Intel® Active Management Technology (Intel® AMT) 7.0 Release

FW & SW Product Requirements Document (PRD)

October 2010

Revision 1.0

Intel Confidential

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.

This document contains information on products in the design phase of development.

All products, platforms, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. All dates specified are target dates, are provided for planning purposes only and are subject to change.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

Intel® Active Management Technology requires the computer system to have an Intel® AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/technology/platform-technology/intel-amt/

The original equipment manufacturer must provide TPM functionality, which requires a TPM-supported BIOS. TPM functionality must be initialized and may not be available in all countries.

Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain computer system software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses. For more information, see http://www.intel.com/technology/security

No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology for data protection requires the computer system to have an Intel® AT-enabled chipset, BIOS, and SATA hard disk drive properly connected to the chipset. Intel AT protects the data on the SATA hard drive disk only after that drive is set up for encryption and does not protect any data after it leaves the hard disk drive. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks. Certain functionality may not be available in all countries.

ENERGY STAR denotes a system level energy specification, defined by the US Environmental Protection Agency, that relies upon all of the system's components, including processor, chipset, power supply, HDD, graphics controller and memory to meet the specification. For more information, see
http://www.energystar.gov/index.cfm?fuseaction=find_a_product.showProductGroup&pgw_code=CO

Systems using Client Initiated Remote Access require wired LAN connectivity and may not be available in public hot spots or “click to accept” locations. For more information on CIRA visit http://www.intel.com/products/centrino2/vpro/index/htm

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Intel, Intel Viiv, and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

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

Contents

Tables

Revision History

Document Number	Revision Number	Description	Revision Date
Anacapa# 27155	0.8	Initial release of the document. Include feedback from engineering, architecture, Marketing and approved RCR. Carry over AMT 6 PRD revision 1.03.	August 2009
Anacapa# 28716	0.9	Customer Feedback updates, CPT Committed RCR updates, carry over AMT 6.1 PRD, SKU updates, POR updates: Tacoma pass removal, IPT removal, WOX removal, QST removal.	July 2010
CDI# 460623	1.0	RPAT removal and additional updates for document accuracy.	October 2010

§

1 Introduction

1.1 Purpose and Scope of this document

This Product Requirements Document captures the requirements for Intel® Active Management Technology (Intel® AMT) 7.0. Intel® AMT 7.0 will be supported on corporate desktop (program's code name Sugar Bay), on mobile (program's code name Huron River), and on workstation (program's code name Bromolow). This document contains requirement for all programs.

Since workstation's requirements are similar to corporate desktop's requirements, in this document will be mentioned only requirements for corporate desktop.

The requirements were driven by both external customers and Intel-internal stakeholders. This PRD contains both functional and non-functional requirements that shall govern the development and release of all product components and collateral distributed under the name Intel® AMT.

This PRD provides the product development team with the information necessary to understand and design the product and plan for project management. It also provides a basis to plan for implementation of the product and its support. The requirements recorded here are considered the "Plan of Record" (POR) once the document has reached revision level 0.80.

The PRD is intended for the following audiences and purposes:

- Customers use the PRD to understand the feature set of the product.
- Engineers refer to it as they create a high-level design (including user interface) based on requirements.
- Functional area managers and the Program Manager use it to help estimate resource needs and schedules and identify risks for the Program Management Plan.
- Quality Assurance and Test engineers use it to set quality criteria and plan for testing.
- Writers use it to plan product documentation.
- Marketing uses it to plan how the organization shall launch and sell the product.
- Product Support engineers use it to plan how the product shall be supported.

The approved PRD serves as a reference for the project team and internal suppliers to develop a product that adheres to the product requirements. PRD updates shall be communicated to the entire project team.

1.2 Acronyms and Definitions

1.2.1 General

Acronym or Term	Definition
ACL	Access Control List
AD	Active Directory
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AES-CCMP	AES-Counter Mode CBC-MAC Protocol (and with the inner acronyms: Advanced Encryption Standard Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)
AMTHI	AMT Host Interface
AMTNI	AMT Network Interface
API	Application Programming Interface
ARGB	Alpha Red Green Blue color space
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ASF	Alert Standard Format
BIOS	Basic Input Output System
CA	Certificate Authority
CCMP	Counter Mode with Cipher Block Chaining Message
CI	Client Initiated
CIFS	Common Internet File System
CPU	Central Processing Unit
CRL	Certificate Revocation List
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual In-line Memory Module
DLL	Dynamic Link Library
DN	Domain Name
DNS	Domain Name System
DoS	Denial of Service

Acronym or Term	Definition
DSCP	Differentiated Services Code Point
EAC	Endpoint Access Control
EC	Embedded Controller
EEPROM	Electrically Erasable Programmable Read Only Memory
EOI	External Operation Interface
FPACL	Factory Partner Allocation Control List
FQDN	Fully Qualified Domain Name
FW	Firmware
GbE	Gigabit Ethernet
HAP	Hardware Assistant Protocol
HCT	Hardware Compatibility Test
HECI (deprecated)	Host Embedded Controller Interface (now known as Intel® MEI)
HMAC	Hash Based Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IBV	Independent BIOS Vendor
ICH	I/O Controller Hub
ID	Identification
IDE	Intelligent Drive Electronics
IDE-R	Integrated Device Electronics-Redirect
Intel® VT	Intel® Virtualization Technology
Intel® ME	Intel® Management Engine
Intel® Management Engine WOL	Intel® Management Engine Wake on LAN
Intel® MEI	Intel® Management Engine Interface (renamed from HECI)
IPMI	Intelligent Platform Management Interface
IPS	Internet Provider Security
IPV4 filter	A HW filter that can match IPV4 packets, Ethernet packets and Non IP packets.
IPV6 filter	A HW filter that can match IPV6 packets.
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISV	Independent Software Vendor

Acronym or Term	Definition
IXIA ANVL	Automated Network Validation Library is an automated testing package developed by IXIA that validates the protocol implementations and operational robustness of networking devices.
JTAG	Joint Test Action Group
KaY	Key Agreement Entity
KDC	Key Distribution Center
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control
MCB	Manageability Engine Communication Bridge
MCH	Memory Controller Hub
MCTP	Management Component Transport Protocol
MPG	Mobile Platform Group
MPS	Management Presence Server
MRA	Multiple Receive Aggregation
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NCPA	Network Control Panel Applet
NOS	Network Operating System
NVM	Non Volatile Memory
NVRAM	Non-Volatile Random Access Memory
OCC	Occasional Connected Computing
OID	Object Identifier
OOB	Out of Band
Opt-in	User consent to allow certain action on his/her platform
OS	Operating System
PAVP	Protected Video and Audio Path
PCI	Peripheral Component Interconnect
PCIe*	Peripheral Component Interconnect Express
PEAP	Protected Extensible Authentication Protocol
PHY	Physical Layer
PKI	Public Key Infrastructure - Set of security protocols.
PPPoE	Point-to-Point Protocol over Ethernet

Acronym or Term	Definition
PRTC	Protected Real Time Clock
PTNI	Proactive Network Interface (now called AMTNI)
PXE	Pre-Boot Execution Environment
QoS	Quality of Service
RFC	Request For Comments
RNG	Random Number Generator
RSA	RSA is a public key encryption method.
RSN-PSK	Robust Security Network Pre-shared Key
RTC	Real Time Clock
RTFD	Return To Factory Defaults
SATA	Serial Advanced Technology Attachment
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SKU	Stock Keeping Unit
SMB	Small/Medium Business
SMBus	System Management Bus
SOAP	Simple Object Access Protocol
SOL	Serial Over LAN
SOS	Service OS
SPI Flash	Serial Peripheral Interface Flash
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP / IP	Transmission Control Protocol / Internet Protocol
TFTP	Trivial File Transfer Protocol
TGT	Ticket-Granting-Ticket
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOS	Type of Service
TPM	Trusted Platform Module
TTLS	Tunneled Transport Layer Security
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locator

Acronym or Term	Definition
USB	Universal Serial Bus
USBr	Universal Serial Bus redirect
UTF	Unicode Transmission Format
UUID	Universally Unique Identifier
VLAN	Virtual Local Area Network
VMM	Virtual Machine Manager
VoIP	Voice over IP
VPN	Virtual Private Network
WD	Watchdog
WEP	Wired Equivalency Protection
WHQL	Windows* Hardware Quality Labs
WOL	Wake on LAN
WPA/WPA2	Wi-Fi Protected Access
WS	Web Service
WSDL	Web Services Description Language
WS-I	The Web Services Interoperability Organization (WS-I), an open industry group committed to promoting interoperability among Web services
WS-MAN	Web Services Management
XML	Extensible Markup Language

1.2.2 Intel® Management Engine

Acronym or Term	Definition
3PDS	3rd Party Data Store
Agent	Software that runs on a client PC with OS running.
Alert	An alert occurs when the Intel® Management Engine Firmware notifies the remote console that an event has happened in the system. An event can be a fan failure or a virus attack.
CBM	ME CBMs - Core Base Modules. Refer to Figure: ME FW partitioning
CEM	ME CEMs - Core Extension Modules. Also called ME CS. Refer to Figure: ME FW partitioning
Closed configuration network.	A closed configuration network is a special network that is set for configuration purposes only. It has no connection to the regular company network.
CM	Capability module. Old MAPD architecture, which is being replaced by Intel® ME Applications and Intel® ME CEMs (Core Extension Modules).

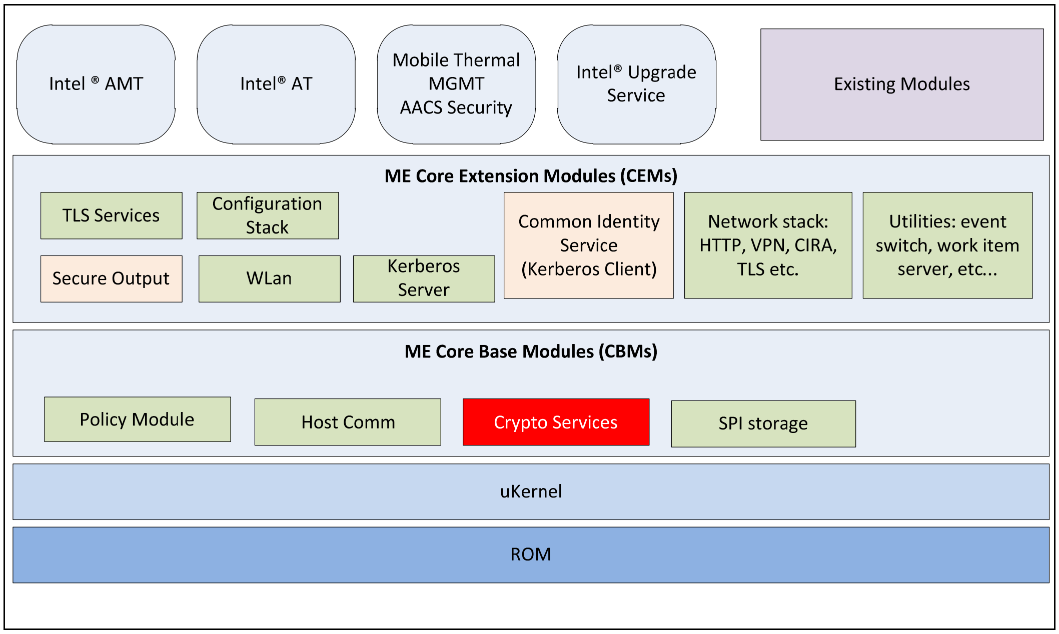
Acronym or Term	Definition
CMSI	Common Management Service Interface - an MAPD defined interface between a capability module and the core.
Configuration server	SW that runs at the user setup and configuration station. This SW is responsible for connecting to the Intel® Management Engine Firmware and automatically configuring it with pre-defined parameters.
Corwin Springs	See WoX
CS	Intel® ME CS – Common Services. Also called ME CEMs.
EIB	Extended Ingredient Brand. Consumer targeted desktop platform.
End User	The person who uses the computer (either Desktop or Mobile). In corporate, the user usually does not have an administrator privileges. The end user may not be aware to the fact that the platform is managed by Intel® AMT.
Enterprise Mode	A setup and configuration mode that is used within an enterprise environment rather than an SMB environment.
Factory partner	An Intel partner ISV that has signed an agreement with Intel to able to run their code in the reserved NVM FW space.
Fast Call for Help	A user initiated keystroke sequence (from outside the firewall or inside the firewall) that sends a maintenance request to the management console.
Host or Host CPU	The processor that is running the operating system. This is different than the management processor running the Intel® Management Engine Firmware.
Host Service/Application	An application that is running on the host CPU.
IANA	International association of North America. A standards body.
IDE-R	Integrated Device Electronics-Redirect
INF	An information file (.inf) used by Microsoft operating systems that support the Plug & Play feature. When installing a driver, this file provides the OS the necessary information about driver filenames, driver components, and supported hardware.
Intel® AMT 1.0/ Intel® AMT 2.0/2.1 Firmware mode	A backwards compatible Intel® Management Engine Firmware mode where the new generation Intel® Management Engine Firmware supports the exact same feature set and security mechanism as the previous generation Intel® Management Engine Firmware.
Intel® AMT emulator	A software emulation for silicon/firmware features that enables ISVs to develop and test Intel® AMT code prior to silicon arrival.
Intel® AMT Firmware	The Intel® AMT Firmware running on the embedded processor. Can not use "FW" generically in this PRD as there is Fan FW too.
Intel® AT	Intel® Anti-Theft Technology. Intel® Anti-Theft Technology is a feature that uses the Manageability Engine to provide hardened anti-theft security and theft management.
Intel® Management Engine Firmware Compression utility	Used internally only by the Intel® Management Engine Firmware team to compact the Intel® Management Engine Firmware code to fit into the system flash.

Acronym or Term	Definition
Intel® Management Engine Firmware Image Creator	Used internally only by the Intel® Management Engine Firmware team to compact the Intel® Management Engine Firmware to create the Intel® Management Engine Firmware Image.
Intel® Management Engine Interface (Intel® MEI)	Interface between the Management Engine and the Host system.
Intel® ME	Intel® Management Engine, The embedded processor residing in the chipset GMCH.
Intel® MEBx	Intel® Management Engine BIOS Extensions
Intel® MEI driver	Intel® AMT host driver that runs on the host and interfaces between ISV Agent and the AMT HW.
Intel® Quiet System Technology (Intel® QST)	Fan speed control architecture that allows multiple sensors to control a single fan as well as allow a single sensor control of multiple fans.
Intermittent connection	An intermittent connection is a connection that is not always available. This may be a mobile system roaming around whether it is on site, or outside, or a remote system.
IT User	Information Technology User.
LMS	Local Management Service, A SW application which runs on the host machine and provide a secured communication between the ISV agent and the Intel® Management Engine Firmware.
MPS	Manageability Presence Server
MSM	Intel® ME Services Manager
Non partner ISV	Any 3rd party ISV that does not have a contract with Intel and would like to use the general purpose NVM space to run their code. Development support model differs from the “high touch” relationships with Partner ISVs.
Notification Policy	A policy that defines how the Intel® Management Engine Firmware shall notify the remote console that an event has happened. Example for notification policy can be: Send an alert, log an alert, Do nothing.
NVM	Non-Volatile Memory. A type of memory that will retain its contents even if power is removed. In the Intel® AMT current implementation, this is achieved using a FLASH memory device.
OOB interface	Out Of Band interface. This is SOAP/XML interface over secure or non secure TCP protocol.
OS not Functional	The Host OS is considered non-functional in any one of the following cases: System is in Sx power state. System is in S0 power state and: OS is hung After PCI reset OS watch dog expires OS is not present
OTG	On the Go

Acronym or Term	Definition
PET	Platform event trap is a specification format for sending platform alerts in case of events.
Remote Access	Formerly known as CIRA. Remote Access is the term describing Fast Call for Help, Remote Scheduled Maintenance and Remote Alerts from outside the firewall. Fast Call for Help in some cases can also be requested from inside the firewall.
Remote Alerts	The ability for a PC that is outside the firewall to send a request to the management console if an alert occurs that the management console has subscribed to occurs (i.e., system defense alert, agent presence alert, etc.).
Remote connection	A remote connection is a connection between 2 systems that are not on the same intranet. That means that they have to go through the internet and establish some kind of tunneled connection. Usually these will be IPSEC or TLS VPN connections. An example would be a user at home connecting into the corporate.
Remote Management application	An application that sends commands and configurations to the Intel® Management Engine Firmware via the OOB interface. Examples: firewall, ISV NVM application
Remote Scheduled Maintenance	The ability for a PC that is outside the firewall to connect to the management console at a pre-defined periodic rate (i.e., once a week, once a day, etc.) to check for scheduled maintenance.
RSR	Remote System Repair
Scratch Pad	Partner ISVs and 3rd party ISVs that do not have a contract with Intel may use the general purpose NVM space to run their code on a first come, first served basis at run-time.
SEI	Sensor Effecter Interface. This is an MAPD specification for accessing sensors and effectors. Effectors for example can be remote control devices or System Defense filters.
Setup And Configuration	Setup and configuration of network access for Intel® ME and Intel® ME applications on corporate networks. This is the process by which Intel® vPro™ technology features are made available to management applications
System Defense (SD)	System Defense. System Defense identifies incoming or outgoing packets, and based on the packet type will take actions such as blocking a specific type of packet. System Defense also will take action if the agent has been removed from the system, implying an application issue or tampering.
System Defense Filter	A HW mechanism that scans incoming and outgoing network packets to identify if they match a defined pattern.
System Defense Policy	This is the action that occurs when a filter indicates a match, or when the Intel® Management Engine Firmware detects that an agent is not present on the host system.
System States	Operating System power states such as S0. See detailed definitions in system state section.
TDT	Theft Deterrence Technology. Previous name for AT-p, which is part of the Intel® Anti-Theft Technology.
UIM	User Identifiable Mark

Acronym or Term	Definition
Un-configured state	The state of the Intel® Management Engine Firmware when it leaves the OEM factory. At this stage the Intel® Management Engine Firmware is not functional and must be configured.
VE	Virtualization Engine
WoX	Wake on Event or Wake on VoIP. Also called Corwin Springs

Figure 1. Intel® ME FW Repartitioning


Intel ® AMT
Intel® AT
Mobile Thermal MGMT AACS Security
Intel® Upgrade Service
Existing Modules
ME Core Extension Modules (CEMs)
TLS Services
Configuration Stack
Secure Output
WLan
Kerberos Server
Common Identity Service (Kerberos Client)
Network stack: HTTP, VPN, CIRA, TLS etc.
Utilities: event switch, work item server, etc...
ME Core Base Modules (CBMs)
Policy Module
Host Comm
Crypto Services
SPI storage
uKernel
ROM

NOTES:

1. Throughout this document some mentioning of Intel® AMT refers to Intel® AMT Firmware application and sometimes to Intel® ME Common Services.

1.3 System States and Power Management

Acronym or Term	Definition
M0	Intel® Management Engine power state where all HW power planes are activated. Host power state is S0.
M3	When Intel® Management Engine and deeper power planes activated however the host power state is different than S0 (Some host power planes are not activated). Host PCI-E* interface are unavailable to the host SW. Main memory is **not available** for Intel® Management Engine use.
M-Off	No power is applied to the management processor subsystem. Intel® Management Engine is shut down.
OS Hibernate	OS state where the OS state is saved on the hard drive.

Acronym or Term	Definition
S0	A system state where power is applied to all HW devices and system is running normally.
S1	A system state where the host CPU is running in halted state, however power is connected to the memory system.
S3	A system state where the host CPU has no power; RAM is in slow refresh; the power supply is in a reduced power mode. This mode is commonly referred to as 'Suspend To RAM' or ‘stand by’
S4	A system state where the host CPU and memory are not active.
S5	A computer state where the computer consumes a minimal amount of power. No user mode or system mode code is run. This state requires a large latency in order to return to the Working state. The system’s context will not be preserved by the hardware. The system must be restarted to return to the Working state. It is not safe to disassemble the machine in this state
Shut Down	All power is off for the host machine however the power cord is still connected.
Standby	OS state where the OS state is saved in memory and resumed from the memory when mouse/keyboard is clicked.
Sx	All S states which are different than S0.
H0	User OS up and running
Hx	User OS down
Deep Sx	A System state, which, if supported by board design, keeps ME in Moff, host in S4 or S5 (as defined at the time of entry into this state) and majority of PCH logic turned off resulting in very minimal power consumption in the system

1.4 Wireless and Mobile

Acronym or Term	Definition
AP	Access Point - bridge between the wired LAN and the Wireless LAN
BSS	Basic Service Set - A basic configuration of a wireless LAN network comprising an Access Point. All communications to and from the wireless nodes flow through the AP.
CCX	Cisco Client Extensions
DCF	Distributed Coordination Function
EAP	Extended Authentication Protocol
ESS	Extended Service Set
IBSS	Independent Basic Services Set
IEEE	Institute of Electrical and Electronics Engineers
MAC	Media Access Control Hardware

Acronym or Term	Definition
MIB	Management Information Base
OFDM	Orthogonal Frequency Division Multiplexing
PCF	Point Coordination Function
RSSI	Receive Signal Strength Indicator
Supplicant	A Supplicant is an 802.1x entity that is being authenticated by the Authenticator.
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN
WPA	Wi-Fi Protected Access

§

2 Product Deliverables

For Intel® Active Management Technology, there are two types of product deliverables: platform deliverables and SDK deliverables.

Table 1. Platform Deliverables

	Purpose	Role
Firmware	Enables all Intel® AMT functions on the system	Base Functionality
Intel® MEI Driver	Enables local agents to directly communicate with firmware	Base Functionality
BIOS Extension (Intel® MEBx)	Enables interface between Intel® Management Engine Firmware and BIOS	Base Functionality
Local Manageability Services	An OS service that enables local applications running on the Intel® AMT machine to use the same SOAP functionality that is available to remote applications.	Base Functionality
Manufacturing and validation tools	A set of tools for use internally and by OEM customers for interacting with the Intel® ME Firmware	Manufacturing & Validation
UNS	A user notification service	
NAC PP	NAC posture plug-in	
NAP SHA	SHA (System Health Agent) plug-in for the NAP agent	

Table 2. SDK Deliverables

	Purpose	Role
Documentation	Interface definitions, product specification and usage information for application developers	Documentation
Sample Code	Facilitates ISV software development by describing common API usage	Documentation / SW design
Sample Applications	Facilitates ISV software development	Validation
Validation Applications	Enables testing of ISV software	Validation/Compliance
Object code libraries	Library interface for ISV application code	Development
Setup and Configuration Service	Configuration of Intel® AMT	Validation

	Purpose	Role
Manageability Presence Server	A Server that allows management via remote access to Intel® AMT clients outside the LAN	
NAP SHV	A system health validator that is installed on the NPS (Network Policy server)	
NAC PVS	A Posture Validation Server incorporated into the organizational AAA server	
Intel® Management and Security Status	An application that indicates whether Intel® AMT and Intel® TPM are running on the platform. The icon is located in the system icon tray	Software
SOL Driver	Enables redirection of the platform's output and input when booting.	Software

2.1 Intel® Management Engine Firmware SKUs

The following firmware SKUs will be created and supported.

