Start Here Guide

INTEL® ACTIVE MANAGEMENT TECHNOLOGY (INTEL® AMT)

Start Here Guide

CONTENTS

1 Getting Started 4

1.1 What is Intel® Active Management Technology? 4

1.1 Preparing your Intel® AMT Client for use 6

2 Manual Configuration Tips 7

2.1 Manual Setup 8

3 Client Control Mode and Admin Control Mode 8

3.1 Client Control Mode Limitations 8

3.2 Manually Configuring an Intel AMT 7.0 Client 9

3.3 Manually Configuring an Intel AMT 8.0 Client 10

4 Accessing Intel® AMT via the WebUI Interface 10

5 Intel® AMT Drivers and Services 11

5.1 NIC: Intel 82577LM Network Interface Controller 11

5.2 Intel® Management Engine Interface 12

5.3 Serial-Over-LAN (SOL) Driver 12

5.4 Intel® Active Management Technology LMS Service 13

5.5 Intel® AMT User Notification Service 13

5.6 Intel Management and Security Status Tool 14

6 Intel® AMT Software Development Kit (SDK) 16

6.1 Other SDK Resources 17

Appendix A: 19

A.1 Intel® AMT Release 2.0/2.1/2.2 Architecture 22

A.2 Intel® AMT Release 2.1Improvements 24

A.3 Intel® AMT Release 2.2 Improvements 24

A.4 Intel® AMT Release 2.5/2.6 Architecture 24

A.5 Intel® AMT Release 3.0 Architecture 25

A.6 Intel® AMT Release 4.0 Architecture 25

A.7 Intel® AMT Release 5.0 Architecture 26

A.8 Intel® AMT Release 5.1 Architecture 26

A.9 Intel® AMT Release 6.0 Architecture 26

A.10 Intel AMT Release 7.0 and 8.0 Architecture 27

A.10.1 Host-Based Setup and Configuration 27

A.10.2 Snippets Added to Intel AMT Feature Use Cases 27

A.10.3 KVM 28

A.10.4 Redirection Library 28

A.10.5 Intel(R) vPro(TM) Gateway, also known as the Management Presence Server (MPS) 28

A.10.6 Digest Master Password 28

A.10.7 Deprecated EOI (SOAP) Samples Moved 29

This document contains information that aids developers in getting started with implementing Intel® Active Management Technology (Intel® AMT). It provides an overview of the features in various versions of Intel® AMT, as well as information on minimum system requirements, configuration of an Intel® AMT client, and the various developer tools that are available to help program for Intel® AMT.

Intel® AMT supports remote applications running on Microsoft Windows* or Linux*. Intel® AMT Release 1.0 supports both Linux and Windows local applications. Intel® AMT Release 2.0 and higher support only Windows-based local applications. For a complete list of system requirements, please refer to the documentation in the latest Intel® AMT Software Development Kit (SDK).

The following paragraphs summarize what is new in Intel® AMT 8.0. For a full comparison of all features across Intel AMT, see Appendix A:

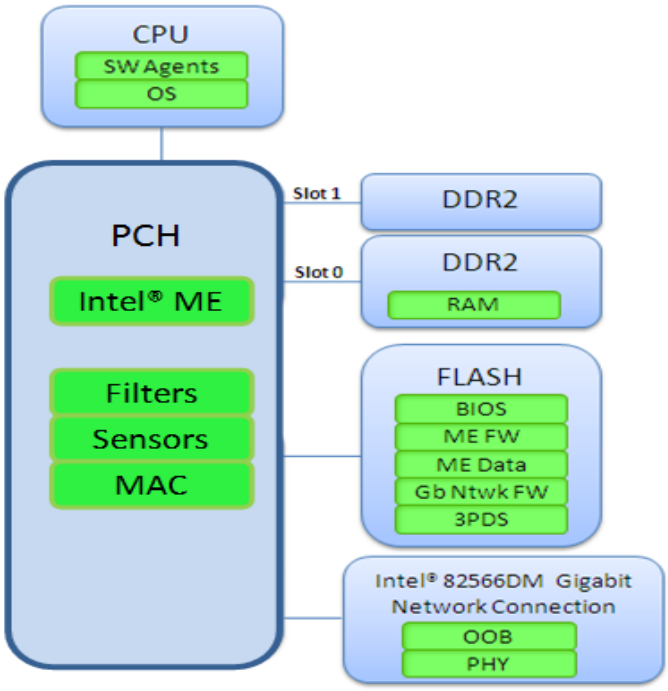
1 GETTING STARTED

In order to begin compiling or running samples from the SDK, you will need a separate system to use as a management console for remotely managing your Intel® AMT client. For more detailed explanations, please refer to the *Intel® AMT Implementation and Reference Guide* located in the *Docs* folder of the Intel® AMT SDK (Release 8.0).

1.1 WHAT IS INTEL® ACTIVE MANAGEMENT TECHNOLOGY?

Intel® AMT is part of the Intel vPro Technology offering. Platforms equipped with Intel AMT can be managed remotely, regardless of whether they are powered up and regardless of whether or not they have a functioning OS.

The Intel® ME is the steam behind Intel Active Management Technology. Intel AMT is a component of the Intel vPro platform. It uses a number of elements in the Intel vPro platform Architecture. The following figure shows the relationship between these elements.



The Intel AMT functionality is contained in the ME firmware (Manageability Engine Firmware).

- The firmware image is stored in the Flash memory.

- The Intel AMT capability is enabled using the Intel® Management Engine (Intel® ME) BIOS extension as implemented by an OEM platform provider. A remote application can be used to perform enterprise setup and configuration
- On power-up, the firmware image is copied into the Double Data Rate (DDR) random-access memory (RAM).
- The firmware executes on the Intel ME processor and uses a small portion of the DDR RAM (Slot 0) for storage during execution. RAM slot 0 must be populated and powered on for the firmware to run.
- Intel AMT stores the following information in the Flash **(ME Data)**:
- OEM-configurable parameters
- Setup and configuration parameters such as passwords, network configuration, certificates, and access control lists (ACLs)
- Other configuration information, such as lists of alerts and System Defense policies
- The hardware configuration captured by the BIOS at startup

2012 Intel® vPro Technology Platform details are as follows:

- Process is 22nm
- Mobile Platforms are codenamed "Chief River"
- Desktop Platforms are codenamed "Maho Bay"
- CPU: Ivy Bridge
- PCH: Panther Point

