsoft* NAP)*

Intel AMT helps secure network endpoints by validating their compliance with network policies. Endpoint Access Control (EAC) feature allows the IT administrators to implement differentiated policy enforcement and configuration based on the security state of the end point. This example examines the case where a system with non-compliant software configuration is attempting to request the access to the network. Intel AMT 2.5, 3.x, 4.x, 5.x, 6.x, and 7.x support Cisco* SDN. Intel AMT 4.x, 5.x, 6.x, and 7.x support Microsoft* NAP.

Greater connectivity options, including public wireless hotspots, hotels and home networks increase the vulnerability of notebook PCs. Notebook PCs often become vulnerable when disconnected from the network. When the PC is reconnected to the network, there is the potential threat to the business. Rogue desktop systems (non-IT managed, not properly configured, or a visitor's system) plugged into a corporate network could open a security hole, allowing an external visitor or hacker to snoop the network, and could be the source of spreading malware onto the network. This example includes efforts to isolate the non-compliant systems and automate the system remediation to bring them into compliance with network security policies.

Conventional Endpoint Access Control Limitations

802.1x networks have the ability to authenticate systems before allowing them on the network, but have no ability to validate postures to ensure proper virus protection, proper OS patches, and that no unauthorized software is installed. Non-compliant systems (those without proper virus protection, OS patches, or unauthorized software) can connect to the network and potentially become the source of distributing malware into the network. Visitors have the ability to connect to the network. Once connected to the network, they can sniff traffic and view mission critical application traffic and/or access data stored on the network.

Using Intel AMT to Overcome Limitations

At every connection or on demand, a client system's profile is securely surveyed in a trusted manner. The "system posture" (including credentials, configuration, and system data) along with Intel AMT configuration parameters (Firmware Version, TLS enabled, SOL enabled *etc.*), is compared to current requirements. For systems not meeting the minimum standards, the Policy Decision Point (PDP) conveys a health assessment for the system and limits or denies network access. If network access is restricted, a User Notification is displayed to convey to the end user that normal network operation will be delayed until remediation is complete. The system is then redirected to a software configuration system or placed in a remediation network for upgrading to minimum standards. Rogue systems plugged into the network are now identified and the access is controlled based on policy. Full authentication and posture checking before allowing network access can greatly reduce the potential for malware to propagate onto the network, allows for the IT admin to maintain all systems in compliance with current policies, and limits rogue or visitor systems from gaining network access.

For more information:

- [Intel Active Management Technology Use Case #9: Endpoint Access Control \(Protect\)](#)

Use Case 10: One-Touch Configuration

Intel AMT technology can perform automated setup and configuration of an Intel AMT device, either using credentials stored on a USB key storage device or by keying credential information manually into the BIOS.

Overview

In this use case example, an IT manager receives shipment of several PCs that he wants to configure to use Intel AMT. These PCs are all shipped with Intel AMT turned off (the manageability mode set to "None"). Intel AMT must be configured prior to deployment to users' desks so that the management console can securely identify and communicate with an Intel AMT enabled PC.

Using Intel AMT One-Touch Configuration to Enable Provisioning of Business PCs

One-Touch Configuration of Intel AMT-enabled business PCs encompasses a number of setup scenarios:

- *Automated setup* using a USB key storage device (for both dynamic IP and static IP environments): An IT administrator requests provisioning passphrase

(PPS) and provisioning ID (PID) pairs for all systems requiring setup from the configuration server. The configuration server stores the PPS/PID pairs and an administrator password and other configuration data on the USB storage device. The IT administrator plugs the USB storage device into the PC and powers the PC on. As the PC loads, the BIOS and MEBx (Management Engine BIOS Extension) reads the administrator password, PPS, PID, and other required information from the USB storage device.

- *Manual setup for dynamic IP networks:* The IT administrator requests PPS and PID pairs for all systems requiring setup from the configuration server. The administrator powers on the PC to be set up, and during the boot, he or she presses the appropriate key to display the MEBx configuration screen. The IT administrator logs into the MEBx using the factory default administrator username and password and changes the username and password when prompted. The IT administrator ensures that the MEBx manageability mode is set to Intel AMT, turns on SOL/IDE-R, if desired, verifies that the power policies are set for sleep state operation as desired, enters the PPS/ PID pair, and exits the MEBx screen. The BIOS will then continue to load.
- *Manual setup for static IP networks:* This sequence is the same as for dynamic IP networks until the step where the PPS/PID pair is entered. At that point, the IT administrator assigns a name to the PC's operating system for identification purposes and selects the TCP/IP option. The IT administrator then disables DHCP and then sets TCP/IP and DNS settings appropriately for the static IP network. The IT administrator then enters the PPS/PID pair, exits the MEBx, and allows the system to complete booting.
- *Final automated configuration for all setup methods:* The PC is connected to power, and the Intel AMT device automatically initiates the configuration process over the network by locating the configuration server and establishing secure communications via the PPS/PID. The configuration server loads the settings and data required for the environment and reboots the PC.

For more information:

- [Intel AMT Use Case #10: One-Touch Configuration](#)

Use Case 11: Remote Configuration

Under Remote (previously known as Zero-Touch) Configuration, the PC is connected to power and the network, and Intel AMT automatically initiates the configuration process:

- *Delayed configuration:* When an Intel AMT 5.0 or earlier system is first turned on, it automatically sends out "hello" packets. After a timeout period has elapsed, it stops sending these packets until it receives a message from the configuration server. When a configuration message is received by a third-party software agent running in the client PC operating system, the configuration process begins. This agent based Remote Configuration process can configure any version of Intel AMT PCs. Certificates are exchanged and compared to hashes stored in the Intel AMT firmware, and passwords are exchanged. The client system also ensures that the configuration request has been received

from a server on its network before allowing configuration to occur. Once all of the proper checks have occurred, the configuration server loads the settings and data required to enable Intel AMT to reboot the system.

- *Bare Metal configuration:* The process for bare metal configuration is the same as for delayed configuration, except that a third-party software agent is not needed, and the configuration server can configure Intel AMT 5.0 and earlier without the onetime password. Once the Intel AMT PC is configured, an operating system can be loaded from the network onto the PC, allowing for a completely no-touch configuration of the system with an IT-specified operating system.

With the release of Intel AMT 7.0 and Intel Setup and Configuration Service 7.0, users can now use Host Based Configuration for all versions of Intel AMT firmware. The Unified Configuration Process can be used to detect the firmware version and use Remote Configuration with Intel AMT 6.0 and earlier systems.

For more information:

- [Intel AMT Use Case #11: Remote Configuration](#)
- See also: [Host Based Configuration](#)

Use Case 12: Fast Call for Help

Fast Call for Help allows Intel vPro technology platforms to initiate a secured connection to a gateway server residing in the enterprise's so-called network "De-Militarized Zone" (DMZ). Using this call for help feature, Intel vPro technology-based clients can be managed remotely by the IT Administrator when the system is located outside the corporate network.

The solution using Fast Call for Help requires three components:

- Intel vPro technology-based client PCs with Intel AMT configured for remote access connectivity
- Intel vPro Enabled Gateway (formerly called the Manageability Presence Server or MPS)
- A third-party management console

In the conventional network infrastructure, the connection is initiated by the management console and the Intel AMT management engine in the client acts as a TCP server responding to management console's connection attempts. When the client is outside the intranet, this model doesn't exist due to security concerns and the inability to find the client.

To address this situation, the Intel AMT client is first configured for remote connectivity, then the client can initiate a secure TLS connection to an intermediate server (the Intel vPro Enabled Gateway) located in the enterprise network's DMZ environment. The Intel vPro Enabled Gateway mediates the connection between the remote Intel AMT device located outside the intranet and the management console located inside the corporate network. Communication between the management console and Intel AMT client is protected using a secure TLS connection.

Once a secured TLS tunnel is established between Intel AMT client and Intel vPro Enabled Gateway, multiple management consoles can then communicate with the same device and all of the traffic is piped through the same secured tunnel. The Intel vPro Enabled Gateway is responsible for connecting and disconnecting sessions as management consoles initiate and complete their actions. The Intel AMT client can also drop the secure connection after a defined period of inactivity.

With the 2nd generation Intel Core i5 vPro and Intel Core i7 vPro processors, Fast Call for Help can be used with Intel AMT clients on wireless networks outside the corporate firewall.

For more information:

- [Fast Call for Help Overview](#)

Use Case 13: Intel® Anti-Theft Technology (Intel® AT)

With Intel Anti-Theft Technology (Intel AT), businesses now have built-in client-side intelligence to help secure sensitive data regardless of the state of the operating system and network connectivity. This hardware-based technology provides compelling tamper-resistance and increased protection to extend your security capabilities anywhere, anytime, on or off the network, and minimize business risk.

