REFERENCE ARCHITECTURE

Business Client
Client Security & Manageability

Using Intel vPro® Platform Management for a Smart, Connected World

Using Intel vPro® Technology, enterprises can improve security and manageability across the diverse landscape of devices—even beyond the firewall—help cut the cost of support, and streamline resolution times

If you are responsible for...

- **IT investment decisions and business strategy:** You'll learn how Intel® AMT and Intel® EMA can simplify the management of your diverse fleet of devices, to help reduce costs and increase uptime and user satisfaction.
- **Managing or supporting your organization's devices, including remote devices:** You'll learn about the architecture components and how they work together to create a cohesive solution for managing these devices remotely in all deployment scenarios, including beyond the firewall.

Table of Contents

Executive Summary

With smart devices such as personal computers, digital signage, point-of-sale (PoS) systems, and ATMs, the fleet of devices that IT organizations manage, as well as where they connect, is becoming increasingly diverse. Every additional type of device and location has the potential to increase the cost and complexity of support. At the same time, support organizations are challenged to help reduce operational cost while improving responsiveness and user productivity. To do that, organizations need to successfully resolve more issues the first time, helping to cut the costs associated with shipping devices to the support center or making a desk visit. Working within their existing tools and best practice processes, automation and scalability can help IT organizations achieve these goals, as well as reduce errors.

This paper discusses the following technology and tool:

- **Intel® Active Management Technology** (Intel® AMT) is a feature of Intel vPro® platforms that provides remote hardware-based capabilities for asset management that enables out-of-band management from the operating system.
- **Intel® Endpoint Management Assistant** (Intel® EMA) is a software tool designed to modernize Intel AMT and reach beyond the corporate firewall for managing devices in hosted and cloud-based environments. Intel EMA can communicate in-band through a software agent or out-of-band through Intel AMT.

Together, the technology and tool are an effective solution to help lower service costs while improving responsiveness, security, and user satisfaction. This paper details how the solution integrates with current processes and existing security and manageability enterprise architectures, including the architecture components of the complete solution.

Introduction

Economic transformation is accelerating, changing the way we work and the technologies we use, as new devices and working models emerge in all industries. The result of this transformation is the Smart World with over 50 billion connected devices predicted by 2020.[1]

Across industries, organizations must support an increasingly diverse range of devices, well beyond PCs and mobile devices. In retail, connected point-of-sale (PoS) and vending systems are mission critical. In banking, ATMs must remain secure and available for the self-service business model customers rely on. Digital signage must be tamperproof while connected for updates. IT organizations have never faced a more complex landscape of devices, nor experienced business objectives more dependent on those devices.

This creates a challenge for IT: All devices must be secured and managed, yet it's impractical to send an engineer out every time a device has an issue. There's also a challenge for operational technology (OT) as innovative workers want the right devices to do the job, but those devices must be secure and easy to use. To transform successfully, businesses must bring IT and OT together, whether the IT function is performed by a service provider, a systems integrator, or in-house. A well-managed device can be more secure and allows IT organizations to respond more swiftly to security incidents.

Many organizations have spent years developing processes and software tools for managing their device fleets, based on IT Infrastructure Library (ITIL) and other industry standards. Starting over is not an option. Instead, they need new ways to manage the rising complexity in a way that fits within their existing management frameworks. Even as more capable devices are added, older devices must be kept secure and reliable, increasing the support burden. An estimated 72 percent of users will be mobile, working from anywhere by 2020.[2] These users need a reliable solution, and organizations want consistent standards of security and availability across all devices, wherever they are.

Systems integrators are constantly looking for new ways to lower support costs while ensuring user satisfaction. Annual cost reductions are often included in support contracts as clients want to avoid overpaying when technology improvements reduce costs. Offering better service at a lower cost requires automation and scalability.

Intel® Active Management Technology (Intel® AMT), which has been a component of Intel vPro® platform for over a decade, provides simple and powerful out-of-band endpoint management for devices. Now, with Intel® Endpoint Management Assistant (Intel® EMA), IT organizations can reach devices beyond the corporate firewall and into cloud-based environments, helping address today's challenges no matter where the device is located (see Figure 1).

