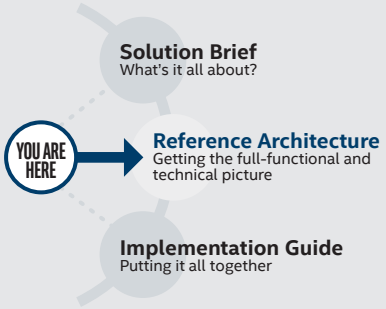
REFERENCE ARCHITECTURE

Business Client
Client Security & Manageability

Streamline Device Management in a Smart, Connected World

Using Intel® Active Management Technology, enterprises can improve security and manageability across their increasingly diverse estate of devices, cut the cost of support, and delight end users with faster resolution times



What You'll Find in This Document

If you're responsible for IT investment decisions and business strategy...

- You'll learn how Intel® Active Management Technology can simplify the management of your diverse estate of devices, driving down support costs while increasing uptime and user satisfaction.

If you're responsible for IT investment decisions and business strategy...

- You'll learn about the architecture components and how they work together to create a cohesive business solution.

Executive Summary

The estate that an IT organization must manage is becoming increasingly diverse, with smart connected devices such as personal computers, digital signs, point of sale (POS) systems and ATMs increasing the cost and complexity of support. At the same time, support organizations are challenged to deliver year-on-year cost savings while improving their responsiveness and the end user's uptime. To do that, they need to successfully resolve more issues first time, drastically cut the costs associated with shipping a device to a support center or making a desk visit; and reduce the errors introduced by manual intervention. Working within their existing tools and best practice processes, IT organizations need a way to drive down the cost of servicing, managing and securing user-facing devices and smart connected devices.

In this paper, we outline Intel Active Management Technology, or Intel® AMT, a capability of Intel® vPro™ platforms, that is an effective tool for lowering service delivery costs while improving responsiveness and service levels. It enables the remote management of devices, even when powered off or when the operating system is not available. We will show how it can integrate with current processes and leverage the existing security and manageability infrastructure, and we will share the architecture components that make up the complete solution.

Introduction

Economic transformation is accelerating, changing the way we work and the technologies we use, as new devices and working model emerge in all industries. The result of this transformation is the Smart World with over 20 billion connected devices predicted by 2020.

It's not just PCs and mobile devices any more: across industries, service providers need to take on an increasingly diverse range of devices. In retail, connected point of sale (POS) and vending systems are mission critical. In banking, ATM machines must remain secure and available to enable the self-service business model that customers rely on. Across industries, digital signage must remain tamperproof, but be connected for updates. IT organizations have never faced a more complex estate of devices, nor lived through a time when the business was more dependent on those devices.

This creates a huge challenge for IT: All these devices need to be secured and managed but it's impractical to send an engineer out every time one device has an issue. There's a challenge for operational technology (OT) too: the innovative worker wants to have the right device to do their job, and they need it to be secure and easy to use. To transform successfully, businesses must bring IT and OT together, whether the IT function is performed by an IT service provider, a systems integrator or an in-house IT department.

Table of Contents

Many organizations have spent years developing processes and protocols for managing their device fleets, based on IT Infrastructure Library (ITIL) and other industry standards for IT service management. Starting over is not a viable option. Instead, they need a way to manage the rising complexity that fits within their existing management frameworks. It needs to cover not only the new devices, but also the existing estate. Older devices must be kept secure and reliable, even as more capable devices join the organization, which potentially increases the support burden. Further complexity arises as users can and do now work from anywhere. Organizations want consistent standards of security and availability across all their devices, wherever they are.

As service organizations are driven to offer better service year on year—at a lower cost—IT organizations need to find more automated and scalable ways to manage assets, so they can cut costs while improving their responsiveness and service levels. Annual cost reductions are often written into a support contract and clients often worry about overpaying in later years when improvements in technology could enable lower cost service. Systems integrators are constantly seeking new ways to lower the cost of support while ensuring that the SLAs and user satisfaction metrics specified in the contract are met.

