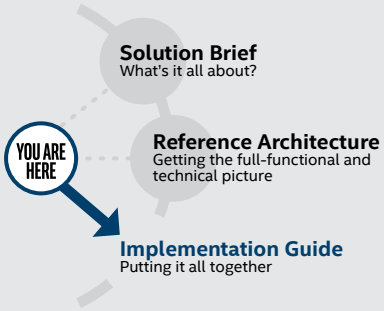
IMPLEMENTATION GUIDE

Business Client
Client Security & Manageability

Achieve easier device management at scale in the smart world

Discover how you can improve the security and manageability of your estate of devices, by enabling remote access and management with Intel® vPro™ technology



What You'll Find in This Implementation Guide

This solution provides a starting point for using Intel AMT to manage a diverse estate of devices.

If you are responsible for:

- **Investment decisions and business strategy... You'll learn how Intel AMT can improve your security and software upgrade processes, making them more cost effective.**
- **Figuring out how to implement Intel AMT... You'll learn about how Intel AMT devices can be enabled and managed using a number of different management consoles and solutions.**

Introduction

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

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

It can be used, for example, to:

- Provide remote access to a device to reduce maintenance and support costs and avoid desk-side visits;
- Improve system deployment, rebuild and upgrade processes;
- Keep devices updated with the latest patches and avoid working hours reboots, even for remote employees; and
- Provide a secure and effective decommissioning process for lost or retired devices, including a remote secure erase.

Contents

Introduction 1
Contents 2
Solution Overview 2
Solution and System Requirements ... 3
Client software components 3
System requirements for Intel SCS ... 3
System requirements for McAfee ePO 4
Solution and System Setup and Configuration 4
Deploying the configuration/ maintenance commands 5
Using database or non-database mode 5
Operation and Utilization of the Intel Solutions 5
Good: Using Client Control Mode (CCM). 6
Better: Using Intel Setup and Configuration Software to enable Admin Control Mode (ACM) 7
Best: Using McAfee ePO Deep Command in Admin Control Mode (ACM) 8
Alternative management solutions .. 8
Use Cases 9
Security use cases 9
Remotely resolve hardware encryption issues 9
Location aware encrypted drive unlock 10
Secure hardware platform with Intel® Enterprise Digital Fence .. 10
Remote Secure Erase 11
Control, initiate and monitor Microsoft Windows 10 deployments 11
Validation 14
Known Issues 14
Summary 15
References 16

Solution Overview

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

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

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

- **On-device:** the Intel AMT technology, drivers and software. The software includes The Intel® Management Engine (Intel® ME) firmware; the Intel® Management Engine BIOS Extension (Intel® MEBX); the Intel® Management Engine Interface (Intel® MEI) driver, which is the operating software interface to the Intel AMT device; the Intel® Local Manageability Service (LMS.exe), which provides OS-related Intel ME functionality; and the Intel Management and Security Status (IMSS), which provides status information to the local user about Intel AMT including messages and an indication that Intel AMT is configured.
- **Activation solutions:** To enable Intel AMT, you can use Intel® Setup and Configuration Software (Intel® SCS) tools and utilities, McAfee ePO Deep Command for remote configuration, or boot from a USB key on the device.
- **Management solutions:** After activation, you can manage your estate of Intel AMT enabled devices with McAfee ePO Deep Command, or use use Intel SCS to integrate with third-party solutions including Microsoft System Center Configuration Manager*, Microsoft PowerShell*, VNC Viewer Plus*.

Three ways to use Intel AMT

This document outlines three main approaches to using Intel AMT, described as good, better and the best solutions. They are:

- **Good:** Using Client Control Mode (CCM). There are a number of restrictions in CCM, in particular the need for user consent for a redirection operation or change to the boot process.
- **Better:** Using Intel Setup and Configuration Software to enable Admin Control Mode (ACM). ACM provides access to all the supported Intel AMT capabilities.
- **Best:** Using McAfee ePO Deep Command. This solution enables easier activation of devices, and offers rich management capabilities.

Once Intel AMT has been configured (and where necessary integrated) using Intel SCS tools and utilities, it is possible to use Intel AMT with alternative solutions, including the Intel AMT SDK and Mesh Commander, which are also covered briefly here, and third-party solutions from companies including Microsoft and VNC.

Solution and System Requirements

We assume that your organization has an existing estate of Intel® Core™ vPro™ processor-based devices, which may span several generations of Intel AMT. Before you begin, you don't need to know how many Intel vPro devices you have, or where they are. Intel SCS can be used to discover the devices prior to activation of the Intel AMT capabilities.

Client software components

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

- The Management Engine Interface (MEI) driver provides the software interface to the Intel AMT device and is installed as a system device.
- The Intel Local Manageability Service (LMS.exe) is a Windows service installed on an Intel AMT system that has Intel AMT Release 9.0 or greater. LMS enables local applications to send requests and receive responses to and from the Intel Management Engine, via the Intel MEI. LMS is required for host-based provisioning (CCM) but not for remote provisioning (ACM).
- The Intel Management and Security Status (IMSS) provides status information to the local user about Intel AMT including messages and an indication that Intel AMT is configured.
- A Serial-Over-LAN (SOL) device installed as a COM port.