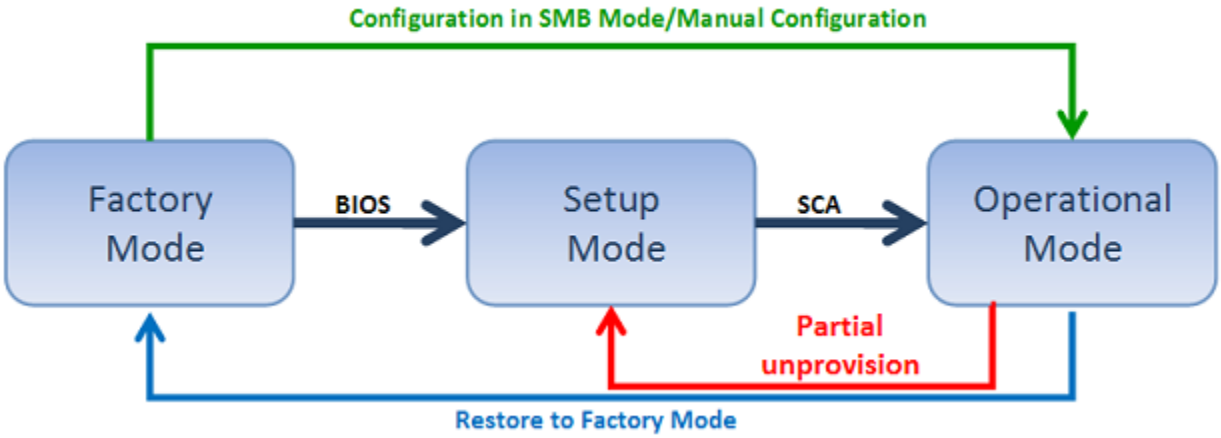
Intel® AMT Release 8.0 adds the following features to Intel AMT:

- The Intel® Small Business Technology (Intel® SBT) platform has been introduced providing in-band host-based management. See the *Intel® Small Business Technology Platform* section in the Intel® AMT SDK (Release 8.0).
- • The Access Monitor feature has been simplified to make it easier to use. Among other things, multiple admin users can perform auditor functions until an audit user is identified. Also, there is a pre-defined list of auditable events, to save having to enable events. See the "*Comparison of Access Monitor Pre-8.0 and Release 8.0"* section in the Intel® AMT SDK (Release 8.0).
- The wired 802.1x configuration interface has been revised to support a CIM-compliant format. See "*802.1x Profile Configuration*" section in the Intel® AMT SDK (Release 8.0).

- Agent presence alerts now contain the agent GUID as a string so that an application can easily identify which agent triggered the alert.

1.1 PREPARING YOUR INTEL® AMT CLIENT FOR USE

The following diagram illustrates the modes or stages that an Intel® AMT device passes through before it becomes operational.



Before an Intel® AMT device can receive its configuration setting from the Setup and Configuration Application (SCA), it first must be prepared with initial setup information and placed into Setup Mode. The initial information will be different, depending on the available options in the Intel® AMT release and the settings performed by the platform OEM. The following table summarizes the methods you can use to perform setup and configuration on the different releases of Intel® AMT.

Setup Method	Applicable to Intel® AMT Releases	For More Information See...
Legacy	1.0; Releases 2.x and 3.x in legacy mode	Setup and Configuration in Legacy Mode
SMB	2.x, 3.x, 4.x, 5.x	Setup and Configuration in SMB Mode
PSK	2.0 and later	Setup and Configuration Using PSK

PKI	2.2, 2.6, 3.0 and later	Setup and Configuration Using PKI (Remote Configuration)
Manual	6.0 and later	Manual Setup and Configuration (from Release 6.0)
CCM, ACM	7.0 and later	Client Control Mode and Admin Control Mode Manually Configuring Intel AMT 7.0 and Intel AMT 8.0 Clients

Note that the Intel Setup and Configuration Software (Intel SCS) is capable of provisioning systems back to Intel AMT 2.X. For more information about the Intel® Setup and Configuration Service and provisioning methods as they pertain to the various Intel AMT Releases, visit the download page: Download the latest version of Intel® Setup and Configuration Service (Intel® SCS)

2 MANUAL CONFIGURATION TIPS

From release 6.0 there are no feature limitations when configuring a platform manually, but there are some system behaviors to be noted:

- API methods will not return a PT_STATUS_INVALID_MODE status, as there is only one mode.
- TLS is disabled by default and should be explicitly enabled during configuration. This will always be the case with manual configuration, as there is no way to set TLS parameters locally.
- The local platform clock will be used until the network time is set remotely. Automatic configuration will not complete successfully unless network time was set, only when TLS or Kerberos was configured. Enabling TLS or Kerberos after configuration completion will not succeed if the network time was not set.
- WEBUI is enabled by default, unless a configuration server disables it.
- SOL and IDE-R are enabled by default, but the redirection listener is disabled by default.

If KVM is enabled locally via the MEBx, it still will not be enabled until an administrator activates it over the network.

2.1 MANUAL SETUP

During power up, the Intel® AMT platform first displays the BIOS startup screen, and then the BIOS Extensions are processed. Entry into the Intel® AMT BIOS Extension is BIOS vendor dependent. Some OEM platforms display a screen prompting you to press <Ctrl+P>. When you press <Ctrl+P> control passes to the Intel® Management Engine BIOS extension (MEBx) Main Menu. Some OEMs integrate the MEBx configuration inside the BIOS and some OEMs have an option in the BIOS to show/hide the <Ctrl+P> prompt.

3 CLIENT CONTROL MODE AND ADMIN CONTROL MODE

When any method of setup completes, Intel AMT 7.0 and Intel AMT 8.0 are placed into one of two control modes. The modes are:

- Client Control Mode – Intel AMT enters this mode after performing a basic host-based setup (see Host-Based (Local) Setup). This mode limits some of Intel AMT functionality, reflecting the lower level of trust required to complete a host-based setup.
- Admin Control Mode – After performing any of the existing setup and configuration methods – remote setup (TLS-PSK or remote configuration) or a manual setup via the MEBx – Intel AMT enters Admin Control Mode. Also, performing a host-based AdminSetup before any provisioning was done or an UpgradeClientToAdmin when Intel AMT is already in Client Control mode moves Intel AMT to Admin Control mode. In this mode, there are no limitations to Intel AMT functionality. This reflects the higher level of trust associated with these setup methods.

3.1 CLIENT CONTROL MODE LIMITATIONS

When a simple host-based configuration completes, the platform enters Client Control Mode, which imposes the following limitations:

1. The System Defense feature is not available.
2. Redirection (IDE-R and KVM) actions (except initiation of an SOL session) and changes in boot options (including boot to SOL) require user consent in advance (see User Consent). This still enables IT support personnel to remotely resolve end-user problems using Intel AMT.
3. If an Auditor user is defined, the Auditor's permission is not required to perform unprovisioning.

4. A number of functions are blocked from execution to prevent an untrusted user from taking over control of the platform.

3.2 MANUALLY CONFIGURING AN INTEL AMT 7.0 CLIENT

During power up, the Intel AMT platform first displays the BIOS startup screen, and then the BIOS Extensions are processed. Entry into the Intel AMT BIOS Extension is BIOS vendor dependent. Intel AMT reference platforms display a screen prompting you to press <Ctrl+P>. When you press <Ctrl+P> control passes to the Intel® Management Engine BIOS extension (MEBx) Main Menu.