The key to addressing these issues may already be at your fingertips. Intel® Active Management Technology is an established Intel solution that has been a standard component of Intel® vPro™ platform for over a decade. By activating Intel Active Management Technology, you can enable remote incident management, service asset and configuration management, and release and deployment management. As a consequence, business users can enjoy improved security and uptime, with lower technological risk.

Industry applications include:

- Improving the maintenance of shared devices in healthcare and keeping security patches updated to help protect patient data;
- Streamlining the management of diverse devices in retail, including remote vending machines, point-of-sale (POS) systems and digital signs; and
- Improving the user experience in financial services, by enabling devices to be aware when they are in a trusted environment so users do not need to remember as many passwords.

For IT service providers, the Intel vPro platform presents an opportunity to deliver innovative services. It can also play an important role in enabling greater responsiveness for both business and IT, so organizations are better positioned to compete in the smart world.

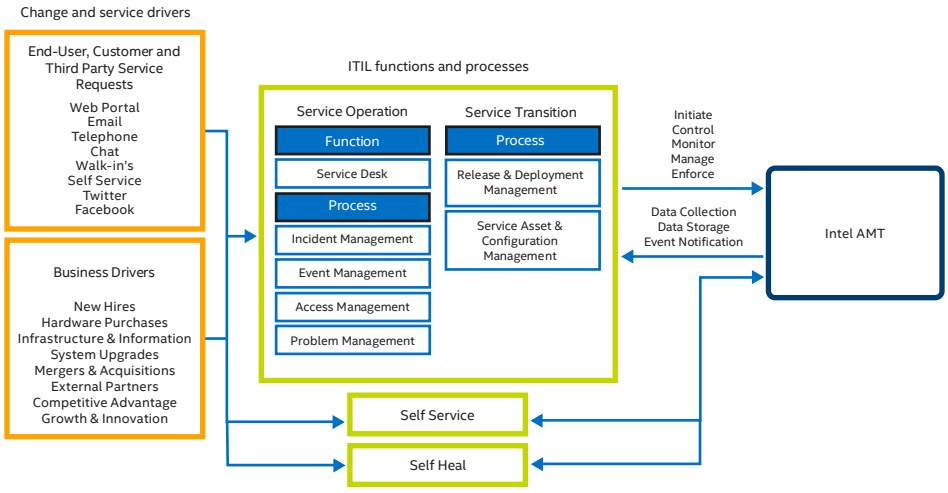


Figure 1. Intel® Active Management Technology enhances existing processes and functions to improve end-user experience and asset data quality.

Intel Active Management Technology Services and Capabilities

Intel Active Management Technology provides remote access to a device for diagnostic and management functions, even if it is powered down or the operating system is unavailable. The access is secured using SSL and Microsoft Active Directory* credentials. All of the capabilities are available either via a remote wired or wireless connection and include:

- **Power Control:** Power on a single system or multiple systems for remediation and patching.
- **Alarm Clock:** Remotely program your devices to wake up or power on at predetermined dates and times. For example, you can schedule devices to power on 10 minutes before the scheduled start of the working day.
- **Remote Control over Keyboard, Video and Mouse (KVM):** View and solve user PC and operating system issues with hardware-based KVM remote control, maintaining the KVM connection through reboot cycles.
- **Temporary Working Environment:** Provide an alternative operating system, update system BIOS, firmware or CPU microcode, or enable system rebuilds by using PXE and Microsoft WinPE.
- **Event Notification:** Trigger event messages from the device. For example, a key combination can be used to create a support ticket and request remote assistance from the service desk or an alert can be raised when the cover of a device is opened or a sensor is triggered.
- **Access to Hardware Asset Information:** Provides remote visibility of the hardware configuration, even when the PC is off or asleep, including parameters such as its CPU, memory and type of disk. This enables automated update and verification of data within a Configuration Management Database (CMDB). This capability can also be used to populate fields in a ticketing system, which are time consuming and expensive to verify manually. If a part fails, the hardware asset capability can be used to confirm the correct replacement part before a desk visit, cutting the number of visits required and improving the time to resolution.
- **Web Application Hosting:** IT and ISV can store a web application in Intel Active Management Technology's locally managed Non-volatile Memory (NVM) to supplement or even replace the default Intel Active Management Technology web UI. Push web pages and other files into Intel Active Management Technology and have them served by the Intel Active Management Technology web server.
- **Discovery:** Enables the IT organization to remotely discover the hardware asset, its configuration, and its Intel vPro platform capabilities without need for a site visit. The discovery of Intel vPro platform capabilities enables an organization to automatically identify how many Intel vPro systems they have within their environment, which is one of the first major steps towards using Intel Active Management Technology. Products such as Microsoft System Center Configuration Manager* (Microsoft SCCM*) can leverage this capability for large client estates.
- **Microsoft Active Directory Integration:** Supports layered access control using Microsoft Active Directory users and groups. For example, you can enable front line support to have access to device information but restrict system rebuilds to second line support.
- **Auditing of Intel Active Management Technology Operations:** Particularly useful in highly regulated industries or applications, this provides an audit trail for Intel Active Management Technology operations.
- **Optional User Consent:** A mechanism for displaying a 6-digit authorization code outside of the operating system, to ensure that user consent is granted for device access and operations.
- **Event Driven Notification:** Enables the device to raise an event using Client Initiated Local and Remote Access (CILA and CIRA). The device can use this to request an unlock key from the server when it knows it is in a trusted environment. This capability can also be used to require a device to check in regularly with the network to help maintain the visibility and security of the device.
- **System Defense:** Hardware-based network filters to isolate a device from an untrusted network and shut down the network interface from the Operating System, without affecting the ability of the IT organization to manage that device remotely.
- **Agent Presence:** Monitors critical software agents on the operating system, such as antivirus protection. Can generate an event and raise an alert if these agents are not present or disabled for any reason.

Used together with existing IT management tools and processes, these services and capabilities improve the manageability of the organization's devices, enabling remote management and access, with a consistent process and toolset for managing both old and new devices. They also improve security by enabling more timely security patches and a higher proportion of devices to be reached. Because Intel Active Management Technology works over wired and wireless connections, and works with many classes of devices, it is able to support the innovative, mobile and disruptive business models of today.

ITIL Use Case Examples

Intel Active Management Technology enables IT organizations to discover, manage and help secure their devices without the need for a desk visit, in a way that fits with existing ITIL and IT organization functions and processes.

Service Desk

With the capabilities provided by Intel Active Management Technology, the service desk function can increase customer satisfaction, improve the speed of response to user requests, and reduce the cost of support. Using remote access to devices, service desks can:

- Reduce desk-side visits by up to 90 percent for remote employees[1]; and
- Reduce employee downtime by 98 percent[2];

Service agent productivity and time-to-resolution can be improved by automatically providing complete and accurate configuration information. Intel Active Management Technology can be remotely queried and the hardware asset and configuration information can be used to populate a ticketing application, such as Remedy*, when a support request is submitted through a service desk or self-help portal. Using Intel Active Management Technology, service desks can quickly provide an environment to enable a user to continue working while a device is repaired, and can request real-time access and control over the device for diagnostics and problem resolution.

Self-service can be introduced for simple tasks such remotely resetting a passphrase that a user has forgotten or requesting a machine rebuild. The cost of support and the impact on the user increase as requests are escalated through the tiers of support. Intel Active Management Technology enables IT organizations to adopt a "Shift Left Strategy", de-escalating common support requests by enabling self-service, and empowering lower tiers of support with the information and tools required for remote resolution. This cuts the time to resolution and improves the service desk experience for everyone. In the longer term, this delivers further cost savings by reducing the training and documentation required for the service desk function.