	Applicability				FIRMWARE PACKAGE		
Firmware feature	Mobile	Desktop	Server	Workstation	Intel® ME 5MB Firmware 7.0 for 8MB SPI	Intel® ME 5MB Firmware 7.0 for 8MB SPI - Consumer	Intel® ME 1.5MB Firmware 7.0 for 4MB SPI -Consumer
Intel˙ Active Management Technology 7.0	✓	✓		✓	✓	✗	✗
Intel Anti Theft (OOB over 3G -Mobile)	✓	✓		✓	✓	✓	✓
Wireless Display – HDCP 2 AKE content protection (NEW)	✓				✓	✓	✓
Int. Clock Control (w/ Performance Tuning)	✓	✓	✓	✓	✓	✓	✓
Intel Upgrade Service	✓	✓			✓	✓	✓
PAVP Content Protection for Intel• 6 Series Chipset	✓	✓		✓	✓	✓	✓
Dynamic Fusing (Desktop/Server/WS)		✓	✓	✓	✓	✓	✓
Intel• AMT Over Wireless LAN (On NB and DT)	✓	✓			✓	✓	✓
BIOS Size					3	3	2.5
EST. SPI Size Required (MB)					8	8	4

NOTES:

1. **Feature targeted with an upgrade to Intel® RST 10
2. Actual SPI Device size will depend on BIOS

2.1.1 SKU Manager

2011 Platforms will have the ability to create various firmware product SKUs via software configuration interfaces. Product SKU may include capabilities of Intel® AMT as well as other Intel® Management Engine applications such as Intel® Anti-Theft Technology.

2.1.1.1 SKU Manager - Intel® AMT

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100014981	SKU configurable capability--HomeIT (Intel RPAT-consumer)	The Intel® AMT HomeIT (Intel RPAT-consumer) capability shall support the option to be disabled or enabled by the SKU Manager.	No	No	Yes	No	No
CCG0100014980	SKU configurable capability --Intel® AMT	The entire Intel® AMT interface including all Intel® AMT features shall support the option to be disabled or enabled by the SKU Manager.	Yes	Yes	Yes	Yes	Yes

2.2 Intel® Standard Manageability SKU

Manageability support is required from top-to-bottom (Good, Better, Best) in order to maintain competitive advantage on corporate platforms. In order to maintain clear value proposition on Intel® vPro™ (Best segment), the "Intel Standard Manageability" SKU (Better segment) has been defined beginning with McCreary platforms.

Processor Compatibility:

Standard Manageability features are available for all processors when paired with Q65 and Q67 (All Intel® Core™ i7; All Intel® Core™ i5; All Intel® Core™ i3; All Intel® Pentium®; All Intel® Celeron®).

NOTE: Q67 SKUs when paired with Intel® vPro™ CPUs (Core i7 and Core i5), have FULL MNG enabled and thus all STD MNG features would be available too as it is a subset of FULL MNG.

PCH HW	Intel® vPro™ technology eligible CPUs*	Intel® Core™ i3 processors**	Intel® Pentium™ processors	Intel® Celeron™ processors
Q67	Full Manageability	STD MNG	STD MNG	STD MNG
Q65	Standard Manageability	Standard Manageability	Standard Manageability	Standard Manageability

* Sugar Bay Intel® vPro™ technology eligible processors include Core™ i7 and Core™ i5 processors with Intel® VT-d and Intel® TXT

** Also includes all non-vPro eligible Core™ i7 or Core™ i5 processors (i.e., processors without Intel® VT-d or Intel® TXT)

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15923	Intel Standard Manageability - Details	Intel will offer a scaled- down version of Intel AMT 6.0 for corporate desktop For Intel AMT 6.0, Standard manageability mode excludes the following features: - KVM - Fast Call for Help, Remote Scheduled Maintenance, and Remote Alerts - Intel RPAT for business	Yes	No	No	No	No
CCG01000 60108	Intel Standard Manageability 2011 - Details	Intel will offer a scaled- down version of Intel AMT 7.0 for corporate desktop For Intel AMT 7.0, Standard manageability mode excludes the following features: - KVM - Fast Call for Help, Remote Scheduled Maintenance, and Remote Alerts - Intel® AMT Over Wireless LAN - NAP support - Alarm Clock	No	No	No	Yes	Yes
CCG010001 5922	Intel Standard Manageability- - FW Size	This Firmware version is targeted to fit in a 64 Mbit flash size including Bios, option ROMs, etc	Yes	No	No	Yes	No
CCG01000 15921	Intel Standard Manageability- - HW Requirements	Platforms that do not have a vPro eligible CPU (as identified by the CPU string) will automatically default to Standard Manageability,	Yes	No	No	Yes	No
CCG01000 15920	Changing between Intel Standard Manageability and Intel full Manageability	When changing from Intel standard manageability to Intel Full manageability or other way around, Intel® AMT will go through the unconfiguration process	Yes	No	No	Yes	No
CCG01000 15919	Firmware Upgrade and Manageability Mode	FW upgrade will keep the current Manageability mode and will not change it	Yes	No	No	Yes	No

2.3 Supported Operating Systems

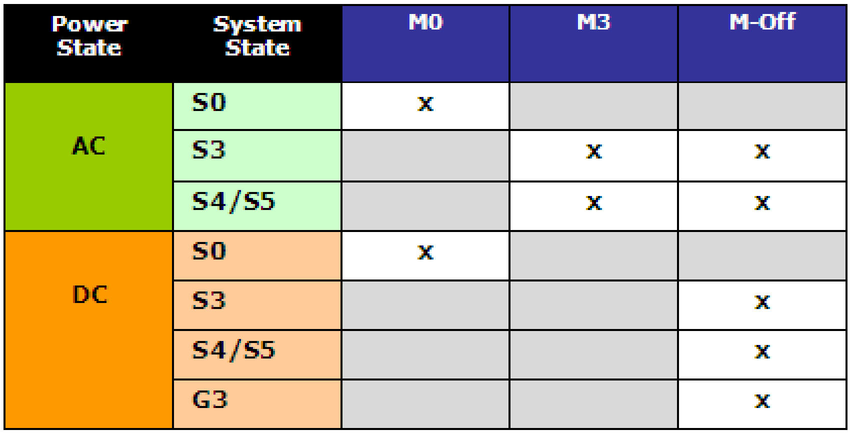
OS Platforms	Local (AMT) System					Mgmt. Console	
	Intel® AMT 6.0 Corporate (Desktop & Mobile)	Intel® AMT 6.0 Consumer (Desktop & Mobile)	Intel® AMT 6.0 Workstation	Intel® AMT 7.0 Corporate (Desktop & Mobile)	Intel® AMT 7.0 Workstation	Intel® AMT 6.0	Intel® AMT 7.0
Windows* 2000	N	N	N	N	N	N	N
Windows* XP Pro with latest SP	Y	N	Y	Y	Y	Y	Y
Windows* XP x64 Edition	Y	N	Y	Y	Y	Y	Y
Windows Vista* 32 bit with latest SP	Y	Y	Y	Y	Y	Y	Y
Windows Vista* 64 bit with latest SP	Y	Y	Y	Y	Y	Y	Y
Windows Vista* Home - Basic Edition with latest SP	Y	Y	Y	Y	Y	N	N
Windows Vista* Home - Premium Edition with latest SP	Y	Y	Y	Y	Y	N	N
Windows Vista* Ultimate - Media Center Edition with latest SP	Y	Y	Y	Y	Y	N	N
Windows* 2003 Standard Edition R2	N	N	Y	N	Y	Y	Y
Windows* 2003 x64 Edition	N	N	Y	N	Y	Y	Y
Windows* 2000 Advanced Server	N	N	N	N	N	N	N
Windows Server* 2008 x86	N	N	Y	N	Y	Y	Y
Windows Server* 2008 x64	N	N	Y	N	Y	Y	Y
Windows* Server 2008 R2 64 Bit	N	N	N	N	Y	Y	Y

OS Platforms	Local (AMT) System					Mgmt. Console	
	Intel® AMT 6.0 Corporate (Desktop & Mobile)	Intel® AMT 6.0 Consumer (Desktop & Mobile)	Intel® AMT 6.0 Workstation	Intel® AMT 7.0 Corporate (Desktop & Mobile)	Intel® AMT 7.0 Workstation	Intel® AMT 6.0	Intel® AMT 7.0
Windows 7* Ultimate 32 bit	Y	Y	Y	Y	Y	Y	Y
Windows 7* Enterprise 32 bit	Y	Y	Y	Y	Y	Y	Y
Windows 7* Professional 32 bit	Y	Y	Y	Y	Y	Y	Y
Windows 7* Ultimate 64 bit	Y	Y	Y	Y	Y	Y	Y
Windows 7* Enterprise 64 bit	Y	Y	Y	Y	Y	Y	Y
Windows 7* Professional 64 bit	Y	Y	Y	Y	Y	Y	Y
Windows 7* Premium 64-bit	Y	Y	Y	Y	Y	N	N
Windows 7* Home Premium 32 bit	Y	Y	Y	Y	Y	N	N
Windows 7* Home Basic 32 bit	Y	Y	Y	Y	Y	N	N
Linux, Red HAT 32 bit (Intel® 64) - RHEL5.3	N	N	N	N	N	Y	Y
Linux, Red HAT 64 bit (Intel® 64) - RHEL5.3	N	N	N	N	N	Y	Y
Linux, Novell/SUSE* 32 bit (Intel® 64) - SLES11	N	N	N	N	N	Y	Y
Linux, Novell/SUSE* 64 bit (Intel® 64) - SLES11	N	N	N	N	N	Y	Y
Linux, Red HAT 32 bit (Intel® 64) - RHEL5.2	N	N	N	N	N	N	N

OS Platforms	Local (AMT) System					Mgmt. Console	
	Intel® AMT 6.0 Corporate (Desktop & Mobile)	Intel® AMT 6.0 Consumer (Desktop & Mobile)	Intel® AMT 6.0 Workstation	Intel® AMT 7.0 Corporate (Desktop & Mobile)	Intel® AMT 7.0 Workstation	Intel® AMT 6.0	Intel® AMT 7.0
Linux, Red HAT 64 bit (Intel® 64) - RHEL5.2	N	N	N	N	N	N	N
Linux, Novell/SUSE* 32 (Intel® 64) - SLED10 SP2	N	N	N	N	N	N	N
SUSE* Linux Enterprise Server 10: 32-bit (Intel® 64)	N	N	N	N	N	**Y-for MPS**	**Y-for MPS**

2.4 Power State Table

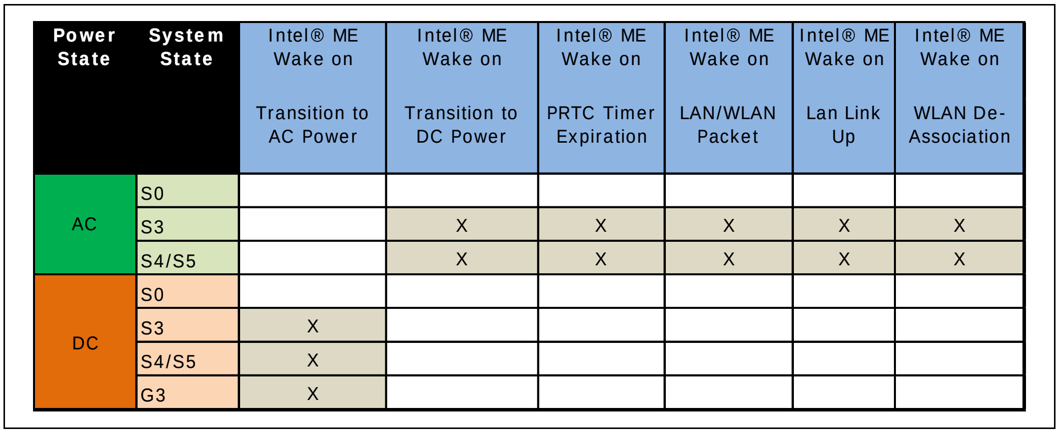
This table describes the possible M-States in relation to the System Power State.



Power State	System State	M0	M3	M-Off
AC	S0	x		
	S3		x	x
	S4/S5		x	x
DC	S0	x		
	S3			x
	S4/S5			x
	G3			x

Intel® ME Wake Support

Intel® ME Wake - any wake from MOff to M3. The following table summarizes the triggers for Intel® ME Wake and the power states in which they are supported.



Power State	System State	Intel® ME Wake on Transition to AC Power	Intel® ME Wake on Transition to DC Power	Intel® ME Wake on PRTC Timer Expiration	Intel® ME Wake on LAN/WLAN Packet	Intel® ME Wake on Lan Link Up	Intel® ME Wake on WLAN De-Association
AC	S0						
	S3		X	X	X	X	X
	S4/S5		X	X	X	X	X
DC	S0						
	S3	X					
	S4/S5	X					
	G3	X					

2.5 Supported Active Directory

The following operating systems for Active Directory will be supported:

AD OS Platform	Intel® AMT 6.0	Intel® AMT 7.0
Windows* 2000 Server Edition	Y	Y
Windows* 2003 Server Edition	Y	Y
Windows Server 2008 Active Directory	Y	Y
Windows Server 2008 R2 Active Directory	N	Y

2.6 Intel® Active Management Technology Performance

Intel® Active Management Technology Performance targets detailed in this chapter. Please note performance section applies to both Desktop and Mobile unless specifically excluded.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100008470	Overarching limit on remote operations	Performance of remote operations will be equal or better than previous generation	No	No	No	Yes	Yes

2.6.1 Redirection Performance Targets

<table>
<tr><th>Feature</th><th>Tools/Protocol</th><th>Meter</th><th>Target</th></tr>
<tr><td><b>Wired LAN Redirection IDER Performance</b> [1]</td><td>IDER test application</td><td>Use the IDER speed test application : The application reads data from the remote CD and computes the average bit rate</td><td>1050 Kbytes / second</td></tr>
<tr><td><b>Wireless LAN Redirection IDER Performance</b> [1]</td><td>IDER test application</td><td>Use the IDER speed test application : The application reads data from the remote CD and computes the average bit rate
Measured in <b>Host preference</b> mode (Wireless driver installed)</td><td>630 Kbytes / second</td></tr>
<tr><td><b>Wired and Wireless LAN Redirection SoL Performance</b> [1]</td><td>SoL speed test application</td><td>Use the SoL speed test application :
The application sends data via the SoL interface
An application running on the console echoes the received characters and computes the bit rate</td><td>150 Kbits / second</td></tr>
<tr><td><b>Wired and wireless IDER Performance over CIRA (Outside Enterprise)</b></td><td>IDER test application</td><td colspan="2">
<table>
<tr><th></th><th>Downlink Speed</th><th>Uplink Speed</th><th>RTT Latency</th><th>IDE-R over CIRA Throughput</th></tr>
<tr><td>High BW (FIOS, Cable etc.)</td><td>2 Mbps</td><td>2 Mbps</td><td>80 ms</td><td>125KB/s</td></tr>
<tr><td>Medium BW</td><td>768 Kbps</td><td>256 Kbps</td><td>80 ms</td><td>48KB/s</td></tr>
<tr><td>Medium-Low BW</td><td>512 Kbps</td><td>512 Kbps</td><td>80 ms</td><td>32KB/s</td></tr>
</table>
</td></tr>
</table>

Feature	Tools/Protocol	Meter	Target
SOAP session open time [2,4]	Management console open Soap Session	Using the management console and measuring the response time AMT to the console	3 Seconds
HTML server (WebUI) response time [2,4]	Web Browser and WebUI	Using a standard web browser and measuring the response time AMT the browser side	3 seconds
Number of concurrent TCP connections [3]	Console applications	Measure the maximum number of connection that can be opened using running several console application in parallel	8 (4 for remote and 4 for local)

NOTES:

1. During the test operation there is no other OOB operations active in the Intel® ME FW such as: Opening TLS session, Reading NVM information via OOB
2. Note: these numbers are both for S0/M0 and Sx/M3. This also assumes a configuration of TLS enabled without mutual authentication. M-off cases are not included in this target requirement.
3. The number of concurrent TCP connections the Intel® Management Engine Firmware shall be handling. This includes SOL, IDER, HTTP and any SOAP commands. Managing TCP connections consumes memory and CPU processing power. However the Intel® Management Engine Firmware must be able to process many requests in parallel for consoles to have quick response time and avoid time outs. Out of the 8 open connections up to two active simultaneous connections.
4. TLS Network assumptions: encryption with Cipher Suite AES 256 CBC SHA & key Size of 2048.

2.6.2 Intel® AMT remote operation time performance targets

This section provides overview of the performance requirements for remote operations focusing on “remote power-on and patch” use case.

Assumptions for performance targets:

- Wired/Wireless configuration inside the organization (not limited by networking environment (Latency, bandwidth))
- Flash part used/platform is meeting Intel SPI flash specifications
- Assuming that the commands in the tested flow are using a single persistent authentication token (Digest/Kerberos) where applicable
- Intel AMT is initialized as minimum (manual configuration or minimal configuration through the ISV application)

Possible combinations of console and starting power state of ME:

	M-off	M3
Console1	11 seconds	7 seconds
Console2	7 seconds	3 seconds

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100008467	Environment setup for Console1 performance testing	For the performance requirements below, Setup1 will be defined as a network environment where the AMT client is connected to the Management Console server (Console1) through a wired LAN connection. Console1 is Using dash compliant commands (WS-Man) to wake up machine to S0/M0. Network Authentication method used is Kerberos with ticket size of 10KB (maximum size). Following the Console1 test flow for remote power-on.	No	No	No	Yes	Yes
CCG0100008468	Environment setup for Console2 Performance testing	For the performance requirements below, Setup2 will be defined as a network environment where the AMT client is connected to the Management Console server (Console2) through a wired LAN connection. No Network authentication method is used (no-TLS). Following Console2 flow for remote power on.	No	No	No	Yes	Yes
CCG0100008469	Console1 test flow for Power-on	Console1 test flow comprised of the following operations: 1) CONSOLE1:AMT_BootConfigSetting.ChangeBootOrder() 2) CONSOLE1: AMT_BootSettingData.Get() 3) CONSOLE1: AMT_BootSettingData.Put() 4) CONSOLE1:CIM_AssociatedPowerManagementService.Get() 5) CONSOLE1: AMT_BootCapabilities.Get() 6) CONSOLE1: AMT_BootSettingData.Get() 7) CONSOLE1: AMT_BootSettingData.Put	No	No	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		8) CONSOLE1: CIM_BootConfiSetting.Get() 9) CONSOLE1:CIM_BootService.SetBootConfigRole (1) 10) CONSOLE1:CIM_ComputerSystem.Enumerate() 11) CONSOLE1: CIM_ComputerSystem.Pull() 12) CONSOLE1: RequestPowerStateChange (2(on))					
CCG0100058018	Console2 test flow for power on	Console 2 test flow comprised of the following operations: Console2: RemoteControlService.GetRemoteControlCapabilities() Console2: RemoteControlService.RemoteControl(17(on),343(IanaOEMNumber))	No	No	No	Yes	Yes
CCG0100008471	Max remote power on time target	Under Setup1 remote power on operation following Console1 test flow shall take less than 7 seconds (Start in M3) and 11 seconds (start in m-off)	No	No	No	Yes	Yes
CCG0100008472	Min remote power on time target	Under Setup2 remote power on operation following Console2 test flow shall take less than 3 seconds (Start in M3) and 7 Seconds (start in M-off).	No	No	No	Yes	Yes

2.6.2.1 Detail performance requirements

There are several SYSTEM and OEM and Application-specific functional and performance requirements regarding Resume and Boot operation that need to be comprehended in the 2011 firmware. OEMs are very concerned about ensuring that these resume and boot requirements are met. Microsoft, via the WLP (Windows Logo Program), also provides incentives to OEMs if systems meet quality and performance requirements defined by Microsoft. In addition to the general targets specified by Microsoft, OEMs have also stated some performance related requirements related to boot and resume operation that need to be met.

This section details the requirements and recommendations for implementation of the Power Transition Time feature for the 2011 Cougar Point/PCH platform

Assumptions for performance targets:

- Applicable to ALL FW-enabled SKUs including ME. Excludes G3 exit, 1st boot, boot with configuration change detected

- Flash part used/platform is meeting Intel SPI flash specifications

Not covered in this document:

- Where applicable this document will guidance to meeting Microsoft “Velocity” (the newest incentive program for OEM systems) requirements that may also applicable (or common with current requirement); given that Velocity requirements are subject to change, this document may not fully comprehend all of the of Velocity program targets as of 2011 launch of the platform.
- Support for Enhanced security requirements such as TXT, which extend capabilities beyond those of the base platform, may have additional impact on the overall boot/resume time and initialization some ME/VE applications/components, that may not be fully comprehended for CPT.
- Resume time targets specified in the System Requirements Specification do not account for time to perform user-input; the time specified for a given flow do not account for the time to perform user-input.
- Support for External, 3rd Party Applications and Option ROMs including Pre-Boot Authentication implemented in native EFI environment, may have impact on the overall boot/resume time and initialization of some ME/VE applications/components that are not fully comprehended for CPT.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 01807	GUIDELINE Typical BIOS POST S4/Moff->S0/M0 (not Ignition) <= 8000ms after CPURST# de-assertion	GUIDELINE Typical BIOS POST S4/Moff->S0/M0 (not Ignition) <= 8000ms after CPURST# de-assertion The intent of this requirement is to ensure that FW and HW does not delay the completion of typical BIOS POST beyond this point. Measured from CPURST# de-assertion to BIOS Completing POST. Applicable to ALL FW-enabled SKUs including ME, VE, ME-Lite. Excludes: Ignition FW (or NON-ME) SKUS, G3 exit, 1st boot, boot/w config change detected.	No	No	No	Yes	Yes
CCG01000 01808	GUIDELINE Typical BIOS POST S5/Moff->S0/M0 <= 8000ms after CPURST# de-assertion	GUIDELINE Typical BIOS POST S5/Moff->S0/M0 <= 8000ms after CPURST# de-assertion The intent of this requirement is to ensure that FW and HW does not delay the completion of typical BIOS POST beyond this point. Measured from CPURST# de-assertion to BIOS Completing POST. Applicable to ALL FW-enabled SKUs including ME, VE, ME-Lite. Excludes Ignition FW (or NON-ME), G3 exit, 1st boot, boot/w config change detected.	No	No	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100001809	S3->S0 (full) <= 2000ms (minimum) / 1800ms (target) after CPURST# de-assertion as measured by Microsoft Windows Logo Test S3 test.	S3->S0 (full) <= 2000ms (minimum) / 1800ms (target) after CPURST# de-assertion as measured by Windows Logo Test S3 test. This requirement indicates that S3 resume time as measured by the Microsoft Logo Tool Kit passes; System resume as measured by the sum of the BIOS and Driver Init Phases for the Windows tool is <2.0s for 3 of past 4 power transitions (http://msdn.microsoft.com/en-us/library/dd424544.aspx). Note that this requirement is identical whether ME is resuming from S3/M3 or S3/Moff. Measured from CPURST# de-assertion to OS completes S0_IRP_COMPLETE. Excludes: system with FB DIMMs, boot with PBA or authentication user entry; boot w/docking, hot-swap, or config change detected. Applicable for all FW SKUs and flash speeds. Measured by Microsoft WHQL and Velocity tools WHQL WLP3.x requires 2.0s/Velocity V4 recommends 1.8s.(GEN ME/VE)	No	No	No	Yes	Yes
CCG0100001811	TYPICAL BIOS Init: S3/Moff->S0/M0 <= 250ms after CPURST# de-assertion.	TYPICAL BIOS Init: S3/Moff->S0/M0 <= 250ms after CPURST# de-assertion. Measured from CPURST# de-assertion to BIOS exit to OS S3 JMP. Excludes: boot with PBA or authentication user entry; boot w/docking, hot-swap, or config change detected. Applicable for all FW SKUs and flash speeds. Intent of this requirement is to emphasize that FW and Platform HW requirements shall not delay ability typical, optimal BIOS to resume from S3 in this time duration. Measured by Microsoft WHQL and Velocity tools. Recommended value from OEMs is 250ms; Velocity recommends 500ms.(GEN ME/VE)	No	No	No	Yes	Yes
CCG0100001814	During S3->S0 resume,FW_INIT_DONE <= 5s after ME ACK of DID.	During S3->S0 resume,FW_INIT_DONE <= 5s after ME ACK of DID. Excludes boot/wconfig change.(GEN ME/VE)	No	No	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 01815	During S5->S0 and S4->S0 resume, all firmware is loaded <= 10s after ME ACK of DID.	During S5->S0 and S4->S0 resume, all firmware is loaded <= 10s after ME ACK of DID. Applicable for all FW SKUs, flash speeds. Excludes G3 exit, 1st boot, boot w/config change detected. (GEN ME/VE)	No	No	No	Yes	Yes
CCG010000 1819	During S5->S0 resume, OS completes Velocity Boot to Desktop in <= 25s after OS load begin.	During S5->S0 resume, OS completes Velocity Boot to Desktop in <= 25s after OS load begin. Measured by xperf and Velocity tools. Measured from start of OS load (AFTER BIOS POST/INT19h) to when the desktop is available to the user. Measured by xperf and Velocity tools. Microsoft Velocity V4 recommends 25s for Desktops; 35s for Mobile platforms.(GEN ME/VE)	No	No	No	Yes	Yes
CCG01000 01820	During S5->S0 resume, OS completes Velocity Boot Complete in <= 35s after OS load begins.	During S5->S0 resume, OS completes Velocity Boot Complete in <= 35s after OS load begins. Measured from start of OS load (AFTER BIOS POST/INT19h) to the point after Desktop available when the system is reasonably idle and responsive to user input. Measured by xperf and Velocity tools. Microsoft Velocity V4 recommends 35s for Desktops; 45s for Mobile platforms. Completion of the PostBoot phase is defined as the time that is required for the system to reach a performance level that does not interfere with typical usage. Low-priority CPU and disk activity is ignored.(GEN ME/VE)	No	No	No	Yes	Yes
CCG01000 01821	OS completes Velocity S0->S5 shutdown in <= 15s after user initiates shutdown.	OS completes Velocity S0->S5 shutdown in <= 15s after user initiates shutdown. Measured by xperf and Velocity tools. Measured from the point when user initiates shutdown, including the system session and kernel shutdown process; it ends just prior to when the OS initiates final shutdown and SLP_EN. Microsoft Velocity V4 recommends 8-15s for all platforms to complete OS shutdown. NOTE: For most firmware modules, the shutdown related activities occur after the OS has completed shutdown and the system SLP_EN has been set and are not measured by the xperf/Velocity tools.(GEN ME/VE)	No	No	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 01822	OS completes Velocity S0->S3 standby in <= 4.8s after user initates standby.	OS completes Velocity S0->S3 standby in <= 4.8s after user initates standby. Measured by xperf and Velocity tools. Measured from the point when user initiates standby request including the SuspendApps, SuspendServices, QueryDevices and SuspendDevices stages; it ends just prior to when the OS initiates final standby and SLP_EN. Microsoft Velocity V4 recommends 2-4.8s for all platforms to complete suspend to S3 (S0->S3). NOTE: For most firmware modules, the shutdown related activities occur after the OS has completed shutdown and the system SLP_EN has been set and are not measured by the xperf/Velocity tools.(GEN ME/VE)	No	No	No	Yes	Yes
CCG01000 01827	During Sx/Moff->S0/M0 transitions, ALL Modules that are involved with critical BIOS tasks of memory initialization and PCI Enumeration are LOADED/STARTED <=500ms of ME ACK of DID.	During Sx/Moff->S0/M0 transitions, ALL Modules that are involved with critical BIOS tasks of memory initialization and PCI Enumeration are LOADED/STARTED <=500ms of ME ACK of DID. These modules must be loaded at this time in order minimize any delays to the BIOS during the POST process: VE copy to SRAM, uKernel, Policy, VENOM, HostComm (GEN ME/VE)	No	No	No	Yes	Yes
CCG01000 01829	During S5->S0 and S4->S0 resume, ALL Modules that must be completed prior to end of BIOS POST are loaded <=6s after ME ACK of DID in order to allow sufficient time for the BIOS to complete POST.	During S45->S0 resume, ALL Modules that must be completed prior to end of BIOS POST are loaded <=6s after ME ACK of DID in order to allow sufficient time for the BIOS to complete POST. These modules must be loaded at this time in order to minimize any delays to the BIOS during the POST process: TLS, RSA, TDT, MPC, QST, AMT, CastlePeak, CommonServices, UTILITIES, EAC, SECIO, WoX, IPT, NETSTK, WLAN, WLAN uCode. This is applicable for TYPICAL, Normal Boot Flow only and excludes boot where configuration changes or extraordinary circumstances may have occurred; 1st boot, boot with configuration changes since last known good boot may take longer to boot/init. (GEN ME/VE)	No	No	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 01833	During S5->S0 and S4->S0 resume, ALL remaining modules that were not loaded in earlier load groups and/or are NOT associated with HDD visibility or pre-INT19h BIOS handshakes shall START <= 10s after ME ACK of DID	During S5->S0 and S4->S0 resume, ALL remaining modules that were not loaded in earlier load group or require pre-INT19h BIOS handshakes shall START <= 10s after ME ACK of DID. Modules can be loaded opportunistically while priority is retained for modules with HDD visibility and pre-INT19h BIOS handshakes. (GEN ME/VE)	No	No	No	Yes	Yes

2.6.3 Intel® Client Initiated Remote Access Technology Performance targets

There are many possible combinations of environment and client configuration that Client initiated remote access (CIRA) can be used, we choose 4 representative cases that represent the best, worst and average cases for KVM performance testing.

Below you can see the relevant configuration and performance target for the KVM performance testing:

	Download	Upload	RTT	BPP	Resolution	FPS	Time First frame
Best scenario (high bandwidth low resolution)	5120	2048	80	3	800x600	3 fps	1.2 sec
Standard I	5120	2048	160	6	1280x1024	1.8 fps	2.5 sec
Standard II	1536	384	80	8	1280x1024	1.42 fps	4.3 Sec
Most taxing (low bandwidth max resolution)	1536	384	160	16	1920x1200	0.82 fps	9.6 Sec

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 16010	ENV1 definition	For the performance requirements below, ENV1 will be defined as a network environment where the client is connected to the MPS server through an ADSL connection with 1536Kbps download bandwidth, 384Kbps upload bandwidth and 160msec end to end RTT. The console is connected to MPS through a broadband network.	No	No	No	No	Yes
CCG01000 16011	ENV2 definition	For the performance requirements below, ENV2 will be defined as a network environment where the CastlePeak client is connected to the CCK server through an ADSL connection with 5120Kbps download bandwidth, 2048Kbps upload bandwidth and 160msec end to end RTT. The console is connected to CCK through a broadband network.	No	No	No	No	Yes
CCG01000 16012	ENV3 definition	For the performance requirements below, ENV3 will be defined as a network environment where the CastlePeak client is connected to the CCK server through an ADSL connection with 1536Kbps download bandwidth, 384Kbps upload bandwidth and 80msec end to end RTT. The console is connected to CCK through a broadband network.	No	No	No	No	Yes
CCG01000 16013	ENV4 definition	For the performance requirements below, ENV4 will be defined as a network environment where the CastlePeak client is connected to the CCK server through an ADSL connection with 5120Kbps download bandwidth, 2048Kbps upload bandwidth and 80msec end to end RTT. The console is connected to CCK through a broadband network.	No	No	No	No	Yes
CCG01000 16015	SOL performance 1	SOL Rx (''file copy'' scenario) bandwidth will be at least: 116 KBps in ENV1 116 KBps in ENV2 116 KBps in ENV3 116 KBps in ENV4	No	No	No	No	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 16016	SOL performance 2	SOL Tx (''file copy'' scenario) bandwidth will be at least: 33 KBps in ENV1 33 KBps in ENV2 33 KBps in ENV3 33 KBps in ENV4	No	No	No	No	Yes
CCG01000 16017	IDER performance 1	IDER big blocks read (32K blocks, i.e OS reading a big file) bandwidth using host DMA mode will be at least: 93 KBps in ENV1 150 KBps in ENV2 120 KBps in ENV3 239 KBps in ENV4	No	No	No	No	Yes
CCG01000 16018	IDER performance 2	IDER small blocks read (2KB blocks, i.e. BIOS boot) bandwidth using host DMA mode will be at least: 11 KBps in ENV1 12.5 KBps in ENV2 22 KBps in ENV3 24 KBps in ENV4	No	No	No	No	No
CCG01000 08586	Framerate test definition	Framerate test for KVM performance defined as: 10% screen change ,RLE compression rate of 1:6.6 and ZLib compression enabled.	No	No	No	No	Yes
CCG01000 08587	First frame Arrival test definition	First frame Arrival test definition defined as: time for first full screen frame on an image with RLE compression rate of 1:6.6 and ZLib compression enabled.	No	No	No	No	Yes
CCG01000 08618	KVM Most taxing (low bandwidth max resolution) performance target	In 16bpp, 1920x1200 screen resolution, Avg over predefined tests in ENV1 first frame time will be at most 9.6 seconds, average frame throughput will be at least 0.8 FPS.	No	No	No	Yes	Yes
CCG01000 08619	KVM standard II performance target	In 8bpp, 1280x1024 screen resolution, Avg over predefined tests in ENV3 first frame time will be at most 4.3 seconds, Average frame throughput will be at least 1.4 FPS.	No	No	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100008620	KVM standard I performance target	In 6bpp, 1280x1024 screen resolution, Avg over predefined tests in ENV2 first frame time will be at most 2.5 seconds, average frame throughput will be at least 1.8 FPS.	No	No	No	Yes	Yes
CCG0100008621	Best scenario (high bandwidth low resolution	In 3bpp, 800x600 screen resolution, Avg over predefined tests in ENV4 first frame time will be at most 1.2 seconds, average frame throughput will be at least 3 FPS	No	No	No	Yes	Yes

2.7 Intel® Active Management Technology High Level Features

2.7.1 Network Protection - System Defense and Agent Presence

System Defense is able to remotely lock down infected systems from a centralized management console. The detection and isolation of infected systems is done via firmware that does port blocking and IP address filtering via simple packet filtering. The health of the system can be verified by checking the presence of the agents running on it and issuing an alert or System Defense isolation action in case they are not.

2.7.2 802.1x support

To enhance security of wired connectivity and to support the 802.11i standard in wireless the Intel® Management Engine Firmware shall support 802.1x connectivity over wired and wireless. The list of EAP methods supported is listed later in this document.

2.7.3 Dual Interface

Intel® Management Engine Firmware shall support network connectivity over wired and wireless simultaneously on mobile platforms. This enables managing the system from both interfaces at the same time.

2.7.4 Extended ISV storage

Enhanced asset management includes providing additional NVM storage space to save data which can be leveraged by other applications within the system management universe. This capability is used for providing internal enterprise support and life-cycle management of computing infrastructure.

2.7.5 Intel® Management Engine<->Embedded Controller communication

The Intel® Management Engine Firmware shall communicate with the Embedded Controller resident on mobile systems. The goals of this communication are:

1) To receive information about the power source of the platform (AC/DC).

2) To send information to the Embedded Controller to indicate when it is OK from Intel® Management Engine perspective that EC power-down the Suspend Well

2.7.6 Power Policy Packages

The setup and configuration of Intel® Management Engine power behavior shall be done by use of pre-configured rule packages stored in the Flash. Intel shall define and provide a number of basic rule packages. Some of the rule packages are optional, and can be removed by OEMs using the FITC tool. Details on the included packages and instructions on how to remove optional packages will be provided in the documentation that accompanies the tool. The IT user will be able to select among these packages to determine the Intel® Management Engine system power behavior using either MEBx or remotely via AMTNI.

In general, the packages allow that in low power states on AC, i.e. S3/AC, S4/AC, S5/AC, the Intel® Management Engine shall operate in one of the following modes:

- AAC (Always Available) - implemented either by:
    1. Intel® Management Engine continuously on or
    2. Intel® Management Engine Wake On LAN: While in Sx/Moff, Intel® Management Engine can still be woken by specific packets where system moves from Sx/Moff to Sx/M3 for Intel® AMT operation. Once the Intel® AMT operation is done system returns to Sx/Moff.
    3. Intel® Management Engine Wake On Wireless LAN: While in Sx/Moff, Intel® Management Engine can still be woken by specific packets where system moves from Sx/Moff to Sx/M3 for Intel® AMT operation. Once the Intel® AMT operation is done system returns to Sx/Moff.
- OCC (Occasionally Connected)
    1. Intel® Management Engine is off until the power state transitions to S0.

2.7.7 User Notification

The Intel® Management Engine Firmware shall provide a notification interface to local host SW for the purpose of notifying end users of predefined events (i.e. critical System Defense policies which limit the users networking capabilities have been applied).

The following table shows the Category Event ID and Event Description for all of the defined alerts:

Category	Event ID	User Message
System Defense	1001	Security policy invoked. Some or all network traffic (TX) was stopped.
System Defense	1002	Security policy invoked. TX Network connectivity was reduced.
System Defense	1003	Security policy invoked. Some or all network traffic (RX) was stopped.
System Defense	1004	Security policy invoked. RX Network connectivity was reduced.
Remote Diagnostics	1201	A remote Serial Over LAN session was established.
Remote Diagnostics	1202	Remote Serial Over LAN session finished. User control was restored.
Remote Diagnostics	1203	A remote IDE-Redirection session was established.
Remote Diagnostics	1204	Remote IDE-Redirection session finished. User control was restored.
WLAN	1104	Management session was established over WLAN interface.
WLAN	1105	Management session over WLAN interface has finished.
WLAN	1101	WLAN Profile sync enablement state changed

2.7.8 Link Policies

There will be a network interface to control availability of the network interfaces in certain system statuses, e.g. in S4 close the interface.

2.7.9 Environment detection

On link up, Intel® ME FW shall determine if system is inside or outside the organization. Determination will happen according to DNS suffix or IPv6 address prefix. An OOB interface identified to be outside the organization will be blocked, unless the system is configured to support Remote Access. Note that outside the organization, the Host VPN is open.

2.7.10 Intel® Management Engine - Embedded Processor

Manageability service processor functions: control, status, monitor, and security for the management sub-system.

2.7.11 Connectivity policies

On Mobile platforms, Intel® ME FW has connectivity policies to preserve battery life when operating in Low Power States (such as Sx). An example is Occasionally Connected Computing (OCC) which gives Intel® AMT the ability to cease operation during Sx Battery operations.

Interaction with OEM's Platform Embedded Controller (EC)

Intel® AMT will interface with the OEM's platform EC in order to acquire any platform state information (e.g. Battery level, System State information) required for Intel® AMT support.

2.7.12 Redirection Capabilities

Intel® AMT will support SoL, IDE, and KVM redirection.

The SoL feature will emulate a serial device to the host platform, while actually sending and receiving the data to and from the management console. This feature can be used by the system BIOS to redirect the BIOS data to remote terminal.

The IDE redirection feature will expose two IDE devices to the host (one floppy and one CD), and will redirect all the traffic over these devices to the management console.

Intel® AMT 7.0 provides KVM redirection capability, which enables IT to remotely control an end-user's platform using a remote Keyboard, Mouse and being able to see the managed end-user machine's screen output at the remote screen on the IT management console.

2.7.13 IPv6 Support

Starting Intel® AMT 6.0 IPv6 network stack will be supported.

2.7.14 Intel® Management Engine Secure Output

Starting 2009, Intel platforms that include the Intel® Management Engine will be able to provide a new secure output service to Intel® Management Engine applications. The secure output service is intended to display messages from the Intel® Management Engine to the user.

2.8 WLAN Manageability

The following section refers to Intel® AMT 7.0 on mobile platforms (Huron River) and some of the desktop platforms (Sugar bay).

Intel® AMT 7.0 on mobile platforms (Huron River) provides the ability to manage client systems out of band over a WLAN connection in S0/H0, S0/Hx and Sx system states. Intel® AMT 7.0 will also support Agent Presence checking/alerting and Asset inventory in the presence of a host based L3 VPN while in S0/H0.

Features available over a WLAN connection:

- System Defense (includes system isolation + recovery and Agent presence checking + alerting)
- SOL/IDE-R
- KVM
- Hardware Inventory
- Third Party Data Store (3PDS).
- Connectivity to Intel® Management Engine in Sx
- Remote Connectivity

Features not available over WLAN:

- Setup and Configuration
- Static IP with dedicated MAC address.
- Base Heuristics

Use Cases**	Wired & Wireless						Usages	Benefits
	AC Power			DC Power				
	S0 / H0	S0 / Hx	Sx	S0 / H0	S0 / Hx	Sx		
Remote Platform/HW/SW Asset tracking	Yes[1] Also supported in presence of L3 VPN	Yes[1]	Yes[1]	Yes Also supported in presence of L3 VPN	Yes[1]	NA[3]	Discover platform/HW & SW inventory regardless of OS or power state	Reduce IT desk visits/user interruptions due to manual inventory audits and improve accuracy
Remote diagnosis & repair	Yes[1]	Yes[1]	Yes[1]	Yes[1]	Yes[1]	NA[3]	IT diagnoses remotely, out-of-band via event log stored in non-volatile memory & serial-over-LAN/IDE-redirect remote boot/KVM-redirect remote	Reduce IT desk visits/user trips to PC depot
Encrypted, remote software update	Yes[1]	Yes[1]	Yes[1]	Yes[1]	Yes[1]	NA[3]	ISV app discovers/updates down-rev anti-virus engines and signatures	Minimize employee interruptions and reduce security risk posed by non-compliant systems
System isolation & recovery	Yes[1]	Yes[1]	Yes[1]	Yes[1]	Yes	NA[3]	Day zero virus protection	Stop virus/malware threats at the source before they infect the network
Agent presence checking and alerting	Yes[1] Also supported in presence of L3 VPN	Yes[1]	NA	Yes Also supported in presence of L3 VPN	Yes[1]	NA[3]	Ensure critical applications are running	Minimize security gaps by ensuring critical SW apps are running

NOTES:

1. Controller Link 1 required for wireless Intel® AMT functionality
2. System Defense filter configuration over LAN is available in SX
3. Intel® AMT disabled during SX operation on DC to minimize impact to battery life
4. S0 = System is on | Sx = System is in standby, hibernate or off | H0 = User OS up and running | Hx = User OS down
5. **Wireless use case support requires WPA1 or WPA2 security. L3 VPN support where noted.

§

3 Detailed Product Requirements

3.1 Hardware Requirements

3.1.1 Intel® Management Engine Pre-allocated Memory Requirements

Pre-allocated memory is the ability of the PCH to request memory allocation from the BIOS. The BIOS in turn reserves system memory for exclusive use by the Intel® Management Engine controller (no operating system access).

For systems with 512MB of system memory or more:

- The pre-boot Intel® Management Engine requests the BIOS to allocate for Intel® ME use 32 MB of UMA
- The pre-boot Graphics requests the BIOS to allocate for it 32 MB of UMA space In the case of a 512 MB system, we would have 512 - (32+32) = 448 MB for the OS which meets WHQL requirements of 448 MB for Windows Vista* Basic.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15819	Intel® Management Engine is M0 functional if any of the memory channels is populated. Intel® Management Engine receives UMA allocation on any one of the channels from the BIOS.	Intel® Management Engine is M0 functional if any of the memory channels is populated. Intel® Management Engine receives UMA allocation on any one of the channels from the BIOS.	Yes	Yes	Yes	Yes	Yes
CCG01000 15820	If there is no memory in any of the channels, Intel® Management Engine will be functional. In this state, only M3 functionality is available	If there is no memory in any of the channels, Intel® Management Engine will be functional. In this state, only M3 functionality is available	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015821	Intel® Manageability Engine always takes only 32 MB from one of the populated channels (when either one or both channel are occupied)	Intel® Manageability Engine always takes only 32 MB from one of the populated channels (when either one or both channel are occupied)	Yes	Yes	Yes	Yes	Yes

3.2 Intel® Management Engine Firmware Requirements

3.2.1 Intel® Management Engine Flash Size Requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100014608	NVM Sector Erase Size	The Intel® ME FW shall support flash devices that have 4 Kbyte sector erase size.	Yes	Yes	Yes	Yes	Yes
CCG0100014968	The size of the Flash will be 8 MB	Can consist of single 8 MB part or two 4 MB parts	Yes	Yes	Yes	Yes	Yes
CCG0100014967	Flash Partitioning	Partitioning of Flash will be as follows: - Intel® ME FW code and Data up to 5.0 MB o Intel® ME descriptor, GbE, PDR - BIOS up to 3.0 MB	Yes	Yes	Yes	Yes	Yes
CCG0100015180	Sector size supported is 4 KB	Sector size supported is 4 KB	Yes	Yes	Yes	Yes	Yes

3.2.2 Intel® Management Engine BIOS Extensions (Intel® MEBx)

Intel® Management Engine BIOS Extension (Intel® MEBx) is a software module that is loaded by PC BIOS to perform Intel® AMT specific setup and initialization. Intel® MEBx communicates with Intel® AMT device through Intel® Management Engine Interface (Intel® MEI).