Perform the following steps to perform manual setup:

1. Enter the MEBx default password ("admin")
2. Change the default password to a new value (this step is required in order to proceed). The new value must be a "strong" password: It should contain at least one upper case letter, one lower case letter, one digit and one special character, and be at least eight characters. A management console application can change the Intel AMT password without modifying the MEBx password.
3. Select **Intel(R) AMT** Configuration.
4. Select **Manageability Feature Selection**.
5. Select ENABLED to enable Intel(R) AMT.
6. Exit to the Main Menu.
7. Select **Intel(R) ME General Settings**.
8. The default setting for IP address acquisition is to use a DHCP server. If you are setting the platform IP address manually perform the following steps:
   a. Select **Network Setup**.
   b. Select **TCP/IP Settings**.
   c. Select **Wired LAN IPV4** Configuration.
   d. Select **DHCP Mode**.
   e. Set the mode to DISABLED.
   f. Once the DHCP mode is set to DISABLED, the static IPv4 options appear. Select **IPv4 Address** and enter an IP address.
   g. Select **Subnet Mask Address** and enter a subnet mask.
   h. Set other parameters as required.
   i. Exit to the ME General Settings menu.
9. Return to the **Intel(R) AMT Configuration** menu; Select **SOL/IDE-R**, select **Legacy Redirection Mode** and select ENABLED to enable the redirection listener. This can ensure compatibility with management consoles created to work with the legacy SMB mode and do not have a mechanism implemented to enable the listener.
10. Return to the **Intel(R) ME General Settings** menu. Select **Activate Network Access**. Press <Y> in response to the confirmation message.

The platform is now configured. You can set additional parameters using the web interface or a remote console.

3.3 MANUALLY CONFIGURING AN INTEL AMT 8.0 CLIENT

During power up, the Intel AMT platform first displays the BIOS startup screen, and then the BIOS Extensions are processed. Entry into the Intel AMT BIOS Extension is BIOS vendor dependent. Intel AMT reference platforms display a screen prompting you to press <Ctrl+P>. When you press <Ctrl+P> control passes to the Intel® Management Engine BIOS extension (MEBx) Main Menu.

Many of the menus are the same from Intel AMT 7.0 to Intel AMT 8.0. Perform the following steps to perform manual setup:

1. Review the steps above for configuring an Intel® AMT 7.0 system. It is still necessary to verify that SOL/IDER/KVM and Power Control settings are as desired. Also if static IP addresses are required then those will need to be set up in the MEBx menus as well.
2. From the main menu, select **Intel(R) ME General Settings**.
   a. Select **Manageability Feature Selection** and make sure it is "enabled."
3. Exit to the Main Menu.
4. Go into the **Intel(R) AMT Configuration** menu.
   a. Select **Activate Network Access**. Press <Y> in response to the confirmation message.

The platform is now configured. You can set additional parameters using the web interface or a remote console. For a video on Configuring and Un-configuring an Intel AMT 8.0 Client via the MEBx menus see this blog on the ISN Network: **Video: How to Configure and Un-configure an Intel® vPro™ technology client (Intel® AMT) inside the MEBx Menus**

Note that configuring the Intel AMT Client via the MEBx menus will result in the system being in ***Admin Control Mode***.

4 ACCESSING INTEL® AMT VIA THE WEBUI INTERFACE

An administrator with user rights can remotely connect to the Intel® AMT device by entering the IP address and one of the following port numbers into the address bar of the web browser:

- 16992 – Use if TLS is NOT configured (use http)
- 16993 – Use if TLS is configured (use https)

For example: http://134.134.176.1:16992

The Intel® AMT device can also be addressed using the device's fully qualified domain name (FQDN). If using TLS, Intel recommends using the Intel® AMT FQDN rather than the IP.

For example: https://amtsystem.domain.com:16993

The following web browsers were validated and can be used remotely to connect to any configured Intel® AMT system.

- Microsoft* Internet Explorer 6.0 SP1 or later
- Netscape* 7.2 or later for Windows* and Linux*
- Mozilla* Firefox 1.0 or newer for Windows and Linux
- Mozilla* 1.7 or later for Windows and Linux

5 INTEL® AMT DRIVERS AND SERVICES

In addition to having the BIOS and ME extensions set up correctly, there are also drivers and services to be installed and running in order to fully utilize Intel® AMT once it has been properly configured. In order to verify that the AMT drivers and services are loaded correctly, look for them in the host operating systems' Device Manger and Services. Note that there should be a CD included with every Intel® AMT system that includes all of the required Firmware and Drivers. Be sure to check the OEM's download site frequently for upgraded versions of the BIOS, Firmware and Drivers.

Here is a list of drivers and services that should appear in the host operating system:

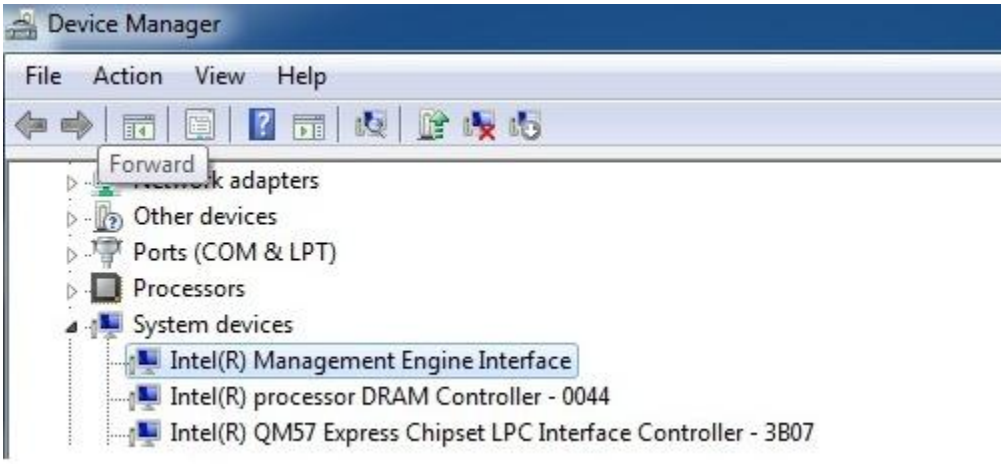
- Intel 82577LM Network Interface Controller*
- Intel® Centrino® Ultimate-N 6300 AGN *
- Intel Management Engine Interface (aka HECI driver)
- Serial-Over-LAN (SOL) Driver
- Intel® Active Management Technology LMS Service
- Intel® AMT System Status Service

*Network controller and wireless interface versions will vary depending on the generation of Intel® vPro platform.

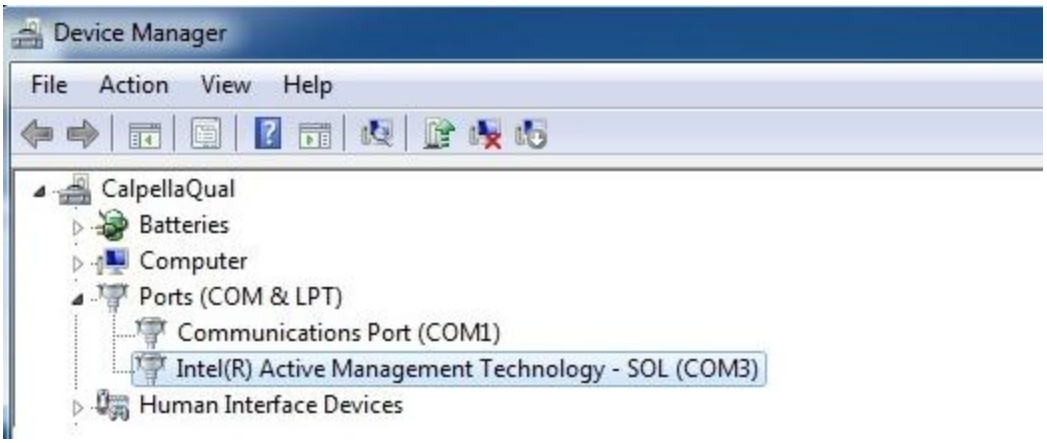
Note: The version level of the drivers must match up to the version level of the Firmware and BIOS. If non-compatible versions are installed, Intel® AMT will not work with the features that require those interfaces.