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

System requirements for Intel SCS

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

Component	CPU Cores	RAM (GB)	Hard Drive (GB)
RCS	8 logical processors (Two Intel® Xeon® E5345 processors)	16	136
AD Domain Controller	4 logical processors (Four Intel® Xeon® E5420 processors)	4	30
Certification Authority	2 logical processors (Two Intel® Xeon® E5420 processors)	1	30
SQL Server	2 logical processors (Two Intel® Xeon® E5420 processors)	4	66

Table 1: Recommended hardware requirements for Intel SCS.

System requirements for McAfee ePO

One McAfee ePO server has no technical limit on how many nodes it can manage. Many McAfee ePO servers manage 200,000 or more nodes and the fewer McAfee ePO servers you have, the easier it is to maintain your environment.

You must use a 64-bit operating system for the McAfee ePO server. You can use either 32-bit or 64-bit operating systems for the SQL database server, which stores all the data about your network managed systems.

The McAfee ePO server performance is determined by the SQL database. The three items that affect SQL performance are CPU, RAM, and disk performance. McAfee recommends that you exceed the minimum recommendations wherever possible.

Table 2 lists the hardware recommend for various sized organizations. The rule of thumb is to add 16GB of RAM for every 25,000 nodes.

Up to 10,000 nodes you can use a single server for the McAfee ePO instance and the SQL server. Beyond that, McAfee recommends that you host the McAfee ePO server and the SQL servers on their own physical servers.

Full information, including more details on how to best host the solution, can be found in the McAfee ePolicy Orchestrator 5.1.0 Software Best Practices Guide.

Node count	McAfee ePO server			SQL Server			Agent Handler			Notes
	CPU cores*	RAM (GB)	Hard drive (GB)	CPU cores*	RAM (GB)	Hard drive (TB)**	CPU cores*	RAM (GB)	Hard drive (GB)	
<10,000	4	8	20	4	8-16	0.5-1.0	_	_	_	You can use a single server or VMs
10,000-25,000	4	8-16	20-40	4	8-16	0.5-1.0	4	8	20-40	See SAN information and RAID information for redundancy
25,000-75,000	8	16-32	20-40	8	16-32	0.5-1.0	4	8	20-40	
75,000-150,000	8	32-64	40-80	16	32-128	1-2	4	8	40-80	
150,000+	16	64-128	40-80	32+	64-128	1-2	4	8	40-80	

* These are physical Quad CPUs running at 2.2 GHz and 7.2 Gigatransfers per second (GT/s)
** Estimated event load for six months

Table 2: Minimum hardware requirements for McAfee ePO.

Solution and System Setup and Configuration

By default, Intel AMT firmware is unconfigured as a security precaution to ensure that unauthorized users cannot access the manageability and security features of Intel AMT. The main objectives of the setup and configuration process are to:

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

A number of different configuration options are available:

- **Intel AMT Configuration Utility Command Line Interface:** Using profiles, it is possible to apply a common configuration to multiple Intel AMT systems with this tool.

- **Remote configuration with Intel SCS.** This provides access to the full range of Intel AMT features but requires a domain provisioning certificate and also needs DHCP Option 15 to be enabled on the target device. See the Operating and Utilization section of this document for more information.
- **Remote configuration with McAfee ePO Deep Command.** Using this solution removes many of the infrastructure dependencies associated with Intel SCS.
- **Manual configuration of multiple systems:** Manual configuration requires a touch of the device, but enables you to enable Admin Control Mode (ACM) so you can access the full range of features offered by Intel AMT. Rebooting with the USB key enables Intel AMT on the device. For a discussion of Client Control Mode (CCM) and ACM see the Operating and Utilization section of this document.
- **Intel AMT Configuration Utility Wizard:** This is a GUI application that can be used to configure Intel AMT individually, and it runs on the Intel AMT system.

Intel SCS and infrastructure best practices for distribution of Intel AMT configuration and management commands

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

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

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

Using database or non-database mode

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

- Non-Database Mode – In this mode, the RCS does not store any data about Intel AMT systems.
- Database Mode – In this mode, data about each Intel AMT system is stored in a SQL database. This includes data that can be used to connect to the system and the admin password that was configured in the Intel AMT device.

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

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

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

Operation and Utilization of the Intel Solutions

This paper covers three different approaches available when using Intel AMT. A good approach is to enable Client Control Mode with host-based configuration; a better approach is to use Intel SCS to enable Admin Control Mode, and the best approach is to use McAfee ePO Deep Command to enable Admin Control Mode with fewer infrastructure dependencies. Devices enabled with Intel AMT can also be managed using tools including Microsoft SCCM.

Good: Using Client Control Mode (CCM)

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

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

- User consent is required for all redirection operations (including KVM) and changes to the boot process. When a remote connection to the computer starts, a message shows on the computer of the user. The message contains a code (see Figure 1) that the user must give to the person who wants to connect to their computer. The remote user cannot continue the operation until this code has been provided. (Whether consent is required or not, several visual mechanisms on the user's device indicate when the device is being remotely accessed using Intel AMT.)
- To help ensure that untrusted users cannot take control of the system, some Intel AMT configuration functions are blocked.
- Intel® MEBX is a BIOS menu extension used to view and manually configure some of the Intel AMT settings. During configuration, the password for Intel® Management Engine BIOS Extension (Intel® MEBX) is not changed in Client Control Mode. In Admin Control Mode, the password is replaced during AMT configuration if the password is set to the default (usually "admin").