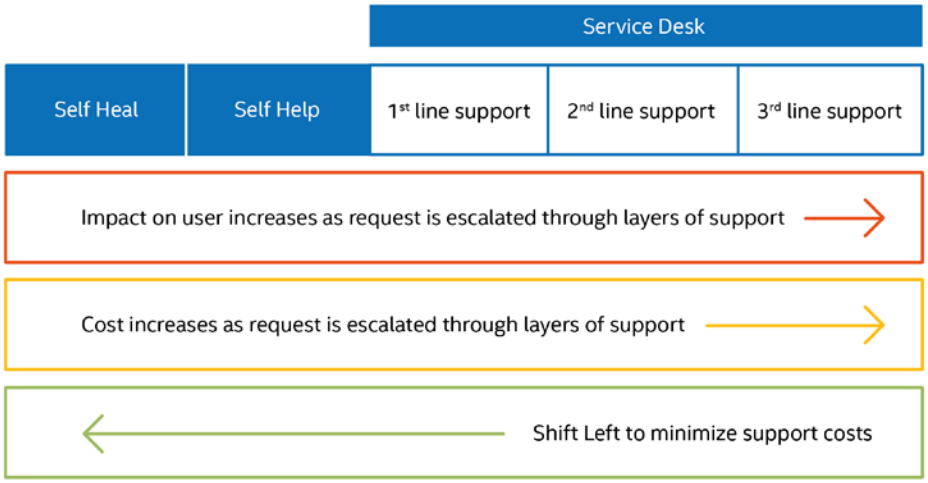


Figure 2. The Shift Left Strategy for support cuts the cost of support and increases user satisfaction.

[1,2] Principled Technologies, "Change your desktops, change your business," report commissioned by Intel, March 2015, http://www.principledtechnologies.com/Intel/Desktop_upgrade_0315_v3.pdf

Incident Management

Intel Active Management Technology helps accelerate incident response and handling, regardless of the state of the systems affected. In contrast to PC management software often used in support functions, Intel Active Management Technology provides access to the device irrespective of whether the OS is running or can run, and enables remote management of the device as long as the device is connected to power and the network. Relevant information such as the device configuration and installed version of critical software agents (such as antivirus) can be provided to agents immediately without user intervention. Agents can use KVM access to repair a device, quickly set up a temporary work environment, and schedule a machine rebuild outside of the user's working day. This can reduce employee downtime by nearly eight hours for a single repair.

More incidents can be fixed remotely, eliminating the delay and cost associated with bringing a support agent and the device together in the same room, whether that requires a courier, a site visit, or an employee trip to the IT base. For devices in remote locations, which are a common occurrence in industries such as oil and gas and telecommunications, off-shore travel or transportation by helicopter or ship can be extremely expensive for routine repairs.

Common key performance indicators (KPIs) for support include measures of how quickly an issue was resolved. Shipping a device for repair causes several days of user downtime, and even a desk visit can severely affect the user's uptime. In many industries, including retail and financial services, downtime of connected devices such as point of sale or trading systems can have an immediate and measurable impact on profitability and customer satisfaction. Short recovery times are business critical. KPIs for Service Operation under ITIL also often include the number of incidents resolved remotely, the first time resolution rate, and the number of incidents resolved within the SLA. Intel Active Management Technology has an impact across all these metrics, enabling devices to be fixed more quickly, with less impact on users, and with a greater first time resolution rate.

Service Asset and Configuration Management

A common problem is that assets are entered into the CMDB when built or bought, and are not updated in line with changes over time. That typically happens when those devices cannot be reached by software tools that take an inventory of the assets and their hardware and software configurations. While it is relatively rare for a failed audit or inventory to trigger a desk-side visit or shipment of a system to a support center, inaccurate data can result in the wrong parts being fitted in repair, or a delay sourcing the parts when the correct configuration is discovered by the support engineer. Non-compliant systems can be vulnerable to virus attacks, and it can be difficult for the IT organization to have a view of these vulnerabilities if the devices are not regularly audited.