5.1 NIC: INTEL 82577LM NETWORK INTERFACE CONTROLLER

5.2 INTEL® MANAGEMENT ENGINE INTERFACE

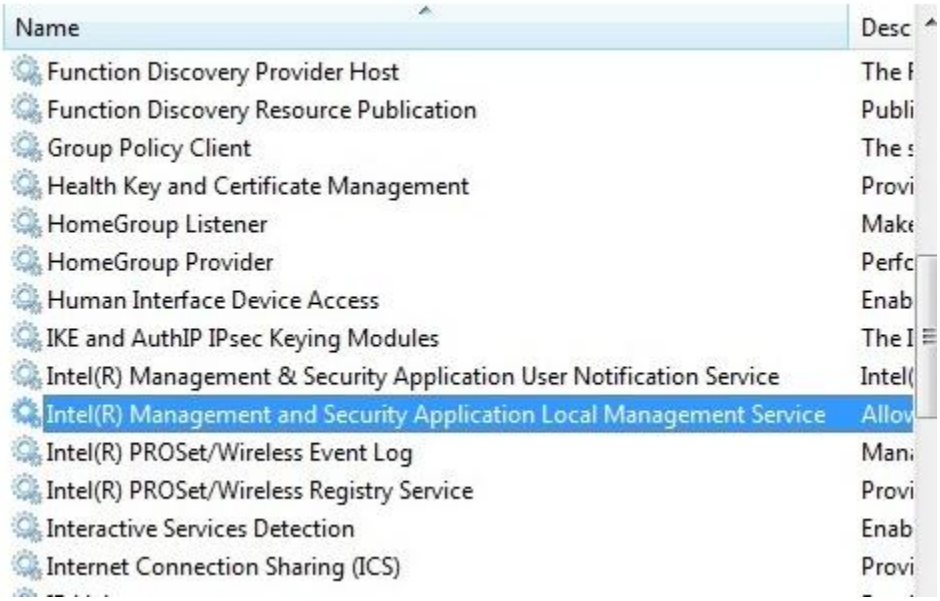


5.3 SERIAL-OVER-LAN (SOL) DRIVER



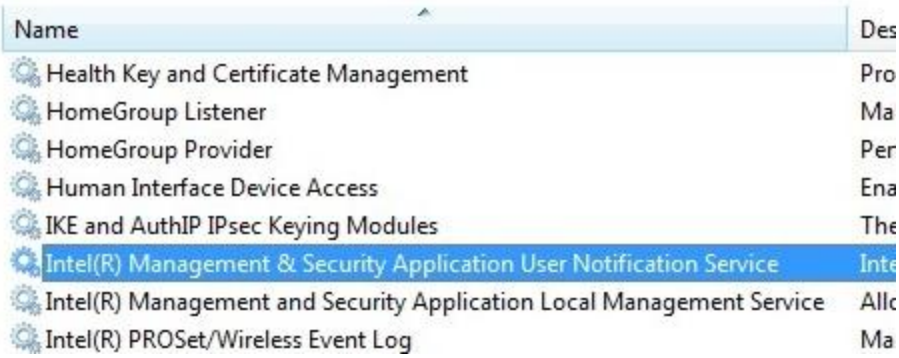
5.4 INTEL® ACTIVE MANAGEMENT TECHNOLOGY LMS SERVICE

(Local Manageability Service) This service runs locally in an Intel® AMT device and enables local management applications to send requests and receive responses to and from the device. The LMS listens for and intercepts requests directed to the Intel® AMT local host and routes them to the Management Engine via the Intel Management Engine Interface driver.



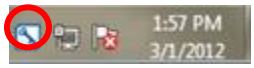
5.5 INTEL® AMT USER NOTIFICATION SERVICE

The User Notification Service (UNS) is a Windows service installed on the host on a platform that has Intel® AMT Release 2.5 or greater. The UNS registers with the Intel® AMT device to receive a set of alerts. When UNS receives an alert it logs the alert in the Windows "Application" event log. The Event Source will be "Intel(R) AMT".



5.6 INTEL MANAGEMENT AND SECURITY STATUS TOOL

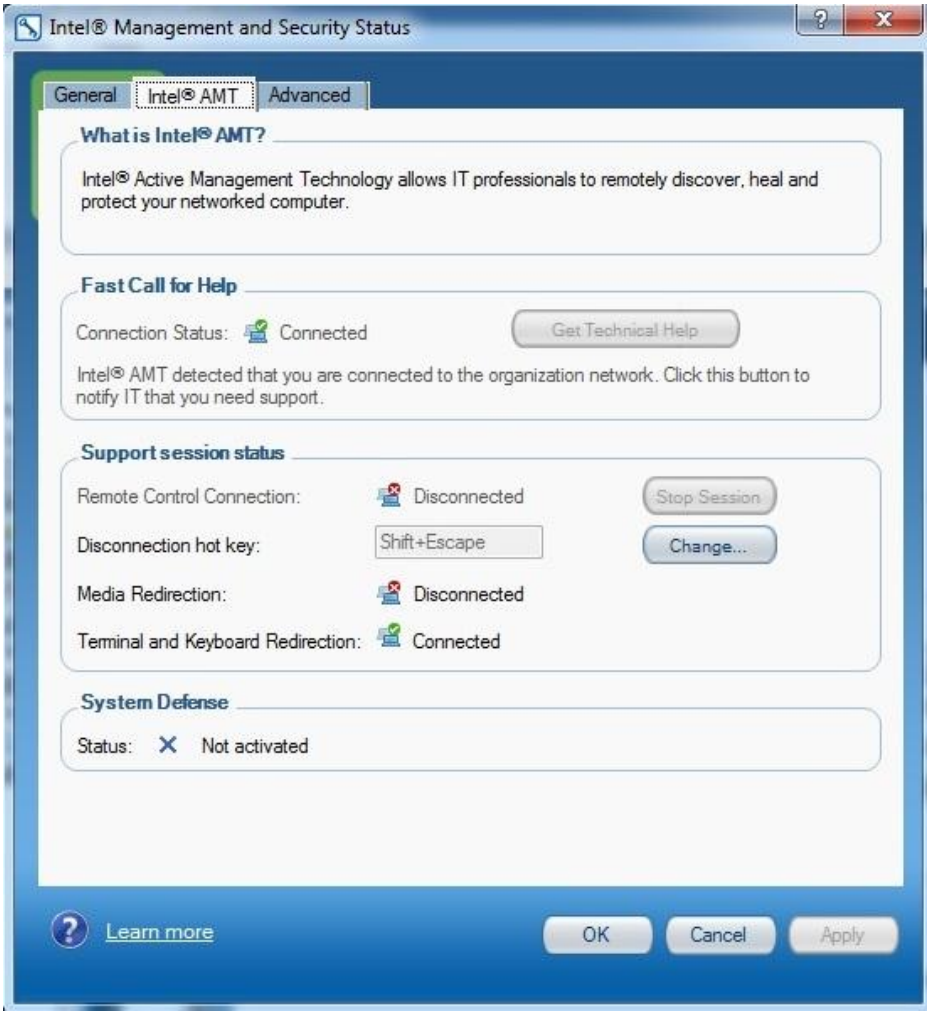
The Intel Management and Security Status (IMSS) tool can be accessed by the "blue key" icon in the Windows tray.