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

CCM can be enabled on a device using host-based configuration (from Intel AMT 6.2 and higher), which enables an application running locally on the device to configure its own Intel AMT functionalities. The application can be based on a GUI or command line interface, and can be distributed like a software upgrade using Microsoft SCCM or other management tools.

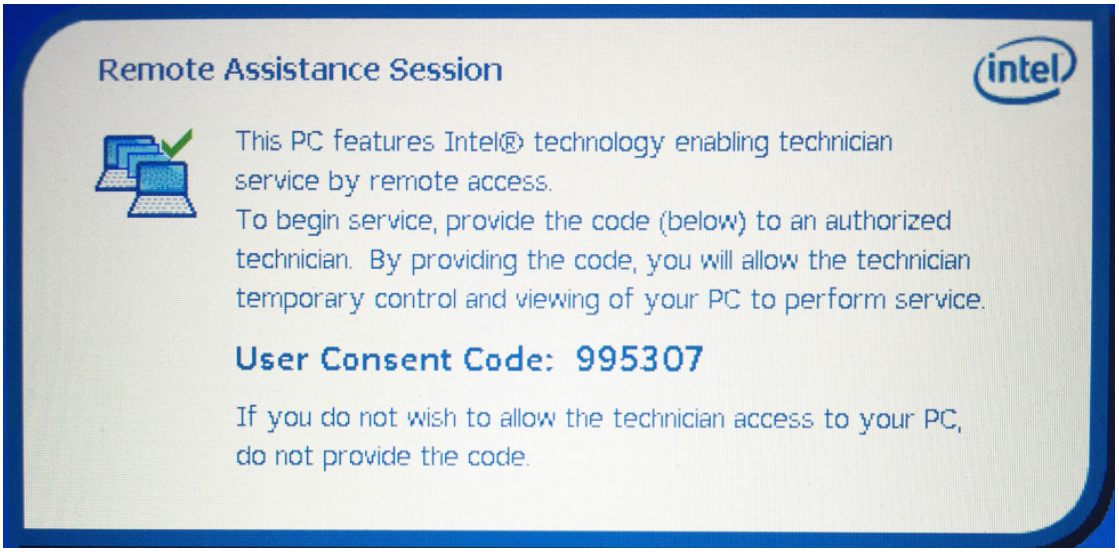


Figure 1: Client Control Mode requires user consent for redirection operations and changes to the boot process.

Host-based configuration does not require a provisioning certificate, so it can be easier to implement than the other approaches in this document, both technically and organizationally. Used together with Microsoft PowerShell or VNC Viewer Plus, it provides a lightweight and low-cost way to manage the estate of Intel AMT

devices. Use cases supported by PowerShell and VNC Viewer Plus include power control, hardware inventory, boot to alternative OS, boot to BIOS, wake and rebuild, and scheduled wake. VNC Viewer Plus additionally supports KVM full remote control. See Table 3 for details of the use cases supported by different solutions.

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

Intel SCS is well documented and updated by Intel in line with each generation of Intel vPro. It is considered the system of record for Intel AMT activations and has proven scalability to discover, configure and maintain tens of thousands of Intel AMT devices[2].

Admin Control Mode (ACM) can enable all Intel AMT features that are available on the client hardware. In this mode, there is no requirement for user consent for redirection operations and changes to the boot process. As a result, ACM makes it possible to carry out processes such as operating system upgrades at scale, without dependence on user availability or intervention.

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

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

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

Although the Intel SCS console offers a single pane to view the estate of devices, it is not recommended for advanced monitoring of devices. Intel SCS is able to do carry out basic monitoring functions, using a query to the configuration database or the end point for the specific AMT object information required. For monitoring tasks that require event-based notifications, McAfee ePO Deep Command is the recommended solution.

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

Dependent upon AMT Release, the Intel AMT firmware contains root certificate hashes from a number of commercial certificate authorities including GoDaddy, Starfield, Verisign, Comodo, EnTrust, Baltimore CyberTrust, GTE CyberTrust, and Verizon. You can also add your own root certificate hash into the Intel MEBX. To support Intel AMT remote configuration, an SSL certificate from one of these embedded hashed root certificates must be purchased from a commercial SSL certificate provider.

Best: Using McAfee ePO Deep Command in Admin Control Mode (ACM)

McAfee ePO Deep Command is a commercial solution that enables the configuration and management of Intel AMT devices in Admin Control Mode.

It simplifies the configuration process by removing some of the infrastructure dependencies associated with Intel SCS, and so removing the barriers to adoption for many organizations. It includes its own provisioning certificate and the dependency on DHCP option 15 being enabled on the client devices is negated. Because it provides its own certificate, it can be useful for organizations that cannot get a certificate for their domain.

McAfee ePO Deep Command enables end-to-end management, from configuration through to event-based notifications and reporting.

It supports a full range of use cases including power control, hardware inventory, boot to alternative OS, boot to BIOS, wake and rebuild, scheduled wake, KVM full remote control, and remote wake and patch. The ability to remotely wake and patch a machine enables organizations to:

- deploy security updates ahead of an attack;
- conduct intensive security tasks out-of-hours for minimal impact on the end user;
- cut power consumption by encouraging power-off policies without compromising on the ability to manage the machines remotely; and
- connect to disabled endpoints to conduct remote remediation.