Note: 16-bit refers to legacy BIOS implementations, whereas EFI refers to the Extensible Firmware Interface, also known as UEFI or Tiano. These designations are for the compatibility of the MEBx, not Intel® AMT itself. Intel® AMT is a separate entity from either of these.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015367	Intel MEBx User Interface	For Intel® ME configurations, graphical user interface shall be provided which can be invoked by hotkey (Ctrl-P) for use on platforms which do not customize the Intel MEBx.	Yes	Yes	Yes	Yes	Yes
CCG0100015341	Intel MEBx menu item visibility control	Intel MEBx shall provide the ability for the OEM to hide / unhide the following menu options: - Intel® ME Configuration - Intel® ME Features Control - Intel® Quiet System Technology - Intel® ME Power Control - Any combination of Power policies - Intel® AMT Configuration - Provisioning Model - VLAN - SoL / IDE-R - Additional derivative requirement: Whenever the OEM has indicated that the VLAN setup option is not available from Intel MEBx, Intel® ME FW must fail any attempt to modify the VLAN configuration using the PTNI command, SetVlanParameters. The reason is to avoid situations in which an incorrect setting will deem the system unusable, without the ability to remedy the situation (or diagnose) it using the Intel MEBx.	Yes	Yes	Yes	No	No
CCG0100124559	Intel MEBx menu item visibility control 2011	Intel MEBx shall provide the ability for the OEM to hide / unhide the following menu options: - Intel® ME Configuration - Intel® ME Features Control - Intel® ME Power Control - Any combination of Power policies - Intel® AMT Configuration - Provisioning Model - SoL / IDE-R	No	No	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15337	Legacy BIOS Intel MEBx	The Legacy BIOS binary of the Intel MEBx	Yes	Yes	Yes	Yes	Yes
CCG01000 15336	Native EFI32 BIOS Intel MEBx	A Native EFI binary of the Intel MEBx	No	No	No	No	No
CCG01000 15335	Intel MEBx BIOS Integration document	Provide a document which details steps required to include the Intel MEBx binary in the system BIOS (Intel® Management Engine (Intel ME) Features BIOS Writer's Guide.)	Yes	Yes	Yes	Yes	Yes
CCG010001 5334	Diagnostic Information	The opening screen of the Intel® ME configuration shall display the following items as they are currently configured or configured per interface (Wired + Wireless): - Hostname - Provision State (Mode / Status) - SOL/IDE-R configurationenabled - KVM-R configuration - Certificate information - Per interface - IP configuration mode - The IP Address - Subnet mask - Default Gateway - DNS server - DNS suffix * Note: It is OK to use this screen to make changes if UI architects determine this is the easiest method	No	No	No	No	No
CCG01000 15917	Intel AMT Intel MEBx Menu changes and New General Settings Menu	The following settings shall be moved from the Intel AMT configuration menu to a general settings configuration menu: - Networking settings - Provisioning settings - Password Policy - Secure Firmware Update - Set PRTC Idle Timeout	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015333	Intel MEBx Opening Screen	The Opening screen of the Intel MEBx shall display : - System UUID - Intel® ME State Control - Enable / Disable - Manageability Features / Status - Intel® Power Policy *Note: it is OK to use this screen to make configuration changes if UI architects determine this is the easiest method.	Yes	Yes	Yes	Yes	Yes
CCG0100013927	Firmware version on opening screen	The firmware version should be displayed on the main MEBx screen, along with MEBx version.	Yes	Yes	Yes	Yes	Yes
CCG0100013926	MEBx Summary screen	MEBX should display a summary screen which shows which configuration options are been enabled / disabled on an AMT platform. ME Status: - ME State Control - Enable / Disable - Manageability Feature - None / AMT -Intel ME State upon initial Power On - Enable / Disable -Intel ME in host Sleep States - Never / S3 / S3+S4 / Always AMT Status: - Host Name - FQDN (Host name + Domain Name) - TCP/IP - Static / DHCP Show following information for Static IP (If possible for DHCP also): - IP address - Subnet Mask - Default Gateway address - DNS address - Provisioning Model : - AMT 2.0 / AMT 1.0 - Manual/Automatic This is only for Enterprise Mode: - Provisioning server address	No	No	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		- IP:Port -PID and PPS - Set / Not Set (Just show whether it was already set or not. No need to show PID/PPS) - SOL / IDE-R -User & Password - Enable / Disable -Serial Over LAN - Enable / Disable -IDE Redirection - Enable / Disable					
CCG0100015331	Password Synchronization	The remote Admin Password and the Intel MEBx Password must be synchronized before remote update. The Password must be able to be updated remotely from an authorized console.	Yes	Yes	Yes	Yes	Yes
CCG0100015330	Customer enabled Intel MEBx interface	Provide a documented method to BIOS writers to write their own replacements to the UI for the Intel MEBx for purposes of integration with their own BIOS	Yes	Yes	Yes	Yes	Yes
CCG0100015326	Intel MEBx Timeout / Hotkey Settings	If the default timeout is not desirable the OEM may provide their own hotkey to enter the Intel MEBx and for that key they may specify whatever timeouts they wish	Yes	Yes	Yes	Yes	Yes
CCG0100015325	Intel MEBx Display settings	Allow the BIOS to control whether or not Intel MEBx displays to screen	Yes	Yes	Yes	Yes	Yes
CCG0100015324	Lockable Option: Intel ME Platform State Control	This option should be lockable to Enable only. Locking to Disable is not supported	Yes	Yes	Yes	Yes	Yes
CCG0100015039	CIRA BIOS Boot End-User Screen	A new BIOS screen must be created for the BIOS Boot use case. The BIOS screen does not require that the end user have specific credentials such as a BIOS or Intel MEBx user name and password. This is a new Intel MEBx Activate Healing Process screen for the end user. As is the case with the OEM process, the end user does not require specific credentials in order to access this screen. There must be a method to disable this screen if the OEM chooses to use their own interface.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15038	CIRA BIOS Boot OEM Interface	Intel MEBX must also enable the OEM by creating an interface for Activate Healing initiation. The BIOS passes the trigger from the BIOS screen to Intel MEBx in the form of a new parameter in the MEBx parameter frame or alternative API mechanism. The OEM will incorporate in their BIOS an Activate Healing Process screen for the end user. Such a screen is created by the OEM to conform with other OEM BIOS screens.	Yes	Yes	Yes	Yes	Yes

3.2.3 OEM PC BIOS

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15654	Trigger method	OEM BIOS must support at least one method of triggering MEBx-based Intel® Remote PC Assist Wizard: - Preferred: BIOS traps CTRL-ALT-F1 through entire period until handoff to OS, and displays message ''Press and hold CTRL-ALT-F1 to enter Intel® Remote PC Assist Wizard'' - Less desired: BIOS allows MEBx to trap CTRL-ALT-F1 through entire period MEBx is running, and display message ''Press and hold CTRL-ALT-F1 to enter Intel® Remote PC Assist Wizard'' - Least desired: BIOS has menu option in BIOS setup to go to Intel® Remote PC Assist Wizard in MEBx BIOS must not support the above if RPAT capability bit is not enabled or firmware has completed Setup and Configuration	Yes	Yes	Yes	No	No

3.2.4 Intel® Management Engine Platform Configuration and Feature / SKU Management

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15380	Feature Enable/Disable and Lock Support	Intel ME Firmware shall provide the capability to ''lock'' certain features to assist in using uber-hw-sku with uber-fw-sku and selectively enable/disable features (and lock them) to define the resulting platform SKU.	Yes	Yes	Yes	Yes	Yes
CCG01000 15379	Support SKU-Agnostic Manufacturing Process	All Intel ME SKUs should have the same manufacturing process	Yes	Yes	Yes	Yes	Yes
CCG01000 15378	Flexible Feature Selection	Intel ME Firmware shall not require flashing a new image to change feature selections.	Yes	Yes	Yes	Yes	Yes
CCG01000 15377	BIOS Interface For Selecting SKUs	Intel ME Firmware shall allow OEMs to robustly change SKU's. Intel AMT shall provide an interface for the BIOS to communicate to the firmware what SKU it wants.	Yes	Yes	Yes	Yes	Yes
CCG01000 15376	Multiple SKUs and BIOS Images Not Required	Intel ME Firmware shall not require the OEM to maintain multiple hardware SKUs, firmware SKUs or BIOS images.	Yes	Yes	Yes	Yes	Yes
CCG01000 15375	Feature Selection Automation Support	Intel ME Firmware shall support automation of feature selection on the manufacturing line.	Yes	Yes	Yes	Yes	Yes

3.2.5 Brand Attribute Compliance

OEMs are required to run and submit output from an Intel-developed Brand Verification Tool (BVT) on at least one production platform sample to qualify for the branding dollars and Intel® vPro™ logo.

OEM systems shall be required to adhere to an Intel-defined Brand Attribute Policy (BAP). The Intel® ME FW will support special commands over the Intel® MEI in both pre-OS and OS runtime states. All ME factory firmware releases will include a BAP image (i.e., BAP plus Manifest) that captures the BA appropriate for that platform.

Note: TPM 1.2 can be disabled to meet certain import restrictions.

3.2.6 2011 Intel® vPro™ Technology Brand Requirements for Desktop

Component	Brand Verification
Sandy Bridge CPU with Intel® VT and Intel TXT	Required
Cougar Point Digital Office PCH (Q67)	Required
TPM 1.2	Required
Intel® VT-x2 capable BIOS	Required
Intel® VT-d capable BIOS	Required
Intel® TXT capable BIOS	Required
TPM 1.2 capable BIOS	Required
Intel® AMT capable BIOS	Required
Intel® vPro™ firmware with Intel® AMT Release v7.0	Required
Lewisville Gigabit LAN (DM SKU)	Required
Intel® Management and Security Status Icon	Recommended

3.2.7 2011 Intel® vPro™ Technology Brand Requirements for Mobile

Component	Brand Verification
Sandy Bridge CPU with Intel® VT and Intel TXT	Required
Cougar Point Digital Office PCH (QM67)	Required
TPM 1.2	Required
Intel® VT-x2 capable BIOS	Required
Intel® VT-d capable BIOS	Required
Intel® TXT capable BIOS	Required
TPM 1.2 capable BIOS	Required
Intel® AMT capable BIOS	Required
Intel® vPro™ firmware with Intel® AMT Release v7.0	Required
Lewisville Gigabit LAN (DM SKU)	Required
Intel® WiFi Link (Puma Peak) or Intel® WiMAX/WiFi Link (Kilmer Peak) or WiFi/Bluetooth (Rainbow Peak) or WiFi link (Taylor Peak)	Required
Intel® Management and Security Status Icon	Recommended

3.2.8 Intel® Management Engine Firmware Manufacturing Requirements

The purpose of this section is not to detail all the requirements for manufacturing, but rather to serve as a repository for required changes.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015321	Fixed Offset Enhancements	All Intel MEBx settings which apply to the platform should be made available to Fixed Offsets unless explicitly excluded in this PRD. Those settings which are client configuration specific such as hostname or IP address are excluded from this requirement	Yes	Yes	Yes	Yes	Yes
CCG0100015320	Firmware supports MEInfo tool regardless of SKU	MEInfo will provide accurate information about the Intel ME firmware regardless of what Firmware SKU MEInfo is run on	Yes	Yes	Yes	Yes	Yes
CCG0100015179	Intel® MEI Client Status Communication	The Intel® MEI shall have a defined message that is sent to all Intel® MEI clients for the purpose of polling their readiness for communication	Yes	Yes	Yes	Yes	Yes
CCG0100015178	Close of Manufacturing Procedure	A flag shall be configurable in the FPT tool that shall do the following: - Lock the descriptor region as described in the table below - Set the MEManuf Counter to 0 - Set the Global Valid bit - Signal to Intel ME that Global Valid Bit was set in the Fixed Address - Intel ME would then move the data in the Fixed Address Variables into the Named Variable region. - Receive from Intel ME hashed value of Fixed Address Variables for manufacturing test purpose Tool will return the response (success) only after move of the Fixed Address Variables into the Named Variables has been completed. The flag should set the descriptor region to a pre-defined lock sequence	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015916	Manageability Engine Watchdog timer disable.	The Firmware shall allow the Intel® ME Watchdog timer to be disabled (for debugging purposes to prevent platform reset due to timer expiration) through the FITc tool while the descriptor values for BIOS, GbE and ME are un-locked.	Yes	Yes	Yes	Yes	Yes

3.3 Intel® Active Management Technology Requirements

3.3.1 Intel® Active Management Technology System State Management

One of Intel® AMT features is being always on. This section will define the Intel® AMT system behavior according to the power state of the managed platform.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100014979	System State counter	The Firmware shall maintain a count of all flash activities and present this upon an API call, noting the amount of remaining writes applied to the part.	No	No	No	No	No
CCG0100015355	System Power State Transitions	The Intel® Management Engine Firmware shall support the transitions: See CCG0100015596 and CCG0100015340 below.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15596	Supported Power State Transitions - Desktop	The Intel® Management Engine Firmware shall support the transitions below: - G3/MOff to S0/AC/M0 - G3/Moff to S5/AC/M3 - Sx/AC/MOff to S0/AC/M0 - Sx/AC/MOff (with Intel® Management Engine WOL) to Sx/AC/M3 - Sx/AC/M3 to Sx/AC/Moff (with Intel® Management Engine WOL) - S0/AC/M0 to Sx/AC/M3 - Sx/AC/M3 to S0/AC/M0 - S0/AC/M0 to Sx/AC/Moff	Yes	Yes	Yes	Yes	Yes
CCG01000 15595	System State presence	An SMBIOS table entry indicating ability and presence shall be included in ALL Intel® AMT-capable systems. Recommended states would be: 0 - AMT capable, not configured 1 - AMT capable, configured 2 - AMT incapable (decommissioned) * For more information see the Intel® AMT BIOS Writers Guide	Yes	Yes	Yes	Yes	Yes
CCG01000 15481	Intel® AMT wake events	The Intel® AMT firmware and system BIOS shall support Intel® AMT wake events.	Yes	Yes	Yes	Yes	Yes
CCG01000 15480	Intel® Management Engine Wake on Wireless LAN	Intel® Management Engine Wake on Wireless LAN shall be supported for wireless LAN device. - In the Sx/M3 state, Intel ME can set up filters in the WLAN NIC to look for such packets as EAP_START packet, TCP ACK packet to the Intel AMT port and ARP request packet to Intel AMT IP address before it goes to Moff. This will provide the mechanism for IT shops to send a wake packet to the NIC. - When system is in Sx/Moff, the WLAN NIC shall have the ability to operate and filter incoming packets; upon a filter match the WLAN NIC should perform WoWME; i.e. wake up Intel ME to M3 (system stays Sx). ME will perform specific manageability tasks in the M3 state. WoWME solution will be robust and symmetrical to manageability through LAN.	No	Yes	No	No	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		- NIC shall also have the ability to perform WoWME upon detecting loss of connection to AP so that Intel ME (in M3 state) can look for another access point to connect to. For the purpose of security 802.1x should be used for authentication. Once in low power (Sx/Moff) state, the NIC should be able to decrypt received encrypted packets (e.g. using 80.211i) before performing the filtering. VPN support will not be provided.					
CCG01000 15479	Enable Intel® Management Engine WOL	The Intel ME WOL feature can be enabled by the ConfigServer.	Yes	Yes	Yes	Yes	Yes
CCG01000 15354	Intel® Management Engine Wake on LAN	Intel® Management Engine Firmware shall provide power saving behavior when the system is running on AC and in Sx This mode defines the following behavior: a) Intel® Management Engine is transitioning between M-off and M3 state triggered by any manageability packet received by Intel® Management Engine. b) The transition back from M3 to M-off will be triggered by the idle timer. c) During this mode the Intel® Management Engine Firmware will maintain its network presence by additional wake-up events for the purpose of DHCP address lease	Yes	Yes	Yes	Yes	Yes
CCG01000 15353	Intel® Management Engine Wake on LAN System Requirements	Intel® AMT must be installed on the system and configured appropriately. Intel® Management Engine Wake on LAN must be enabled. Intel® Management Engine Wake on LAN must be enabled on the console application. The console application must have the capability to wake the system. The idle timer must be configured to the desired value to turn off the Intel® Management Engine.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15352	Intel® Management Engine Wake on LAN Enable/Disable	The Intel® ME FW shall allow the Intel® Management Engine Wake on LAN feature to be enabled and disabled in the following manner: Enable: The ''Enable'' setting allows Intel® AMT to go to Moff upon inactivity in Sx states and wake up from either a WoL event generated by a LAN packet directed to Intel® Management Engine or a periodic alarm that Intel® Management Engine configures to allow AMT to renew DHCP and DNS registration. Disable: The ''Disable'' setting will mean that the Intel® Management Engine can not up from Moff remotely, and only a Host wake event will bring the system back to S0, if Host WOL was set. This will effectively prohibit platform Management once the platform initially transitions to Moff.	Yes	Yes	Yes	Yes	Yes
CCG01000 15340	Supported Power State Transitions - Mobile	The Intel® Management Engine Firmware shall support the transitions below: - G3/MOff to S0/DC/M0 - G3/MOff to Sx/AC/M3 - G3/Moff to S5/Moff - Sx/DC/MOff to S0/DC/M0 - Sx/DC/MOff to Sx/AC/M3 - Sx/AC/M3 to Sx/DC/Moff - S0/DC/M0 to Sx/DC/Moff - S0/AC/M0 to S0/DC/M0 - S0/DC/M0 to S0/AC/M0	No	Yes	No	No	Yes
CCG01000 15339	Legacy Power Packages - Desktop	The following packages will be supported: Required: - Desktop: ON in S0 - Desktop: ON in S0, S3 - Desktop: ON in S0, S3, S4-5 - Optional: - Desktop: ON in S0; ME WoL in S3 - Desktop: ON in S0; ME WoL in S3, S4-5	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15338	Legacy Power Packages - Mobile	The following packages will be supported: Required: - Mobile: ON in S0 - Mobile: ON in S0, S3/AC - Mobile: ON in S0, S3/AC, S4-5/AC - Optional: - Mobile: ON in S0; ME WoL in S3/AC - Mobile: ON in S0; ME WoL in S3/AC, S4-5/AC	No	No	No	No	No
CCG01000 15915	Power Packages - Desktop	The following packages will be supported: Required: - Desktop: ON in S0 Desktop: ON in S0; ME Wake in S3, S4-5	Yes	No	Yes	Yes	No
CCG01000 15914	Power Packages - Mobile	The following packages will be supported: Required: - Mobile: ON in S0 - Mobile: ON in S0; ME Wake in S3/AC, S4-5/AC	No	Yes	No	No	Yes
CCG01000 15319	Intel ME Reset independent of system power policies	No change to Intel ME settings will require the system to enter a different power state. The Intel ME must be able to do a complete reset and reload of the firmware without the system state changing. Moreover at no time will the Intel ME change the system power state unless specifically directed by a user (ex. Using Intel AMT or WebUI).	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14965	Supported Power State Transitions - Mobile for Sx/DC	The Intel® Management Engine Firmware shall support the transitions below: - Sx/DC/M3 to S0/DC/M0 - S0/DC/M0 to Sx/DC/M3 - Sx/DC/M3 to Sx/AC/M3 - Sx/AC/M3 to Sx/DC/M3 - Sx/DC/MOff to Sx/DC/M3 - Sx/DC/M3 to Sx/DC/MOff - G3/MOff to Sx/DC/M3 - Sx/DC/M3 to G3/MOff To be changed to Y for mobile if Sx/DC is supported	No	No	No	No	No
CCG01000 15033	Enable Intel® Management Engine Wake on Wireless LAN	The Intel ME Wake on Wireless LAN feature can be enabled by the ConfigServer.	No	Yes	No	No	Yes
CCG01000 15032	Intel® Management Engine Wake on Wireless LAN Enable/Disable	The Intel® ME FW shall allow the Intel® Management Engine Wake on Wireless LAN feature to be enabled and disabled in the following manner: Enable: The ''Enable'' setting allows Intel® AMT to go to Moff upon inactivity in Sx states and wake up from either a WoL event generated by a LAN packet directed to Intel® Management Engine or a periodic alarm that Intel® Management Engine configures to allow Intel® AMT to renew DHCP and DNS registration. Disable: The ''Disable'' setting will mean that the Intel® Management Engine can not up from Moff remotely, and only a Host wake event will bring the system back to S0, if Host WOL was set. This will effectively prohibit platform Management once the platform initially transitions to Moff.	No	Yes	No	No	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15031	Intel® Management Engine Wake on wireless LAN System Requirements	Intel® AMT must be installed on the system and configured appropriately. Intel® Management Engine Wake on wireless LAN must be enabled. Intel® Management Engine Wake on wireless LAN must be enabled on the console application. The console application must have the capability to wake the system. The idle timer must be configured to the desired value to turn off the Intel® Management Engine.	No	Yes	No	No	Yes

3.3.2 Intel® Active Management Technology KVM Redirection

KVM redirection provides keyboard, video and mouse redirection over IP. The feature enables IT manager to use a remote machine as if he was sitting in front of it.

3.3.2.1 KVM General Requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14964	KVM support by integrated GFX	Support KVM Video sample and sprite with Intel integrated GFX (Also in switchable GFX configuration). When iGFX is enabled through BIOS, the KVM session can start any time.)	Yes	Yes	Yes	Yes	Yes
CCG01000 14963	KVM support by interface to discrete GFX card	Support KVM Video sample and sprite with Discrete GFX card that will support the following Discrete GFX requirements (specify in other items)	No	No	No	No	No
CCG01000 15913	KVM behavior with switchable GFX when only dGFX enabled	If only dGFX is enabled through the BIOS, the KVM session will not open, and if already open will be closed	Yes	Yes	Yes	Yes	Yes
CCG01000 15912	KVM behavior with switchable GFX and a dynamic switch to dGFX	If the OS (Windows Vista*, for example) dynamically switches to dGFX the KVM session will be closed	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14962	KVM Intel Discrete GFX Larrabee	Support KVM Video sample and sprite by Intel Discrete GFX - Larrabee	No	No	No	No	No
CCG01000 14961	KVM keyboard and mouse support	Support KVM Keyboard and Mouse through PCH ME USB composite device	Yes	Yes	Yes	Yes	Yes
CCG01000 14960	KVM local user opt-in	Support Local user opt-in using Intel® ME sprite	Yes	Yes	Yes	Yes	Yes
CCG01000 14959	KVM feature use-case	KVM is used for remote diagnostics and repair. KVM is used by remote operator to view PC screen and control it from remote.	Yes	Yes	Yes	Yes	Yes
CCG01000 14957	KVM connectivity	KVM feature will be offered on all the different Intel® AMT connectivity options	Yes	Yes	Yes	Yes	Yes

3.3.2.2 KVM HW Requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14956	GFX display screen sampling to Intel ME memory	GFX HW shall support sampling Display screen to ME memory when Intel® ME FW initiates a request	Yes	Yes	Yes	Yes	Yes
CCG01000 14955	GFX display sample resolutions	The KVM supported GFX screen resolutions: - Max resolution: 1600 x 1200 - Other resolutions to support: - 640x480 (4:3 aspect ratio) - 800x600 (4:3 aspect ratio) - 1024x768 (4:3 aspect ratio) - 1280x1024 (5:4 aspect ratio) - 1280x800 (16:10 aspect ratio) - 1366x768 (16:9 aspect ratio) - 1440x900 (16:10 aspect ratio) The required performance associated with above resolutions is defined in the Performance req. The maximum required Intel ME memory for screen sample is 3.84Mbytes (16Bits/pixel x 1600 x 1200)	Yes	Yes	Yes	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 49611	KVM GFX display sample resolutions	The KVM supported GFX screen resolutions: - Max resolution: 1920 x 1200 - Other resolutions to support: - 640x480 (4:3 aspect ratio) - 800x600 (4:3 aspect ratio) - 1024x768 (4:3 aspect ratio) - 1280x1024 (5:4 aspect ratio) - 1280x800 (16:10 aspect ratio) - 1366x768 (16:9 aspect ratio) - 1440x900 (16:10 aspect ratio) - 1920x1080 (16:9 aspect ratio) - 1600x1200 (4:3 aspect ratio) - 1920x1200 (16:10 aspect ratio) The required performance associated with above resolutions is defined in the Performance req. The maximum required Intel ME memory for screen sample is 4.4Mbytes (16Bits/pixel x 1920 x 1200)	No	No	No	Yes	Yes
CCG01000 14954	GFX refresh rate	Minimum refresh rate to be supported is 50Hz. This influences the maximum screen sampling rate that KVM can perform.	Yes	Yes	Yes	Yes	Yes
CCG01000 14953	Dual display selection	The Intel ME will be able to control which of the two displays to sample and on which display to present the sprite.	Yes	Yes	Yes	Yes	Yes
CCG01000 14952	GFX screen configuration change notification to Intel ME	When the Host OS changes GFX screen configuration/setting, the Intel ME will be notified by an interrupt.	Yes	Yes	Yes	Yes	Yes
CCG01000 14951	Intel ME and PCH KVM HW Communication with Discrete GFX	Support Communication with Discrete GFX card using MCTP protocol for KVM through the PEG/digital Display port (PCI-e*)	No	No	No	No	No
CCG01000 14950	PCH KVM Tiles comparator	HW will provide Tile comparator functionality that is controlled by Intel ME.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14949	PCH KVM Tiles compression	The KVM HW will provide the following Tile compression methods (as defined in VNC protocol): - Raw encoding (no compression) - RLE with Raw pixel data - RLE with Packet palette types - RLE with Plain RLE - RLE with Palette RLE	Yes	Yes	Yes	Yes	Yes
CCG01001 24560	PCH KVM Tiles compression 2011	The KVM HW will provide the following Tile compression methods (as defined in VNC protocol , in addition to legacy compression methods mentioned in CCG0100014949) : - ZLIB encoding * Zlib encoding is used only when connecting using CIRA	No	No	No	Yes	Yes
CCG01000 14947	Secured ME sprite - integrated GFX	Support the requirements as specified in the Secure Output section.	Yes	Yes	Yes	Yes	Yes
CCG01000 14946	Secure ME sprite sampling by KVM	The KVM HW will not sample the ME Sprite from GFX Video since it might include user sensitive data.	Yes	Yes	Yes	Yes	Yes
CCG01000 14945	Secured input - USB and PS/2 (for USB host controllers that reside in the PCH)	Support the requirements as specified in the Secure Output section..	No	No	No	No	No
CCG01000 14944	KVM Remote Keyboard and Mouse	PCH exposes USB ME configured and controlled composite device. The PCH HW enables ME to expose to host SW a USB Keyboard and Mouse.	Yes	Yes	Yes	Yes	Yes