The General tab of the IMSS tool shows the status of vPro services available on the platform and an event history. There are tabs for additional details of each.

Intel® Management and Security Status
General
Intel® AMT
Advanced
Monitor the status of management and security technologies provided by Intel® Management Engine (Intel® ME) using Intel® Management Engine Interface (Intel® MEI).
intel
Service Status
Intel® Active Management Technology (Intel® AMT): Enabled
Intel® Remote PC Assist Technology (Intel® RPAT): Disabled
Event History
Comment
Application
Event
Time
Reviewed Intel® AMT Media redirection sessi... 1/20/2010 2:15:57 PM
Reviewed Intel® AMT Media redirection sessi... 1/20/2010 2:07:47 PM
Reviewed Intel® AMT Terminal and keyboar... 1/20/2010 2:07:35 PM
Note: No action is required on your behalf due to any of the above events.
Enable user notification
Intel® Management and Security Status will be available next time I log on to Windows*
Learn more
OK
Cancel
Apply

The Intel® AMT tab of the IMSS tool shows more detailed information on the configuration of AMT and its features.



6 INTEL® AMT SOFTWARE DEVELOPMENT KIT (SDK)

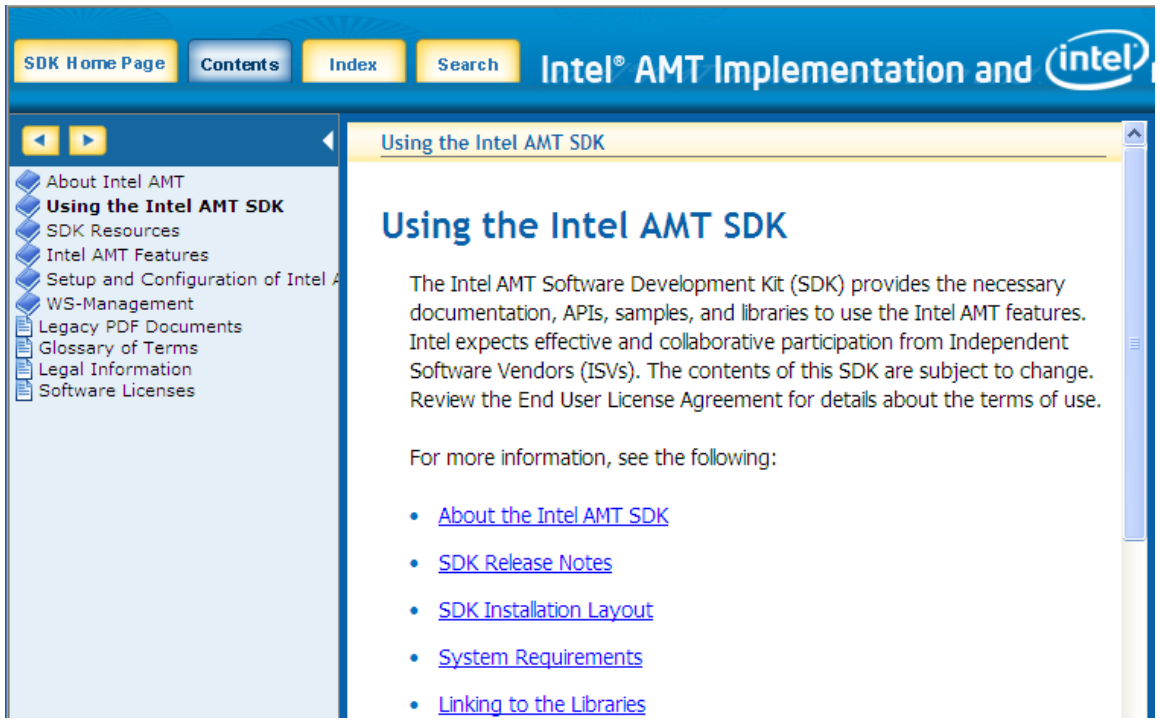
The Intel® AMT Software Development Kit (SDK) provides the low-level programming capabilities to enable developers to build manageability applications that take full advantage of Intel® AMT. Inside the SDK is a full set of documentation, sample code, and APIs needed for implementing Intel® AMT.

The Intel® AMT SDK provides sample code and a set of application programming interfaces (APIs) that let developers easily and quickly incorporate Intel® AMT support into their applications. The SDK supports C++ and C# on Microsoft Windows and Linux operating systems. Refer to the User Guide and the Readme files in each directory for important information on building the samples.

Also see the video tutorials Introduction to Intel® AMT SDK and How to compile Intel® AMT SDK sample code

The SDK is delivered as a set of directories that can be copied to a location of the developer's choice on the development system. Because of interdependencies between components, the directory structure should be copied in its entirety. There are three folders at the top level: one called DOCS (which contains SDK documentation), and one each for Linux and Windows (which contain all of the sample code.) For more information regarding how to get started and how use the SDK, see the "Intel® AMT Implementation and Reference Guide."

Below is a screen shot of the Intel® AMT Implementation and Reference Guide – for more information on system requirements and how to build the sample code, read through the "Using the Intel® AMT SDK" section. The documentation is available on the ISN network here: Intel® AMT SDK (Release 8.0)