Intel AT offers the option of activating hardware-based client-side intelligence to secure the PC and its data if a notebook is lost or stolen. Because the technology is built into PC hardware, it provides local, tamper-resistant defense that works even if the operating system is re-imaged, a new hard-drive is installed, or the notebook is not connected to the network.

The following table provides an overview of Intel AT features.

Table 1: Intel Anti-Theft Technology 3.0 Features

Intel® AT Feature	How it works	Benefit
Detection (Triggers)	<ul style="list-style-type: none"> • Excessive login attempts - The system keeps track of an IT-determined number of login failures in a pre-boot authentication (PBA) module. • Timeframe login requirement – If the software agent does not log in to central server by a specific time/date (per IT policy), the Intel AT firmware can trigger a response. • Notification from the central server – Upon notification from the end-user (loss/theft), IT flags the notebook in a central server database (hosted in the Internet). The next time the flagged notebook connects on the internet, it synchronizes with the central server and receives the 	<ul style="list-style-type: none"> • Local detection mechanisms (login failures and timeframe login requirement) work even if no network connection is available. • Ability to integrate with existing encryption solutions' pre-boot authorization (PBA). • Flexible policy engine allows IT to determine which detection mechanism should be used and what action to take.

Intel® AT Feature	How it works	Benefit
	<p>“poison pill” (PC Disable and/or Data Disable) per IT policy.</p> <ul style="list-style-type: none"> • Resume from S3 timeout – If the user doesn’t login within a set time limit after the system comes out of the S3 sleep state, the system will shut down to the S4 or S5 sleep state to protect the data on the encrypted hard drive. 	
Data disable	Poison pill deletes the software-based encryption keys or other cryptographic credentials required to access encrypted data on the hard drive. This feature requires a third-party encryption program.	<ul style="list-style-type: none"> • Protects the data on the hard drive
PC disable	Poison pill message renders the PC inoperable by blocking the OS from booting.	<ul style="list-style-type: none"> • Minimizes the potential of a stolen notebook being used and sensitive data being accessed. • PC Disable can be triggered locally or remotely Tamper-resistant. • Over time, it becomes a theft deterrent.
Reactivation	<p>Return notebook to full functionality via:</p> <ul style="list-style-type: none"> • Local passphrase that was set by user. • Recovery token (one-time use) provided by IT over LAN, wireless LAN, or encrypted SMS message over a 3G network. 	Simple way to restore notebook to full functionality without compromising local security features for data access disable or PC disable.

How It Works

Intel AT includes two programmable, interdependent hardware-based timers to help identify unauthorized access to the system: a *disable* timer and an *unlock* timer. Using these programmable timers, Intel AT can detect potential loss or theft situations, shift into “theft mode,” and then respond according to configured IT policy.

Local, hardware-based detection and trigger mechanisms include:

- Excessive login attempts—the system is disabled after an IT-determined number of login failures in the pre-operating system screen.
- Timeframe login requirement—the system is disabled if the software agent does not log in to central server by a specific time/date.
- Notification from the central server—If IT flags the notebook in the central server database, the next time that notebook’s software agent logs into the network, the notebook synchronizes with the central server and, after receiving the server’s notification, performs IT defined policy based actions.

Poison Pill Responses

There are several poison-pill responses to theft mode. The responses are flexible, and can be programmed to do the following:

- Disable access to data, by deleting components of software-based encryption keys or other cryptographic credentials required to access encrypted data on the hard drive.
- Disable the PC by blocking the boot process, even if the hard drive is replaced or reformatted.
- Disable both the PC and access to the Intel AT data storage area.
- After the PC is disabled, the PC displays a user-configured message to help whoever finds the lost PC return it to the owner.

Excessive Login Attempts Can Trigger Poison Pill for PC Disable

Disabling a PC after excessive login attempts can be an effective way to prevent loss of encrypted data. For example, an engineer's notebook and wallet might be stolen in an airport. The thief might try to log in using information from the engineer's wallet, but—based on IT policy—after three login attempts, the Intel Anti-Theft trigger is tripped, and the system locks down.

If an encryption software vendor has provided this feature, encryption keys for encrypted data (or software components that are needed to access these keys) can be erased from the hard drive and thereby disabling the PC. In this case, even if the thief removes the hard drive and installs it in another device, the security credentials that provide access to encrypted data on the hard drive have been erased or disabled and the data cannot be stolen. Until reactivated by the authorized user or IT, the PC will not boot and the encrypted data cannot be accessed.

Server Login Timeout Can Trigger Poison Pill for PC Disable

In another example, a research scientist's notebook might contain highly sensitive data about a new invention. In this case, IT has defined the triggers on the scientist's notebook to require the notebook to log in daily. During a family event, the scientist takes time off and does not log in for two days. Based on locally stored policy for the login timeframe, the notebook enters "theft mode," disables itself (and erases the encryption keys for encrypted data on the hard drive, if an encryption software vendor has provided this feature). Even if the notebook is removed from the lab while the user is away, the notebook has secured itself until the scientist returns and reactivates the system.

Reactivation

To recover when a notebook is being returned to service, Intel AT also includes two reactivation mechanisms:

- Local passphrase, which is a strong password pre-provisioned in the notebook by the user. To reactivate the system, the user simply enters this passphrase in a special BIOS login screen.
- Recovery token, which is generated by IT or by the user's service provider via the theft management console, upon request by the user. For reactivation, a one-time recovery token is provided to the user via phone or other means, and the user enters the token in a special BIOS login screen.

Both passphrase and recovery token return the PC to full functionality. Both methods offer a simple way to recover the notebook without compromising sensitive data or the system's security features.

Reactivation is integrated with existing software vendor pre-boot login process (for example: Absolute* software or WinMagic* SecureDoc) for simpler reactivation.

For PCs with whole disk encryption, the data disable feature renders the data inaccessible if the PC is stolen by removing access to the decryption keys. The data can be easily recovered remotely, or locally, using a pass-phrase or token. This feature requires support by the whole disk encryption software application and the remote management console software (*for example*: WinMagic* SecureDoc).

Wireless 3G support

Intel AT 3.0 now has support for 3G cell phone networks (with the appropriate modem installed in the PC). Wireless 3G SMS messages can be used to check-in, send a poison pill to the PC, or to send a recovery token to the PC.

To test the client readiness for Intel AT, use the following tool:

- Intel Anti-Theft Technology—Data Protection Test and Control Console ([link](#)).

For more information on Intel AT, see:

- WinMagic* [website](#)** (**This URL to a third-party website is provided for the reader's convenience. Inclusion of this link should not be construed as a recommendation by Intel. Intel is not responsible for the content of third-party websites.)
- [Intel Anti-Theft Technology is here!](#)
- [Computrace with Intel Anti-Theft Technology Whitepaper](#)
- [Success Story: Securing Success for Polycom, Inc.](#)
- [Webinars: Learn More About Intel vPro Technology](#)
- [Virtual Conference Series: Securing Your Environment with Intel Anti-Theft Technology](#)
- [Protecting Sensitive Data on Laptops is More Important Now than Ever, Intel Anti-Theft Technology version 3.0](#)

Use Case 14: Access Monitor

The Access Monitor feature supports detection of security policy violations, based on the principle of accountability. The Access Monitor log tracks Intel AMT actions based on policies set by the IT professional in the *Auditor* role. The Auditor is the only person allowed to access the Audit log. By checking the Access Monitor log activity, suspicious or non-complaint activities may be detected. ®

The Access Monitor feature provides oversight into Intel AMT actions to support your IT security requirements.

By default, the Access Monitor logs nothing when first enabled. The Auditor must choose what is logged and the severity level. Once this policy is set, the Access Monitor behaves as follows:

- Events can be set to "Enabled" or "Critical".

- When the log is about 75% full, events marked “Enabled” are no longer logged. However, the action that triggers the event still succeeds.
- When the log is 100% full, events marked critical are no longer logged and are blocked from operation. For example, if SOL is being logged as critical and the log is full, AMT returns “PT_STATUS_AUDIT_FAIL” the next time SOL is attempted. This will continue until the Auditor clears the log.

For more information:

- *Intel Active Management Technology Access Monitor*, available in the Intel AMT SDK (see: page 32)

Use Case 15: Remote Power Control

Power control operations enable you to remotely control the power states of Intel vPro technology enabled systems. In most cases, the third-party management software will support all the power control operations listed below.

In general, you can apply the following power control operations to Intel vPro technology enabled systems:

- power-up
- power-down
- power cycle
- reset

You can also specify the way that a system should boot, depending on the specific system implementation.

The Intel AMT Remote Power Control Utility is a simple command line utility that allows users to remotely control the power state of an Intel AMT system without requiring a separate management console. This utility supports Intel AMT systems configured for basic, standard and advanced modes, using digest authentication (simple username and password) or Kerberos authentication.