A few of the industries that benefit from this technology include:

- **Healthcare.** Improved maintenance of shared devices with up-to-date security patches helps protect patient data.
- **Retail.** Streamlined management of diverse devices in retail, such as remote vending machines, PoS systems, and digital signage.
- **Financial.** Time is money, and well-managed devices bring employees back to productivity faster in cases of device downtime.

For IT service providers, the Intel vPro platform presents an opportunity to deliver innovative services. Intel AMT with cloud-enabled Intel EMA plays an important role in greater responsiveness, positioning businesses to compete better in the Smart World.

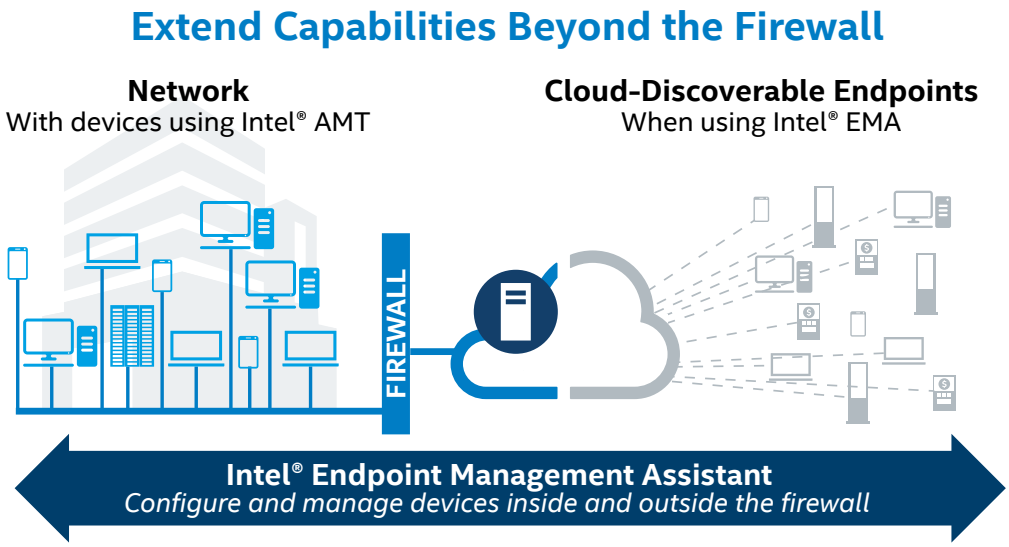

Figure 1. Intel® Active Management Technology (Intel® AMT) enhances existing processes and functions to improve end-user experience and asset data quality. Intel® Endpoint Management Assistant (Intel® EMA) extends capability beyond the firewall and into the cloud.

Remote Capabilities in All Deployment Scenarios

Intel AMT provides remote access to a device for diagnostic and management functions, even if it is powered down or the operating system is non-functional. The access is secured using TLS and digest credentials.

Intel EMA extends that capability across all environments inside and outside the corporate firewall, including on-premise, off-premises, hybrid cloud-based, and within the DMZ. Access to the Intel EMA console can be controlled through directory services credentials.

Remote management capabilities are available through wired or wireless LAN connections and include:

- **Power control.** Power on a single system or multiple systems for remediation and patching. This capability can also be accessed through APIs.
- **Alarm clock.** Remotely program devices to wake up or power on at predetermined dates and times. Devices can be powered on 10 minutes before the start of the working day or for a scheduled maintenance task, for example.
- **Remote control over hardware-based Keyboard, Video, and Mouse (KVM).** View and resolve user PC and operating system issues with hardware-based KVM remote control, maintaining the KVM connection through reboot cycles.
- **Access to hardware asset information.** Remotely view hardware configurations—even when the PC is off or asleep—including parameters such as CPU, memory, and disk type. If a part fails, the hardware asset capability can confirm the correct replacement part before a desk visit, helping to reduce the number of visits and speeding time to resolution.
- **Discovery and inventory.** Remotely discover the hardware asset, its configuration, and its Intel vPro platform capabilities. Automatically identifying how many Intel vPro platform-based systems are within the environment is the first step to using Intel AMT.
- **Optional user consent.** Display a 6-digit random authorization code independent of the operating system to ensure that user consent is granted for remote remediation commands on the device.
- **Beyond the firewall support.** With Intel EMA, IT organizations can now use Intel AMT functionality to remotely manage devices beyond the corporate firewall.
- **Cloud-based manageability.** Intel AMT with cloud-enabled Intel EMA allows IT organizations to manage their worldwide fleet of devices hosted inside or outside the firewall, even within the DMZ.