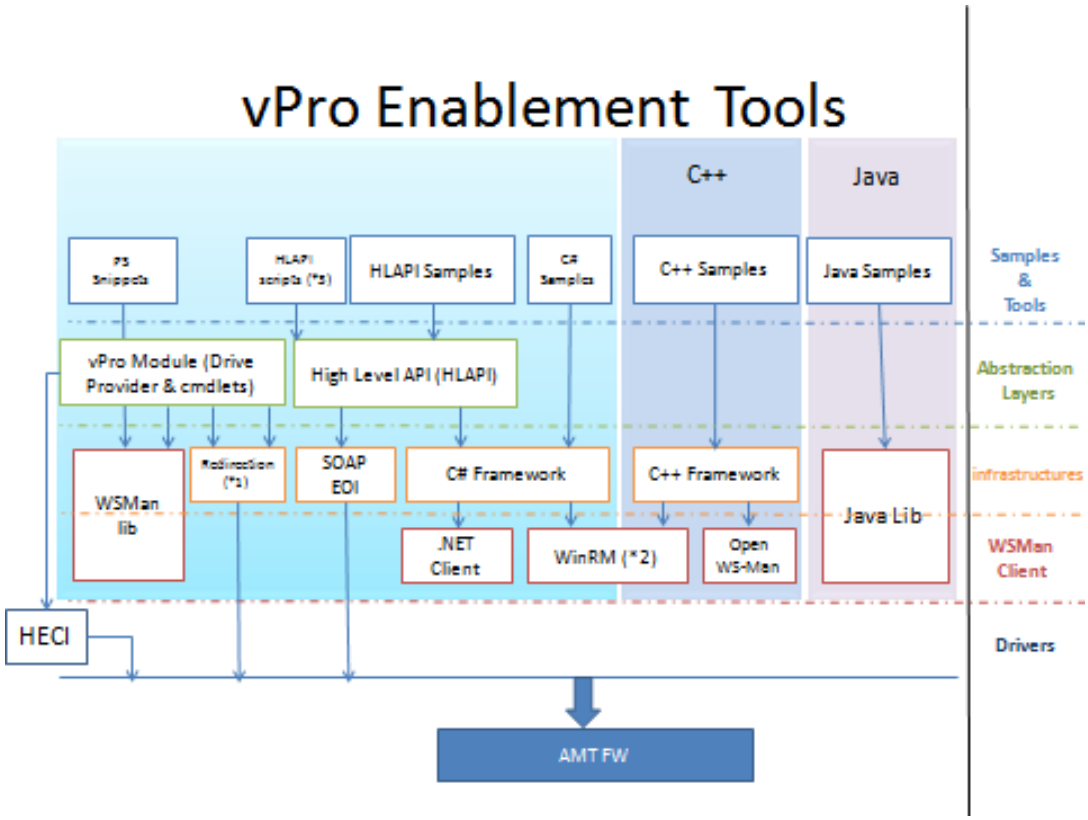
6.1 OTHER SDK RESOURCES

The Intel® AMT SDK provides frameworks and samples that simplify WS-Management development and demonstrate how to take advantage of the advanced product features. For more information, see the following:

- KVM Application Developer's Guide
- Redirection Library
- C++ CIM Framework API

- C# CIM Framework API
- WS-Management Clients Supporting C# and C++ Development
- Intel ME WMI Provider
- Management Presence Server Sample
- Posture Validation (NAC)
- System Health Validation (NAP)
- Remote Encryption Management
- User Consent Tool

There are a variety of development environments for which to write software that supports Intel® AMT. Please see the figure below for more details.



*1) Availably only in C++, (C# wrapper in SDK)
*2) COM object by MSFT
*3) Not just .NET

APPENDIX A:

The following table provides a snapshot of features supported by prior all versions of Intel® AMT. Note that for Intel® AMT 8.0 there are no new features, only changes to some.

	Intel® AMT 1.0 Desktop	Intel AMT 2.0/2.1 Desktop	Intel AMT 2.5/2.6 Mobile	Intel AMT 3.0 Desktop	Intel AMT 4.0 Mobile	Intel AMT 5.0 Desktop	Intel AMT 6.0 Desktop and Mobile	Intel AMT 7.0 and 8.0 (Desktop and Mobile)
Hardware Inventory	X	X	X	X	X	X	X	X
Persistent ID	X	X	X	X	X	X	X	X
Remote Power On/Off	X	X	X	X	X	X	X	X
SOL/IDER	X	X	X	X	X	X	X	X
Event Management	X	X	X	X	X	X	X	X
3rd Party Data Storage	X	X	X	X	X	X	X	X
Built-in Web Server	X	X	X	X	X	X	X	X
Flash Protection	X	X	X	X	X	X	X	X
Firmware Update	X	X	X	X	X	X	X	X
TCP/IP, SOAP	X	X	X	X	X	X	X	

XML/EOI								
HTTP Digest/ TLS	X	X	X	X	X	X	X	X
Static and Dynamic IP	X	X	X	X	X	X	X	X
System Defense		X	X	X	X	X	X	X
Agent Presence		X	X	X	X	X	X	X
Power Policies		X	X	X	X	X	X	X
Mutual Authentication		X	X	X	X	X	X	X
Kerberos		X	X	X	X	X	X	X
TLS-PSK		X	X	X	X	X	X	X
Privacy Icon		2.1	X	X	X	X	X	X
ME Wake-on-LAN		2.1	X	X	X	X	X	X
Remote Configuration		2.2	2.6	X	X	X	X	X
Wireless Configuration			X		X		X	X
Endpoint Access Control (EAC) 802.1			X	X	X	X	X	X

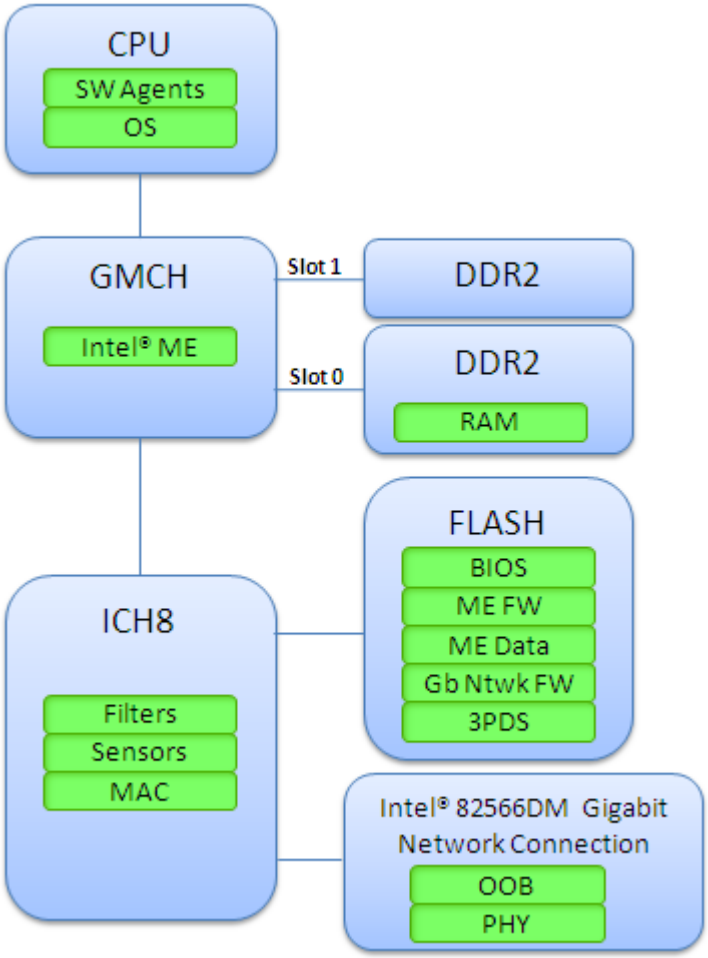
Power Packages			X		X		X	X
Environment Detection			X		X		X	X
Event Log Reader Realm			2.6	X	X	X	X	X
System Defense Heuristics				X		X	X	X
WS-MAN Interface				X	X	X	X	X
VLAN settings for Intel® AMT network interfaces				X		X	X	X
Fast Call For Help (CIRA)					X	X	X	X
Access Monitor					X	X	X	X
MS NAP* Support					X	X	X	X
Virtualization Support for Agent Presence						X	X	X
PC Alarm Clock						5.1	X	X
KVM Remote Control							X	X
Wireless Profile Synchronization							X	X

Support for Internet Protocol Version 6							X	X
Host Based Provisioning								X

Below are block diagrams representing the evolution of Intel AMT. The architecture of each Intel® AMT Release (2.0 and later) is shown below.