3.3.2.3 KVM 3d party GFX adapter requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14943	KVM interface to 3rd party GFX adapter	3rd party GFX adapter shall support Communication with ME and KVM HW using MCTP protocol for KVM through the PEG/digital Display port (PCI-e*). The detailed support is defined in the KVM MCTP specification.	No	No	No	No	No
CCG01000 14942	Secured ME sprite	Same definition and support level as for Intel's integrated GFX. Support as defined in Secure I-O section.	No	No	No	No	No
CCG01000 14941	Display output sampling to ME memory	Same definition and support level as for Intel's integrated GFX. The detailed support is defined in the KVM MCTP specification.	No	No	No	No	No
CCG01000 14940	Hybrid GFX support for Mobile	KVM should support hybrid GFX in mobile platform. Hybrid means that both Integrated and Discrete GFX are enabled on the platform. The GFX Host SW selects which one of the GFX to use at given time. In case of KVM, it will be supported only with the Integrated GFX. ME will ask the GFX host SW to switch to Integrated GFX mode when KVM session started. In hybrid GFX the default for BIOS mode is to use the integrated GFX HW. Limitation: When GFX HW was set by Host SW to Discrete GFX mode and the Host SW don't function any mode (Ex: Blue screen) KVM feature will not be supported.	No	No	No	No	No

3.3.2.4 KVM FW Requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14938	KVM FW using KVM HW components	KVM FW shall provide KVM redirection functionality using the PCH and GFX HW components as defined in the KVM HW requirements section above.	Yes	Yes	Yes	Yes	Yes
CCG01000 14937	GFX screen configuration change	When Host OS change GFX screen configuration/setting the ME will be notified by an interrupt. The KVM FW will need to re-initialize all the KVM FW and HW components to work with the new GFX configuration and to notify the VNC Viewer about the change using the RFB protocol.	Yes	Yes	Yes	Yes	Yes
CCG01000 14936	KVM Network protocol for Data Session	FW shall support standard VNC RFB protocol as VNC Server as defined in: http://www.realvnc.com/docs/rfbproto.pdf - RFB protocol spec	Yes	Yes	Yes	Yes	Yes
CCG01000 14935	KVM Network protocol for Data Session protocol versions	FW VNC Server shall support the following VNC RFB protocol versions: - RFB v3.8 or previous versions - RFB v4.0 The protocol version should be automatically detected by the VNC server when the VNC Viewer connecting to it.	Yes	Yes	Yes	Yes	Yes
CCG01000 14934	KVM additions outside to RFB protocol	Additions outside to VNC RFB protocol: - Enable VNC to run over TLS to extend protocol security - Additional Viewer Authentication methods - Kerberos*, Digest	Yes	Yes	Yes	Yes	Yes
CCG01000 14933	KVM Network Control protocol	KVM Management Console SW shall support control protocol over WS-Man. Additional support in control protocol: - KVM Server TCP/TLS listening port - Sample screen selection in case of dual screen	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100014932	KVM FW local user opt-in	KVM FW shall support the following local opt-in options according to the opt-in policy as defined in the KVM CAS. - User agreement for the KVM session opening. - User notification on the KVM session existing during all the life of the session, by providing periodic ME sprite screen pop-up and/or direct screen notifications and/or notification in the Intel® Management and Security Status tray icon. The local user opt-in provided by using ME Secure sprite and/or Intel® Management and Security Status tray icon application.	Yes	Yes	Yes	Yes	Yes
CCG0100014931	Secure Intel® ME sprite localization	Supported Languages: • Ascii and Latin-1 (8859-1) - US - US English, DEU – German, FRA – French, ITA - Italian, ESP - Spanish, PTB - Brazilian Portuguese. • Additional languages - CHT – Chinese Traditional, JPN – Japanese, RSU – Russian, KOR - Korean, CHS - Chinese Simplified The languages will be supported by configuring ME sprite with pallet bitmaps with the appropriate language. The FW will support one set of bitmaps for each language. See Secure Output requirement section for the detailed requirements.	Yes	Yes	Yes	Yes	Yes
CCG0100054807	Secure Intel® ME sprite localization additional languages	in addition to eleven supported legacy languages, support 16 additional languages: 1. Arabic, 2. Czech, 3. Danish, 4. Greek, 5. Finnish, 6. Hebrew, 7. Hungarian, 8. Dutch, 9. Norwegian, 10. Polish, 11. Portuguese-Portugal,	No	No	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		12. Slovak, 13. Slovenian, 14. Swedish, 15. Thai, 16. Turkish The languages will be supported by configuring ME sprite with pallet bitmaps with the appropriate language. The FW will support one set of bitmaps for one language. See "Bitmap field" in Secure Output requirement section. See Secure Output requirement section for the detailed requirements.					
CCG01000 14930	Keyboard input to Intel ME localization	Supported Languages: 1: English and Latin-1 (8859-1) 2: Additional languages will be supported by configuring ME with the appropriate keyboard ''scan codes''. The FW will support one set of Keyboard ''scan codes'' for one language. See Secure Output requirement section for the detailed requirements.	No	No	No	No	No
CCG01000 14929	KVM Audit Log	KVM component should log the following events in the Intel® AMT/ME Audit log: - KVM control Session establishment from remote MC - Log: Time, MC source address, username (if available) - KVM Data Session establishment from remote MC - Log: Time, MC source address, username (if available) Local end user opt-in session open approved and session close operations, if required by KVM configuration policy - Log: Time, opt-in action	Yes	Yes	Yes	Yes	Yes
CCG01000 14928	KVM over WLAN in case of platform boot flow	In order to prevent disconnection on the Sx to S0 transition the KVM FW shall keep Intel® ME control over the WLAN MAC until the KVM session ended and not transition the control to the WLAN Host driver. This uses the same mechanism that already exists for SOL/IDER.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100014927	GFX Display screen selection when dual display is used	The KVM FW shall support remote selection of which screen to sample and present Intel® ME sprite on. The screen selection is part of the KVM network protocol. The default screen to use is display 0 (pipe 0)	Yes	Yes	Yes	Yes	Yes
CCG0100014926	KVM Keyboard and Mouse support	KVM FW should expose to host over ME USB composite device HW a USB keyboard and mouse according to USB HID spec. The supported keyboard and mouse should support both legacy boot keyboard and mouse protocol and full HID class compatible keyboard and mouse devices. The keyboard and Mouse devices inputs are redirected to the FW from remote KVM Viewer in the VNC RFB protocol.	Yes	Yes	Yes	Yes	Yes
CCG0100014925	KVM USB Mouse types	The full HID mouse implementation should be of an absolute mouse and not relative (since KVM redirection protocol is redirect the absolute mouse location). Note: the legacy/boot mouse implementation can be only of a relative mouse according to USB HID spec	Yes	Yes	Yes	Yes	Yes
CCG0100014924	EAC posture extension for KVM	AMT EAC posture should be extended with KVM session information the same as done for SOL/IDER	Yes	Yes	Yes	Yes	Yes
CCG0100014923	Performance Corporate LAN network BW	The minimum required supported network BW by KVM HW, FW and SW inside the corporate network is 10Mb/sec.	Yes	Yes	Yes	Yes	Yes
CCG0100014922	Performance Corporate WLAN network BW	"The minimum required supported network BW by KVM HW, FW, and SW inside the corporate WLAN network is 8Mb/sec. Note: Performance over WLAN is highly dependent on environment factors such as the connection's band (802.11a/b/g), number of STAs associated with the serving AP, and - for pipe mode connection - the host WLAN traffic *Note: Performance numbers are currently being re-evaluated and are expected to change."	No	Yes	No	No	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14921	Performance Corporate Local LAN/Local WLAN Frames Updates per second	Support 15 screen updates per second (FPS) to KVM viewers. Assumptions: - For resolution (1600 x 1200) and 16Bits/pixel - For steady state of average 10% screen change between samples - The compression rate of KVM server is 1/6.6 (based on RLE Algorithm POC)	Yes	Yes	Yes	Yes	Yes
CCG01000 14920	Performance Corporate Local LAN/Local WLAN First full screen redirection time	The Maximum time required for first full screen sampling and transition to Viewer according to the required resolutions over corporate LAN/WLAN BW (see above items) will be less than 1 Second (For maximum resolution 1600x1200, 16Bit/Pixel)	Yes	Yes	Yes	Yes	Yes
CCG01000 14919	Performance ZLIB support for Broadband (ADSL, Cable Modem) connections	The KVM FW shall support ZLib compression on top of the RLE compression by HW to provide full ZRLE. This is to improve the compression ratio by 2-3X for slow Broadband connections.	No	No	No	Yes	Yes
CCG01000 14915	KVM local Enable Disable	"MEBx should provide control option to Enable/Disable KVM feature (similar to what already supported for SOL/IDER). The default setting is disabled in the FW image. OEM will have the option to change the default to enable at manufacturing time."	Yes	Yes	Yes	Yes	Yes
CCG01000 14914	KVM local session start opt-in Enable Disable	KVM local session start opt-in option should be controlled by OEM configuration through FIT/FPT flag. This flag determines whether this option can be disabled from MEBx by Intel® AMT user. The default setting of the FIT/FPT flag is enabled. The FIT/FPT flag can be differently configured for Consumer and Corporate platforms.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100014913	Handling BIOS Boot flow while KVM session is active	While KVM session is active and the PC is doing boot process the BIOS should get indication from KVM ME FW that the FW initialized all the KVM HW devices before BIOS enumerate the platform devices. This is to enable KVM redirection for the BIOS boot flow. This specifically related to initialization of the KVM USB keyboard and Mouse	Yes	Yes	Yes	Yes	Yes
CCG0100014912	KVM over WLAN in S0/H0	As part of KVM session creation the KVM network protocol will define link sensitive policy this will determine whether to keep ME control over the WLAN MAC or leave the control to the WLAN host driver.	Yes	Yes	Yes	Yes	Yes
CCG0100014911	KVM Server data session listening port	KVM data session is supported on the following TCP/TLS server ports (only one at given time): - AMT redirection TCP/TLS port - 16994 and 16995 respectively. - VNC server port -- 5900	Yes	Yes	Yes	Yes	Yes
CCG0100014910	KVM usage of Intel® Management and Security Status tray icon	The KVM FW shall work with the Intel Management and Security Status tray icon application for the following support for KVM: Provide to Tray icon the Status of KVM session - Active/not Active - Notify to user to close protected content (PAVP) to allow Sprite usage, when PAVP is operational.	Yes	Yes	Yes	Yes	Yes
CCG0100014909	KVM session behavior when protected content (PAVP) is enabled	Intel® ME receives indication from GFX HW (by HW registers) if the PAVP functionality is enabled. In case user will not close protected content (PAVP) after notification using Intel® Manageability and Security Status Tray Icon, the KVM FW will fail any Console request for new KVM session. If PAVP is enabled while KVM session is active, KVM FW will get an interrupt and will close KVM session with appropriate error message.	Yes	Yes	Yes	Yes	Yes

3.3.2.5 KVM MEBx/BIOS Requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14908	KVM Enable Disable	MEBx should provide control option to Enable/Disable KVM feature (similar to what already supported for SOL/IDER). The default setting is enabled. OEM will have the option to change the default at manufacturing time.	Yes	Yes	Yes	Yes	Yes
CCG01000 14907	KVM session start opt-in Enable Disable	When KVM feature is enabled, MEBx should provide control option to force ME Secure opt-in option when KVM session is started (for the first session approval). This control should have FW image FIT/FPT flag that control if this control option can be disabled from MEBx by AMT configuration. The default setting of the FIT/FPT flag is enabled. The FIT/FPT flag can be set differently for Consumer and Corporate platforms.	Yes	Yes	Yes	Yes	Yes
CCG01000 14906	Handling BIOS Boot flow while KVM session is active	While KVM session is active and the PC is doing boot flow the BIOS should get indication from KVM ME FW that the FW initialized all the KVM HW devices before BIOS enumerate the platform devices. This is to enable KVM redirection for the BIOS boot flow. This specifically related to initialization of the KVM USB keyboard and mouse.	Yes	Yes	Yes	Yes	Yes

3.3.2.6 KVM SW Requirements

KVM SW support includes the following parts:

- Intel® Management & Security Status tray icon (IMSS)
- Intel® AMT SDK
- Intel® AMT SCS
- KVM Viewer application
- FAUPD tool update

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14905	SDK: KVM Network protocol for Data Session	SDK should include KVM Viewer SW that shall support standard VNC RFB protocol as VNC Viewer as defined in: <http://www.realvnc.com/docs/rfbproto.pdf> - RFB protocol spec	Yes	Yes	Yes	Yes	Yes
CCG01000 14904	SDK: KVM Network protocol for Data Session protocol versions	KVM VNC Viewer and SDK shall support the following VNC RFB protocol versions: - RFB v3.8 or previous versions - Only Over TCP - RFB v4.0 - Only Over TCP - RFB v4.0 with Intel extensions - Over TCP or TLS The protocol version should have user selection option.	Yes	Yes	Yes	Yes	Yes
CCG01000 14903	SDK: KVM additions outside to RFB protocol	Additions outside to VNC RFB protocol: - Enable VNC to run over TLS to extend protocol security - Additional Viewer Authentication methods - Kerberos*, Digest	Yes	Yes	Yes	Yes	Yes
CCG01000 14902	KVM Host SW: Secure Intel ME sprite localization and keyboard localization	The KVM Host SW shall configure KVM FW to one of the following supported Languages: 1: English or Latin-1 (8859-1) 2: Additional languages available as defined in ''Bitmap field'' in Secure Output requirement section.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14901	SDK: Secure Intel ME sprite localization bitmap preparation tools	Intel will provide a tool that will prepare ME sprite pallet bitmaps of the KVM opt-in screens.	No	No	No	No	No
CCG01000 14900	Intel® Management and Security Status tray icon support for KVM	Intel Services tray icon application shall have following support for KVM: - Status of KVM session - Active/not Active - Configurable option to get event when KVM session is starting. Notify user to close secured content (PAVP) to allow Sprite usage. - Configuration of KVM FW to support one of the following languages: 1: English or Latin-1 (8859-1) 2: Additional languages available as defined in ''Bitmap field'' in Secure Output requirement section.	Yes	Yes	Yes	Yes	Yes
CCG01000 14899	SDK: KVM Viewer application	Intel KVM Viewer library shall be provided as binary library. The library will be customizable, allowing ISVs to apply their own branding and ''look and feel''. The Viewer application Binary will be provided on the following OSs: Windows* XP Windows Vista* Windows Server 2003* Redhat Enterprise Linux	Yes	Yes	Yes	Yes	Yes
CCG01000 14898	SDK: KVM Samples	The SDK will provide samples for doing a remote control operation, opening a KVM session + GUI front end for the sample (Windows only)	Yes	Yes	Yes	Yes	Yes
CCG01000 14897	SDK: EAC posture extension	EAC posture should be extended with KVM session information similar to IDER session information - including session status(open, closed), console IP and port	Yes	Yes	Yes	Yes	Yes

3.3.3 IPv6 Support

3.3.3.1 Network Topology Requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14874	Connect IPv6 over wired interface	FW will support receiving and sending data over IPv6 on wired Ethernet interface	Yes	Yes	No	Yes	Yes
CCG01000 14873	Connect IPv6 over wireless interface	FW will support receiving and sending data over IPv6 on WiFi interface.	No	Yes	No	No	Yes
CCG01000 14872	Connect IPv6 over WiMAX interface	Transmission of IPv6 packets over 802.16(e) is not specified yet.	No	No	No	No	No
CCG01000 14871	Connect IPv6 over WWAN interface	FW will support receiving and sending data over IPv6 on WWAN interface.	No	No	No	No	No
CCG01000 15448	Connect IPV6 shared MAC with dedicated IPV6 address	The FW wired and wireless LAN interfaces share the MAC address with the host. In the process of IPv6 auto-configuration FW supports generating an IPv6 address from the shared MAC address to produce a unique 64-bit identifier as required by RFC 2373. However, since FW is interested in generating a unique IPv6 address that differs from the host address, FW does not derive this address form the MAC address according to IEEE EUI-64 format global identifier standard as recommended by RFC 2373 when an IEEE EUI-48 bit identifier is available. Instead, when generating the address FW replaces the EUI-64 FFFE in the 4th and 5th octets with 8086. For compliance with RFC 2373 it is required that FW sets the "u" bit (universal/local bit in IEEE EUI-64 terminology) to zero (0) to indicate local scope of this auto-generated address.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14870	Connect IPV6 dual Stack support	FW will support dual IPv4/IPv6 on each network interface. FW will support both IPv4 and IPv6 address configuration and packet transmission (TCP connections and UDP) on each network interface. The IPv4 configuration will be shared with host or manually configured. The IPv6 configuration will be dedicated (not shared with host) configuration possibilities are described separately.	Yes	Yes	No	Yes	Yes
CCG01000 14869	Connect IPV6 IPV4-IPV6 static point to point Tunneling	Intel® Management Engine Firmware will support a configured IPV6 over IPV4 tunnel so that it can communicate with an IPV6 Network over an IPV4 infrastructure (IPV6 packets are encapsulated in IPV4 headers). Requirements: - The IPV4 address of tunnel end point is configured by the user - A globally unique IPV4 global address is assigned to the Intel® Management Engine Firmware - IPV6 prefix is assigned to the Intel® Management Engine Firmware	No	No	No	No	No
CCG01000 14868	Connect IPV6 IPV4-IPV6 6to4 Tunnel	When Intel® Management Engine Firmware is configured to enable IPV6 it will support connecting to "6to4" address via a "6to4" router that has advertised a "6to4" prefix on the Intel® Management Engine Firmware's link. The form of a 6to4 prefix is: 0x2002<6to4 router IPV4 address><subnet ID>/64 Remark: Intel® Management Engine Firmware will not support creating a 6to4 prefix for itself it must get the prefix from a "6to4" router. It is required that the infrastructure is IPv6 capable and supports 6to4.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14866	Connect IPV6 IPV4-IPV6 automatic Tunnel using ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) addressing	When Intel® Management Engine Firmware is configured to enable IPV6 and it is configured with an IPV4 address it will automatically configure itself with an ISATAP address and try to connect to an ISATAP router to get the ISATAP router prefix advertisements over the ISATAP tunnel. Once all is configured Intel® Management Engine Firmware may communicate with other ISATAP hosts via the ISATAP tunnel or with Native IPV6 hosts via a tunnel with the ISATAP router. The form of an ISATAP address is: <prefix>:0:5EFE :<IPv4 Address of host> (ISATAP defines a method for generating a link-local IPv6 address from an IPv4 address, and a mechanism to perform Neighbor Discovery on top of IPv4 without using IPv4 multicast).	No	No	No	No	No
CCG01000 14865	Connect IPV6 IPV4-IPV6 Protocol translation	When Intel® Management Engine Firmware is configured with an IPV6 address and an IPV4 address it will support translation of IPV6 protocol packets to IPV4 protocol packet in order to connect to IPV4 nodes.	No	No	No	No	No
CCG01000 14864	DHCPv6 interoperability	The Intel® Management Engine Firmware DHCPv6 client implementation should be interoperable with the following DHCPv6 servers/routers (listed by importance): Minimum: - Cisco - server, relay (stateless DHCPv6 only) - Windows Server 2008 - Dibbler	Yes	Yes	No	Yes	Yes
CCG01000 14863	IPv6 Routers interoperability	- Cisco - Foundry	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 19860	WLAN RF transition to WiMAX	When the wireless is operating in ME link control the transition to wiMAX will fail. When operating in host link control, the transition to WiMAX will succeed, and there will be no manageability features available over WiMAX	N/A	Yes	N/A	TBD	TBD