Intel AMT Supported Solutions

Solution / Use Case	VNC® Viewer Plus	Intel vPro Technology Windows* PowerShell module	McAfee ePO Deep Command	Microsoft SCCM 2012	Microsoft SCCM 2012 (Build 1511)
Power Control	YES	YES	YES	YES	Intel AMT Add-On
Hardware Inventory	YES	YES	YES	YES	Intel SCS Add-On
Boot to Alternate OS	YES	YES	YES	YES	Intel vPro PowerShell
Boot to BIOS	YES	YES	YES	YES	Intel vPro PowerShell
Wake and Reimage	YES	YES	YES	YES	Intel AMT Add-On
KVM Remote Control	YES		YES	Intel vPro Add-on	Intel vPro Add-on
AMT Alarm Clock		YES	YES	Intel vPro Add-on	Intel vPro Add-on
Wake and Patch	Wake Only	Wake Only	YES	YES	Intel AMT Add-On

Table 3: Standard AMT use cases and solutions are supported by a range of solutions, with Microsoft PowerShell and VNC Viewer Plus providing lightweight but more limited options.

Alternative management solutions

Following configuration using one of the previously mentioned solutions, an estate of Intel AMT devices can be managed by or integrated with third-party solutions including Microsoft SCCM, VNC Viewer Plus, and products from Bomgar, LANDESK, and Symantec.

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

PowerShell cmdlets can also be used to remotely access and manage Intel AMT devices.

A web-based Intel AMT Console called Mesh Commander is available, which provides access to management capabilities and features including hardware KVM viewer, power control, hardware asset information etc. For further information, see: http://www.meshcommander.com/meshcommander

Use Cases

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

Security use cases

The following security use cases assume you are using devices with the following specification:

- Intel® Core vPro™ processors;
- Microsoft Windows 7 and 10
- Intel® SSD Pro Series
- Intel® Enterprise Digital Fence
- McAfee ePolicy Orchestrator
- McAfee ePO Deep Command
- McAfee Drive Encryption

Remotely resolve hardware encryption issues

Drive encryption can result in an increase in helpdesk calls because of users forgetting their passwords or losing their physical tokens, especially where policies do not require them to be used every time the machine is switched on. Intel AMT can help to resolve these issues more quickly and at lower cost (see Figure 2).

Drive unlock and encryption keys are stored in hardware and provide automatic disk encryption authentication when on any network. The Trusted Platform Module (TPM) protects the disk unlock code and checks the system boot integrity to validate the platform security.

If there is a problem, the service desk is able to remotely manage the systems to resolve any disk encryption issues through direct access to the pre-boot environment. The devices can be turned on and patched remotely, including automatically unlocking the hardware-encrypted SSDs.

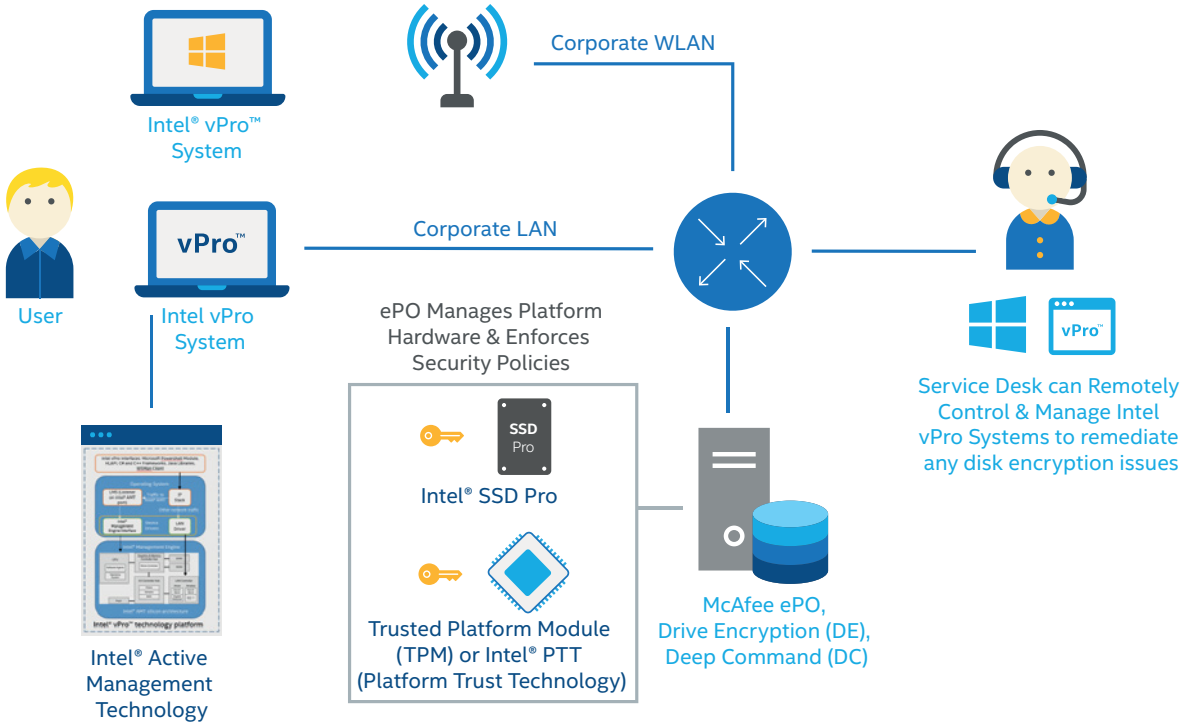


Figure 2: Intel AMT can be used to enforce security policies

Location aware encrypted drive unlock

Encryption keys can be protected in hardware and automatic authentication can be used when on a trusted network. When outside the network, preboot authentication can be enforced to protect data when off-site or in the event that the device is lost or stolen (see Figure 3). This provides an excellent user experience.