For tools and more information:

- [Intel AMT Remote Power Control Utility](#)
- Manageability Monitor Tool—monitors Intel AMT client power state (download the [Manageability Developer’s Toolkit](#))
- [ROI Analysis: Premiere Hospital Realizes Significant ROI Using Remote Power-on and Remote Boot Capabilities via Intel vPro Technology](#)

Use Case 16: PC Alarm Clock

The PC Alarm Clock feature allows the IT management console to schedule power events on a remote Intel vPro technology enabled PC. The remote PC can be scheduled by the management console to locally wake-up at a scheduled time. This allows the PC to be disconnected from the network when the scheduled power-on event occurs. The operating system task scheduler will then run any scheduled tasks and scripts to power-down the PC.

This feature requires a third-party software application to schedule a task after the PC wakes up.

Potential applications of this feature include:

- Scheduling resource intensive applications to run during off-peak hours. For example, the IT department might schedule a full virus scan or a disk defragmentation on the remote PC.
- Executing periodic backups.
- Ensuring that PCs pull and apply scheduled updates.
- Turning on PCs in anticipation of the start of work or the scheduled opening of the business.

Use Case 17: KVM Remote Control

The 2nd generation Intel Core i5 or i7 vPro processor with Intel processor graphics includes a hardware-based KVM Remote Control capability that lets IT remotely see what their users see through all states (such as an operating system blue screen), even beyond the firewall.

In 2011, the KVM Remote Control feature has been extended to quad-core 2nd generation Intel Core vPro Processors and enhanced to support HD screen resolutions of up to 1920 x 1200, 16-color.

Once IT, or a service provider, has access to the PC, he can remotely boot the PC by remotely redirecting the PC's boot process, causing it to boot from a different image, such as a network share, bootable CDROM or DVD, remediation drive, or other boot device. This feature supports remote booting a PC that has a corrupted or missing operating system. The software problem on the PC can be fixed remotely via a remediation "fix it" drive on the network.



NOTE

KVM Remote Control requires an Intel processor with Intel processor graphics. This feature is not available on some previous generations of Intel vPro processors. For a list of processors that support the KVM Remote Control feature, click [here](#).

KVM Remote Control only operates with Intel processor graphics. However, a platform may also have an external (discrete) graphics system that allows users to switch back and forth between the graphics interfaces.

Intel AMT 6.0 adds KVM Remote Control to the existing redirection features of Serial Over LAN (SOL) and Redirected IDE (IDE-R). With KVM Remote Control, a Remote Console can open a session with an Intel AMT platform and control the platform using a mouse and keyboard and display at the console what is displayed on the local monitor. The KVM Remote Control capability is enabled in the same way that SOL/IDE-R is enabled—with network administration commands. KVM Remote Control first must be enabled in the Intel Management Engine BIOS Extension (MEBx) and the listener enabled (as with SOL/IDE-R) before it can be enabled remotely.

KVM Remote Control is based on the RealVNC Limited* Remote Frame Buffer (RFB) protocol. Off-the-shelf viewers based on the RFB protocol should work in conjunction with Intel AMT without modification.

Protecting User Privacy

When User Opt-in is enabled in the MEBx, the firmware generates a “sprite” (a pop-up graphic displayed to the PC user directly, even if the graphics driver is disabled) with a one-time password (OTP) that the KVM Remote Control client must send to complete establishment of a session. The PC user has to tell the IT operator what the password is, for example, by telephone or text message. Note that any sprites displayed to the local operator are not echoed to the KVM Remote Control client (this is configurable).

If there is no connection activity for a configurable pre-defined period (defined as no keyboard or mouse activity), the server at the PC will drop the connection.

If there are three consecutive failed login attempts, Intel AMT will delay subsequent attempts and log the occurrence.

Enabling KVM Remote Control

The KVM capability is enabled in the same way that SOL/IDE-R is enabled--with network administration commands using WS-Management calls. In most cases, administrators will use a management console with built-in KVM Remote Control viewer that sends the appropriate WS-Management calls.

For more information:

- For manual configuration of the KVM Remote Control for use with an off-the-shelf viewer, refer to the following site for instructions and sample configuration scripts: [Use Case Reference Designs for Intel vPro Technology](#)
- Intel AMT SDK (see page 35)
- For detailed instruction on how to configure KVM Remote Control for secure communications, refer to the *KVM Application Developer's Guide* in the Intel AMT 6.0 SDK (see page 35).

Use Case 18: Remote Encryption Management

Full disk encryption typically blocks remote management consoles by requiring a local password or pass-phrase to boot past the pre-boot authentication screen. Intel vPro technology provides a method to remotely unlock and manage the encrypted PC without compromising the security or remote manageability. PCs with full disk encryption may be shut down at night and then remotely powered-on, patched, and shut down again without user intervention.

This capability can be used by the IT department in several ways:

- Remotely wake and patch the PC
- Automatically enter the hard drive password when the PC is on a trusted network segment
- Manage the user account and password
- Enable or disable disk encryption
- Repurposing the disk

For more information:

- [Intel Remote Encryption Management Software Development Kit \(SDK\)](#)

Use Case 19: Unattended Software Updates

Intel vPro technology, with third-party management software, speeds-up security patches and makes them less intrusive. For example, a third-party software vendor management application can update anti-virus engines and signatures remotely, regardless of the operating system or power state of the client.

To do an unattended software update, the management application accesses the software inventory databases or platforms' software inventory stored in non-volatile memory (even in a pre-boot state). The management application then uses Intel AMT technology to wake-up the platform and deliver or install the required updates based on the software inventory. Finally, the application then uses Intel AMT to return platform to its previous power state (hibernate, stand-by, *etc.*).

Use Case 20: Host Based Configuration

Starting with Intel AMT 7.0 and the release of Intel Setup and Configuration Service (Intel SCS) 7.0, users can now perform the setup and configuration of Intel AMT clients using a utility running on the local Intel AMT client. This simplifies the setup and configuration process. Intel AMT 6.0 and earlier versions can also be setup and configured using the Intel SCS 7 tools by automatically having the local utility communicate with the Intel SCS provisioning server (this is called the *Unified Configuration Process*).

Host Based Configuration has two modes: Client Control Mode and Admin Control Mode. The IT administrator can choose which mode to use. The two different modes have different requirements for obtaining the user's consent, credentials for unprovisioning, and the ability in the ability of the Intel AMT client to support system defense filters after it is setup. The following table summarizes the features of these two modes.

Table 2: Intel Anti-Theft Technology 3.0 Features

	Admin Control Mode	Client Control Mode
User Consent	For Intel AMT 7.x devices in Admin Control mode, you can define which operations require user consent. The choices are: Not Required; KVM Remote Control Only; Required for All. For Intel AMT 6.x devices, you can choose to enable user consent only for KVM Remote Control.	User consent is always required for setup and configuration, KVM Remote Control, IDE Redirection, Serial Over LAN, and boot control
System Defense Filters	Fully supported	Not Supported
Unprovisioning	Unprovisioning can be performed only with Intel AMT credentials	Unprovisioning can be performed with Windows Administrator rights on the local machine, or with Intel AMT credentials for the client

The following steps outline how the IT administrator can use Host Based Configuration to setup and configure Intel AMT clients:

1. Install the Intel SCS 7.0 package.
2. From Intel SCS, create an XML file that contains the Intel AMT settings (as in previous versions of Intel SCS, this collection of settings is referred to as the profile).
3. Distribute the XML file and the required Intel SCS utility to the Intel AMT client. Run the package.
4. If the IT administrator has selected Client Control Mode, the user on the Intel AMT 7.0 client machine will be prompted to consent to running the utility and configuring the client. For clients with prior versions of Intel AMT, the Intel SCS utility will contact the Intel SCS 7 provisioning server and use the existing remote configuration methods.

For more information, refer to the documentation provided with the Intel SCS package. For more information about Host Based Configuration support in third party management software packages, refer to the ISV documentation.

Use Case 21: Intel® Identity Protection Technology (Intel® IPT)

Starting with the 2nd generation Intel Core vPro Processors, Intel vPro Technology now includes Intel Identity Protection Technology (Intel IPT). This technology provides a hardware-based one time password that can be used to add a second level of security

when the user is logging on to a web application or VPN. Instead of a separate token or key fob, the Intel Identity Protection Technology uses the Intel Management Engine to securely generate the six digit code that is used as the one time password.

Intel Identity Protection Technology (Intel IPT) is available on 2nd generation Intel Core vPro Processor-based systems with Intel AMT 7.1 or later and the Intel IPT software stack (provided by the PC manufacturer). Intel IPT works with any website that has been enabled for Intel IPT by a third-party software vendor.

For more information:

Intel IPT website (<http://ipt.intel.com>)

Selected Intel® vPro™ Technology Features

Compliance with Industry Standards

Intel has been an active participant in the Distributed Manageability Task Force (DMTF) for many years. Intel vPro technology supports many of the networking and manageability standards that are in widespread use today.