By activating Intel Active Management Technology, service organizations can increase their ability to reach systems remotely, so they can maintain complete, current and accurate configuration information. This reduces physical interventions and increases the accuracy of the CMDB. Using a tool such as Microsoft SCCM*, a small binary can be regularly distributed across the estate of connected devices with Intel Active Management Technology to audit the devices and update the CMDB. Assets can be inventoried and validated for network connectivity, even when powered off.

Intel Active Management Technology maintains important configuration information in non-volatile memory which is tamperproof and persistent across changes to operating systems and hardware components. Additionally Intel Active Management Technology enhances an organization's ability to identify physical and logical relationships, and identify and schedule any required changes.

The physical and logical elements of configuration management, implemented within the ITIL framework, provide a solution to the problems of unauthorized and unrecorded asset modification. Effective configuration management is also the basis for effective incident management, problem management, change management, and service level management. Effective configuration management also improves the ability to adhere to legal obligations, provide reliable risk management, and identify IT infrastructure components that are targets for upgrade and/or cost saving actions.

KPIs for configuration management include the effort required for CMS validations, the frequency of physical validations, the number of incidents reported where the root cause is inaccurate configuration information, and the number of CMDB errors. Intel Active Management Technology helps to improve

results across all of these KPIs by eliminating manual work that might otherwise be required for validations, making it easy to conduct regular CMDB validations, and improving the timeliness, accuracy and completeness of the CMDB contents.

Intel® Active Management Technology Enabled System	
Class	**Description**
AmtInformation	Information about the Intel AMT device
BaseBoard	Information about the motherboard of the host computer
BIOSInfo	Information about the BIOS and its capabilities
ComputerSystem	Information about the computer system
Processor	Information about the processor (manufacturer, model, clock speed, role, etc.)
Fan	Information about the fans (desired speed, active cooling, variable speed, etc.)
FieldReplacementUnit	Information about the "Field Replaceable Units" - add-in cards, such as graphics cards, including PCI ID information
MediaDevice	Information about disks and CD/DVD drives
MemoryModule	Information about memory modules (manufacturer, capacity, etc.)
PowerSupply	Information about the power supply
Sensor	Information about the sensors (for example, heat sensors) available on the system (type, enabled status, etc.)
VproVerificationTable	Information about the capabilities of the CPU and the chipset, PCI IDs and so on.

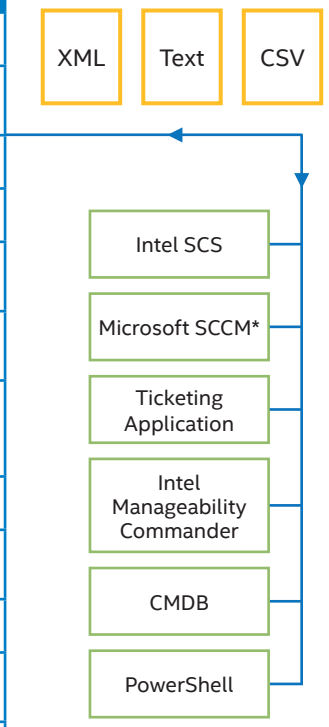


Figure 3. Data from Intel Active Management Technology devices can be advertised, acquired or driven by events via open existing interfaces and "consumed" or "re-used" by any number of critical business applications

Release and Deployment Management

Whether the release is a major software release and hardware upgrade containing large amounts of new functionality, a minor software update, or an emergency working environment to ensure users remain productive, Intel Active Management Technology enables IT organizations to deploy to more systems in a more timely fashion, with less manual intervention.

Using the latest IT management consoles with Intel Active Management Technology support, the deployment can be initiated, monitored and controlled with minimal disruption to the end user.

One recent example concerns a major retailer, whose IT organization was responsible for a large and geographically dispersed estate of devices handling sensitive payment information, including credit card details. To improve the security of the devices, the organization wanted to upgrade from Windows* 7 to Windows* 10, but its estate included many 18-month-old PCs on which it had not enabled all the platform settings. In particular, the Trusted Platform Module (TPM) cryptographic store and Unified Extensible Firmware Interface (UEFI), used to certify a secure boot, had to be enabled in the BIOS to take advantage of Windows 10's enhanced security features.