3.3.3.2 IPv6 Setup and Configuration Requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15444	IPv6 Setup and Configuration of the IPV6 options	The FW will export an API for the user to determine the following IPv6 settings from BIOS MEBx screen or USB Key and over the WS-MAN and WebUI interfaces: Global IPv6 settings - available over WS-MAN only: - Select Precedence of IPv4 over IPv6 interface or vice versa (default is that IPv4 has precedence) - DHCPv6 solicit timeout Per Interface settings - WS-MAN, MEBx, WebUI: - Enable/Disable IPv6 per interface - default is disabled - Setting static IPv6 configuration for wired LAN interface - Select the mechanism for generation of IPv6 Interface ID that is used for link local address and router auto-configured global address. - Interface ID (see separate sections for details on the different options)	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015443	IPv6 Setup and Configuration over IPv6	Intel® Management Engine Firmware will support provisioning over IPv6 if FW has initialized an IPv6 interface successfully (see details on IPv6 interface initialization in separate section). By default IPv6 will be disabled on all interfaces. Hence zero touch bare metal provisioning will not be supported. For provisioning over IPv6 it is required to first enable the FW ipv6 interfaces either using a local SW command or via MEBx/USBKey. The FQDN of the Intel® AMT Configuration Server (SCS) will be resolved to IPv4 and IPv6 addresses as registered in DNS. The FW will give precedence to the IPv4 address and will try to reach the configuration server over the IPv4 address. If the Configuration Server is not reachable via the IPv4 address or the FQDN was resolved only to an IPv6 address then FW will attempt to connect to the IPv6 address of the Configuration Server and send Hello messages over IPv6. Before provisioning takes place the FW is not yet configured with a FQDN and hence cannot register it in DNS (or other Presence Server - Open). Since the FW IPv6 address is not shared with the host, the Configuration Server must use the IPv6 address in the Hello packet sent by FW or find other means to obtain the FW IPv6 address using local host SW in order to connect back to Intel® ME to start the provisioning process over IPv6.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15705	IPv6 SKUing	IPv6 capability may differ from one platform SKU to another. FW should determine IPv6 capability by checking platform information using the FW SKU manager. On platforms with SKU that has IPv6 disabled all the ME IPv6 configuration interfaces including host (MEBx screens, ME INFO etc, Intel® Management and Security Status), WS-MAN and WebUI will be disabled. MEBx and WebUI will not display IPv6 configuration options. Intel® ME will not accept IPv6 addresses as parameter to interfaces.	Yes	Yes	Yes	Yes	Yes
CCG01000 14862	Soft SKU for IPv6	The Intel® Management Engine Firmware soft SKU manager will support enabling and disabling IPv6. On platforms with SKU that has IPv6 disabled all the ME IPv6 configuration interfaces including host (MEBx screens, ME INFO etc, Intel® Management and Security Status), WS-MAN and WebUI will be disabled. MEBx and WebUI will not display IPv6 configuration options. ME will not accept IPv6 addresses as parameter to interfaces.	No	No	No	No	No
CCG01000 14861	IPv6 Setup and Configuration of Manually set Interface ID	Support setting the IPv6 Interface ID per interface from BIOS MEBx configuration screen, USB Key, WS-MAN. This should be used only if collision was detected and the auto-configured FW interface ID cannot be used. (Not supported by WebUI)	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14860	IPv6 Setup and Configuration of the global static IPV6 address	FW will support manual configuration of a static global IPv6 address on the wired LAN interface. This address is configured as an alternative address and may be used in parallel to auto-configured IPv6 addresses. The following parameters may be set for static IPv6 address configuration in BIOS MEBx configuration screen, USB Key, WS-MAN or WebUI: - Additional IPv6 address - DNS primary IPv6 address - DNS secondary IPv6 address - Additional Default IPv6 router The DNS address settings will be overridden by settings that FW gets from DHCPv6 server.	Yes	Yes	No	Yes	Yes
CCG01000 14859	IPV6 Setup and Configuration of the globally unique 64 bit Interface ID	There are several options for configuration of the unique 64-bit IPv6 Interface ID that constructs the lower part of the auto-configured IPv6 address. The user may select one of the following options in BIOS MEBx configuration screen, USB Key, WS-MAN interfaces: 1. Intel® AMT creates the 64-bit Interface Identifier according to RFC 3041.(using MD5 on the interface's MAC address and a 64 bit random number generated using the Intel® AMT RNG) - this will be the default. 2. Intel® ME generates the 64 bit Interface ID from the 48-bit MAC address in EUI-64 format and replaces 0xFFFE in octets 4 and 5 with - 0x8086 while flipping the u bit appropriately. Suitable for privacy considerations. 3. Manual configuration (Not supported by WebUI)	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14858	IPv6 Setup and Configuration global setting to enable/disable IPv6	Intel® ME FW will support an option to disable and enable IPv6 per interface in BIOS MEBx configuration screen, USB Key, WS-MAN or WebUI. . If IPv6 is disabled on a specific interface then: - FW will not configure IPv6 addresses on any of the network interfaces. - The Web GUI and MEBx will not display IPv6 configuration options. - Intel® ME FW will still accept IPv6 addresses in settings such as PET subscriptions, MPS IP addresses etc.	Yes	Yes	No	Yes	Yes
CCG01000 14856	IPv6 Setup and Configuration Intel® AMT IPv6 FQDN	Intel® ME will be configured with a dedicated IPv6 address hence it must also be configured with a dedicated (not shared with host) FQDN that will be associated with this address in the DNS. In order to register this FQDN in DNS Intel® ME FW is required to integrate a dynamic DNS Update client. If the Intel® ME FW Dynamic DNS Update client is enabled, then the FW will register in DNS the ME FQDN A and AAAA RRs for the IPv4 and all the IPv6 addresses that Intel® ME is configured with. This Intel® ME FQDN should be the FQDN used in the: - TLS certificate for TLS Server, TLS Client and 802.1x - Kerberos SPN = FQDN + port (Active directory has pointer to FQDN). - NAC Posture For backward compatibility with Management Consoles that do not support IPv6, the TLS certificate and Kerberos SPN should include both the host and the ME FQDN. SCS and SDK configuration sample should support generating these certificates. *** Additional requirements for the FW Dynamic DNS Update Client are in the Intel® ME Presence section.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14855	IPv6 Setup and Configuration of multicast group address	FW will support configuring an IPv6 group multicast address that the LAN interface will listen on. This is defined for future use.	No	No	No	No	No
CCG01000 14854	IPv6 Setup and Configuration getting status of IPv6 auto-configuration	FW will supply a host (AMTHI, MEBx) and network interface (Web-UI and WS-MAN method) for getting the status of auto-configuration of the IPv6 interface (this may be the same API that gets IP settings from FW). The status will be displayed by the WebUI, MEBx and the ME Tray Icon. The following should be returned per interface: - List of Configured IPv6 addresses, address type (auto-conf etc) and status (collision detected, preferred, valid etc.) - Default GW. - DNS primary and secondary IPv6 addresses	Yes	Yes	No	Yes	Yes
CCG01000 14853	IPV6 Setup and Configuration of IPv6 addresses for client initiated features	Intel® AMT may be configured with: - FQDN/URL of target - Literal IPV6 address in URL e.g. [2001:db8:100:2a5f::1] (RFC 2732) for client initiated connections. - IPv6 address in string format (RFC 1884) Intel® AMT will not accept link local addresses since Intel® AMT is multi-homed and the network stack will not know which interface to use for the outgoing connection.	Yes	Yes	No	Yes	Yes
CCG01000 14852	IPv6 Setup and Configuration WSMAN	All WSMAN Profiles and classes that configure IP addresses for different Intel® AMT features such as Network Configuration, WS-Eventing, MPS addresses etc. will be updated to support IPv6.	Yes	Yes	No	Yes	Yes
CCG01000 14851	IPv6 Setup and Configuration EOI	No EOI, PTNI, AMTNI or OS accessible PTHI APIs will be updated to support IPv6. Backward compatibility will be kept.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14850	IPv6 Setup and Configuration MEBx	All relevant MEBx APIs that allow configuration of IP addresses for different AMT features such as Configuration Server address will be updated to support configuration of IPv6 addresses. In addition MEBx will support configuring IPv6 options - see separate MEBx section for details. All fields configurable via MEBx will also be configurable via USB Key	Yes	Yes	No	Yes	Yes
CCG01000 14849	IPv6 Setup and Configuration WebUI	WebUI will support configuring IPv6 options per interface: - Enable/Disable IPv6 per interface Static IPv6 configuration (details in separate section) WebUI will support getting IPv6 configuration: - List of Configured IPv6 addresses. - addresses Any other pages that allow setting IP addresses for different features will be updated to support configuration of IPv6 addresses as well. Backward compatibility will be kept.	Yes	Yes	No	Yes	Yes

3.3.3.3 IPv6 Network Presence Requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15447	Connect IPV6 DNS Resolving for IPV6 A6 records	FW will support name resolution to IPV6 addresses of A6 records (RFC 2874)	No	No	No	No	No
CCG01000 15446	Connect IPV6 DNS Resolving for IPV6 AAAA records	FW will support name resolution to IPV6 address of AAAA records (RFC 1886)	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15441	Connect IPV6 Network Presence Stateless address auto-configuration with IPv6 router discovery	Intel® Management Engine FW will support automatically configuring a link local IPV6 address (RFC 2462). FW will support discovering an IPv6 router on the link and automatically configuring a global IPV6 address based on router advertisements of the IPV6 address prefix (RFC 2462). FW will support requesting network configuration options (DNS primary and secondary addresses) from a DHCPv6 server on the link (stateless DHCPv6 - RFC 3736). FW will fail to resolve host names if the DNS address was not configured by either the DHCP/DHCPv6 server or manually. FW will use a unique interface ID that is different from the host interface ID to maintain its own dedicated set of IPv6 addresses.	Yes	Yes	No	Yes	Yes
CCG01000 15440	Connect IPV6 Network Presence stateful DHCPv6 address configuration with DHCPv6	FW will support negotiating with a DHCPv6 Server configuration of a global IPV6 address per interface (RFC 3315). FW will use a unique DUID that is different from the host DUID to maintain its own dedicated set of IPv6 addresses.	Yes	Yes	No	Yes	Yes
CCG01000 15439	Connect IPV6 Network Presence WLAN L3 and L4 IPV6 Filters	The FW will configure the manageability IPV6 filters in the WLAN SW and FW drivers to forward packets that are destined to the FW IPV6 addresses to the FW. WLAN FW and SW need to filter and forward the following packets to ME FW: - 4 MNG L3 ME dedicated IPv6 addresses filters (can filter by 24 LSB) - Filters for ICMPv6 packets - port filters for TCP over IPv6 - port filtering for UDP over IPv6 WLAN Microcode will support these filters for ME WoL	No	Yes	No	No	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15438	Connect IPV6 Network Presence WLAN MAC Filters	The FW will configure the manageability dedicated L2 MAC filters in the WLAN SW and FW drivers to receive the All Nodes Multicast IPV6 address and to receive solicited node multicast addresses for each address configured on the network interface. Remark: SW/FW will supply 4 MAC L2 multicast filters. WLAN Microcode will support these filters for ME WoL	No	Yes	No	No	Yes
CCG01000 15437	Connect IPV6 Network Presence LAN HW MAC Filters	The FW will configure the manageability dedicated L2 MAC filters in the LAN HW to receive the All Nodes Multicast IPV6 address and to receive solicited node multicast addresses for each address configured on the network interface. Remark: HW will supply 4 shared L2 MAC filters that can be locked for write by ME FW so that not be set by host	Yes	No	No	Yes	No
CCG01000 14847	Connect IPV6 Network Presence LAN IPV6 L3 and L4 Filters	The FW will configure the manageability IPV6 filters in the LAN hw to forward packets that are destined to the FW IPv6 addresses to the FW. - 4 MNG L3 ME dedicated IPv6 addresses filters (can filter by 24 LSB) - Filters for ICMPv6 packets - port filters for TCP over IPv6 port filtering for UDP over IPv6	Yes	Yes	No	Yes	Yes
CCG01000 14846	Connect IPV6 support of IPV6 header extensions by LAN OOB Rx filters	The LAN HW OOB Rx filters support processing the following IPV6 extension headers: - Hop-by-Hop Option - Destination Option - Routing	Yes	Yes	No	Yes	Yes
CCG01000 14845	Connect IPV6 Network Presence support of IPV6 header extensions by WLAN OOB Rx filters	The WLAN FW/SW OOB Rx filters supports processing the following IPV6 extension headers: - Hop-by-Hop Option - Destination Option - Routing Fragment	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15402	Connect IPV6 Network Presence Static IPv6 address configuration	The network stack will support: - Auto-configuration of 1 link-local IPV6 address - Auto configuration of a node local (loopback) IPv6 address - One global IPv6 address manually configured from the BIOS screen, USB Key, WS-MAN or WebUI. This address may be configured in parallel with auto-configured IPv6 addresses configured by router advertisements and dhcpv6 server.	Yes	Yes	No	Yes	Yes
CCG01000 14843	Connect IPV6 Network Presence dynamic IPv6 address configuration	The network stack will support: - Auto-configuration of 1 link-local IPV6 address - Auto configuration of a node local (loopback) IPv6 address - Two auto-configured global IPV6 addresses configured based on router advertisements (this allows FW to have both a native IPv6 address and a 6to4 IPv6 address if advertised by a 6to4 router) One global address configured by the DHCPv6 server.	Yes	Yes	No	Yes	Yes
CCG01000 15401	Connect IPV6 Network Presence support of IPV6 header extensions in ME Network Stack	The Intel® Management Engine FW Network Stack supports processing the following IPV6 extension headers: - Hop-by-Hop Option - Destination Option - Routing	Yes	Yes	No	Yes	Yes
CCG01000 15436	Connect IPV6 Network Presence stateful DHCPv6 FQDN option	If dynamic IP addressing is enabled FW will support maintaining the DNS presence of the AMT machine configured with an IPV6 address by using the DHCPv6 FQDN option. Restriction: The FQDN option will not be used if Secure Dynamic DNS Update is enabled.	No	No	No	No	No
CCG01000 14844	Connect IPV6 Network Presence DNS registration of IPV6 address with dynamic DNS update	Intel® ME FW will support dynamic DNS update /creation of the AAAA record entries in the DNS server for its global IPV6 addresses. FW will maintain these records in the DNS to prevent aging of the records.	Yes	Yes	No	Yes	Yes

3.3.3.4 SW Support for IPv6

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14842	LMS Support for APF over IPv6	LMS must support forwarding to Intel® AMT TCP connections established by MC over IPv6, and sending on behalf of Intel® AMT both UDP and TCP packets over IPv6 to destinations requested by Intel® AMT. For this end LMS must support APF protocol with IPv6 support. LMS must be written as a dual IPv4/IPv6 application	Yes	Yes	No	Yes	Yes
CCG01000 15901	UNS connects to LMS via IPv6	UNS connects (subscribes for events or sends WS-MAN requests) to LMS via IPv6	No	No	No	No	No
CCG01000 14841	LMS Support for local connections over IPv6	For local connections LMS supports both IPv4 loopback and IPv6 loopback connections.	Yes	Yes	No	Yes	Yes
CCG01000 14840	Intel® Management and Security Status Support for IPv6	Intel® Management and Security Status will support displaying the FW IPv6 addresses received through UNS.	Yes	Yes	No	Yes	Yes
CCG01000 15900	SDK ZTCLocalAgent support for Setup and Configuration over IPv6	FW IPv6 functionality is disabled by default. For delayed setup and configuration over IPv6 the local configuration SW will need to call a FW local API that enables IPv6	Yes	Yes	No	Yes	Yes
CCG01000 14838	Management Console and SDK support for IPv6 communication	The MC SDK must be able to perform communication within an IPv6 network including communicating with ME FW and SCS over IPv6.	Yes	Yes	No	Yes	Yes
CCG01000 14837	Management Console and SDK dual stack support	The MC SDK should be a dual stack client application so that it may communicate with both IPv6 capable and IPv4-only capable Intel® AMT systems.	Yes	Yes	No	Yes	Yes
CCG01000 14836	Management Console and SDK configuration of IPv6 options in FW	The MC SDK must support WSMAN methods for configuring the IPv6 addressing options	Yes	Yes	No	Yes	Yes
CCG01000 14835	Management Console and SDK support for IPv6 configuration of client initiated FW applications	The MC SDK must support configuration of IPv6 addresses for Intel® AMT CI features via WSMAN methods	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14834	Management Console and SDK support for IPv6 configuration of Environment Detection	The MC SDK must support WSMAN method for configuring the local IPv6 Prefixes for Environment Detection	Yes	Yes	No	Yes	Yes
CCG01000 14833	Redirection Console support for IPv6	The redirection console should support connecting to Intel® AMT over IPv6.	Yes	Yes	No	Yes	Yes
CCG01000 14832	KVM Redirection Console Support for IPv6	The KVM redirection console should support connecting to Intel® AMT over IPv6.	Yes	Yes	No	Yes	Yes
CCG01000 14831	Management Console and SDK and redirection consoles support for Intel® AMT dedicated FQDN	MC and redirection consoles should support Intel® ME FW using a different FQDN and different IPv6 address from the host.	Yes	Yes	No	Yes	Yes
CCG01000 14830	Management Console and SDK support for IPv6 SAL	MC must support parsing IPv6 address in Secure Audit Log locations table	Yes	Yes	No	Yes	Yes
CCG01000 14829	ME INFO Tool IPv6 support	ME INFO Tool will display IPv6 configuration options - via MEI interface	Yes	Yes	No	Yes	Yes
CCG01000 14827	SCS support for IPv6 communications	The SCS must be able to perform communication within an IPv6 network Console --> SCS --> Database. SCS --> ME FW Etc.	No	No	No	No	No
CCG01000 14826	SCS dual stack support	The SCS Server should be a dual stack server application so that it may communicate with both IPv6 capable and IPv4 only capable Intel® AMT systems and MNG Consoles.	No	No	No	No	No
CCG01000 14825	SCS and support for dedicated Intel® AMT FQDN	SCS must support Intel® AMT using a dedicated IPv6 address and dedicated FQDN that differs from host. SCS must accommodate registration of dedicated FQDN within AD. SCS must export an API for MC to get the AMT FQDN by host FQDN and vice versa. SCS must accommodate issuance of device SSL server certificate using the dedicated FQDN instead of the Host FQDN for: TLS (RSA) certificate for TLS Server, TLS Client, 802.1x Kerberos* SPN = FQDN + port (Active directory has pointer to FQDN).	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14824	SCS support for configuring Intel® AMT IPv6 options	SCS Must support WSMAN methods for configuring the FW IPv6 functionality:	No	No	No	No	No
CCG01000 14823	SCS support for WS-MAN methods for configuring Intel® AMT with IPv6 addresses for client initiated Intel® AMT applications	SCS must support configuration of IPv6 addressing information for all WS-MAN methods supported by SCS. Such as MPS addresses, notification sinks etc.	No	No	No	No	No
CCG01000 14822	SCS support for extending API between SCS and Management Consoles for configuring IPv6 options and addresses for client initiated Intel® AMT applications	SCS SOAP API with MNG Consoles should be extended to support IPv6 addressing, where applicable including: - New APIs to configure IPv6 addressing functionality of AMT - Existing APIs that should be extended to include also IPv6 addresses.	No	No	No	No	No
CCG01000 14821	SCS support for IPv6 configuration of Environment Detection	The SCS must support WSMAN method for configuring the local IPv6 Prefixes for Environment Detection	No	No	No	No	No
CCG01000 14820	MPS support for IPv6 communications	The MPS must be able to perform communication within an IPv6 network Console --> MPS --> ME FW. ME FW --> MPS --> Console	Yes	Yes	No	Yes	Yes
CCG01000 14819	MPS support for IPv6 in APF protocol	MPS will implement support for IPv6 in Intel® AMT Port Forwarding Protocol	Yes	Yes	No	Yes	Yes
CCG01000 14818	NAC/NAP Plug-in support for IPv6	NAC/NAP Plug-in must support parsing the IDER console IPv6 address in the NAC/NAP posture.	Yes	Yes	No	Yes	Yes
CCG01000 14816	SDK Sample for Secure Audit Log support for IPv6	Will need to support parsing IPv6 addresses in the log	Yes	Yes	No	Yes	Yes
CCG01000 15704	Tools Support for IPv6	As detailed in the Tools PRD	Yes	Yes	No	Yes	Yes

3.3.3.5 Intel® MEBx support for IPv6

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14815	MEBx support for configuring IPv6 options	MEBx must support AMTHI set and get IPv6 configuration APIs. Per interface settings: - Enable/Disable IPv6 - Interface ID generation method - Interface ID - Static IPv6 configuration (details in separate section) MEBx will support getting and displaying the current static IPv6 settings. Should be supported by USB Key as well These APIs must be disabled when MEBx is finished, before BIOS loads, OS, bootloader or diagnostic image	Yes	Yes	No	Yes	Yes
CCG01000 14814	MEBx support for configuring AMT Configuration Server IPv6 address	MEBx must support AMTHI API for configuration of Intel® AMT Configuration Server IPv6 address Should be supported by USB Key as well This must be disabled when MEBx is finished, before BIOS loads, OS, bootloader or diagnostic image	Yes	Yes	No	Yes	Yes
CCG01000 14813	MEBx support for static IPv6 address	MEBx must support AMTHI API to manually configure an IPv6 address and network settings on the wired LAN interface: - Additional IPv6 address - DNS primary IPv6 address - DNS secondary IPv6 address - Additional Default IPv6 router The DNS address settings will be overridden by settings that FW gets from DHCPv6 server This API must be disabled when MEBx is finished, before BIOS loads, OS, bootloader or diagnostic image.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15703	MEBx support for IPv6 Skuing	IPv6 capability may differ from one platform SKU to another. MEBx should check FW support for IPv6. FW provides an AMTHI API for MEBx to query FW whether the platform is IPv6 capable. On platforms with SKU that has IPv6 disabled all the ME IPv6 configuration interfaces including MEBx screens will be disabled. MEBx will not display IPv6 configuration options.	Yes	Yes	Yes	Yes	Yes