For more information:

- [Distributed Manageability Task Force \(DMTF\)](#)

Alert Standard Format Support

The capabilities of Intel AMT technology go far beyond what is supported by the Alert Standard Format. However, Intel AMT 5.x and earlier platforms do support an ASF mode. Intel AMT 5.0 supports ASF 2.0. In this mode, an Intel AMT platform can generate and log alerts related to platform events. The events are selected by configuring “filters” on the Intel AMT platform. Event alerts conform to the Alert Standard Format (ASF) Specification DSP0136. Users can choose either Intel AMT or ASF modes in the Management Engine BIOS extension (MEBx). The Intel AMT mode is preferred to the ASF format because only the Intel AMT mode offers the full range of management capabilities included with Intel vPro technology.

For more information:

- [Transition from ASF to Intel AMT](#)

WS-MAN Compliance

The new Intel AMT 6.0 release is compliant with the WS-MAN standard. Intel Intel AMT can be managed using the WS-Management protocol. Starting with Release 3.0, all Intel AMT features have been supported with WS-Management.

For more information, see the following:

- *Intel Active Management Technology Comparison of WS-Management Capabilities Across Releases (Releases 3.0, 3.2, 4.0, 5.0, and 5.1)*, provided in the Intel AMT SDK (see page 35)
- *Intel Active Management Technology WS-Management Flows*, provided in the Intel AMT SDK (see page 35)

DASH Compliance

The Intel AMT 7.0 release supports compliance with the DASH 1.1 standard. (Compliance with the DASH standard is performed at the system level by the OEM.) As the DASH specification has evolved, Intel AMT has moved toward additional support for the emerging standards. Prior to the release of Intel AMT 7.0, Intel AMT 6.0 was

DASH 1.0 compliant and Intel AMT 5.1 was released coincident with the establishment of the DASH 1.0 specification as a standard.

IPv6 Support

IPv6 is the next generation of the Internet Protocol (IP). For background information on IPv6 and links to the underlying specifications, see [More Information](#) at the end of this section.

IPv6 support exists with Intel AMT as of version 6.0. (While Intel AMT supports IPv6, there is still very limited Intel AMT software support for IPv6.)

Requirements:

- IPv6 enabled infrastructure
- Routers and switches
- DHCP
- DNS

When deploying Intel AMT into an IPv6 environment, the network infrastructure setup requires careful consideration. IPv6-enabled systems will have multiple IP addresses. Since the IP address of Intel Management Engine (ME) will differ from the IP address of the host operating system, therefore care needs to be taken when working with DNS. For example, if the IT administrator were to try to connect to a fully-qualified domain name (FQDN) to resolves to the host IP address then there will be no Intel AMT functionality for that FQDN. Similarly there could be DNS resolution issues if the host operating system is using IPv6 and Intel AMT is using IPv4 depending on how the IT console resolves an FQDN (whether it returns to IPv6 or IPv4 address).

For more information:

- [ipv6 home page*](#)

*This URL to an independent third-party website is provided for the convenience of the reader. The link should not be construed as an endorsement or recommendation by Intel.

AES-NI Support

All 2nd generation Intel Core i5 and i7 vPro Processors include hardware support for the Advanced Encryption Standard—New Instructions (AES-NI). AES-NI is a group of processor instructions used to accelerate encryption and decryption using the AES standard. These six new instructions are included in selected Intel Core i5 and i7 vPro processors. (Contact your Intel sales representative for more information on supported processors.)

What is AES?

AES is an encryption standard adopted by the U.S. government and around the world. It is used in disk encryption, TLS web transactions, Voice over IP, and other applications.

For more information:

- [Advanced Encryption Standard \(AES\) Instructions Set](#), Intel Corporation, July 2008.
- *Federal Information Processing Standards Publication 197*, November 26, 2001, [FIPS PUBS 197](#)

How is AES used?

The following is a list of typical applications for the AES standard on a PC:

- Full disk encryption (for example, using Microsoft* BitLocker)
- File storage encryption (for example, using WinZIP*)
- Conditional access of high definition content
- Voice over IP (VoIP)
- Internet security (https protocol)

To use the AES-NI feature, simply choose a processor and software application that supports AES-NI. You do not need to setup or configure this feature. Software applications instrumented for AES-NI will automatically use the new instructions when an AES-NI capable processor is present.

Cisco* Self-Defending Network Architecture (SDN)

Intel Active Management Technology (Intel AMT) Release 2.5 and later releases can generate posture messages that are compatible with the Cisco* Self-Defending Network Architecture (the Cisco* product for Network Admission Control or NAC). In support of this feature, the Intel vPro Software Development Kit includes a NAC Posture Plug-In that, in conjunction with a Cisco Trusted Agent (CTA) running on the host computer, forwards posture information to an Authentication, Authorization, and Admission (AAA) server (an alias of an Admission Control Server, or ACS).

For more information:

- *Intel Active Management Technology Posture Validation Server Sample*, provided in the Intel AMT SDK (see page 35)

Microsoft* Network Access Protection (NAP)

Microsoft* Network Access Protection (NAP) controls network access on a computer by computer basis, granting or denying access based on identity information on each computer and on configured corporate policies. An individual computer's identity information is referred to as its "posture" in Microsoft* NAP.

Microsoft* NAP lets network administrators categorize groups of users and grant or deny network access based on the groups to which a user or computer belongs. They can also grant or deny access based on an individual computer's compliance level with corporate policies. NAP can even repair a given client's non-compliance and then upgrade its network access level once the repairs are complete.

For more information on Microsoft* NAP, follow the link below:

- <http://technet.microsoft.com/en-us/network/bb545879.aspx>

Intel AMT can be incorporated into a NAP environment. This provides two main benefits:

- When the operating system is unavailable (non H0 or S0 states), Intel AMT can authenticate to NAP, thereby gaining access to the network and enabling down the wire OOB access.
- Intel AMT posture can be sent in H0/S0 states as part of authentication, ensuring that only properly provisioned Intel AMT systems are granted access.

For more information:

- *Intel Active Management Technology System Health Validator Sample*, provided in the Intel AMT SDK (see page 31)

Software Tools

Intel vPro technology is supported by a wide variety of tools for the IT professional, software developer, evaluators, and validation engineer. This section lists the tools that are available from Intel Corporation and third-party software vendors that support Intel vPro Technology.

Intel® Anti-Theft Status Utility

This tool is a Windows* command-line utility that provides the capability to check the status of Intel Anti-Theft Technology (Intel AT). Use this tool to determine if the computer's Intel AT status is active or inactive.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® Remote Configuration Certificate Utility

To use remote configuration for provisioning a system, a special remote configuration (RCFG) certificate is needed. Selecting this certificate can be complex. This utility automates and simplifies the selection process.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)
- [Intel AMT Remote Configuration Certificate Selection](#)
- [Intel AMT Remote Configuration Certificate Utility Frequently Asked Questions](#)

Intel® Remote Configuration Scout

This simple command line utility returns the Intel Management Engine firmware version and DHCP option 15 value when run on Intel vPro technology enabled clients. This utility helps complete remote configuration certificate decisions.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® AMT Scan

Pre-activation utility that captures Intel ME information about non-provisioned clients and writes this data back into the Microsoft Windows* registry for use by the management console. This helps in planning activation deployment in your enterprise.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® Client Manageability Add-on for Microsoft* SMS 2003

(This software is listed for completeness and is currently unsupported.)

The plug-in extends Microsoft* SMS to take advantage of the advanced, hardware-based system management capabilities of Intel AMT technology, which are built into PCs with Intel VPro technology. These capabilities help reduce the cost of discovering, managing and securing desktop PCs in the enterprise and thereby improving compliance with corporate policies.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® WS-Management Translator

The Intel WS-Management Translator makes it possible for WS-Management based software to be used in conjunction with Intel AMT platforms older than version 3.0. Using the translator, management software can send WS-Management commands to the translator, the translator will in turn perform the equivalent operation on an Intel AMT device using a proprietary SOAP based protocol understood by all Intel AMT platforms.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® AMT USB Key Provisioning Utility

This tool creates the USB flash drive file in the format needed to perform Intel vPro technology One-touch provisioning.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® AMT SCSDiag Utility

This utility enables debugging of the Setup and Configuration Service and its database. It connects to the Intel SCS database and collects debug and ongoing database data. It assists in helping provide debug and maintenance assistance for the Intel SCS and the Intel SCS database.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® vPro™ Activator Wizard

This tool allows you to generate client-side "Hello" packets that are required for remote configuration. (This tool has been superseded by the Intel AMT Configuration utility that is part of the Intel SCS 7.0 package.)

