Executive Summary
Intel vPro technology provides powerful out-of-band management and remote remediation capabilities enabling IT organizations to reduce costly desk side visits, improve end-user and IT employee productivity and improve client security posture. Organizations using, or considering using, these out-of-band management and remote remediation capabilities may be required to audit their IT operations. This whitepaper explores options available in environments containing Microsoft System Center* 2012 Configuration Manager, McAfee ePolicy Orchestrator*, RealVNC VNC* Viewer Plus and Windows PowerShell® for auditing Intel vPro technology out-of-band management and remote remediation operations.

Introduction
Intel vPro technology based systems include Intel® Active Management Technology (Intel® AMT), a hardware management capability allowing systems to be remotely managed regardless of their power state or host Operating System state. In the typical scenario, management applications send out-of-band operations via the network to an Intel AMT controller (embedded in Intel vPro technology based systems) to remotely perform actions such as power control, boot device selection, redirection of peripherals such as keyboard, video, mouse, serial port and IDE boot devices. The ability to remotely perform these types of actions enables IT organizations to implement use cases such as remotely powering up systems outside of business hours to distribute software updates without interrupting users and remotely remediating non-booting systems to reduce costly and time consuming desk-side visits.

Whilst exploring options for auditing IT operations that use Intel AMT, this paper considers the following characteristics, components and scenarios...

- Management and security software suites such as Microsoft System 2012 Center Configuration Manager and McAfee ePolicy Orchestrator include built-in reporting and auditing capabilities.

- Multiple applications that are capable of initiating Intel AMT out-of-band management and configuration operations will be present in the environment. Examples include
Auditing IT Operations That Use Intel® Active Management Technology

manageability and security software application suites, the Intel AMT WebUI and firmware based Manageability Engine BIOS Extension (MEBX) built into Intel vPro systems.

- Applications can initiate Intel AMT out-of-band management and configuration operations through remote or local interfaces. Remote interfaces include wired and wireless LAN. Local interfaces include the Local Manageability Service (LMS) and Intel Manageability Engine (MEI) interface.

- Intel AMT maintains a local access control list (ACL) and all out-of-band management and configuration operations are authenticated and authorized before they are executed.

- Intel AMT includes an access monitor capability that can be configured to log events for out-of-band operations and significant configuration operations regardless of where those operations were initiated from\(^1\). Events are stored in a local embedded firmware based Intel AMT audit log where they can be read by an auditor.

Microsoft System Center 2012 Configuration Manager and Intel Active Management Technology

Microsoft System Center 2012 Configuration Manager (SCCM) includes native out-of-band management support for systems based on Intel AMT versions 3.2.1 and above\(^2\). Support is included for many popular out-of-band management capabilities including remote power control, real-time hardware inventory, boot device control and text based console and IDE storage device re-direction. Not all Intel AMT capabilities are natively supported by SCCM; capabilities such as Intel® KVM technology require additional applications to utilize these capabilities.

Microsoft SCCM 2012 includes native provisioning support for Intel AMT versions 3.2.1 through 8.X\(^2\). Intel AMT versions 9.X and above cannot be natively provisioned by SCCM 2012 and must be provisioned using other software, typically the Intel® Setup and Configuration Service (Intel® SCS) software. To avoid the complexity of operating multiple provisioning solutions and provisioning Intel AMT systems based on their version, the suggested provisioning approach is to use Intel SCS to provision all Intel AMT systems and SCCM’s capability to discover out-of-band support on Intel AMT systems that have been externally provisioned (in this case by Intel SCS). Once externally provisioned Intel AMT systems have been discovered, SCCM’s native out-of-band management capabilities can be used with these systems.

Auditing Intel AMT Operations with Microsoft SCCM 2012 and SCCM Status Messages

Microsoft SCCM 2012 automatically generates status messages that can be used for auditing

---

\(^1\) Intel AMT Access Monitor requires Intel AMT version 4.0 or later

\(^2\) Exact versions of Intel AMT firmware validated with Microsoft SCCM 2012 may differ from the versions stated here
Auditing IT Operations That Use Intel® Active Management Technology

out-of-band operations initiated by SCCM. Queries can be constructed from the SCCM console to retrieve and view status messages of interest and construct audit trails.

The example query shown in Figure 1 can be used to retrieve audit type status messages related to configuration of the out-of-band management component, operations initiated from the out-of-band service point (such as Intel AMT discovery, provisioning, power control) and operations initiated from the separate SCCM out-of-band management console (such as power and boot control, real time hardware inventory and redirection).