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 across environments, with consistent processes and tools. Intel AMT with Intel EMA improves security by enabling more timely patches to a larger population of devices.

Deployment for Every Environment

The following Intel EMA deployment models provide remote access through Intel AMT, enabling flexibility based on an organization's individual needs (see Figure 2):

- **On-premises.** Remotely manage all devices within the corporate environment when there is no cloud instance, or when testing and configuring capabilities.
- **Off-premises.** Remotely manage all devices within a hosted off-premises, private cloud environment. For IT organizations who are new to using Intel AMT and Intel EMA and the array of built-in tools, deploying to an off-premises cloud can provide an excellent environment for initial setup and configuration.
- **Beyond the firewall.** Remotely manage devices through a more secure tunnel access to cloud-based devices outside the firewall.
- **Hybrid cloud.** Remotely manage all devices in hybrid on-premises and hosted private environments, the most common instance with today's mobile clients.

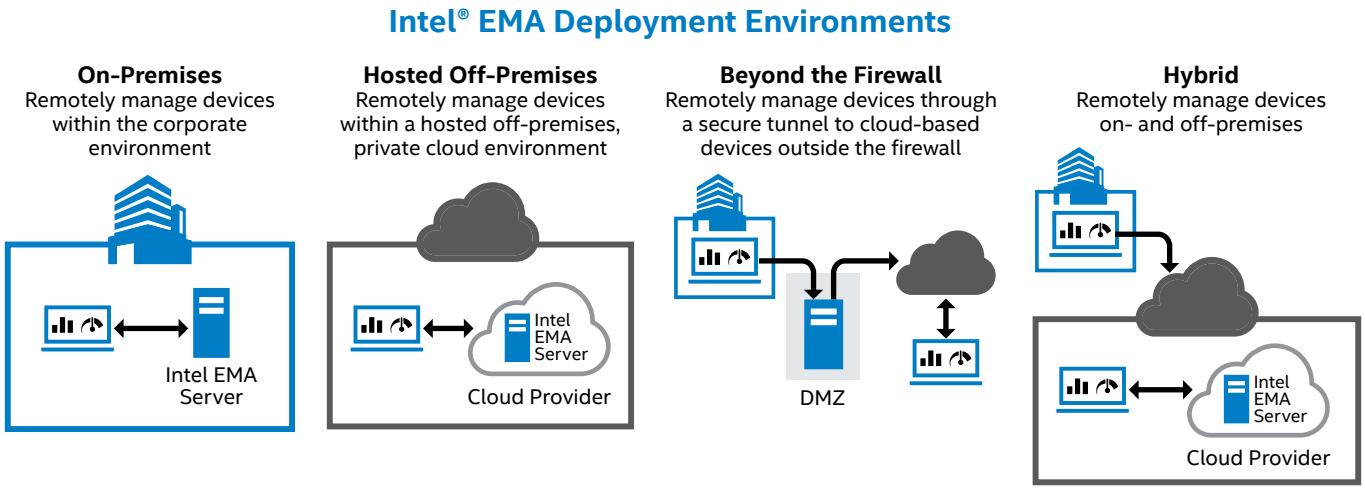

Figure 2. Intel® Endpoint Management Assistant (Intel® EMA) enables remote access to devices through Intel® Active Management Technology (Intel® AMT) inside and outside the corporate firewall.

As seen in Figure 3, using a single-instance base server, global administrators can define one or more tenants (during installation the global administrator and the first tenant are defined). Within each tenant are groups of systems and role-based accounts to manage those systems. For example, a government entity might set up tenants based on different agencies. IT operations or service personnel within each agency are then assigned roles and permissions for specific tenants. Within those tenants, systems can be grouped by the tenant administrator. Each agency can then manage their PCs independently based on their own requirements and operational needs.