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)
- *Intel vPro Technology Activator Utility Version 5.1 User's Guide*, (included in the Intel SCS download package, see page 37)

Intel® vPro™ Activator on LiveCD

Intel vPro Activator on LiveCD is a self-contained Linux* environment with Intel vPro activation software, which can fit on a USB key thumb drive. It allows you to activate your Intel vPro clients without configuring a DNS alias for a provisioning server or using the Bare-Metal Configuration option in Intel AMT (which some OEMs turn off).

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® Remote Power Control Utility

This tool allows you to remotely control the power state of an Intel vPro technology system without requiring a separate management console (this is a command-line utility).

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® AMT Unprovision Utility

This tool allows you to undo provisioning (or activation) to an Intel vPro technology system without requiring a separate management console (this is a command-line utility).

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® AMT Reflector

This tool offers a unique implementation that allows an Intel AMT client to access and manage some Intel vPro technology functionality locally via the OS without entering the management engine directly (usually via BIOS).

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® System Defense Utility

This is an easy to use tool for small and medium businesses to take advantage of valuable proactive security and manageability features of Intel vPro processor technology. Combined with systems built on Intel Desktop Boards Executive Series, it enables remote security and manageability functions such as setting security policies, BIOS configuration, remote reboot, asset management, event logging, and more.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)
- Intel Desktop Boards, [Intel System Defense Utility](#)
- [Intel System Defense Utility Product Brief](#)

Intel® IT Director

This is an intuitive, easy-to-use dashboard that delivers Intel vPro technology-based benefits to your small business customers. This tool can help your small business customers manage their network PCs, strengthen security and data protection, and know when to place a call for help before the problem becomes critical.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)
- [Intel IT Director](#)

Microsoft* ConfigMgr Bare-metal Provisioning Script

This download package outlines the necessary security configuration and points you to resources you can use to create a script for automating Microsoft ConfigMgr bare-metal provisioning.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® SCS to ConfigMgr Migration Utility

Migrates client systems—originally configured using Intel SCS and managed by any management console—to be managed by Microsoft* System Center Configuration Manager (SCCM) SP1.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Microsoft* ConfigMgr Log Parser Script

Reading through the wealth of information in Microsoft* ConfigMgr logs can be a challenge, especially if you are provisioning a lot of systems at one time. To help with this, Intel has put together a VBScript example to help make the job of debugging provisioning problems easier. This script parses through the Microsoft* ConfigMgr log file you specify and creates a new log file containing entries relevant to the string you are searching for.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Microsoft* ConfigMgr OOB Settings Update Script

This script automates the process of pushing out-of-band configuration settings to your Intel vPro clients.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Microsoft* ConfigMgr Console VBScript

This script launches the Microsoft* ConfigMgr Management Console.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® Remote Encryption Management Software Development Kit (SDK)

The Remote Encryption Management SDK gives source code (as well as a working sample executable) that can be used to add the ability to remotely unlock an Intel vPro system in a powered off state to an existing hard drive encryption solution. It also provides a Linux* based ISO image that is loaded on the Intel vPro system and contains the functionality used to unlock the system remotely. This ISO is not required; the functionality it contains can be integrated into an existing encryption solution's pre-boot environment. This SDK is intended to be used with the Intel AMT SDK, which contains more detailed documentation on provisioning the Intel vPro systems and the SOL and IDE-R functionality that the Remote Encryption Management SDK makes use of.

The SDK runs in a Microsoft Windows* .NET 2.0 environment and builds on top of WinRM in the default WS-Man mode, and requires Microsoft* Visual Studio 2008. In legacy mode (also known as EOI), WinRM is not required, and for a deployed solution WinRM would not necessarily be required (the Intel AMT SDK provides examples using the OpenWSMan library). The ISO image that is transferred to the Intel vPro system is built using Linux*, and the source code for this image is included in the SDK.

For more information, or to download the SDK:

- [Remote Encryption Management Software Development Kit \(SDK\)](#)

Intel® vPro™ Packet Decoder

This tool sniffs and decodes non-TLS Intel AMT SOAP packets for software developers and testing purposes. This tool only supports the Basic Intel AMT provisioning mode.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® Manageability Developer's Toolkit (DTK)

This toolkit enables testers, developers, and designers to better understand the benefits of Intel vPro technology and assist in the testing of Intel vPro technology applications.

The Manageability Developer Tool Kit is a free set of tools for designers, developers and testers that are building and testing Intel Active Management Technology (Intel AMT) applications. To help developers build applications that make use of Intel AMT, Intel also provides a Software Development Kit (SDK) with source code and basic building blocks (see: page 32). The DTK is designed to complement the Intel AMT SDK by adding solid and easy-to-use reference and test tools.

The Manageability Developer's Toolkit includes the following tools:

- [Manageability Commander Tool](#)
- [Manageability Outpost Tool](#)
- [Manageability Outpost Service Control Panel Tool](#)
- Manageability Connector Tool

The following tools have reached the End of Life (EOL) stage, but can still be downloaded.

- Manageability Automation Tool (EOL)
- [Manageability Flash Drive Tool](#) (EOL)
- [Manageability Monitor Tool](#) (EOL)
- Manageability Resource Translator Tool (EOL)
- [Manageability Network Defense Tool](#) (EOL)
- [Manageability Directory Tool](#) (EOL)
- [Manageability Net Status Tool](#) (EOL)
- [Manageability Net Traffic Tool](#) (EOL)
- [Manageability Network Connection Reflection Tool](#) (EOL)

For more information, or to download the free DTK:

- [Tools and Utilities for Intel vPro Technology](#)
- [Download the latest version of Manageability Developer Tool Kit](#)

Manageability Network Connection Reflection Tool

Allows for limited management console functionality from the local Intel AMT client by running a "reflector" program on a second computer that redirects packets sent from the client's OS level application back to the client's Intel AMT sub-system.

For more information, or to download the free tool:

- [Download the latest version of Manageability Developer Tool Kit](#)

Manageability Monitor Tool

This tool is used to monitor the Intel AMT client's power state.

For more information, or to download the free tool:

- [Download the latest version of Manageability Developer Tool Kit](#)

Manageability Network Connection Reflection Tool

Allows for limited management console functionality from the local Intel AMT client by running a "reflector" program on a second computer that redirects packets sent from the client's OS level application back to the client's Intel AMT sub-system.

For more information, or to download the free tool:

- [Download the latest version of Manageability Developer Tool Kit](#)

Manageability Flash Drive Tool

This utility allows for reading and formatting flash thumb drives used in remote configuration (see the description for the Manageability Director Tool).

For more information, or to download the free tool:

- [Download the latest version of Manageability Developer Tool Kit](#)

Manageability Terminal Tool

Sample terminal emulator that is used to interact with the remote client's SOL.

For more information, or to download the free tool:

- [Download the latest version of Manageability Developer Tool Kit](#)

Manageability Net Traffic Tool

A graphical tool that allows the user to send various network packets to the Intel AMT client. This tool is useful when setting up filters in Manageability Commander and Manageability Defense Tools as well as flooding a network for testing purposes, if needed.

For more information, or to download the free tool:

- [Download the latest version of Manageability Developer Tool Kit](#)

Manageability Net Status Tool

A graphical tool that simply pings an IP address and displays the connection is active. Shows ping response to a high level of granularity (much finer than the ping in a Windows command window). This tool is useful when setting up filters in Manageability Commander and Manageability Defense Tools.

For more information, or to download the free tool:

- [Download the latest version of Manageability Developer Tool Kit](#)

Manageability Network Defense Tool

A simplified management console utility that takes advantage of only the network defense features available with Intel AMT. This tool has a slightly different user interface than the Manageability Commander Tool and some nice graphical indicators for events.

For more information, or to download the free tool:

- [Download the latest version of Manageability Developer Tool Kit](#)

Manageability Director Tool

Sample remote Intel AMT provisioning utility that provides access to setup of One-Touch (OTC) and remote configuration models for provisioning Intel AMT client computers. This utility allows users to configure security certificates used in provisioning and management as well as setting profiles for clients.

For more information, or to download the free tool:

- [Download the latest version of Manageability Developer Tool Kit](#)

Manageability Outpost Service Control Panel Tool

This tool is a Windows* service allowing for unattended system access—the real-world way such an agent would need to work. Like the Manageability Outpost Tool is described in the next section, the Manageability Outpost Service Control Panel Tool is a sample client agent that provides a local link from the client's Intel AMT firmware to the same client's operating system..

For more information, or to download the free tool:

- [Download the latest version of Manageability Developer Tool Kit](#)

Manageability Outpost Tool

This is a sample client agent that provides local link from a client's Intel AMT firmware to the same client's operating system. This "remote agent" allows the management console to perform operating system level functions through the Serial-over-LAN (SOL) link in Intel AMT—even when the windows network driver is disabled allowing for file and system repair, remote diagnostics via process and device manager views, watchdogs, and many more. This tool is a Windows executable allowing for real-time interaction with the agent – this tool is great for testing.