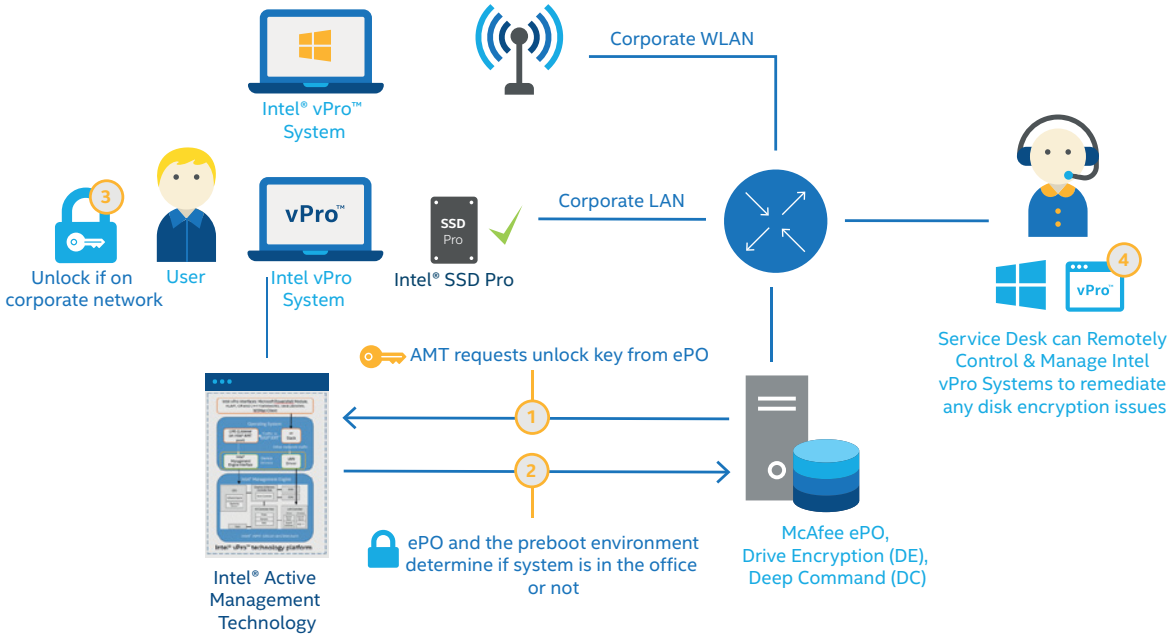


Figure 3: Intel AMT can be used to enable location aware drive unlocking, so the disk encryption key is automatically provided when on the approved network

Secure hardware platform with Intel® Enterprise Digital Fence

Many mobile computer users do not want the inconvenience of putting their system into a hibernation state. They prefer to simply close the laptop lid and let the system go into a suspend/sleep state. Since they know that their data is encrypted, they believe that their systems are safe in any situation. What they do not realize is that when a system goes into a suspend/sleep state, the disk is still encrypted, but the encryption keys remain in the system's RAM, making the system vulnerable to malware attacks.

With Intel Enterprise Digital Fence you can now define safe zones where the computer is allowed to remain in the sleep/suspend state. These are network configurations that you define and consider as trusted. You can include in the Safe Zone workplace networks (Work Zone Detection) and networks outside the workplace (Home Zone Detection). When the system is in a sleep/suspended state, the Windows-based service of Intel Enterprise Digital Fence periodically wakes the system to check if it is located in a Safe Zone. If the system is not located in a Safe Zone, the system is automatically forced into a hibernation state. When the device is powered up by the user, it then requires preboot authentication.

Intel® Enterprise Digital Fence (see Figure 4) works exclusively with the Intel® SSD Professional Family.

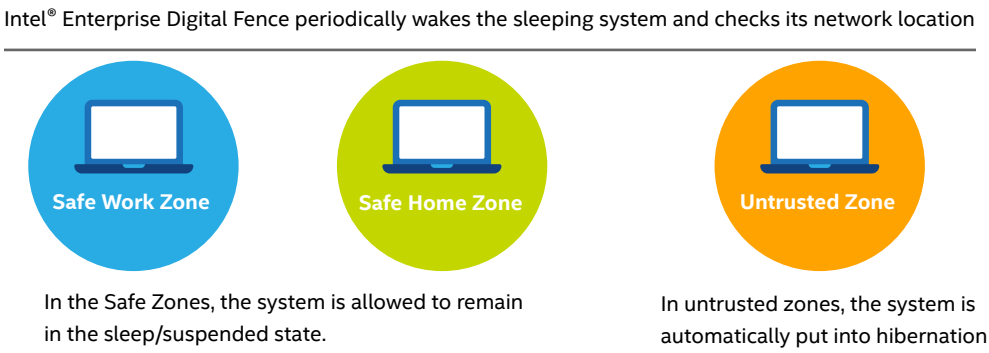


Figure 4: Intel Enterprise Digital Fence improves protection by putting devices into hibernation when they are found to be in an untrusted zone.