The output from this query contains the SCCM site code, time and date stamp information, the originating SCCM component, a detailed description of the event, the user responsible for initiating the event and the target system of the operation where applicable. An example of the output is shown in Figure 2. This information can be exported in tab delimited format to a file for further processing or archiving.
Depending on the audit requirements of the organization, the previous example query can easily be modified to refine the audit information retrieved to produce separate audit trails for configuration activities, software distribution and remote client remediation using out-of-band operations. The example in Figure 3 and resulting output in Figure 4 show how this could be done to audit operations initiated using the SCCM out-of-band management console.
In summary, using SCCM status messages to audit Intel AMT out-of-band operations is simple to implement and provides relevant information for auditing out-of-band operations initiated by SCCM or the SCCM out-of-band console.

Other applications that initiate Intel AMT out-of-band management or configuration operations (e.g. Intel® KVM technology, McAfee’s ePolicy Orchestrator, the Intel AMT WebUI or local MEBX) do not generate SCCM status messages, therefore these status messages cannot be used to audit other applications. The next section explores using the Intel AMT access monitor with Microsoft SCCM 2012 to audit other out-of-band applications.

Auditing Intel AMT Operations with Microsoft SCCM 2012 and the Intel AMT Access Monitor

Microsoft SCCM 2012 can read the Intel AMT audit log from Intel AMT systems that have been natively or externally provisioned.

Intel AMT audit log entries are read using the SCCM out-of-band management console. The console displays all logged events regardless of whether they were initiated by SCCM or other applications. For out-of-band operations and significant configuration events that are natively supported by SCCM, the console is capable of decoding these events into an easily understood format that includes a time and date stamp, the IP source address from where the event was initiated, the event description, the credentials of the event initiator and, where appropriate, extended data that can be used to obtain additional event context information. Figure 5 shows an example of the information available. The console also indicates if the audit log is currently enabled on the Intel AMT system and used event log space which can be used to determine if
Auditing IT Operations That Use Intel® Active Management Technology

the audit log should be cleared.

Figure 5 – SCCM Out-of-Band Console Showing Intel AMT Audit Log and SCCM Initiated Operations

Intel AMT audit log entries read using the SCCM out-of-band management console can be exported in CSV format to a file for aggregation with log files from other clients, further processing or archival.

Reading Intel AMT audit log entries using the SCCM out-of-band management console is a manual process and is performed against an individual system. For automated reading of Intel AMT audit log entries a scheduled scripting approach can be used.

The SCCM out-of-band management console does not fully decode Intel AMT audit log entries for out-of-band operations and significant configuration events that are not natively supported by SCCM (e.g. Intel® KVM technology and user consent related events). These entries are displayed with a time and date stamp and IP source address indicating where the event was initiated from but no further information is displayed. Figure 6 shows an example of this.

Figure 6 – SCCM Out-of-Band Console Showing Intel AMT Audit Log and Operations Initiated Outside of SCCM

Microsoft SCCM 2012 can configure Intel AMT access monitor event logging policies and enable, disable and clear the Intel AMT audit log on Intel AMT systems that have been natively
Auditing IT Operations That Use Intel® Active Management Technology

provisioned but not on those that have been externally provisioned.

Policy settings defining out-of-band operations and significant configuration events to be logged can be configured from the SCCM console using the audit log settings located under the SCCM out of band management component properties. Figure 7 shows the available settings.

Figure 7 – SCCM Policy Settings for the Intel AMT Access Monitor

Available policy settings cover Intel AMT out-of-band management capabilities natively supported by SCCM but do not cover all Intel AMT out-of-band capabilities. Intel KVM technology and user consent event logging policies for example cannot be configured by SCCM.

The lack of native SCCM support for configuring Intel KVM technology and user consent event logging policies and the restriction SCCM imposes of only configuring event logging policies on natively provisioned systems is not a problem for systems based on Intel AMT versions 8.0 and above because these versions implicitly enable logging of these events (and most others) when they are provisioned. For systems based on Intel AMT versions 7.0 or below, other applications can be used to configure and enable event logging.