For more information, or to download the free tool:

- [Download the latest version of Manageability Developer Tool Kit](#)

Manageability Commander Tool

Sample management console that enables users to interact with all Intel AMT functionality including remote connection, power control, agent presence management, watchdogs, Serial-over-LAN (SOL), Remote boot with IDE-Redirect (IDE-R), hardware inventory, access to the 3rd-party-data-store and many more functions. Some functions require an Intel AMT client agent to be installed on the client under management. The Manageability Outpost Tool agent is included in both Windows* executable and Windows* service formats. The Manageability Director Tool is used to help remotely provision Intel AMT clients prior to using a management console.

For more information, or to download the free tool:

- [Download the latest version of Manageability Developer Tool Kit](#)

Intel® AMT Software Development Toolkit (SDK)

Provides the low-level programming capabilities to enable developers to build manageability applications that take full advantage of Intel Active Management Technology built into Intel vPro technology computers.

The Intel AMT SDK includes the following tools for developers:

- MPS.exe—Intel vPro enabled gateway reference design (formerly known as the Management Presence Server or MPS). This sample application demonstrates how to use the MPS service. (Note: third-party software vendors now have fully supported enterprise quality software applications that perform this service.)
- MPSNotification.exe—This samples demonstrates how to receive notifications from MPS when an Intel Active Management Technology machine connects or disconnects.
- APITestRemote.bat—This test runs a series of executables that accesses an Intel AMT machine from a remote host, thus testing the Intel AMT functionality of the remote machine. APITestRemote.bat tests the SOAP functionality of Intel AMT as well as the storage functionality.
- Discovery.exe—This application demonstrates how to discover Intel AMT devices in a network, and how to obtains information about them. It will scan a network for each IP address and then try to determine if there is an Intel AMT device and the firmware version of the device.
- NameResolve.exe—This sample demonstrates how to retrieve an Intel AMT device's name using its IP address.
- AMTRedirection.exe—This sample demonstrates how to use the Intel AMT Redirection commands along with remote boot options.
- IMRGUI.exe—This sample demonstrates how to use the Intel AMT Redirection library (IMRSDK).

For more information, or to download the Intel AMT SDK:

- [Intel Active Management Technology Software Development Kit](#)

Intel® AMT Embedded Tools Suite

Intel AMT Embedded Tools Suite is a set of tools to help board vendors and end customers to design, verify, and deploy the Intel AMT embedded systems, as well as to demonstrate the Intel AMT usage models for embedded applications.

- Intel AMT Firmware Integration Wizard—A GUI-based wizard with step-by-step guidance on how to build and program the appropriate Intel AMT firmware version for your platform. ([video demo](#))
- Firmware Status Debugger—A debugging tool for converting the hex characters to readable text. ([video demo](#))
- Intel AMT Management Express Console—This console was developed based on the Manageability Developer Tool Kit (DTK), but with a simplified user interface and limited functionality that caters to the embedded customer needs. This is an ideal tool for a quick demo setup. ([video demo](#))

For more information, or to download the tools:

- [Intel AMT Embedded Tools Suite](#)
- [Remote Management for Digital Signage usage model](#)
- [Intel AMT for Embedded Systems](#)

Intel® Power Manager (Plug-in for SpiceWorks)

The Intel Power Manager Extension can be used to track overall power-savings due to turning a group of machines on/off per a set schedule. This extension will load a widget on your SpiceWorks* dashboard.

For more information, or to download the free SpiceWorks* management console and Power Manager Plug-in (sponsored by Intel), go to the following links:

- [SpiceWorks* home page](#)

(SpiceWorks* is an independent, third-party software provider. The URL link is provided as a convenience to the reader and should not be construed as an endorsement or recommendation for the web site or software product.)

Intel® Management and Security Status Tool

The Intel Management and Security Status icon indicates whether Intel AMT, Intel TPM and Intel AT are running on the platform.

The Intel Management and Security Status application displays information about a platform's Intel AMT, Intel Trusted Platform Module (Intel AMT 4.0 and 5.0 platforms only), and Intel Anti-Theft Technology (Intel AT) services.

The icon is located in the notification area. By default, the notification icon is displayed every time Windows* starts.

**NOTES**

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

Intel® Setup and Configuration Setup Wizard

This tool simplifies the installation of the Intel Setup and Configuration Service (Intel SCS)—a reference solution for remote configuration.

For more information, or to download the free tool:

- [Tools and Utilities for Intel vPro Technology](#)

Intel® Setup and Configuration Server (Intel SCS)

Intel vPro technology Setup and Configuration Service (Intel SCS) allows for most aspects of setup and configuration to be completed through a remote management console. Note that some third-party manageability software providers have included the Intel SCS software into their products.

For more information, refer to:

- [Download the latest version of Intel AMT Setup and Configuration Service - SCS](#)
- *Intel Setup and Configuration Service, Console User Guide, v5.2*, (included with the Intel SCS download package)
- *Intel Active Management Technology Developers Guide to the Sample Setup and Configuration Application* (included in the Intel AMT SDK)

Third-party Software Vendors

Software products optimized for Intel vPro, Intel Virtualization, and Intel Active Management Technology deliver solutions that solve the most costly IT problems and enable new levels of efficiency for IT managers.

Software applications that can use the features of Intel vPro technology are currently provided by many vendors around the world. The following list will help you identify potential vendors. If the vendor specializes in a certain geographic region, that region is noted after the name. The name of the software product is also noted in some cases if the vendors name or size may be difficult to search for on the web.

**NOTE**

Products, solutions, or services may not be available in all geographical regions. Consult the vendor for details.

- 30Wish* (China region)
- Absolute* Software
- Agree* (China region)
- Airties Wireless Communications*

- Anlou*
- Artin Dynamics* (India region)
- Avocent* (Taiwan region)
- Big Fix* (an IBM company)
- Bit Defender*
- BMC*
- Brainware* (Japan, EMEA region—Europe, Middle East, Africa)
- CA*
- Citrix*
- Computer Associates*
- Comvigo* (US region)
- Check Point*
- Citrix*
- Credant*
- CORE* (Japan region)
- Crypto++*
- Dell Computers*
- Doctor Soft* (Korea region)
- DragonFlow Networks* (China region)
- Farstone* (China region)
- FAMATECH*
- Forquest* (Taiwan region)
- Fractilia* (EMEA region--Europe, Middle East, Africa)
- Fujitsu* (Japan region)
- GeneralSoft* (China region)
- Green Hills*
- HCL* (India and SE Asia region)
- Hewlett-Packard*
- Hitachi* (Japan region)
- Hitachi Business* (Japan region)
- HSBSOFT Technologies* (India region)
- Intel (SCS and development tools)
- JAL Infotec* (Japan region)
- Kaspersky* (Europe region)
- Kaseya*
- KingStar Winning (China region)
- LANDesk*

- Lenovo*
- Level Platforms*
- LightStar* (Taiwan region)
- LogMeIn*
- Manage Operations* (US region)
- Maxigent* (Korea region)
- McAfee* (now a subsidiary of Intel Corp.)
- MediaLand* (Korea region)
- Microsoft*
- Motex* (Japan region)
- MTM Software* (US region)
- N-able* Technologies
- N-Central*
- NEC Fielding* (Japan region)
- NetSupport*
- NSS*
- OneBe* (Japan region)
- Parallels*
- PGP* (now Symantec PGP)
- Phoenix Technologies*
- Quality* (Japan region)
- Rsupport* (Korea region)
- Samsung Elec* (Korea region)
- Samsung SDS (Korea region)
- Secuware* (EMEA region—Europe, Middle East, Africa)
- SOE Software (Australia region)
- SoftLumos* (China region)
- SoftTex*
- SpiceWorks*
- StarSoftComm* (China region)
- SyAM* (North America, Europe)
- Symantec*
- Syscom* (Taiwan region)
- Tectona Softsolutions* (India region)
- Tidaldata Solutions* PVT Ltd.
- Triactive (Europe region)
- TruCrypt*

- Verdiem* (US, Canada, Europe region)
- VMWare*
- VRV* (China region)
- Wave*
- Wipro* (India and SE Asia region)
- WinMagic* (North America, Europe, Japan)
- WinZip* (a Corel Company)
- Yes Information* (Taiwan region)
- Yuguang* (China region)
- Zenith* (India and SE Asia region)

For more information:

- [Software Solutions using Intel vPro Technology](#)
- [Intel Business Exchange—Manageability Home Page](#)
- [Intel vPro Technology Alliance](#)

Appendix A: Intel® vPro™ Brand Ingredients

What ingredients are required for the latest Intel vPro technology branded platforms?