3.3.3.6 IPv6 Support for Intel® ME Features

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15445	Support IPV6 connection to management console in the Enterprise	The Intel® Management Engine FW and SW SDK will support ISV Management Console connecting to Intel® Management Engine firmware over an IPV6 connection. Notes: - In mixed IPV4/IPV6 environments the management consoles must be dual stack so that they can connect to IPV4 and IPV6 managed nodes. - FW will support creating an IPV6 connection only if the corporate/ISP infrastructure supports IPV6 (i.e. there is a router connected to the FW node that supports IPV6)	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15442	IPv6 PETs sending IPV6 SNMPv1 PETs	Intel® Management Engine Firmware will support sending PETs over IPv6 to an IPv6 configured subscriber. The ''agent-addr'' that contains the PET src IP address field in the PET will be set to zeros. Note: The PET collector needs to identify the source of the PET based on the transport layer IPV6 address and community string or by other means such as GUID or device ID.	Yes	Yes	No	Yes	Yes
CCG01000 14812	Support Connect IPv6 connection with Redirection Console	The Intel® AMT FW and the Redirection Console will support redirection console connecting to AMT over IPv6 and SOL/IDER/KVM-R sessions over IPv6	Yes	Yes	No	Yes	Yes
CCG01000 14811	IPv6 Client initiated connections	The Intel® Management Engine FW will support all client initiated connections supported by FW over IPv6	Yes	Yes	No	Yes	Yes
CCG01000 14809	IPv6 PET Collector will support Dual IPv4/ IPv6	The PET collector must be configured to DUAL IPv4/IPv6 so that it can collect PETs from both IPv4 and IPv6 configured Intel® AMT machines	Yes	Yes	No	Yes	Yes
CCG01000 14808	IPv6 LAN QoS Marking	The QoS tagging feature shall use Layer 3 only by using DSCP (6 highest order bits in the TOS field of the IP packet header) QoS marking shall be done to the DSCP part of the IP header TOS (Type Of Service) Field in IPv4 and the traffic class field in IPv6. Like in SD, the filters shall be implemented in HW What about Ethernet header tagging mentioned in SyAS?	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14807	IPV6 anti-spoofing	If Intel® AMT Anti-Spoofing is enabled and IPv6 is enabled then in addition to setting one of the 5 hw Anti-Spoofing filters to the shared IPv4 address Intel® AMT will also set Anti-Spoofing filters for IPv6 addresses as well. Intel® AMT will filter by the 64 bit prefix of the source IPv6 address in host transmitted packets. Intel® AMT learns all the legal IPv6 prefixes on the link from the RA and from the DHCPv6 Server and sets the Anti-Spoofing filters to filter by these prefixes. Intel® AMT does not filter by the 64 bit suffix (Interface ID) since this by standard may be randomly selected by the host for using temporary IPv6 addresses. Limitations: 1. Intel® AMT has only 5 anti-spoofing filters. If the number of legal prefixes on the link exceeds the number of available filters the anti-spoofing for IPv6 packets will be disabled (i.e. all host transmitted IPv6 packets will pass). 2. This feature should be disabled if Host IPv6 prefixes are configured manually. 3. This feature should be disabled if host is automatically configuring tunneling (non-native) IPv6 prefixes. 3. There is no support for inspecting tunneled IPv6 packets in IPv4 frames and vice versa. The filters are matched only against the outer frame. 4. In cases where the FW anti-spoofing capability cannot be used as listed above, IT can configure the CB filters to perform anti-spoofing according to the network configuration known to IT.	No	No	No	No	No
CCG01000 14806	IPv6 ME Wake on LAN	ME Wake on LAN is supported for any IPv6 packet that can pass an OOB MNG Rx filter for both Wired and Wireless LAN interfaces	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14805	IPV6 System Defense Packet scanning filters (SD Filters)	Intel® AMT FW will support configuring the SD filters for IPv6 in LAN HW and WLAN FW/SW. System Defense maximum of packet scanning capabilities: - 30 Transmit IPv6 filters (27 if Base Heuristics are enabled). - 31 Receive IPv6 filters - 1 Else filter for Transmit and 1 else filter for receive Limitations \ Notes : - The logic for a proper use of the filters must be managed by the remote application. The FW shall not apply any rule checking on the policies set from remote. It is expected that the ISV application shall have the proper logic to manage the filters. - Each filter can be either an IPv4 filter or an IPv6 filter or both IPv4 and IPv6 if the filter is layer 4 (port) filter. - Filtering of tunneled IPv6/IPv4 packets is not supported (hw will only look at the outer frame for IP filtering and will fail to filter by L4 for tunneled packets) If Base Heuristics feature is active, the FW will use 3 of the TX System Defense filters to support the heuristics, reducing the number of available Tx filters to 27.	Yes	Yes	No	Yes	Yes
CCG01000 14804	Outbreak Containment Heuristics	FW will support heuristics to detect if the host machine was infected by a network worm using IPv6 communication to spread on the network.	No	No	No	No	No
CCG01000 14803	Ping6 Enable/Disable	When IPv6 is enabled FW will support API to configure whether to answer ping6 requests or not (same setting as FW has for IPv4).	No	No	No	No	No
CCG01000 14802	IPv6 local connections over the IPv6 loopback interface.	LMS will support local connections over the host IPv6 loopback interface on an IPv6-only host: (user notification, FWUpdateLocal tool etc.)	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14801	Connect IPv6 Wake on VoIP	FW will support SIP WoVIP applications over IPv6. IPv6 address is not shared with the host. FW will need to maintain presence of Host IPv6 address with SIP Server. IPv6 addresses of the host must be sent to Intel® AMT. Intel® AMT will wake the host by these addresses. Intel® AMT must support both the host's IPv4 address and host's IPv6 addresses independent of current Intel® AMT IP configuration.	No	No	No	No	No
CCG01000 14800	IPv6 Wake on Event	FW will support wake on Event features over IPv6.	No	No	No	No	No
CCG01000 14798	Connect IPv6 ZTC	ZTC will be supported by FW over IPv6	Yes	Yes	No	Yes	Yes
CCG01000 14797	Home IT	FW will support IPv6 for Home IT SKU of Intel® AMT	No	No	No	No	No
CCG01000 14796	Connect IPv6 Remote Access connectivity using MPS	The Intel® Management Engine Firmware will support opening a TLS VPN tunnel connection to the MPS (in DMZ) over IPv6 and receiving incoming connections forwarded by MPS to FW over this tunnel. The MPS will support Intel® AMT Port Forwarding Protocol with IPv6 support. This includes support for forwarding connections from management consoles to FW over IPV6 and sending PETs to MC over IPv6 to notify that a certain endpoint has connected to MPS. FW can support connecting to an MPS over IPv6 in the following network environments: 1. ISP deployed a native IPv6 service. 2. ISP does not provide native IPv6 but it does provide a public IPv4 address and the home router supports 6to4 tunneling. Note: FW does not support protocol translation (NAT-PT) and Teredo that are used for enabling IPv6 for ISP networks that do not support IPv6	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14795	Connect IPv6 Environment Detection	If Environment Detection is configured by the user Intel® Management Engine Firmware will use the following methods to detect its current location in an IPv6 network environment if detection for the IPv4 network has failed: 1. FW will compare the DNS Suffixes in the DHCPv6 option 24 ''DNS Domain Search List'' (RFC 3646) to the configured corporate valid Suffix List. It is required that the DHCPv6 server be configured with this option. 2. FW will compare the auto-configured IPv6 prefix to the configured IPv6 prefix list. If there is no DHCPv6 server located on the network (or DHCPv6 option 24 is not available) and the configured IPv6 prefix does not match the configured prefix list then Intel® Management Engine Firmware will assume that it is OUTSIDE the corporate network.	Yes	Yes	No	Yes	Yes
CCG01000 14794	802.1x in IPv6 environment	Intel® Management Engine Firmware will support 802.1x in IPv6 environment. Intel® Management Engine Firmware will detect when the ME 802.1x supplicant needs to be active and when it needs to be passive by introducing new logics that can work in IPv6 environments. FW will support logging an IDER console IPv6 address in the NAC/NAP posture.	Yes	Yes	No	Yes	Yes
CCG01000 14793	EAPoUDP in IPv6 environment	EAPoUDP will be supported for IPv6	No	No	No	No	No
CCG01000 14792	Audit Log	FW will support logging IPv6 addresses in the audit log locations table.	Yes	Yes	No	Yes	Yes

3.3.4 SHA-2 Support

Until now Intel® AMT utilized SHA-1 hash function. However, recent research showed that SHA-1 is not collision-resistant enough, and hence the industry shall move to SHA-2 hash function family.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14791	Support SHA-2 SHA-256 and SHA-384	All places in FW where SHA-1 is used should use SHA-2 except places where HMAC (SHA-1) is used and special cases where 3rd party support for SHA-2 is required but non-existent. There is support for SHA-256 in HW and kernel. There is support for SHA-384 in kernel (implemented in FW). SHA-256 must be supported (i.e. minimum requirement) for features that must add SHA-2 support. However, since low effort recommended to support SHA-384 depending on feature (i.e. target requirement). The outstanding requirement is to support SHA-224 and SHA-512.	Yes	Yes	Yes	Yes	Yes
CCG01000 14790	NAC/NAP signature in EAC Posture should use SHA-2	It will be possible to sign NAC posture with SHA-256. It is recommended to also support signing with SHA-384.	Yes	Yes	N/A	Yes	Yes
CCG01000 14789	Audit Log trail signature should use SHA-2	It will be possible and sign Audit Log trail with SHA-256. It is recommended to also support signing with SHA-384.	Yes	Yes	N/A	Yes	Yes
CCG01000 14788	FW TLS stack with TLS 1.0 will accept Digital Certificates that are signed with SHA-2.	FW will support validating the signature of a PKI certificate signed with SHA-2. FW should support certificates signed with the following algorithms: - minimum requirement: SHA-256 - target requirement: SHA-384 - outstanding requirement: SHA-224, SHA-512. For provisioning FW will also support PKI certificate SHA-2 hashes, hashed with SHA-256 (minimum requirement) or SHA-384 (target requirement).	Yes	Yes	N/A	Yes	Yes
CCG01000 14787	Support external API for remote setting of SHA-2 mode for NAC Signature in EAC posture.	Support ability to set different mode of SHA to NAC i.e. SHA-1 or SHA-256 or SHA-384. Default will be SHA-1 for backward compatibility.	Yes	Yes	N/A	Yes	Yes
CCG01000 14786	Support external API for getting the posture SHA-2 Hash	Support ability for NAC/NAP plug-in to determine hash algorithm when getting the posture hash. The hash algorithm can be either SHA-256 or SHA-384 or SHA-1. Default is SHA-1 for backward compatibility	Yes	Yes	N/A	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14785	Support external API for remote setting of SHA-2 mode for Audit Log trail signature	Support ability to set different mode of SHA to Audit Log trail signature i.e. SHA-1 or SHA-256 or SHA-384. Default will be SHA-1 for backward compatibility.	Yes	Yes	N/A	Yes	Yes
CCG01000 14784	WS-MAN Support	Setting SHA-2 for the different applications will be part of a WS-MAN profile. Must support ability to set different mode to NAC and to Audit log (e.g. NAC will work with SHA-1 and Audit Log will support SHA-256).	Yes	Yes	N/A	Yes	Yes
CCG01000 14783	EOI Support	Setting SHA-2 for the different applications will be part of the EOI APIs	No	No	N/A	No	No
CCG01000 14782	Performance must be not more than twice the time it took to sign with SHA-1	Performance will probably be less than twice the time - not crucial since these are one time operations; but it's good to ensure that our SHA-2 implementation is optimized so that we do not have to worry about it later.	Yes	Yes	Yes	Yes	Yes
CCG01000 15702	SDK, SCS: SHA-2 support	All relevant Intel® ME SW components (SCS, SDK samples) should support the WSMAN methods for configuring SHA-2 for the different features. The support of Intel® ME SW components (SCS, SDK samples) for TLS with SHA-2 certificates depends on the OS that the SW is running on. Setup and Configuration SDK and SCS should support generating and provisioning SHA-2 signed TLS certificates.	Yes	Yes	N/A	Yes	Yes

3.3.5 Intel® ME Secure Output

In 2010 platforms, the Secure Output coverage includes the following:

Display output in the form of a sprite that is controlled by the Intel® ME.

The Secure Output service allows Intel® ME applications to communicate with the user by using simple forms that are rendered by the service on the user's monitor. The user communicates with the form to convey data back to the controlling application.

For text I/O, the service provides support for basic ASCII and Latin-1 (8859-1) characters. However, the controlling application can provide a pre-rendered bitmap for the service to display to the user. This allows the controlling application to localize the output while using simple ASCII input (or other ME IO form capabilities such as check box or combo box).

For 2010/11, the following ME applications uses the Secured Output service

to get user consent in a secured (un-spoofable by malware) way:

KVM - when a KVM session is about to start.

Using Serial Over LAN to redirect BIOS screens and OS Boot text screens

IDE-Redirect

Changing boot sources for remote boot (e.g. causing a boot from PXE).

3.3.5.1 Secure output HW requirements

Description of hardware requirements needed to support secure output.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14781	Secured ME sprite - integrated GFx	- 512x256 pixels sprite panel - 8bpp (ARGB - 1,2,3,2 bits coding. A means transparent (see through) pixel) - Support all video modes, including VGA - Keying is disabled - Once ME assumes control, only ME can control its operation and release control. - Using ME UMA memory for raster. - X2 zoom support (into 1024x512 rectangle). - GTT must be bypassed in this mode (physical addresses). - Any intermediate storage after raster has been read from the ME UMA need to be protected.	Yes	Yes	Yes	Yes	Yes
CCG01000 14780	GFX ME and host applications using overlay (sprite) HW (including PAVP) coexistence	Intel® ME is sharing the Sprite HW with other host applications that uses the overlay HW including PAVP. Intel® ME does not have any access to PAVP content. While any Host application is using the overlay HW ME can't use the ME sprite and should wait till the Host applications release the overlay HW.	Yes	Yes	Yes	Yes	Yes

3.3.5.2 Secure output requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14772	Display decision (pipe)	The Intel® ME IO service decides which output pipe should be used for the sprite.	Yes	Yes	Yes	Yes	Yes
CCG01000 14770	Timeout - terminating secIO flow	Upon the following scenario, Secure Output is terminated: - Intel® ME app can ask Secure Output to terminate the sprite.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14769	Logo sprite	Intel® ME application (KVM specifically) can present a sprite that is mostly transparent, to form a logo on the screen. User should be able to continue using the OS normal flow when this logo is presented.	No	No	No	No	No

3.3.5.3 Secure Output requirements

This section describes the requirements on the inter-relationship between the input capability and the output capability of the service.

Main philosophy: a sprite is a form that the user can fill/interact in/with. The controlling application provides the form definition to the secure service and receives back the filled form when the user hits an "OK" button. The sprite has a header and footer that cannot be directly controlled by the application. The rest of the sprite panel is controlled by the application by sending down a detailed description of the form to the IO service. For more data, refer to the ME secure IO SAS.

The form takes the general shape from the complete rendering definition of the controlling application and then the specific form elements are also rendered on top of it to format the complete form. Those elements include: text and bitmaps elements, text input, checkboxes and combo-boxes. The controlling application provides these packed in a specific structure to the IO service. When the user finishes, the service returns the user input (or picks etc) to the controlling application. (i.e., no callbacks supported for this generation).

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14767	Secure Output API for Intel® ME apps	Secure Output will provide Intel® ME apps with the following APIs: - Assume control and release control of Secure Output / sprite (if it is not currently in use) - Send form to Secure Output - Terminate sprite. - Read Secure Output configuration that includes: - Secure Output enabled/disabled - language configuration	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14766	Error codes from Secure Output to Intel® ME app	- no graphics support detected - sprite is owned by SW (and user doesn't want to shut it down) - sprite is in use (by other Intel® ME app)	Yes	Yes	Yes	Yes	Yes
CCG01000 14765	Glyph support (actual character bitmaps)	8x13, as defined in the sprite output spec, for ASCII+8859-1 characters Font: Neo Sans Intel	Yes	Yes	Yes	Yes	Yes
CCG01000 14764	Dialog element 1: Text field	Basic field containing text that can be defined with foreground and background color. Location is within the form.	Yes	Yes	Yes	Yes	Yes
CCG01000 14763	Dialog element 2: Bitmap field	Compressed (1bpp) or uncompressed bitmap that is smaller than the size of the complete form can be placed in a specific location inside the form. This requirement helps with localization. More than one bitmap is allowed in the form.	Yes	Yes	Yes	Yes	Yes

3.3.5.4 Secure Output - sprite synchronization

As the Gfx hardware overlay is shared between the Gfx driver and the Intel® ME, there need to be a synchronization mechanism to eliminate corner cases of SW grabbing control while Intel® ME is using the sprite etc.

For that, the Intel® ME will grab control over the sprite only after it has been notified by Intel® ME-SecOutput-SW entity, that this SW currently owns the sprite resource.

This synchronization mechanism affects Intel® ME FW, SW and validation.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14762	ME FW to implement synchronization mechanism	Per the definition, unless system is in pre-boot.	Yes	Yes	Yes	Yes	Yes
CCG01000 14761	ME SW to implement synchronization mechanism	Per the definition. This should be implemented inside existing ME SW entities.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14760	ME app override (for KVM)	ME application (e.g. KVM) can force Secure Output service to override the use of this synchronization mechanism. It is in the responsibility of the ME app to use this override with care. (e.g., after operator talks with	Yes	Yes	Yes	Yes	Yes

3.3.6 Intel® AMT WLAN (General)

This section refers to Intel® AMT WLAN on Mobile platforms (Huron River) and Desktop platform (Sugar Bay) that are fitted with WLan Card (Taylor Peak).

Intel® AMT 7.0 provides the ability to manage client systems out of band over a WLAN connection in S0/H0, S0/HX and Sx system states. Intel® AMT 7.0 will also support Agent Presence checking/alerting and Asset inventory in the presence of a host based L3 VPN while in S0/H0.

Due to the complexity of the 802.11 MAC layer, the WLAN implementation is not symmetric between the different system states: when OS is functional, and when there is no OS functional. That results in a different requirement set per system state.

The WLAN sections in the PRD describes the sub requirements from the WLAN stack in order to establish WLAN connection; once a WLAN connection was established, all Intel® AMT applications might use that connection very same way as they use the wired connection.

WLAN support will have a major impact (positively) on the adoption rate of Intel® AMT in general. This is a requirement to get to a 50% or higher adoption rate.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15548	WLAN General	The Intel® Management Engine Firmware shall enable an OOB connection over the wireless link in S0/H0, S0/Hx and Sx mode. WLAN OOB connection in Sx mode is operational only on AC power. Note: Sx support is not available in Intel® AMT 2.5 and Intel® AMT 2.6 releases.	N/A	Yes	N/A	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15547	WLAN Power States	The WLAN OOB connection shall be available in S0/H0, S0/Hx, and Sx power states. (and V-aux is provided to the WLAN NIC) > The WLAN OOB won't be available when in S0 and host driver failed to establish WLAN connection (no matching profile, authentication failed etc.) Exception: The Intel® Management Engine Firmware MAY disable the OOB connection (wired and WLAN) according to its link policy.	N/A	Yes	N/A	Yes	Yes
CCG01000 15546	WLAN Symmetric Manageability	The OOB connection over WLAN shall provide the same services the LAN link does as specified in section: Intel® AMT Connection model & OOB. Unsupported AMT features over WLAN connectivity: > Dedicated Mac + Static IP > Setup and configuration over WLAN > Once out-of-band KVM/IDER session is open, host wireless connection is unavailable to the user	N/A	Yes	N/A	Yes	Yes
CCG01000 15545	WLAN Modes	The Intel® Management Engine Firmware shall provide the following operation mode: A WLAN link using the same MAC address and same IP address as the Host's WLAN link.	N/A	Yes	N/A	Yes	Yes
CCG01000 15544	WLAN User Notification	Intel® AMT shall provide User Notification for WLAN events in the following: - Management device overrides host Radio. - Management device relinquishes control over host Radio.	N/A	Yes	N/A	Yes	Yes
CCG01000 14759	WLAN HW Support	Intel® Management Engine Firmware shall support following WLAN network interface cards: - Puma Peak - Intel® AMT 6.0/7.0 - Kilmer Peak - Intel® AMT 6.0/7.0 - Taylor Peak – WiFi 2x2 AGN - (New) Intel® AMT 7.0 - Rainbow Peak 2 – WiFi 2x2 AGN + Bluetooth -(New) Intel® AMT 7.0	N/A	Yes	N/A	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14758	WLAN ME wake support	The Intel® Management Engine Firmware shall enable a ME wake on wireless LAN functionality in Sx states on AC power.	N/A	Yes	N/A	Yes	Yes
CCG01000 15182	WLAN connectivity without a matching profile configured explicitly in the ME	The ME FW shall connect over any host wireless connection (within the limits of Environment Detection) in case no profile was configured in the Intel® ME. The following requirements shall be met to mitigate security risks (switch): 1. The wireless management interface shall be explicitly enabled 2. Environment detection shall be configured for the domains on which this feature will be used 3. The potential security risks associated with this feature are documented in the SDK 4. Optionally, the IT administrator may choose to use TLS for all management traffic to guard against sniffing of wireless traffic 5. Host must connect to a secure wireless profile. Note: this requirement is valid only if WLAN profile synchronization is disabled (needed for WLAN over CIRA feature)	N/A	Yes	N/A	Yes	Yes

3.3.7 Intel® AMT Wireless Profiles

This section refers to Intel® AMT WLAN on Mobile platforms (Huron River) and Desktop platform (Sugar Bay) that are fitted with WLan Card (Taylor Peak).

This section specifies the requirements for managing the WLAN profiles.

When the OS is functional the WLAN connection is managed by the Host wireless link manager (using the Host WLAN profiles and not the Intel® Management Engine WLAN profiles)

Specific details on APIs, interfaces and soap calls required to manage WLAN profiles in the flash either remotely via EOI or WebUI are outside the scope of this document. Please refer to the Intel® AMT SDK for this technical information.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15543	WLAN Profiles Predefined Networks	When OS is not functional, The WLAN stack shall connect only to pre-defined networks; these networks are defined in WLAN profiles	N/A	Yes	N/A	Yes	Yes
CCG01000 15542	WLAN Remote Profiles Mgmt	The Intel® Management Engine Firmware shall provide Remote Management Applications with the functionality to Add, delete, update and enumerate WLAN profiles. (using EOI interface) When the host WLAN driver is not functional, only profiles that are configured in the Intel® Management Engine are used when establishing WLAN connection.	N/A	Yes	N/A	Yes	Yes
CCG01000 15540	WLAN Remote Profiles Number	The wireless stack SHALL support 16 BSS profiles, stored in FLASH, and prioritized by preference. Remark: The profile's priority is used to determine the order for choosing the wireless network to connect to.	N/A	Yes	N/A	Yes	Yes
CCG01000 14757	WLAN Local Profiles Number	The WLAN stack SHALL support 8 BSS profiles for local management, stored in FLASH, prioritized by preference. Remark: The profile's priority is used to determine the order for choosing the WLAN network to connect to.	N/A	Yes	N/A	Yes	Yes
CCG01000 14756	Unprovisioning event	Upon unprovisioning event, both remote and local profile databases should be cleared.	N/A	Yes	N/A	Yes	Yes

3.3.8 Intel® AMT WLAN Miscellaneous

This section refers to Intel® AMT WLAN on Mobile platforms (Huron River) and Desktop platform (Sugar Bay) that are fitted with WLan Card (Taylor Peak).

This section specifies miscellaneous requirements for Intel® AMT WLAN, that are not part of the other Intel® AMT wireless sections.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15539	WLAN HW RF Kill	When end user turns-off the radio by using a HW switch, this will stop both the Intel® AMT WLAN and host use of the radio. The regular operation will be resumed once the radio is turned on, either by the Host driver or by Intel® AMT WLAN, according to the current system state (H0/Hx/Sx)	N/A	Yes	N/A	Yes	Yes
CCG01000 15538	WLAN NIC Configured Param	The parameters used by the WLAN stack for Intel® AMT can be configured from Host OS while the Host driver is alive and running. The parameters are: - Radio State (on/off). - MAC address - Band capabilities Note: Behavior of WLAN Intel® AMT ignores applied NCPA settings when the host driver is down	N/A	Yes	N/A	Yes	Yes
CCG01000 15537	WLAN Watchdog	WLAN Intel® AMT stack shall provide watchdog mechanism detecting when WLAN Host driver is malfunctioning or is disabled. In such cases WLAN Intel® AMT stack will regain ownership on the NIC and a proper notification will be send to OS Log system.	N/A	Yes	N/A	Yes	Yes
CCG01000 14755	WLAN SW RF Kill	When end user turns-off the radio by using a SW switch, provided that the host WLAN driver is enabled and functional, this will stop both the Intel® AMT WLAN and host use of the radio. WLAN Intel® AMT shall store SW RF Kill status when host driver goes down and shall not allow any RF transmit until next time host will be up and radio will be switched on by the user.	N/A	Yes	N/A	Yes	Yes

3.3.9 Intel® AMT WLAN MAC & PHY Capabilities

This section refers to Intel® AMT WLAN on Mobile platforms (Huron River) and Desktop platform (Sugar Bay) that are fitted with WLan Card (Taylor Peak).