If the policy settings defined in the SCCM console are used to configure the Intel AMT access monitor despite the restrictions discussed previously, they must either be applied manually to individual systems from the SCCM console or applied programmatically using the SCCM WMI provider. The code snippet shown in Figure 8 is an example of PowerShell code that can be used to apply policy settings using the SCCM WMI provider; the same functionality could be coded using VBScript or other languages. Programmatic methods of applying policy settings can be automated by scheduling code to run regularly on a server or by packaging and distributing code to Intel AMT systems that have been provisioned by SCCM.

The same manual or programmatic approach must also be used to disable or clear the Intel
Auditing IT Operations That Use Intel® Active Management Technology

AMT audit log from SCCM.

Figure 8 – Sample PowerShell Code for Applying SCCM Policy Settings for Intel AMT Access Monitor

In summary, using Microsoft SCCM 2012 and the Intel AMT access monitor to audit Intel AMT out-of-band operations offers advantages over using only SCCM status messages. Out-of-band operations that are natively supported by SCCM can be audited, even when they are not initiated by SCCM, which is useful in mixed environments where out-of-band applications other than SCCM may be in use (e.g. an Intel KVM technology viewer, McAfee’s ePolicy Orchestrator or the Intel AMT WebUI). Local MEBX activities can also be audited.

Not all Intel AMT access monitor policy settings or Intel AMT audit log entries are capable of being configured or interpreted by SCCM which could be a limitation in environments where Intel AMT capabilities such as Intel KVM technology or user consent are in use. Manual reading and clearing of Intel AMT audit logs could be a limitation in large environments where automation is required to minimize IT workload. The section Windows PowerShell and Intel Active Management Technology later in this document explores using Windows PowerShell scripting to support all Intel AMT access monitor policy settings, audit log entries and IT automation.

McAfee ePolicy Orchestrator and Intel Active Management Technology

McAfee ePolicy Orchestrator (ePO) requires the addition of McAfee ePO Deep Command to support out-of-band management using Intel AMT versions 4.0 and later. Support is included for many popular out-of-band management capabilities including remote power control, boot device control, text based console and IDE storage device re-direction, hardware alarm clock, Intel KVM technology and out-of-band management of Intel AMT systems located outside the corporate firewall. McAfee Device Encryption can also take advantage of out-of-band management to remotely unlock encrypted hard drives, reset passwords and remediate corrupted master boot records.

McAfee ePO Deep Command integrates Intel SCS software for provisioning Intel AMT systems and supports remote configuration (using provisioning certificates) and host based

---

3 Exact versions of Intel AMT firmware validated with McAfee ePO Deep Command may differ from the versions stated here

4 Some Intel AMT out-of-band management features require specific versions of Intel AMT firmware or later
Auditing IT Operations That Use Intel® Active Management Technology

configuration.

Auditing Intel AMT Operations with McAfee ePO Deep Command 2.1 and McAfee ePO Audit Messages

McAfee ePO Deep Command automatically generates audit messages that can be used for auditing out-of-band operations initiated from the ePO console. Queries can be constructed from the ePO console to retrieve and view audit messages of interest and construct audit trails.

The example query shown in Figure 9 can be used to retrieve audit messages related to configuration of out-of-band management components (such as credentials, policies, provisioning operations, tagging etc) and out-of-band management operations initiated from the ePO console (such as power and boot control, user consent, text based and IDE storage redirection).

![Figure 9 – McAfee ePO Query Statement for All Intel AMT Out of Band Operations](image)

The output from the query contains the user responsible for initiating the event, the action, the result of the action (success or failure), time and date stamp information and a detailed description of the event include the target system of the operation where applicable. An example of the output is shown in Figure 10. This information can be exported in a number of different formats including CSV, XML or PDF for aggregation, further processing or archiving.
Auditing IT Operations That Use Intel® Active Management Technology

Figure 10 – Output from McAfee ePO Query Statement for All Intel AMT Out of Band Operations

Depending on the audit requirements of the organization, the example query can easily be modified to refine the audit information retrieved. The example query in Figure 11 and resulting output in Figure 12 show how this could be done to audit Intel AMT configuration operations initiated from the ePO console.
In summary, using ePO audit messages to audit Intel AMT out-of-band operations is simple to implement and provides relevant information for auditing out-of-band operations initiated from the ePO console.
Auditing IT Operations That Use Intel® Active Management Technology

McAfee’s KVMView application (used for Intel KVM technology and part of the Deep Command product) or other applications that initiate Intel AMT out-of-band management or configuration operations (e.g. Microsoft System Center 2012 Configuration Manager, the Intel AMT WebUI or local MEBX) do not generate ePO audit messages, therefore these audit messages cannot be used to audit other applications. The next section Windows PowerShell and Intel Active Management Technology explores using the Intel AMT access monitor to audit KVMView and other applications.