In addition to the relay server and database, Intel EMA single-instance based server components include:

- **Ajax server.** This handles the JavaScript library and API requests such as in-band remote desktop capabilities.
- **Swarm server.** This manages connections between managed devices and the Intel EMA instance in-band and out-of-band.
- **Manageability server.** This manages Intel AMT provisioning and unprovisioning of devices.
- **File actions server.** This is used for in-band file transfers from the Intel EMA server to devices.
- **Intel EMA website.** This supplies a user interface for Intel EMA when not integrated into deployments through APIs.

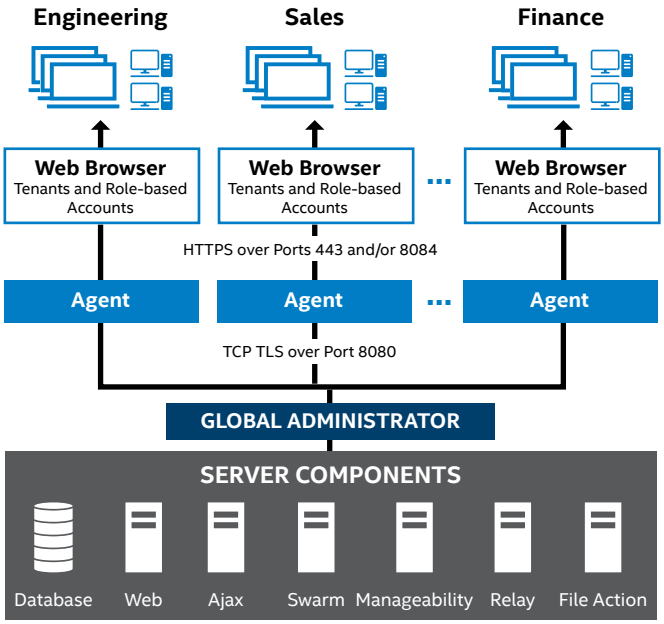

Figure 3. Single-instance base server components allow global administrators to define and manage tenant environments and tenant administrators in any deployment scenario.

Management Architecture

Intel AMT offers a common approach to manageability. IT organizations can manage all of their Intel vPro platforms through a single solution that seamlessly manages machines of different makes, types, and generations—and now with Intel EMA, they can manage them across all environments (see Figure 4).[3]

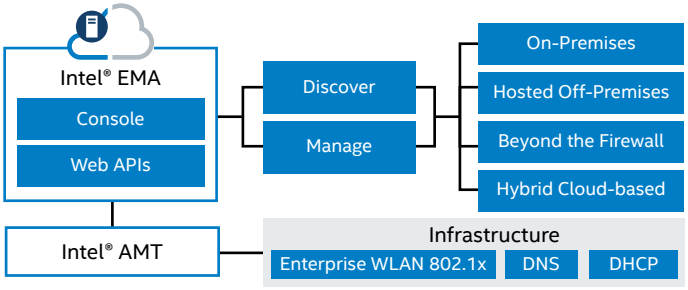

Figure 4. Intel® AMT with Intel® EMA provides end-to-end device management.

Intel EMA is designed to modernize Intel AMT with cloud-based functionality. The back-end server software includes a web user interface, Intel EMA server, and Intel EMA data store. The client software includes the Intel EMA agent with settings and data to establish cloud-based communication. Many familiar tools, such as client initiated remote access, are now built into Intel EMA, reducing the learning curve. Organizations can also manage devices using alternative solutions once Intel AMT is activated, including Intel® Manageability Commander integrated with Intel AMT WebUI, task automation and configuration management scripts, and Web APIs. The solution can be integrated with existing infrastructure such as certificate authorities and directory services or other LDAP-based services. Authentication to the Intel EMA console occurs through a user ID and password defined by the administration or through a domain user ID and email address where Intel EMA can then issue certificates for transport layer security communications.

Use Cases

With the user interface or APIs, manage both in-band and out-of-band functionality. APIs enable Intel EMA integration with additional third-party tools, improving existing ITIL and IT organization functions and processes with Intel vPro platforms.