Remote Secure Erase

When a PC is retired or repurposed, information security policies often require data be sanitized from the drive, which can be difficult, time consuming, and costly if outsourced to a third party. Intel® Remote Secure Erase can provide a solution to all of these issues (see Figure 5).

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

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

This solution requires a compatible 6th Generation Intel vPro platform. The Secure Erase command can be issued using a toolset, such as McAfee ePO Deep Command, LANDESK, Sprinxle, or SCCM via the Sprinxle plug-in.

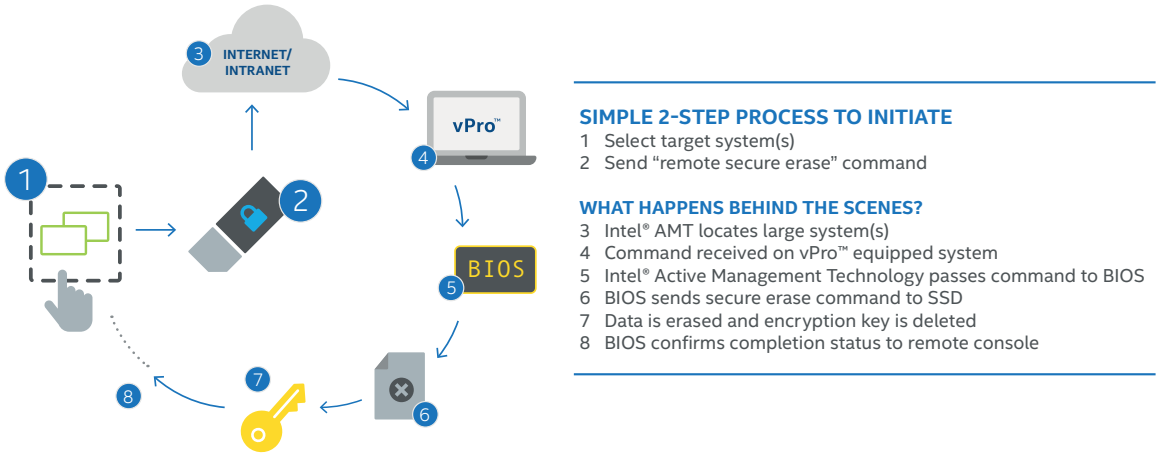


Figure 5: Using Intel® Remote Secure Erase to remotely sanitize an SSD.

Control, initiate and monitor Microsoft Windows 10 deployments

Intel Active Management Technology can help streamline deployments of, and in-place upgrades to, Microsoft Windows 10 (see Figure 6). You can use AMT to control, initiate and monitor the entire build process and it plays a particularly important role in enabling existing hardware features that are supported for the first time in Windows 10, without needing to visit every machine.

For example:

- The Universal Extensible Firmware Interface Secure Boot protocol validates firmware images before they execute to reduce the risk of boot loader attacks and ensure the operating system starts before anything else.
- The Trusted Platform Module (TPM) 2.0 provides cryptographic and system integrity capabilities implemented in either Trusted Computing Group (TCG)-compliant UEFI firmware or Intel's Platform Trust Technology (PTT) a TPM 2.0 implementation available as a firmware application within the Intel Management Engine. These technologies can be used by BitLocker for disk encryption and for device health attestation services.
- CPU virtualization extensions are required to support Windows 10 virtualization based security capabilities, including Credential Guard and Device Guard.

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

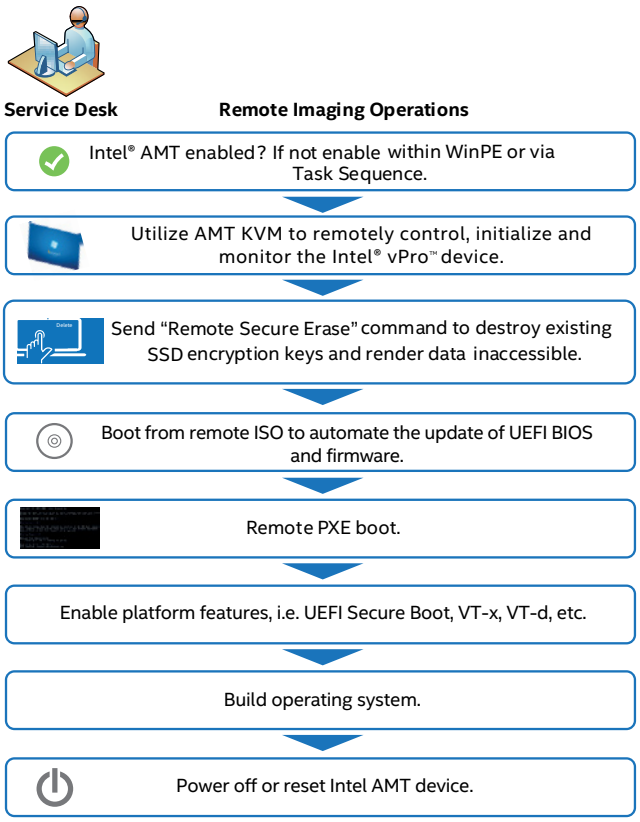


Figure 6: Intel AMT plays an important role in enabling a smooth operating system upgrade or rebuild