2nd Generation Intel Core vPro Processor-based systems:

- 2nd generation Intel Core i5 or i7 vPro Processor
- Intel Q67, QS67, or QM67 chipset
- TPM 1.2 (this requirement may be waived to comply with export restrictions)
- Intel VT capable BIOS
- Intel TXT capable BIOS
- TPM 1.2 capable BIOS
- Intel AMT capable BIOS
- Intel ME firmware 7.0 with Intel AMT 7.0 and Intel AT 3.0 (mobile only)
- Intel 82579LM GbE LAN, Intel Centrino® Advanced-N+WiMAX 6250, or Intel Centrino Ultimate-N/Advanced-N 6000 Series
- Intel Management and Security Status Icon (optional but recommended)

Note: Earlier generations of Intel vPro branded platforms have different platform ingredients. Consult your Intel sales representative for the platform ingredients in earlier generations of Intel vPro technology.

For more information on brand requirements, see:

<http://www3.intel.com/cd/pvp/bvt/asm-na/eng/index.htm?&>

Appendix B: Feature Support Matrix (by Release)

This Appendix shows which features are supported by each Intel AMT release.

Feature	Intel® vPro™ Technology with Intel AMT Version				
	3.x	4.x	5.x	6.x	7.x
DASH 1.0 [1]	X	X	X	X	X
DASH 1.1 [1]					X [1]
Boot Control	X	X	X	X	X
Power State Management	X	X	X	X	X
Hardware Inventory	X	X	X	X	X
Software Inventory	X	X	X	X	X
Hardware Alerting	X	X	X	X	X
Agent Presence	X	X	X	X	X
Serial Over LAN	X	X	X	X	X
IDE Redirection	X	X	X	X	X
Non Volatile Memory (third-party data store)	X	X	X	X	X
Remote Configuration	X	X	X	X	X
TLS-PSK Setup and Configuration	X	X	X	X	X [2]
TLS-PKI Setup and Configuration	X	X	X	X	X
System Defense Filters	X	X	X	X	X
Access Monitor		X	X	X	X
Wireless Management in Sleep States		X		X	X
Microsoft* NAP		X	X	X	X

Feature	Intel® vPro™ Technology with Intel AMT Version				
	3.x	4.x	5.x	6.x	7.x
Fast Call for Help		X	X	X	X
Remote Scheduled Maintenance, Remote Alerts		X	X	X	X
Measured Intel AMT			X	X	X
KVM Remote Control				X	X
PC Alarm Clock				X	X
Intel SCS	X	X	X	X	X
Intel Management Security and Status Icon	X	X	X	X	X
Intel TXT	X	X	X	X	X
Intel VT	X	X	X	X	X
Cisco* SDN	X [3]	X	X	X	X
Intel TPM		X	X		
WS-MAN	X	X	X	X	X
Intel Anti-Theft Technology		X [4]		X	X
Host Based Configuration					X
Automatic Synchronization of Intel ME and host OS static IP addresses					X
Desktop wireless manageability					X [5]
Intel Identity Protection Technology					X [6]
Intel ME firmware roll-back					X
Intel Anti-Theft Technology		X [7]		X [8]	X [8]

1. DASH compliance measured at the OEM system level. OEM platforms based on Intel vPro Technology, Intel Core vPro processors and Intel Standard Manageability with AMT 6.2 or later firmware are capable of DASH 1.0 compliance. As with 1.0, Intel AMT has been developed to conform with the DASH 1.1 specification. Ultimately, compliance for any platform will be verified once the DMTF launches the DASH 1.1 Compliance Test Suite.
2. This feature is deprecated in Intel AMT 7.0 and may not be present in future versions.
3. Cisco* posture support for SDN (NAC) is not supported in v3.1 and later.
4. Version 4.1 and later
5. WiFi is supported but not required on desktop systems. Supported with Intel Centrino Ultimate-N/Advanced-N 6000 Series network adapters.
6. Version 7.1 and later
7. Mobile PCs only; Intel AT PC protection only
8. Mobile PCs only; Intel AT PC and data protection

Glossary

For the latest version of this glossary, see: [Intel vPro Glossary](#).

Activation	The process to configure Intel vPro firmware (specifically Intel AMT), network infrastructure, and third- party system management software to work together in order to allow the management software to fully utilize Intel vPro technology's system management capabilities.
Agent Presence	Monitors agent heartbeats and alerts if agent does not respond.
BIOS	Basic Input Output System
DASH	Desktop and mobile Architecture for Systems Hardware (a Distributed Management Task Force, Inc. standard)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
Enterprise Mode	(Intel AMT 5.x or earlier) Setup and configuration model used for larger organizations
Host Based Configuration	(Intel AMT 7.0 and later) Setup and configuration model that uses a utility (the Intel ACU) on the client to provision the system with the user's consent.
IDE-R	IDE Redirection; sends the IDE input and output of the client with Intel vPro technology to/from the management console machine, allowing the user to remotely interact with the client during pre-boot phase.
Intel AMT	A technology that includes hardware-based remote management features, as well as security, power-management and remote-configuration features. These features allow an IT technician to access a PC with Intel AMT when traditional techniques and methods to manage the PC are not available.
Intel ME	Intel Management Engine; firmware that provides management features for clients with Intel vPro technology.
Intel MEBX	Intel Management Engine BIOS Extension; a

	user interface for configuring the Intel Management Engine.
Intel Remote PC Assist	Allows OEMs, managed service providers (MSP) and IT Outsourcers to connect with end user systems over the public internet and remotely manage enabled systems regardless of system state.
Intel vPro Processor Technology	Intel processor technology that provides a higher level of security and management to desktop computers.
LMS	Local Management Service driver. Provides an interface enabling local management software agents to communicate with the Intel Management Engine using the same high-level protocols as those used for remote management (e.g. XML, SOAP).
MTLS	Mutual TLS (Transport Layer Security). Both the server and the client are authenticated in this variation of the TLS security encryption scheme. Normally in TLS, only the server is authenticated. Requires client-side certificate in addition to the server-side certificate. <i>See also:</i> TLS
Network Filters	System defense filters; monitor incoming and outgoing IP packets for suspicious behavior.
OEM	Original Equipment Manufacturer. Notation used to designate the PC manufacturer.
OOB	Out Of Band. Refers to system management actions performed when the managed system's operating system (OS) is not running or when the system is powered down.
PID	Provisioning ID. First portion of security key used in setup and configuration of clients with Intel vPro technology.
PKI	Public Key Infrastructure
PKI CH	Public Key Infrastructure – Certification Hash
Platform Inventory	Identifies each machine using a unique UUID
PPS	Provisioning Pass phrase. Pre-shared key used in the setup and configuration of clients with Intel vPro technology.
Provisioning	Installing and/or configuring the requisite firmware, software, and authentication components on a managed client to make it ready to be managed. Do not use. Preferred

PSK	term is now <i>Setup and Configuration</i> .
Remote Configuration	Pre-shared key Configures Intel vPro clients with SSL certificates without having to touch the client system (assuming the client has been set up by the OEM for remote configuration).
Remote Diagnostics and Repair	Use Serial Over LAN (SOL) and IDE Redirection (IDER) to remotely reboot and debug a client with Intel vPro technology.
Remote Power Control	Securely and remotely power on and power off a client with Intel vPro technology.
SMB Mode	(Intel AMT 5.x and earlier) Small and Medium Business model used for setting up and configuring a client with Intel vPro technology.
Software Inventory	Inventory of all software installed on a client with Intel vPro technology.
SOL	Serial Over LAN
Setup and Configuration	Installing and/or configuring the requisite firmware, software, and authentication components on a managed client to make it ready to be managed. This term replaces <i>provisioning</i> in documentation related to Intel vPro technology.
TLS	Transport Layer Security. An encryption and authentication scheme in which the server presents a server-side certificate for authentication by the client. <i>See also:</i> MTLS (Mutual TLS)
USB Based One Touch Setup and Configuration	A setup and configuration process in which the administrator only needs to perform actions on each client system one time (i.e., “touch” each client system only once) using a USB flash drive. <i>See also:</i> Setup and Configuration
Zero-Touch Setup and Configuration	A setup and configuration process in which the administrator does not need to perform any installation or configuration actions directly at the client system (i.e., all setup and configuration actions are performed remotely from the management console). This method is also known as Remote Configuration. <i>See also:</i> Setup and Configuration