Service Desk

With Intel AMT and Intel EMA, service desk function can increase customer satisfaction, improve responsiveness to requests, and help reduce support costs. Based on a recent study from Forrester and commissioned by Intel, specialists at a composite organization used Intel vPro platforms to help deliver the following improvements:[4]

- **Reduced security issues.** As part of the Intel vPro platform, Intel AMT can help save an estimated 7,680 security support hours annually with reduced support and management work.[5] Both minor and major security and management issues were reduced due to improvements enabled by the Intel vPro platform, and the remaining issues were resolved more quickly.
- **Reduced security support and management costs.** As part of the Intel vPro platform, Intel AMT can help reduce security support and management costs totaling nearly USD 1.2 million over three years.[5]
- **Improved employee efficiency.** An estimated 28,160 hours can be saved with better device security and management.[6] Employees spent less time waiting for updates to install, dealing with issues that require security and management support, and waiting for devices to wake up from sleep mode.
- **Improved computer and data security.** In addition to security remediation time savings, the Intel vPro platform helped keep company data safer and reduced the risk of a data breach with hardware-enhanced security and manageability features.
- **Faster and more timely IT patch installations.** IT managers and desktop operations specialists at a composite organization used the Intel vPro platform to help save a total of 832 hours deploying patches and handling in-person exceptions, adding an estimated savings of USD 81,000 savings over three years.[7]

Service agent productivity and time to resolution can be improved by automatically providing complete and accurate configuration information. Service desks using Intel EMA can provide an environment for users to continue working while a device is repaired, as well as request real-time access and control through the device for diagnostics and problem resolution.

Incident Management

Common key performance indicators (KPIs) for support include how quickly an issue is resolved. In most industries, device downtime can have an immediate and measurable impact on profitability and customer satisfaction. Short recovery times are business-critical. KPIs for Service Operation under ITIL often include the number of incidents resolved remotely, first-time resolution rates, and the number of incidents resolved within the SLA. Intel AMT with cloud-enabled Intel EMA, significantly improves these KPIs.

Intel AMT 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 AMT 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 it is connected to power and network. Intel EMA extends the reach beyond the corporate intranet network and firewall. Agents can immediately identify relevant information such as the device configuration without user intervention. Agents can use hardware-based KVM access to repair a device.

Service Asset and Configuration Management

Assets are entered into the Configuration Management Database (CMDB) when first built or bought, but are rarely updated with changes over time, creating a common problem. This happens when devices cannot be reached by inventory tools that collect hardware and software configurations. Inaccurate data can result in ordering the wrong parts for repair, or a delay in sourcing parts when the correct configuration is discovered. Non-compliant systems can also be more vulnerable to virus attacks, making it difficult for IT organizations to recognize vulnerabilities.

Intel AMT with Intel EMA allows IT service organizations to reach systems remotely to maintain complete and accurate information, even beyond the firewall. Intel AMT maintains important configuration information in non-volatile memory, which is tamper-resistant and persistent across operating systems and hardware components. Additionally, it enhances an organization's ability to identify physical and logical relationships, as well as identify and schedule any required changes. Intel AMT can be activated in Admin mode, allowing access to devices without user consent, or in Client mode, requiring end-user consent.

Intel EMA enhances Intel AMT to include the following configuration features:

- **Discovery.** Discover, collect, and maintain current, accurate device configuration information across the fleet, regardless of where it resides.
- **Host-based.** Host-based configuration is the preferred, default method with Intel EMA for Intel AMT for devices that are on-premises or off-premises.
- **Remote.** Configure on-premises devices through wired LAN.

Release and Deployment Management

Whether it's a major or minor software release, hardware upgrade, or an emergency, Intel AMT and Intel EMA can help deploy to more systems faster, with less manual intervention, regardless of environment. Deployments can be initiated, monitored, and controlled with minimal disruption to the end user.

Upgrading operating systems can be the most challenging, yet patching and updating are common activities. With hardware-based KVM, Intel AMT and Intel EMA provide the ability to monitor an update process or wake up a device and update it, regardless of its power state, which helps improve security and reliability.

User Interface Examples

Intel EMA enables administrators to monitor and manage both in-band and out-of-band controls on remote devices, providing opportunities within the operating system (see Figure 5).