The operating system build process using Microsoft PowerShell and Intel AMT is as follows:

1. Initiate AMT KVM to ensure that the platform update and operating system build process can be remotely controlled and monitored.
2. Update BIOS, firmware and CPU microcode to a known good level.
   a. Use USB-R/IDE-R to remotely load WinPE disk image.
   b. Identify OEM platform components and versions using the AMT hardware asset information.
   c. Select OEM specific tools to perform updates i.e. OEM BIOS and firmware upgrade binaries.
3. Configure and enable platform BIOS settings including UEFI Secure Boot, VT-x, VT-d, TPM, Device Guard etc. This can be performed in one of two ways:
   a. Use AMT Serial over LAN (SOL) capabilities to automatically navigate the menu system using a VT100 interface, simulated keystrokes, escape codes etc.
      i. Intel® Generic Redirection Tool (GRT) is an executable that supports a subset of Intel AMT functionality for power control and redirection (SOL and IDER) commands. It is invoked from the command line using an XML script that sets the order of operations sent to the BIOS via the AMT SOL interface. See Code Snippet 1 for an example of how the XML is structured.
      ii. McAfee ePO Deep Command BIOS Configuration Templates. Primary focus of this solution is to change BIOS passwords. It uses GRT and XML-based scripts to create BIOS configuration templates and apply custom settings. Current and new BIOS passwords are managed by McAfee ePO Deep Command instead of being exposed in XML, to ensure updates are more secure and scalable.
4. Alternatively use OEM specific tools and utilities:
   a. Use USB-R/IDE-R to load WinPE disk image.
   b. Identify OEM platform components and versions using the AMT hardware asset information.
   c. Select OEM specific tools to perform updates i.e. Dell PowerShell provider.

5. Configure Intel AMT network interface to Static IP for corporate access and configure OS network interface for PXE using DHCP on the build network. See Code Snippet 2 for the PowerShell cmdlet to configure the network interface.
6. Reboot system to PXE using AMT Power Control to begin the operating system build process.
7. Reset AMT interface to DHCP, synchronize hostname and update DNS.

```
<?xml version="1.0"?>
<GrtScript>
  <Instructions>
    <StartSol/>
    <StartIder>{0}</StartIder>
    <Wait>1000</Wait>
    <RemoteControl Power="Reset" BootSource="IDERCD" BootOptions="UseSOL" />
    <WaitFor Timeout="300000" GotoOnTimeout="exit">
      <Text GotoOnSuccess="break">Press any key to continue</Text>
    </WaitFor>
    <Send>k</Send>
    <Log>Iso loaded successfully</Log>
    <WaitFor Timeout="10000" GotoOnTimeout="exit">
      <Text GotoOnSuccess="break">Type your passphrase and press</Text>
    </WaitFor>
    <Log>log on screen found</Log>
    <Wait>2000</Wait>
    <SendKey>TAB</SendKey>
    <Wait>2000</Wait>
    <Send KeyStrokeInterval="200">{1}</Send>
    <Wait>3000</Wait>
    <SendKey>Enter</SendKey>
    <Wait>3000</Wait>
    <SendKey>Enter</SendKey>
    <WaitFor Timeout="10000" GotoOnTimeout="continue">
      <Text GotoOnSuccess="Error1">Incorrect authentication, please try again</Text>
    </WaitFor>
    <Log>passphrase sent successfully</Log>
    <Goto>SuccessTerminate</Goto>
    <Wait>3000</Wait>
    <Label>Error1</Label>
    <Log>Incorrect authentication - check WDRT</Log>
    <Goto>exit</Goto>
    <Label>SuccessTerminate</Label>
  </Instructions>
  <Settings>
    <TlsClientCertificate></TlsClientCertificate>
    <Hostname>{Hostname}</Hostname>
    <User>{user}</User>
    <Password>{password}</Password>
  </Settings>
</GrtScript>
```

Code Snippet 1: Script example to open an IDER and SOL session, boot an ISO image and enter a BIOS password.

```
# Configure connection with client
$wsmanConnectionObject.SetHost($Computer, $Port)
$ethernetPortSettingsRef=$wsmanConnectionObject.NewReference("SELECT * FROM AMT_
EthernetPortSettingsWHERE InstanceID='Intel(r) AMT Ethernet Port Settings 0'")
$ethernetPortSettingsInstance=$ethernetPortSettingsRef.Get()
$ethernetPortSettingsInstance.SetProperty("DHCPEnabled","false")
```

Code Snippet 2: PowerShell cmdlet to configure Intel AMT with a static IP address. For supporting code and documentation, see the Intel AMT SDK which is the system of record for APIs and code examples for using Intel AMT.

Validation

Users can validate the solution and troubleshoot problems by using a range of tools to check the available functionality. See Figure 7 for a guide.