Windows PowerShell and Intel Active Management Technology

The Intel vPro Technology Module for Windows PowerShell software enables Intel AMT out-of-band management and configuration operations to be initiated from Windows PowerShell scripts. The Intel vPro PowerShell module is a loadable PowerShell module that includes a set of pre-written cmdlets and a PowerShell drive for accessing functionality on provision Intel AMT systems based on Intel AMT versions 3.2.1 and later.

In addition to providing pre-written cmdlets and a PowerShell drive, the Intel vPro PowerShell module also exposes a set of objects allowing custom cmdlets to be created to perform out-of-band management operations when the pre-written cmdlets do not provide the required functionality. The exposed objects abstract the complexity of the underlying WS-MAN protocol used to communicate with Intel AMT systems allowing custom cmdlet creators to focus on functionality rather than low level protocol details.

Auditing Intel AMT Operations with the Intel vPro Technology Module for Windows PowerShell

The pre-written cmdlets and PowerShell drive included with the Intel vPro PowerShell module provide support for reading the Intel AMT audit log and policy settings defining the out-of-band operations and significant configuration events to be logged.

Intel AMT audit log entries can be read from provisioned Intel AMT systems using the `Get-AMTAccessMonitor` cmdlet, or a PowerShell drive can be mapped to Intel AMT systems and the `Get-Content` cmdlet used. Objects returned by `Get-AMTAccessMonitor` contain the computer name of the Intel AMT system from which the audit log is being read, a time and date stamp, a message describing the event, the IP source address from where the event was initiated and the credentials of the event initiator. Objects returned by `Get-Content` contain additional information including the application and event ID responsible for generating the event. Figure 13 shows an example of the resulting output from `Get-AMTAccessMonitor`. This information can be piped to other PowerShell cmdlets for further processing or written to a file.

---

5 Exact versions of Intel AMT firmware validated with the Intel vPro Technology Module for Windows PowerShell may differ from the versions stated here.
Policy settings defining out-of-band operations and significant configuration events to be logged can be inspected by mapping a PowerShell drive to provisioned Intel AMT systems and using the `Get-ChildItem` cmdlet. Figure 14 and Figure 15 show examples of PowerShell code and resulting output.

![Figure 13 – Output from Intel vPro PowerShell Drive and Get-Content Cmdlet](image)

![Figure 14 - Sample PowerShell Code for Reading Intel AMT Access Monitor Policy Settings](image)
In summary, the pre-written cmdlets and PowerShell drive included with the Intel vPro PowerShell module offer a rapid route for reading the Intel AMT audit log and Intel AMT access monitor policies from PowerShell scripts and providing relevant information for auditing out-of-band operations initiated by any application or the local MEBX. The pre-written cmdlets and PowerShell drive are supplied on an “as-is” basis.

The pre-written cmdlets are not capable of decoding all Intel AMT audit log entries (i.e. the messages returned for some events contain only application and event ID information rather than descriptive text) and extended data is not returned to provide context information for certain events. The PowerShell drive does not allow Intel AMT access monitor policies to be disabled and the Intel AMT audit log cannot be explicitly cleared, locked or signed. The next section explores using the Intel AMT System Development Kit with Windows PowerShell and the Intel vPro PowerShell module to create custom cmdlets to access all Intel AMT access monitor functionality for auditing Intel AMT operations.

Auditing Intel AMT Operations with Windows PowerShell and the Intel AMT System Development Kit

The Intel AMT System Development Kit (SDK) includes documentation and a set of PowerShell code snippets that can be used with the Intel vPro Technology Module for Windows PowerShell as the basis for a set of custom PowerShell cmdlets for accessing all Intel AMT access monitor functionality for auditing Intel AMT operations.

An example `Get-AMTAuditLog` cmdlet demonstrates how to read and return audit log entry objects containing the computer name of the Intel AMT system from which the audit log is being read, the IP source address from where the event was initiated, a time and date stamp,
Auditing IT Operations That Use Intel® Active Management Technology

the credentials of the event initiator, the application and event ID’s which correspond to the type of event and extended data containing additional context information about the event. Figure 16 shows an example of the output.