A.1 INTEL® AMT RELEASE 2.0/2.1/2.2 ARCHITECTURE

Intel® AMT Release 2.0 is a component of the Intel vPro workstation platform. It uses a number of elements in the Intel vPro platform architecture. The following figure shows the relationship between these elements.



The Intel® AMT functionality is contained in the firmware **(ME FW)**.

- The firmware image is stored in the Flash memory.
- The Intel® AMT capability is enabled using the Intel® Management Engine (Intel® ME) BIOS extension as implemented by an OEM platform provider. A remote application can perform enterprise setup and configuration.
- On power-up, the firmware image is copied into the Double Data Rate (DDR) random-access memory (RAM).
- The firmware executes on the Intel ME processor and uses a small portion of the DDR RAM (Slot 0) for storage during execution. RAM slot 0 must be populated and powered on for the firmware to run.

Intel® AMT stores the following information in the Flash **(ME Data)**:

- OEM-configurable parameters
- Setup and configuration parameters such as passwords, network configuration, certificates, and access control lists (ACLs)
- Other configuration information, such as lists of alerts and System Defense policies
- The hardware configuration captured by the BIOS at startup

Intel® AMT also manages third-party data storage (**3PDS**).The storage area can be allocated by independent software vendor (ISVs) for local storage of information critical to their applications.

The Flash also contains the BIOS executable code **(BIOS)**, as well as the executable code for the Intel® 82566DM Gigabit Network Connection **(GbE Ntwk FW)**.

The Flash is protected against unauthorized host access by a hardware mechanism activated by the OEM during manufacturing.

The **ICH8 interface controller** holds the filter definitions that are applied to incoming and outgoing in-band network traffic (the message traffic to and from the CPU). These include both internally-defined filters and the application filters defined by ISVs using the System Defense and Agent Presence capabilities.

The Intel® 82566 Gigabit **Network Connection** identifies out-of-band (OOB) network traffic (traffic targeted to Intel® AMT) and routes it to the Intel ME instead of to the CPU. Intel® AMT traffic is identified by dedicated IANA-registered port numbers.

The following elements interact with Intel® AMT:

- The **BIOS** can be used to initialize Intel® AMT or to reset it to its initial state. It captures platform hardware configuration information and stores it in NVM so that Intel® AMT can make the information available out of band.
- The **ICH8** sensor capability detects the state of various platform sensors, such as temperatures, fan status, and chassis integrity. Intel® AMT can be configured to store and/or forward an alert when the state of any selected sensor changes or crosses a threshold.
- **Software Agents** (typically written by management ISVs) executing on the CPU can register with Intel® AMT and report their presence to Intel® AMT and to a management console using "heartbeats". Intel® AMT monitors the heartbeats and can take action when there is a problem with Agent execution.
- **ISV Applications** on the CPU can communicate locally with Intel® AMT using dedicated drivers that are compatible with the host operating system.

A.2 INTEL® AMT RELEASE 2.1IMPROVEMENTS

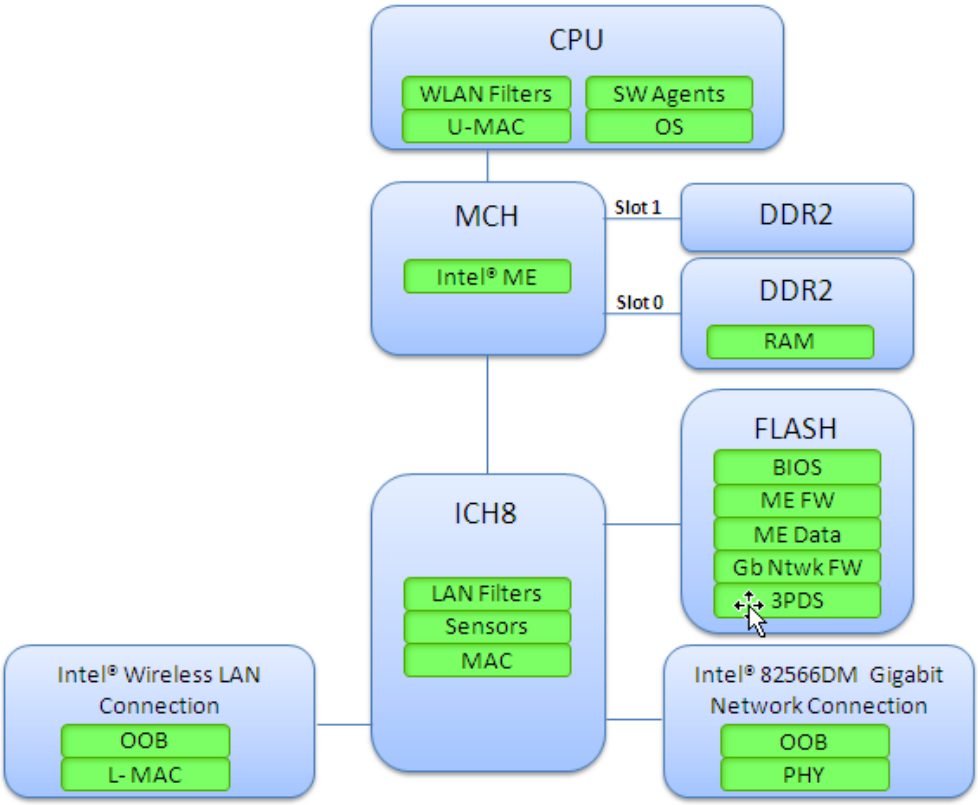
Intel® AMT Release 2.1 enhances the Intel® AMT power savings option by enabling waking the Intel® AMT device on receipt of a message on the network interface when the device is asleep in an Sx power state.

A.3 INTEL® AMT RELEASE 2.2 IMPROVEMENTS

Intel® AMT Release 2.2 adds Remote Configuration (also known as Zero-Touch Configuration, or ZTC), which simplifies the setup and configuration process while maintaining the security of the Intel® AMT device.

A.4 INTEL® AMT RELEASE 2.5/2.6 ARCHITECTURE

Intel® AMT Release 2.5 extends active management to enterprise wireless mobile computing. As shown in the following figure, the architecture has a mobile version of ICH8, the Crestline MCH and a wireless NIC.



A.5 INTEL® AMT RELEASE 3.0 ARCHITECTURE

The Intel® AMT Release 3.0 architecture is similar to the Release 2.0 architecture. The MCH has been upgraded to the GMCH and the ICH8 has been upgraded to ICH9. These changes, combined with a new version of firmware, support all the features of Intel® AMT Releases 2.5 and 2.6 (except for the wireless and mobile features) and provide the following additional capabilities:

- Heuristic System Defense: a basic capability for catching and blocking worm attacks emanating from the host platform before they spread widely across the enterprise network.
- Support for WS-Management: This emerging standard is available as a method for managing the Intel® AMT platform, in addition to the SOAP based API in previous versions.