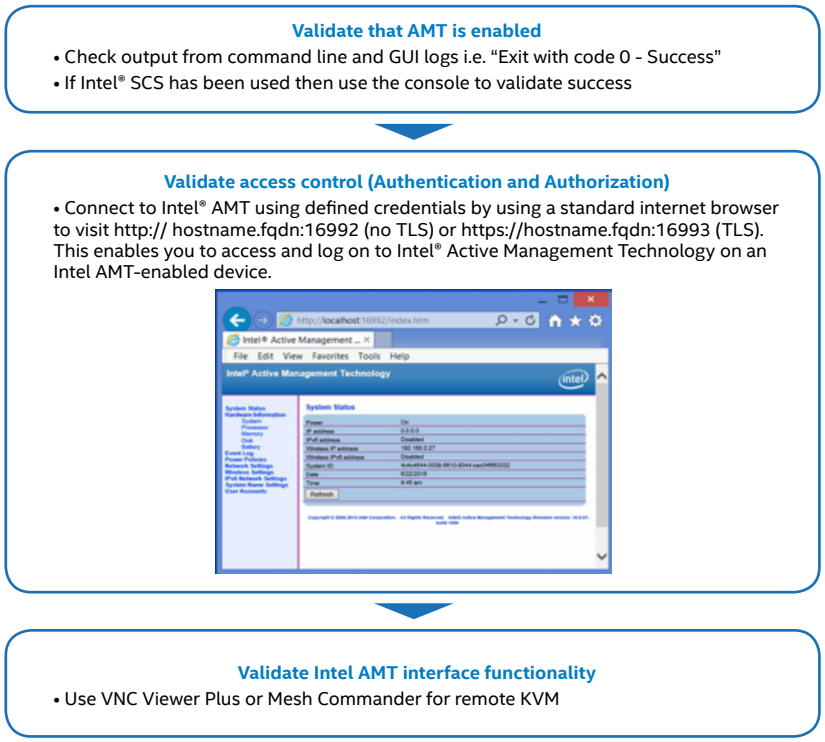


Figure 7: Workflow for validating Intel AMT has been successfully configured

Known Issues

Starting with release version 1511, Intel® AMT Out of Band Management functionality such as 1:1 and 1:Many Intel AMT power management will no longer be available via the native Microsoft SCCM application console. However, alternative methods exist to restore Intel AMT functionality.

Intel® Active Management Technology (Intel® AMT) Technical Advisory - Out-of-Band Management in Microsoft System Center Configuration Manager* (SCCM) ver. 1511

http://www.intel.com/content/www/us/en/support/software/000021063.html

This article explains how to restore the right-click menu for AMT Out of Band functions

https://communities.intel.com/community/itpeernetwork/vproexpert/blog/2016/04/27/sccm-right-click-menu-for-amt-out-of-band-functions

Intel® SCS Add-on for Microsoft System Center Configuration Manager

http://www.intel.com/content/www/us/en/software/setup-configuration-software.html

Summary

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

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

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

Solutions Proven By Your Peers

These solutions are based on real-world experience gathered from customers who have successfully tested, piloted, and/or deployed these solutions in specific business use cases.

Intel Solution Architects are technology experts who work with the world's largest and most successful companies to design business solutions that solve pressing business challenges.

To find the best solution for your organization, contact your Intel representative, register at Intel **IT Center**, or visit **www.intel.com.**

References

Best Practices Guide: McAfee ePolicy Orchestrator 5.1.0 Software

https://kc.mcafee.com/corporate/index?page=content&id=PD25519

Intel® Setup and Configuration Software (Intel® SCS) User Guide

http://www.intel.com/content/www/us/en/software/setup-configuration-software.html

Intel® Setup and Configuration Software (Intel® SCS) Scalability Guidelines

https://downloadcenter.intel.com/download/24584

Intel® Setup and Configuration Software (Intel® SCS) Deployment Guide

http://www.intel.com/content/www/us/en/software/scs-deployment-guide.html

Intel® Enterprise Digital Fence Plugin

https://downloadcenter.intel.com/download/24564/Intel-Enterprise-Digital-Fence-Plug-in

Intel® vPro™ Technology Module for Microsoft* Windows* PowerShell*

https://downloadcenter.intel.com/download/23241/Intel-vPro-Technology-module-for-Windows-PowerShell-Version-3-2-5

Intel® Active Management Technology SDK

https://software.intel.com/en-us/amt-sdk/download

Learn More

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

- Solution Brief: "Optimize Management and Security of Client Devices"
- Reference Architecture: "Streamline Device Management in a Smart, Connected World"

You may also find the following resources useful:

- Intel® Setup and Configuration Software (Intel® SCS)

  http://www.intel.com/content/www/us/en/software/setup-configuration-software.html
- McAfee ePO Orchestrator

  http://www.mcafee.com/uk/products/epolicy-orchestrator.aspx
- Intel vPro Technology

  http://www.intel.co.uk/content/www/uk/en/architecture-and-technology/vpro/vpro-technology-general.html

Solution Provided By:

[1] See Intel® Setup and Configuration Software (Intel® SCS) Scalability Guidelines for details of the scalability test. Virtual devices were used because of the impossibility of setting up a test environment of 100,000 devices, ore of risking an existing production environment.

[2] Intel® SCS Deployment Guide

2016/CAT/SM/PDF ♻ Please Recycle XXXXXX-001US