![Figure 16 – Output from PowerShell Get-AMTAuditLog Cmdlet](image)

PowerShell’s piping capability enables other standard PowerShell cmdlets and operators to be used to transform “raw” Intel AMT audit log output into something that is easily readable for audit purposes. Figure 17 shows the “raw” Intel AMT audit log output after it has been piped through code to convert user information from SID format into Windows credential format and decode the application and event ID information into human readable event descriptions.
Because these transformation operations use standard PowerShell cmdlets and operators, they can easily be coded to support the exact requirements of an organization and updated to support events introduced with future Intel AMT versions.

The example Get-AMTAuditPolicy, Enable-AMTAuditPolicy and Disable-AMTAuditPolicy cmdlets demonstrate how to manipulate Intel AMT access monitor policy settings that define out-of-band operations and significant configuration events to be logged. Figure 18 shows an example of the output from reading the policy settings. Because cmdlets communicate directly with the application programming interface defined in the Intel AMT SDK, all policies can be configured regardless of the Intel AMT versions in use.
In addition to manipulating policy settings that define out-of-band operations and significant configuration events to be logged, custom PowerShell cmdlets can be created to control storage policy for the Intel AMT firmware audit log. Storage policy can be configured so that the audit log wraps when full, never wraps or only wraps for events that have been defined as non-critical. This helps balance the burden of regularly reading and clearing the audit log with the demand not to lose critical events should the log become full.

Custom PowerShell cmdlets can be created to perform a number of other important tasks for managing the Intel AMT access monitor and audit log. These include Enable-AMTAuditing and Disable-AMTAuditing for enabling and disabling the log, Clear-AMTAuditLog for clearing the log (to prevent overflow or possible blocking of operations), Lock-AMTAuditLog and Unlock-AMTAuditLog for locking and unlocking the log (to prevent corruption whilst reading or clearing the log and to allow un-provisioning of Intel AMT systems with losing audit log contents) and Set-AMTAuditLogSigningKey and Get-AMTAuditLogSignature for configuring content signing material if the audit log integrity must be verified.

In summary, using the Intel AMT SDK with the Intel vPro PowerShell module to create custom PowerShell cmdlets requires some scripting effort but enables all the Intel AMT access monitor capabilities to be used to support a comprehensive approach for auditing out-of-band operations initiated by any application or the local MEBX. Use of a standard scripting language provides flexibility and the ability to upgrade the solution to support any auditable events added in future Intel AMT versions.
Auditing IT Operations That Use Intel® Active Management Technology

Summary
Microsoft System Center 2012 Configuration Manager (SCCM) and McAfee ePolicy Orchestrator both include native audit message logging, querying and reporting capabilities that can easily be used to audit Intel AMT out-of-band management or configuration operations initiated from those product suites.

In mixed application environments where Intel AMT out-of-band operations are initiated by multiple applications (e.g. Microsoft SCCM 2012 or McAfee ePO Deep Command and VNC RealVNC Viewer Plus), or where there is a requirement to audit operations initiated using the local MEBX, the Intel AMT access monitor built into Intel vPro based systems can be used. Microsoft SCCM 2012 includes some support for the Intel AMT access monitor and is capable of manually reporting audit information for Intel AMT out-of-band functionality natively supported by SCCM (e.g. remote power control, real-time hardware inventory, boot device control and text based console and IDE storage device re-direction) regardless of which applications initiate these operations.

Complete support for using the Intel AMT access monitor to audit all Intel AMT out-of-band operations and configuration events, and for automating the related processes, can be achieved with some scripting effort by using the Windows PowerShell scripting language and custom cmdlets in conjunction the Intel vPro Technology Module for Windows PowerShell and Intel AMT SDK.

References


Auditing IT Operations That Use Intel® Active Management Technology

Information in this document is provided in connection with Intel products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's terms and conditions of sale for such products, Intel assumes no liability whatsoever and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right.

Unless otherwise agreed in writing by Intel, the Intel products are not designed nor intended for any application in which the failure of the Intel product could create a situation where personal injury or death may occur.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at www.intel.com.

Intel® vPro™ technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit http://www.intel.com/technology/vpro.

Intel® Active Management Technology requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT 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® Active Management Technology.

Copyright © 2014 Intel Corporation. All rights reserved. Intel, the Intel logo and Intel vPro are trademarks of Intel Corporation in the U.S. and/or other countries.

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