A.6 INTEL® AMT RELEASE 4.0 ARCHITECTURE

Release 4.0 extends the capabilities of mobile platforms (Releases 2.5/2.6) with the following features:

- Access Monitor – Provides a means for an auditor independent of the administrator to track events of interest. The events are logged locally in an Audit Log. This log captures critical

Intel® AMT auditable events that only a user with auditor privileges can review. It provides an audit trail in case there is a "rogue administrator" attempting to damage or take over Intel® AMT-based systems, and it serves as a deterrent to such attempts.

- WS-Management – Support for DASH 1.0 included in Release 3.0 is extended to mobile platforms.
- Fast Call for Help – A User can request help via a keystroke from inside or outside the enterprise network from IT support or from a remote service provider.
- Remote Scheduled Maintenance – Platforms can be checked or updated, for example, inventoried, or updated with patches or new versions of software, by connecting with an IT console or service provider from inside or outside the enterprise, when it is convenient.
- Remote Alerts – Platforms can automatically connect to the enterprise IT console or service provider even from outside the enterprise network when potential issues arise. This can speed support and lead to faster solutions.
- In support of the above three features, the SDK includes a Management Presence Server (MPS) that emulates a vPro enabled gateway used to mediate between Intel vPro platforms and enterprise management consoles.
- Support for Microsoft NAP – the endpoint access control feature has been extended to support Microsoft* Network Access Protection (NAP).

A.7 INTEL® AMT RELEASE 5.0 ARCHITECTURE

Release 5.0 includes the features in Release 4.0 except for wireless features.

A.8 INTEL® AMT RELEASE 5.1 ARCHITECTURE

Release 5.1 complies with the DASH 1.0 standard, as approved in February 2009. The release also adds an alarm clock feature. A remote console can configure Intel® AMT to "wake up" the host processor periodically (for example, the same time every day, or once a month), without additional remote intervention.

A.9 INTEL® AMT RELEASE 6.0 ARCHITECTURE

Release 6.0 is a major architecture change: The MCH and ICH chipset has been replaced by the PCH, which contains the ME processor and other logic to support ME-based applications.

Release 6.0 adds the remote KVM (Keyboard, Video and Mouse) feature, which provides the ability to view the client screen and control the platform remotely via a keyboard and mouse. KVM is useful when the host processor is or will be active and a remote IT operator wants to control the client platform.

The SMB (small and medium business) configuration mode has been replaced with a manual configuration option. Unlike the SMB mode, it is now possible to configure an Intel® AMT platform via the MEBx without losing any Intel® AMT capabilities, such as support for TLS.

The product now has an optional dynamic DNS (DDNS) update client. When the client is enabled, Intel® AMT will periodically re-register the platform with a DNS server. It is possible to configure a resource record time-to-live and a periodic DNS update.

Other added features include support for SHA-2 hashes and full support for IPv6.

Note:

- The SOAP API is deprecated in this release. New features are supported only via the WS-Management interface.
- Local applications can no longer subscribe for and receive SOAP alerts.
- Support for mutual authentication on the local interface is deprecated. This capability will be removed in a future release.

A.10 INTEL AMT RELEASE 7.0 AND 8.0 ARCHITECTURE

The following paragraphs summarize what is new in Intel® AMT 7.0.

A.10.1 HOST-BASED SETUP AND CONFIGURATION

The host-based configuration method allows an application running on the local host, with OS Administration privileges, to setup and configure Intel AMT. The two basic configuration modes are now referred to as Client Control Mode and Admin Control Mode. A system that has been configured on the local host is by default, in Client Control Mode and therefore has limitations. For example, System Defense is not available in Client Control Mode and User Consent for Redirection and KVM cannot be disabled.

A.10.2 SNIPPETS ADDED TO INTEL AMT FEATURE USE CASES

The new Implementation and Reference Guide (in the Software Development Kit) now includes nearly 300 snippets – short samples of code that demonstrate a step or sequence of steps in a use case.

The snippets are written using PowerShell 2.0. They depend on a framework called the IntelvProModule located at <SDK_root>\Windows\Common\WS-Management\Scripting Framework.

A snippet can be exercised opposite a configured Intel AMT platform by copying the snippet into a supplied template.

The snippets support backward compatibility and demonstrate, where necessary, the difference between Intel AMT versions, back to Release 3.2. They were validated against Releases 3.2, 4, 5, 5.1, 6, 6.1 and 7.0.

A.10.3 KVM

A new version of the RealVNC library was added to the SDK. This version makes several protocol features available for Intel AMT applications. The SDK documentation includes a spreadsheet showing the features in the RealVNC library that Intel AMT supports.

A.10.4 REDIRECTION LIBRARY

The Windows Redirection library now supports DVDs. The library is compatible with all versions of Intel AMT. The library supports the link preference feature, including an option for legacy behavior, used with earlier releases that do not support link preference.

A.10.5 INTEL(R) VPRO(TM) GATEWAY, ALSO KNOWN AS THE MANAGEMENT PRESENCE SERVER (MPS)

The SDK now includes the MPS source code. A new sample, the MPSInterFaceClient, demonstrates the MPS API.

A.10.6 DIGEST MASTER PASSWORD

The Intel AMT Digest Master Password (DMP) is a single password that is synchronized by the IT administrator among the various management software applications. The protocol described in the SDK defines a method for deriving the Intel AMT administrator password from the DMP that creates a unique password per device. Using this method, the software application does not need to maintain the password database. It simplifies using multiple applications from multiple vendors to manage the Intel AMT device.

A.10.7 DEPRECATED EOI (SOAP) SAMPLES MOVED

The SOAP samples, documentation, Storage library, Crypt32Api and most associated files were moved to a ZIP archive in the SDK root directory.

The SDK general documentation was modified to reflect this change. Most references to SOAP commands were removed.

Certain samples that use SOAP (the sample setup and configuration application, the MPS notification sample, the redirection GUI sample and the AMTRedirection sample) remain in their respective directories.

The WSDLs and other common files remain in place in support of these samples.

About the Authors:

Gael Hofemeier earned her BS in Math/Computer Science and an MBA from the University of New Mexico and has over 20 years of engineering experience. Gael began her career, first working in a Coop position at Kirtland AFB, plotting contour curves that would result from nuclear blasts and determining crater sizes. After graduating she worked for Lockheed Martin writing software for a Simulation Facility (primarily on AWACS simulator) located at Kirtland AFB (10 years). Gael is currently working for Intel as an Application Software Engineer (11+ years) helping Business Client Software Engineers develop applications for Intel® vPro Technologies.

Lance Atencio received his MSCS & BSEE from the University of New Mexico and has over 20 years of engineering experience starting as a civil servant working on missile systems for the U.S. Navy and spending the last 9 years at Intel. He is currently working as an Application Engineer on the Enterprise Manageability Enabling team helping ISVs adopt Intel® vPro™ technologies.

Copyright© 2011 Intel Corporation. All rights reserved.

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 go to: http://www.intel.com/design/literature.htm 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, the Intel logo, Intel. Leap ahead. Intel. Leap ahead. logo, and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

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