Index

- 802.1x networks, end point access control, 10
- Access Monitor, 16
- Activator tool on LiveCD, 29
- Activator Wizard tool, 28
- Advanced Encryption Standard—New Instructions. *See* AES-NI
- AES-NI support, 24
- agent presence use case, 8
- Alert Standard Format (ASF), 23
- AMTRedirection.exe, 35
- APITestRemote.bat, 35
- assets, hardware platform auditing, 4
- Auditor role, for access monitor log, 16
- certificates, Intel Remote Configuration Certificate Utility for, 27
- Cisco Trusted Agent (CTA), support for, 25
- Cisco* SDN (Network Admission Control), 25
- DASH standard, compliance to, 23
- diagnosis and repair, remote, 5
- diagnosis, remote with local repair, 6
- Discovery.exe, 35
- disk encryption management use case, 19
- Distributed Manageability Task Force (DMTF), compliance with, 23
- DTK, Intel Manageability Developer's Toolkit, 32
- Embedded Tools Suite, Intel AMT, 36
- encryption management, use case for remote, 19
- end point access control (EAC), 9
- Fast Call for Help, 12
- Firmware Status Debugger, 36
- full disk encryption, AES-NI support for, 25
- hardware inventory, 5
- Host Based Configuration, 20
- IMRGUI.exe, 35
- IMSS. *See* Intel Management and Security Status Tool
- Intel AMT Embedded Tools Suite, 36
- Intel AMT Firmware Integration Wizard (for embedded applications), 36
- Intel AMT Management Express Console, 36
- Intel AMT Reflector, 29
- Intel AMT Scan utility, 27
- Intel AMT SCSDiag Utility, 28
- Intel AMT Software Development Toolkit, 35
- Intel AMT Unprovision Utility, 29
- Intel AMT USB Key Provisioning Utility, 28
- Intel Anti-Theft Status Utility, 27
- Intel Anti-Theft Technology, 13
- Intel Client Manageability Add-on for Microsoft* SMS 2003, 28
- Intel IT Director, 30
- Intel Manageability Developer's Toolkit (DTK), 32
- Intel Management and Security Status Tool, 36
- Intel Power Manager (plug-in), 36
- Intel processor graphics, use with KVM remote control, 18
- Intel Remote Configuration Certificate Utility, 27
- Intel Remote Configuration Scout, 27
- Intel Remote Encryption Management Software Development Kit (SDK), 31
- Intel Remote Power Control Utility, 29
- Intel SCS
 - Intel AMT SCSDiag Utility, 28

- Intel SCS to ConfigMgr Migration Utility, 30
- Intel Setup and Configuration Server, 37
- Intel Setup and Configuration Setup Wizard, 37
- Intel System Defense Utility, 29
- Intel vPro Activator on LiveCD, 29
- Intel vPro Activator Wizard, 28
- Intel vPro Enabled Gateway, 12
- Intel vPro enabled gateway, reference design for, 35
- Intel vPro Packet Decoder, 31
- Intel WS-Management Translator, 28
- Intel® Identity Protection Technology, 21
- Intel® vPro™ technology, 2
- inventory, hardware, 5
- inventory, software, 4
- IPv6, support for, 24
- KVM Remote Control use case, 18
- KVM Remote Control, requirements for processor graphics, 18
- Manageability Commander Tool, 35
- Manageability Director Tool, 34
- Manageability Flash Drive tool, 33
- Manageability Monitor tool, 33
- Manageability Net Status tool, 33
- Manageability Net Traffic tool, 33
- Manageability Network Connection Reflection tool, 32, 33
- Manageability Network Defense tool, 34
- Manageability Outpost Service Control Panel Tool, 34
- Manageability Outpost Tool, 34
- Manageability Terminal tool, 33
- Microsoft* ConfigMgr
 - bare-metal provisioning script, 30
 - console launching VBScript, 31
 - Intel SCS Migration Utility, 30
 - Log Parser Script, 30
 - OOB Settings Update Script, 31
- Microsoft* ConfigMgr Bare-metal Provisioning Script, 30
- Microsoft* ConfigMgr Console VBScript, 31
- Microsoft* ConfigMgr Log Parser Script, 30
- Microsoft* ConfigMgr OOB Settings Update Script, 31
- Microsoft* Network Access Protection, support for, 25
- Microsoft* SMS 2003, Intel Client Manageability Add-on for, 28
- MPS (now called the Intel vPro Enabled Gateway), 12
- MPS.exe, 35
- MPSNotification.exe, 35
- NAC. *See* Cisco* SDN
- NameResolve.exe, 35
- NAP. *See* Microsoft* Network Access Protection
- network filters for system defense use case, 7
- network packet decoder, utility for Intel vPro, 31
- network tools
 - Manageability Net Status tool, 33
 - Manageability Net Traffic, 33
 - Manageability Network Connection Reflection, 32
 - Manageability Network Connection Reflection tool, 33
 - Manageability Network Defense tool, 34
- New features, 1
- one-touch configuration use case, 10
- packet decoder, utility for Intel vPro, 31
- PC Alarm Clock, 17
- platform auditing, 4
- Power Control Utility, remote, 29
- power control, remote, 17
- power state, monitoring tool, 33
- remote configuration, 11
- Remote Configuration Scout utility, 27
- remote diagnosis and local repair, 6
- remote diagnosis and repair, 5
- remote encryption management use case, 19

- remote power control, 17
- Remote Power Control Utility, 29
- SCS. *See* Intel Setup and Configuration Server
- SDK. *See* Intel AMT Software Development Toolkit
- setup and configuration
 - bare metal (remote configuration), 11
 - delayed (remote) configuration, 11
 - one-touch configuration, 10
 - remote configuration, 11
 - zero-touch (remote configuration), 11
- SOAP packet decoder, utility for, 31
- software inventory, 4
- software updates, use case for unattended, 20
- software version compliance, 7
- SpiceWorks, Intel Power Manager plug-in, 36
- system defense use case, 7
- Third-party Software Vendors, 37
- tools and utilities
 - AMTRedirection.exe, 35
 - APITestRemote.bat, 35
 - Discovery.exe, 35
 - Firmware Status Debugger for embedded applications, 36
 - IMRGUI.exe (redirection library demonstration tool), 35
 - Intel AMT Embedded Tools Suite, 36
 - Intel AMT Firmware Integration Wizard for embedded applications, 36
 - Intel AMT Management Express Console for embedded applications, 36
 - Intel AMT Reflector, 29
 - Intel AMT Scan, 27
 - Intel AMT SCSDiag Utility, 28
 - Intel AMT Unprovision Utility, 29
 - Intel AMT USB Key Provisioning Utility, 28
 - Intel Anti-Theft Status, 27
 - Intel Client Manageability Add-on for Microsoft* SMS 2003, 28
 - Intel IT Director, 30
 - Intel Manageability Developer's Toolkit (DTK), 32
 - Intel Management and Security Status Tool, 36
 - Intel Power Manager (plug-in), 36
 - Intel Remote Configuration Certificate Utility, 27
 - Intel Remote Configuration Scout, 27
 - Intel Remote Encryption Management Software Development Kit (SDK), 31
 - Intel Remote Power Control Utility, 29
 - Intel Setup and Configuration Server, 37
 - Intel Setup and Configuration Setup Wizard, 37
 - Intel System Defense, 29
 - Intel vPro Activator on LiveCD, 29
 - Intel vPro Activator Wizard, 28
 - Intel vPro Packet Decoder utility, 31
 - Intel WS-Management Translator, 28
 - Manageability Commander, 35
 - Manageability Director, 34
 - Manageability Flash Drive, 33
 - Manageability Monitor, 33
 - Manageability Net Status, 33
 - Manageability Net Traffic, 33
 - Manageability Network
 - Connection Reflection, 33
 - Manageability Network
 - Connection Reflection tool, 32
 - Manageability Network Defense, 34
 - Manageability Outpost, 34
 - Manageability Outpost Service Control Panel, 34
 - Manageability Terminal, 33
 - Microsoft* ConfigMgr Bare-metal Provisioning Script, 30

- Microsoft* ConfigMgr Console VBScript, 31
- Microsoft* ConfigMgr Log Parser Script, 30
- Microsoft* ConfigMgr OOB Settings Update Script, 31
- MPS.exe, 35
- MPSNotification.exe, 35
- NameResolve.exe, 35
- unattended software updates use case, 20
- Unprovisioning, Intel AMT Utility for, 29
- USB Key Provisioning Utility, Intel AMT, 28
- USB, Manageability Flash Drive tool, 33
- use case
 - access monitor, 16
 - agent presence, 8
 - end point access control, 9
 - Fast Call for Help, 12
 - hardware inventory, 5
 - Host Based Configuration, 20
 - Intel Anti-Theft Technology, 13
 - Intel® Identity Protection Technology, 21
 - KVM Remote Control, 18
 - one-touch configuration, 10
 - PC Alarm Clock, 17
 - platform auditing, 4
 - remote configuration, 11
 - remote diagnosis and local repair, 6
 - remote diagnosis and repair, 5
 - remote encryption management, 19
 - remote power control, 17
 - software inventory, 4
 - software version compliance, 7
 - system defense, 7
 - unattended software updates, 20
- version compliance, use case for software, 7
- virus attach, protecting from, 7
- virus scan agents, detecting presence, 8
- whole disk encryption, remote unlocking of, 19
- WS-MAN, compliance to, 23
- WS-Management Translator Tool, 28