The USB-R feature of Intel Active Management Technology enables devices to be booted from a remote image, as if it were connected through a USB port, and can be used to apply updates to the UEFI BIOS and enable core platform technologies such as Intel® VT-x, Intel® VT-d, and secure boot.

Using Intel Active Management Technology, the retailer's IT organization was able to turn the PCs on and automate the entire Windows 10 build process including BIOS, firmware and CPU microcode updates, and enablement of platform security features. Using Intel Active Management Technology, agents were able to control, initiate and monitor the process remotely. The automation reduced manual mistakes during the build process and increased the ratio of devices to service agents, cutting the number of full-time equivalents (FTEs) required. The deployment was managed remotely using Windows PowerShell*, with service agents using Intel Active Management Technology KVM to control, initiate and monitor progress. Following the upgrade process, the organization had a more secure estate of devices, across over 1,000 different locations.

Large operating system upgrades like this are among the most challenging of releases, but patching and updating is a regular activity and the ability to wake a device and update it, without the device being powered on or the user being present, improves the security and reliability of any organization's IT.

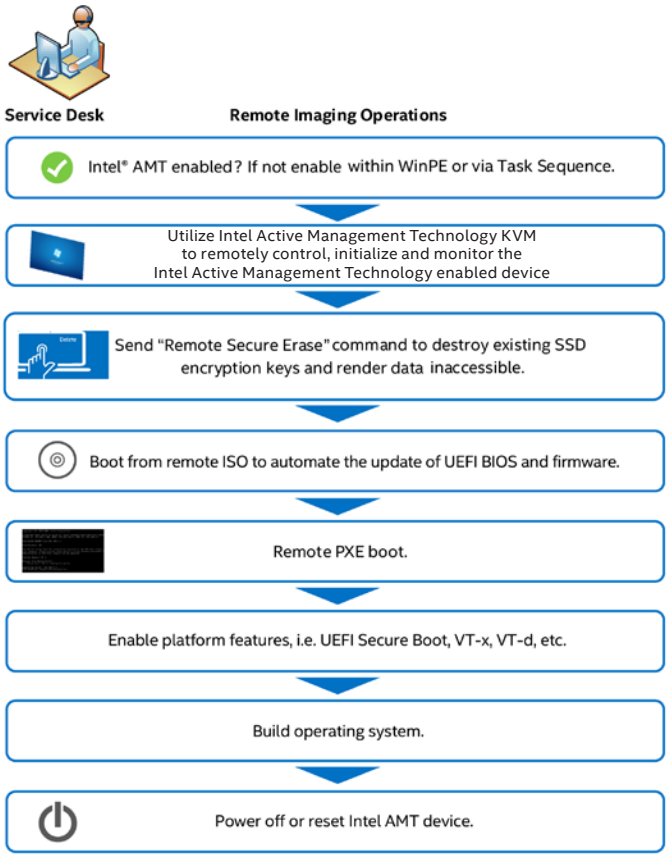


Figure 4. Reimaging a machine for an operating system upgrade can follow a smooth process, managed remotely and enabled by Intel Active Management Technology

Management Architecture of the Intel Active Management Technology Solution

Intel Active Management Technology offers a common approach to manageability, where IT organizations do not need to worry about what's on the end of the connection and can manage all of their Intel vPro platforms through a single solution. The solution seamlessly manages machines of different makes, types, and generations.

Following activation, devices can be managed using tools such as Microsoft SCCM*, Windows PowerShell, Web APIs, and high level APIs (HLAPIs).

Intel® Setup and Configuration Software (Intel® SCS) is a free suite of tools that can be used to configure and activate Intel Active Management Technology, and discover connected Intel® technology-based devices. Intel SCS offers flexible features and capabilities to enable IT services organizations to take a fine-grained approach to integrating with complex information security and privacy solutions, as well as other infrastructure touch points.