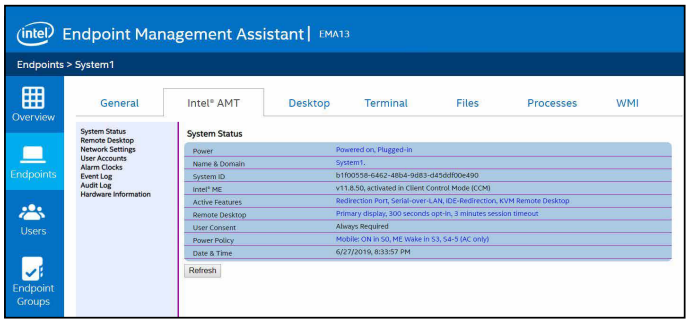

Figure 5. Administrators can review system status and configuration (example shows out-of-band devices).

Intel EMA allows administrators to execute commands through scripts, such as Power On to wake a device (see Figure 6).

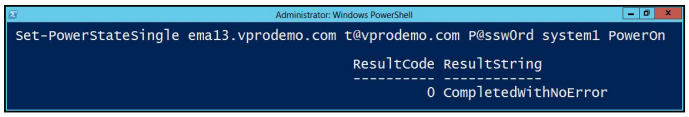

Figure 6. Using a task automation and configuration management framework script (from Microsoft), Intel® EMA controls power functions through the API (example shows out-of-band devices).

Summary

Intel AMT provides a solid foundation for remote management of both user-facing devices and smart connected devices, and Intel EMA extends that capability beyond the corporate firewall. Working within existing business processes and supported by leading IT management tools, Intel AMT helps IT organizations tackle the increasing complexity in their managed device fleets, without complicating their management infrastructure. By providing remote access to devices, no matter where they are, even when powered off or without a functioning operating system, Intel AMT with Intel EMA helps enable faster incident resolution and helps reduce the overall operating cost of the service desk. Intel AMT streamlines common IT activities such as user self-service, patching and upgrading, machine recovery and re-imaging, and configuration auditing. Intel AMT has been a part of the Intel vPro platform for over a decade, and can be activated using a variety of solutions.

References

- Intel® Active Management Technology
- Intel vPro® Platform
- Intel® AMT Software Development Kit Home Page
- Managed Service Providers

[1] Nihar Pachpande, March 18, 2018, "50 Billion Connected Devices by 2020."

[2] IDC Forecasts U.S. Mobile Worker Population to Surpass 105 Million by 2020.

[3] Intel® EMA supports Intel® AMT versions 11.x and higher. Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com/AMT.

[4] "The Total Economic Impact of the Intel vPro Platform" is a study commissioned by Intel and conducted by Forrester Consulting, December 2018. The study states that savings other organizations will receive will vary based on a variety of factors including size and baseline level of security, manageability, and productivity before the business switched to the Intel vPro® platform. Consult other sources and use information specific to your organization to determine benefits for your organization.

[5] Annual reduction of 7,680 security support hours with Intel vPro® platform-based devices, resulting in USD 1.2 million in savings over 3 years as estimated using a composite organization modeled by Forrester Consulting in an Intel-commissioned TEI study (December 2018). Read the full study, "The Total Economic Impact of the Intel vPro Platform."

[6] 28,160 hours saved in improved employee efficiency with the Intel vPro® platform through better device security and management, resulting in cost savings of USD 1.3 million over 3 years as estimated using a composite organization modeled by Forrester Consulting in an Intel-commissioned TEI study (December 2018). Read the full study, "The Total Economic Impact of the Intel vPro Platform."

[7] 832 hours saved with automatic remote patch deployment through Intel® Active Management Technology, resulting in an estimated cost savings of USD 81,000 over 3 years as estimated using a composite organization modeled by Forrester Consulting in an Intel-commissioned TEI study (December 2018). Read the full study, "The Total Economic Impact of the Intel vPro Platform."

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Intel® Active Management Technology requires activation and a system with a corporate network connection, an Intel Active Management Technology-enabled chipset, and network hardware and software. For notebooks, Intel Active Management Technology may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating, or powered off. Results dependent upon hardware, setup, and configuration. For more information, visit intel.com/AMT.

 0819/TCUT/KC/PDF 334533-003US