IT organizations are free to manage their devices using alternative solutions once Intel Active Management Technology has been activated, including Intel® Manageability Commander, Microsoft SCCM*, VNC Viewer Plus, PowerShell, HLAPI and Web APIs.

The solution can be integrated with existing infrastructure such as certificate authorities and Active Directory or other LDAP based services, to enable encryption of management traffic and more granular authentication and permissions management.

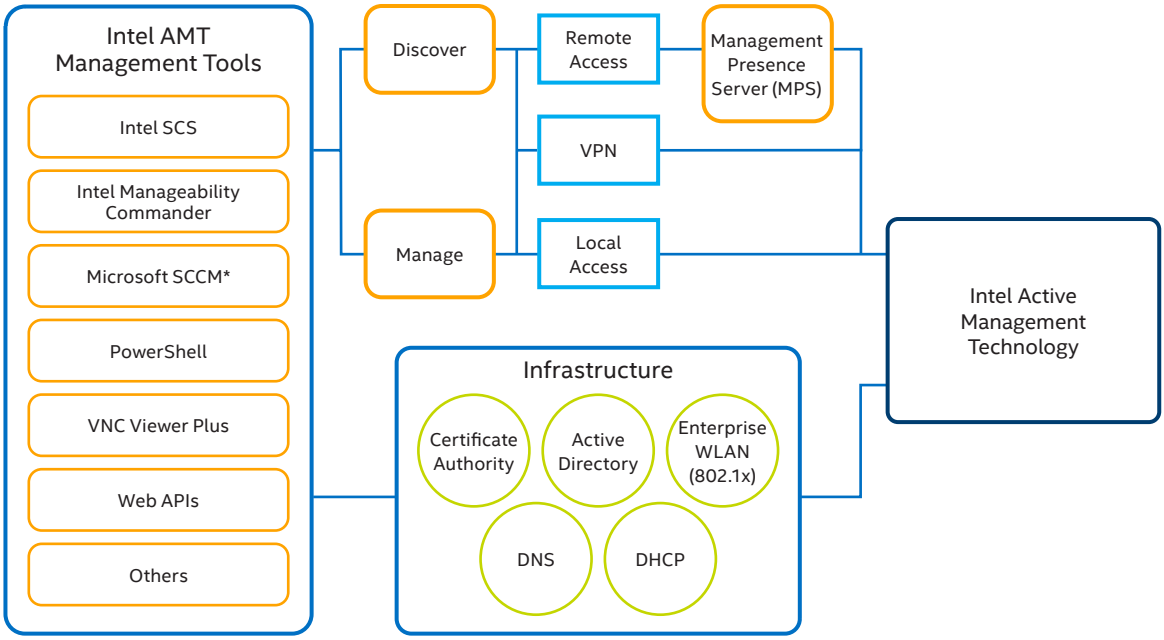


Figure 5. Intel Active Management Technology Management Software Architecture

Summary

Intel Active Management Technology provides a solid foundation for extending ITIL processes into remote management of both user-facing devices and smart connected devices. Working within existing business processes and supported by leading IT management tools, Intel Active Management Technology helps IT organizations to tackle the increasing complexity in their estates of managed devices, without complicating their management infrastructure. By providing remote access to devices, even when powered off or without a functioning operating system, Intel Active Management Technology enables faster incident resolution and drives down the cost of the service desk. Intel Active Management Technology streamlines common IT activities such as user self-service, patching and upgrading, machine recovery and re-imaging, and configuration auditing. Intel Active Management Technology has been a part of the Intel vPro platform for over a decade, and can be activated using Intel SCS, a free tool from Intel, among other solutions.

References

Intel® Active Management Technology

intel.com/AMT

Intel® vPro™ Platform

intel.com/vPro

Intel® Active Management Technology Software Development Kit Home Page

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

Managed Service Providers

msp.intel.com

Solution Provided By:

Printed in USA 0218/SM/KAIA/PDF ♻ Please Recycle 334533-002US