When Intel® AMT WLAN owns the WLAN NIC for OOB Wireless communication, the WLAN connection is achieved with the capabilities described in this section.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15536	WLAN MAC IEEE 802.11	[802.11], 802.11a, 802.11b, and 802.11g mandatory features SHALL be supported. 802.11i mandatory features SHALL be supported. Mandatory features that SHALL NOT be supported: IBSS. (mandatory) and all related PICs PC6: fragmentation.	N/A	Yes	N/A	Yes	Yes
CCG01000 15535	WLAN MAC IEEE 802.11e	[802.11e SHALL NOT be supported. WLAN Intel® AMT stack shall partially support 802.11e as part of 802.11n feature. Please see [802.11n] section. This spec states how STAs and APs define quality of service data flows and how STA and APs access the media to ensure quality of service.	N/A	Yes	N/A	Yes	Yes
CCG01000 15534	WLAN MAC IEEE Regulatory	WLAN out-of-band regulatory shall be based on the following mechanism: On 5.25 - 5.35 GHz channels, AMT WLAN transmit power will be limited to maximum level of 14dbm. On all other channels, transmit power will be limited to corresponding values specified within NIC EEPROM.	N/A	Yes	N/A	Yes	Yes
CCG01000 15533	WLAN MAC IEEE 802.11i	802.11i mandatory BSS operation shall be supported. IBSS operations shall not be supported. The Optional features list of 802.11 IEEE Specs, TGi section defines a Robust Security Network (RSN). A RSN association is based on 802.1X or PSK, and used TKIP or AES -CCMP for encryption	N/A	Yes	N/A	Yes	Yes
CCG01000 15532	WLAN MAC IEEE 802.11j	802.11j mandatory operations SHALL be supported. 802.11j defines 4.9GHz-5GHz Operation in Japan. 10MHz (narrow) channels are not supported in KDR	N/A	No	N/A	Yes	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15531	WLAN MAC IEEE 802.11n	[802.11n] shall be supported according to the following guidelines: When associating with an AP that supports 802.11n, WLAN driver shall declare 802.11n support capabilities (which also require or imply 802.11e support), Overview description: a. Declare support for 20MHz, 2x2, but activate a single transmitter chain (for power) b. Support 11n PHY (GI, coding, and Rx assisted rate control) and MRA c. Ignore frames received at rates > 24Mb/s (CLINK bus bottleneck) Reasoning: 802.11n connections can work at rates 24mb/s, 54Mb/s or higher. Since Clink bus throughput is 33Mb/s, Intel® Management Engine Firmware should ignore frames received at 54Mb/s. Note: This requirement relevant only for 11n supported SKUs.	N/A	Yes	N/A	Yes	Yes
CCG01000 15530	WLAN MAC WFA WPA1	WPA1 BSS operation shall be supported. WPA1] is a subset of a particular draft version of 802.11i Standard. (Security).	N/A	Yes	N/A	Yes	Yes
CCG01000 15529	WLAN MAC WFA WPA2	[WPA2] mandatory BSS operation shall be supported. WPA2 is a subset of a particular version of 802.11i Standard. (Security).	N/A	Yes	N/A	Yes	Yes
CCG01000 15528	WLAN MAC WFA WMM	[WMM] SHALL Not be supported [WMM] is a subset of a particular draft version of 802.11e Standard. (QoS).	N/A	No	N/A	Yes	No
CCG01000 15527	WLAN MAC Cisco CCX	The following features shall be supported: CCXv1: - S01 Compliance to All Mandatory Items of 802.11 is Required - S02 Client required to be able to defragment - S03 CTS/RTS - S05 Clients are required to support active scanning - S08 802.1X-2001 Compliance Required - S11 EAP packets are sent unencrypted	N/A	Yes	N/A	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		- S12 Broadcast key rotation support required - S20 Encapsulation Transformation Rule IE (ignored) - S21 AP IP address IE (ignored) - S22 Symbol IE (ignored) - S25 In multicast and broadcast, traffic may not decrypt correctly (due to VLAN support), ignore if this happens (do not roam) - S28 If the client is configured with an SSID, then it will use that SSID in a probe request - CCXv2: - S24 AP may respond to more than one SSID - S26 Clients should ignore missing SSIDs in beacons - S30 WPA Compliance - S31 AP Control of Client Transmit Power - CCXv3: - S41 EAP-FAST - S44 QoS compatible (only when connecting to 11e network) - S48 WPA2 - CCXv4: - S58 EAP-FAST Enhancements Any other feature of CCX SHALL NOT be supported Disclaimer: There above requirements are not related to Cisco CCX test plans. Cisco test plans cannot be fully verified since some of the functionality is missing (for example: CKIP protocol).					
CCG01000 15526	WLAN MAC Encryption	WLAN Intel® AMT stack shall support the following encryption mechanism: - CCMP - TKIP WLAN Intel® AMT stack shall NOT support CKIP mechanism.	N/A	Yes	N/A	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15525	WLAN MAC Authentication	WLAN AMT stack shall support the following Authentication mechanism: - WPA - RSN - WPA-PSK - RSN-PSK	N/A	Yes	N/A	Yes	Yes
CCG01000 14754	WLAN CCXv5 support	CCXv5: - S67 Management Frame Protection - for Unicast management frames only - S71 - Interpretation of Status and Result Codes	N/A	No	N/A	Yes	No
CCG01000 14753	WLAN security	WLAN Intel® AMT stack shall support the following encryption mechanism: - WEP - No encryption	N/A	Yes	N/A	Yes	Yes
CCG01000 14752	WLAN MAC Authentication	WLAN AMT stack shall support the following Authentication mechanism: - Open	N/A	Yes	N/A	Yes	Yes

3.3.10 WS-MAN Interface Alignment

This section defines the WS-MAN alignment requirements to drive an open interface approach to Intel® AMT across product lines to improve ISV adoption.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15408	External OOB interface	Intel® AMT will support external interfaces as defined in the DMTF DASH 1.0 Implementation Requirements specification. This includes support for the following WS-Man security profiles: http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/mutual/digest http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/spnego-kerberos http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/spnego-kerberos http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/mutual/spnego-kerberos Limitation: Intel® AMT FW shall support the ''interop'' namespace and may support the AMT and IPS namespaces (e.g. http://<fqdn> :<port>/AMT) for all WS-MAN / DASH operations.	Yes	Yes	Yes	Yes	Yes
CCG01000 15406	Profile supported	Intel® AMT will support all the profiles listed in Section 4.3.12.1, Supported CIM Profiles and Interfaces	Yes	Yes	Yes	Yes	Yes
CCG01000 15405	WS eventing	Intel® AMT will support Event Services as specified in the DASH 1.0 Implementation Requirements specification.	Yes	Yes	Yes	Yes	Yes
CCG01000 15404	WS Setup and Configuration	The default interface that Setup and Configuration uses is EOI. Intel® AMT will support Setup and Configuration Services using the WS-MAN interface. The Setup and Configuration tool may be configured to use the AMT WS-MAN or EOI interface.	Yes	Yes	Yes	Yes	Yes
CCG01000 15403	WS Security	Intel® AMT will support equivalent security to current HTTP Basic Authentication by supporting WS-Security Username / Password tokens in the SOAP header.	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15371	WS-MAN un-configuring and partial un-configuring	When set to work in WS-MAN mode, Intel® AMT will support WS-MAN commands for un-configuring and partial un-configuring. Once these commands are executed, Intel® AMT will return to the default interface mode (EOI).	Yes	Yes	Yes	Yes	Yes
CCG01000 15276	WS-MAN Only Mode	The firmware will have an option for WS-MAN / DASH only mode that can be set during setup and configuration or by the management console at any time. This WS-MAN only mode will include all DASH compliant profiles and operation and Intel proprietary WS-MAN / CIM profiles for capabilities not specified by DASH. The option for the management console to switch to WS-MAN only mode from WS-MAN/EOI simultaneous mode shall be a WS-MAN operation.	Yes	Yes	Yes	Yes	Yes
CCG01000 15149	Addition wsmid:Identify response fields	The optional ''wsmid:ProductVendor'' property shall be required and shall contain the value 'Intel® '; the optional ''wsmind:ProductVersion'' property shall be required and shall contain the value 'AMT 6.0' for AMT 6.0 firmware, returning the correct value corresponding to the AMT firmware version.	Yes	Yes	Yes	Yes	Yes
CCG01000 15188	Port Configuration	Intel® AMT Setup and Configuration Services must provide configuration of the manageability service port to be either the Intel defined AMT port(s) or the DMTF defined WS-MAN Port or both active simultaneously. When the service port is configured to be one or the other the specified port will be used to receive remote console requests for the EOI and WSMAN interfaces or for the WS-MAN only mode interface. The default is both ports active simultaneously.	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15043	Persistent EndPointReferences(EPRs)	EPRs must be persistent as long as the referenced resource exists. When AMT issues an EPR to a management client, and the management client uses that EPR to access an AMT resource, AMT must accept that identical EPR and correctly access the referenced resource without fault as long as that resource exists.	Yes	Yes	Yes	Yes	Yes
CCG01000 14749	WS external interface for new features	Any new interface exposed as a web service will be WSMan only. No new EOI commands will be added.	Yes	Yes	Yes	Yes	Yes
CCG01000 14748	Interface Modes	ME Common Services will support two interface modes; 1) An interface with both WS-MAN and EOI (SOAP) simultaneously; 2) a WS-MAN only interface. The interface will be determined during Set and Configuration, and may be changed at any time using a WS-MAN operation. The default interface will be the interface with simultaneous WS-MAN and EOI (SOAP). The WS-MAN only mode will include all DASH compliant profiles and operation and Intel proprietary WS-MAN / CIM profiles for capabilities not specified by DASH. The option for the management console to switch to WS-MAN only mode from WS-MAN/EOI simultaneous mode shall be a WS-MAN operation	Yes	Yes	Yes	Yes	Yes
CCG01000 14747	Equivalent interfaces	All the capabilities, options, methods, operations, settable or configurable variables available in AT6 EOI must have an equivalent via the WS-MAN interface. It is acceptable for WS-MAN to have capabilities, options, method and variables that EOI does not support.	Yes	Yes	Yes	Yes	Yes
CCG01000 14746	Wsa:EndpointReferences	All wsa:EndpointReferences sent by the manageability service in responses to management applications requests shall be provided in the format documented in DMTF DSP0227 Section 5 default addressing model using selector values that specify properties of the CIM class being referenced. All Key properties must be represented.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14745	Persistent EndpointReferences	All EndpointReferences sent by the manageability service in responses to management applications requests, shall be valid as long as entity represented by the referenced instance exists	Yes	Yes	Yes	Yes	Yes
CCG01000 14744	WS eventing (DASH)	Intel® AMT will support Event Services using the DMTF Indications Profile and DASH specifications.	Yes	Yes	Yes	Yes	Yes
CCG01000 14743	Un-configuring and partial un-configuring	Intel® AMT will support WS-MAN and EOI commands/operations for un-configuring and partial un-configuring. Once Intel® AMT is unconfigured, it will return to the default interface mode (WS-MAN and EOI simultaneous mode).	Yes	Yes	No	Yes	Yes
CCG01000 14742	Association Filter Dialect	Intel® AMT shall support Association Filter Dialect defined in DMTF DSP0227. The implementation of Association Filter Dialect may be constrained as follows: Support of IncludeResultProperty is not required.	Yes	Yes	Yes	Yes	Yes
CCG01000 14741	Final DASH 1.0 profiles	DASH profiles supported in AMT before AMT 6.0 shall be upgraded to the final version of the DASH Profile specification if they are not already supporting the final version. This includes upgrading to the CIM Schema version specified in the final specifications and upgrading to Final (if available) or current (if Final is not available) versions of the DMTF infrastructure specifications for WS-MAN, CIM and their mapping and binding specifications. There is no requirement for the firmware to maintain backward compatibility with DMTF specification versions released before the Final versions of the specifications.	No	No	No	No	No
CCG01000 14740	Unique ElementNames	Each instance of a class with an ElementName property shall have a unique "User friendly" ElementName. The ElementName is intended to allow the user to discriminate between several instances of the same class. For example ElementNames for instances of the CIM_CPU class might be "CPU 1", "CPU 2", "CPU 3", "CPU 4".	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14739	Remove ElementName substitutions	Remove the ''Platform Message Registry Substitutions'' shown in Table 30, section 2.12 of the ''AMT 3 0 DWMG 1 0 Upgrade DCR.doc'' also know as the ''Intel® AMT DMWG 1.0 Upgrade''. AMT must use the message arguments specified in the DMTF Platform Message Registry.	No	No	No	No	No
CCG01000 14738	Meaningful status property values	The AMT CIM model must be reviewed to replace various ''status'' type properties (including operationalstatus, primaryhealthstatus, detailedhealthstatus, operatingstatus, communincationsstatus, and other resource instance status properties) currently statically coded with ''unknown'' type values with values indicative of the current status or state of the resource. Dynamically updating the status properties may be deferred until a request is received to provide the current values.	Yes	Yes	Yes	Yes	Yes
CCG01000 14737	Text Console Redirection	AMT shall support the DMTF DSP1024 Text Console Redirection Profile	No	No	No	No	No
CCG01000 14736	Battery Management Profile	AMT shall support the DMTF DSP1030 Battery Management Profile	No	No	No	No	No
CCG01000 14735	USB Redirection	AMT shall support the DMTF DSP1077 USB Redirection Profile	No	No	No	No	No
CCG01000 14734	KVM Redirection	AMT shall support the DMTF DSP1076 KVM Redirection Profile.	No	No	No	No	No
CCG01000 14733	Media Redirection	AMT shall support the DMTF DSP1086 Media Redirection Profile.	No	No	No	No	No
CCG01000 14732	Opaque Data	AMT shall support the DMTF DSP1070 Opaque Data Profile	No	No	No	No	No
CCG01000 14731	Wireless NIC	AMT shall support the DMTF DSP1088 Wireless NIC Profile	No	No	No	No	No
CCG01000 14730	Wired NIC	AMT shall support the DMTF DSP1035 LAN profile, DSP1036 IP Interface profile, DSP1037 DHCP profile, DSP1038 DNS profile,	No	No	No	No	No

3.3.10.1 Supported CIM Profiles and Interfaces

This section defines the supported DMTF DASH profiles, and supported Intel® AMT interfaces in WS-MAN.

Profile	Capability Provided	Version
All DASH 1.0 profiles	As defined in the "DASH 1.0 Implementation Requirements Specification" from the DMTF and the "DASH 1.0 Implementation Requirements for AMT" from the Intel Architecture team.	1.0

Security Profiles
http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest
http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest
http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/mutual/digest
http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/spnego-kerberos
http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/spnego-kerberos
http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/mutual/spnego-kerberos
http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest
http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest

The following list describes Intel® AMT interfaces that will be supported in WS-MAN but do not have mapping to CIM profiles yet:

Interface	Supported
General Info	Y
Power schemas	Y
System Defense filters and policies	Y
System Defense Heuristics	Y
802.1x	Y
Environment detection	Y
EAC/NAC	Y
User Notification	Y
Network Time	Y
Redirection	Y

Interface	Supported
Setup and Config	Y
Authorization	Y
Network Admin	Y
Watchdog	Y
Agent Presence	Y

3.3.11 Intel® Active Management Technology Setup and Configuration

Configuring Intel® AMT systems is the operation IT must perform in order to activate Intel® AMT and set the initial attributes and configuration adequately to support the IT environment that the Intel® AMT machine is running in.

Pre AMT 6.0: Intel® AMT can be configured in two modes: Enterprise and Small Business. The mode is set by the OEM and can be modified by an IT administrator. In Enterprise mode there are two methods for Setup and Configuration: TLS-PSK and TLS-PKI (a.k.a. RCFG). For TLS-PKI refer to Intel® Active Management Technology Remote Configuration Section.

AMT 6.0 provides both Manual Setup and Configuration and Automatic (using Configuration Server) Setup and Configuration. They are no longer configuration modes with different functionality, but different methods of configuring the system. Automatic setup and configuration is equivalent to the pre-AMT 6.0 Enterprise mode configuration, Manual setup and configuration was used pre-AMT 6.0 for SMB mode configuration. It is not required to pre-select automatic or manual; they are both always available.

AMT 7.0 defined two configuration modes:

1. Client Control Mode (new for AMT7.0): when vPro is configured by local SW, with no prior vPro credentials set (i..e MEbx pwd, PSK). In this mode all redirection operations require User Consent and System Defense is disabled

2. Admin Control Mode: When vPro is configured by either of the existing configuration operations: PSK, RCFG, manual.

During setup and configuration, the FW can be in 3 different states:

1. Pre-Configuring: the state before the Setup and Configuration process starts
2. In-Configuring: the state while Setup and Configuration is in process. This state is required only for Automatic setup and configuration.
3. Post-Configuring: the state after the Setup and Configuration process completes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14701	Setup and Configuration for wired -- ''In Configuring'' state	Once the FW is in this state, it opens the network interface, establishing network connectivity and allowing remote users to connect to the device, using SOAP/ WSMAN / HTTP. Communication is only permitted from the configured ConfigServer.	Yes	Yes	No	Yes	Yes
CCG01000 14692	Setup and Configuration wired Exit In Configuration	The FW shall exit from the ''In-Configuration'' state when all the following conditions are met: 1. TLS Configuration: Either 1 of the following: a. If no TLS: User disables Network TLS support. b. If Server authentication: User configures a TLS Server Certificate. c- If mutual authentication: user configures also root of trust certificate (in addition to TLS server certificate). Optional: also DNS Suffix List. 2. RNG Seed is set (not required for AMT 3.0 and above) 3. Networking is configured correctly according to the environment. - 4. Commit Changes command was invoked	Yes	Yes	No	Yes	Yes
CCG01000 14688	Setup and Configuration wired Configuration Server	When the Configuration Server receives a configuration request from the Intel® AMT FW it shall set the configuration parameters. Limitations: Pre AMT6 Configuration Server is used only for machines configured for Enterprise Mode. For AMT6 configuration server may always be used.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14687	Configuration wired Full Un-Configuration actions	When the Intel® Management Engine Firmware moves to full Un-Configured state the Intel® Management Engine Firmware shall delete all the data and the configurations added to the Intel® Management Engine Firmware after the Configuration sequence. The following default factory settings shall be restored including the erasure of the PPS and PID values: - Pre-Configured Event Filters. - Default network settings (DHCP enabled, VLAN ID). - ConfigServer information (DNS Name or IP Address). ISV Storage Global Parameters (Max Partner area size, non-partner area).Refer to Firmware Variable Structures for Intel® Management Engine and Intel® Active Management Technology for additional details. 6.0.	Yes	Yes	No	Yes	Yes
CCG01000 15611	Production Network configuration	Intel® AMT can be configured through: a. Remote configuration b. One-touch configuration at the OEM factory or the IT staging area of the customer's IT organization; in this case the rest of the configuration happens over the enterprise network. Note: Configuration for Intel® AMT platforms are required to be done within the enterprise and over a wired network only.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15606	Setup and Configuration wired partial UnConfiguration	When the Intel® Management Engine Firmware moves to a partial Un-Configured state the Intel® Management Engine Firmware shall delete all the data not related to Setup and Configuration and return to factory defaults. For settings that are maintained as they are required for initiating a new Setup and Configuration sequence please refer to the following document: ''Firmware Variable Structures for Intel® Management Engine'' (Anacapa #26840) This option should also be used when the user Un-configures AMT in order to start RPAS registration sequence if the user desires to maintain the current network setup.	Yes	Yes	No	Yes	Yes
CCG01000 15589	Configure Wireless	Setup and configuration shall be supported in wireless network	No	No	No	No	No
CCG01000 15477	Kerberos* Configuration	During the Kerberos configuration process the key material and other parameters shall be configured.	Yes	Yes	No	Yes	Yes
CCG01000 15469	Un-Configuring Intel® AMT without password using the BIOS setup option	FW shall provide a mechanism that will enable the platform BIOS to reset Intel® AMT information without the necessity of providing the current Intel® AMT authorization information if a user has lost the password for Intel® AMT. For more details on this please refer to the BIOS writer's guide.	Yes	Yes	No	Yes	Yes
CCG01000 15468	Setup and Configuration Locations	Intel® AMT shall be configured with TLS-PSK credentials at the IT staging area. The remaining Intel® AMT credentials shall be configured over the production network. For additional Setup and Configuration options refer to Intel® Active Management Technology Remote Configuration Section.	Yes	Yes	No	Yes	Yes
CCG01000 15467	Setup and Configuration Server	Intel® AMT shall require a Setup and Configuration Server at the enterprise IT staging area to be operated by the IT Technician. The Setup and Configuration server must be capable of generating the Setup and Configuration Pass Phrase (PPS), Setup and Configuration ID (PID) and the TLS Pre-Master Secret as described herein.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15466	Setup and Configuration ID (PID)	Intel® AMT shall require a Setup and Configuration ID (PID). The PID shall be a 64 bit quantity comprised of ASCII codes of some combination of 8 characters - capital alphabets (A-Z), and numbers (0-9). The PID must be a unique within the scope of the Setup and Configuration server database. It is recommended that the Setup and Configuration server generates the PID and PPS in the hyphenated format so that it is easier for the IT technician to use the values.	Yes	Yes	No	Yes	Yes
CCG01000 15465	Setup and Configuration Pass Phrase (PPS)	Intel® AMT shall require a Setup and Configuration Pass Phrase (PPS). The PPS shall be the same as the PSK defined in the Internet Draft (draft-ietf-tls-psk-07.txt). The PPS shall be generated by consuming input from a quality random number generator. The PPS is a 256 bit quantity represented as 32 characters. It is recommended that the Setup and Configuration server generates the PPS in the hyphenated format so that it is easier for the IT technician to use the values. For additional Setup and Configuration options refer to Intel® Active Management Technology Remote Configuration Section.	Yes	Yes	No	Yes	Yes
CCG01000 15464	PPS interface	The interface for updating the PPS attribute shall be "write only".	Yes	Yes	No	Yes	Yes
CCG01000 15463	TLS Pre-Master Secret	Intel® AMT requires a TLS Pre-Master Secret based on the Setup and Configuration Pass Phrase (PPS), using the format per draft-ietf-tls-psk-07.txt.	Yes	Yes	No	Yes	Yes
CCG01000 15462	Setup and Configuration Over Production Network	Intel® AMT must allow Setup and Configuration over the IT Production Network, yet securely, instead of an isolated network at the IT staging area.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15461	One-Touch Setup and Configuration at the OEM Factory	Intel® AMT must allow configuration of pre-shared secret (PSK or PKI-CH) into the Intel® AMT subsystem on the at the OEM's factory. The computer should be in a state to ship directly to the end-user's desk. Once the end user has connected the computer to the network and powered it on, the computer shall be configured securely via the Automatic Setup and Configuration process.	Yes	Yes	No	Yes	Yes
CCG01000 15460	Delayed Setup and Configuration Support	After the initial configuration period expired, Intel® AMT will transition to the Delayed Configuration state, to be configured at a later time over the enterprise network.	Yes	Yes	No	Yes	Yes
CCG01000 15459	TLS Protocol	Intel® AMT shall use the TLS protocol with Pre-Shared Key (PSK) cipher suite, outlined in TLS-PSK Internet Draft RFC 4279 for establishing a secure link between the Intel® AMT subsystem and the Setup and Configuration server.	Yes	Yes	No	Yes	Yes
CCG01000 15458	Secure Setup and Configuration	Intel® AMT Setup and Configuration shall always be done securely, even if TLS is not enabled for use during normal operations. The PSK cipher suite shall be used even with customers who do not have the Certificate Authority (CA) server required for general TLS use. For additional Setup and Configuration options refer to Intel® Active Management Technology Remote Configuration Section.	Yes	Yes	No	Yes	Yes
CCG01000 15457	Setup and Configuration Process	Intel® AMT systems shall be configured according to the following process: 1. Boxed Intel® AMT platforms arrive at the customer's IT staging area. 2. The IT technician requests the Setup and Configuration Server to generate a Setup and Configuration ID (PID) and a Setup and Configuration Pass Phrase (PPS) for the platform. 3. The Setup and Configuration Server generates these 2 pieces of information. 4. The Setup and Configuration Server generates a TLS Pre-Master secret based on the PPS and stores it in a secure database along with the PID.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		5. The Setup and Configuration Server provides a copy of PID and PPS to the IT technician. This may be a printout, or displayed on the screen. 6. The IT Technician removes platform from its box, plugs-in the power cable, and powers-on the platform. 7. The IT Technician hits the appropriate function key to bring up Intel® AMT BIOS Configuration Screen and logs-in to Intel® AMT using Intel factory default BIOS Administrator password. 8. The IT Technician changes the BIOS Administrator password. 10. Pre-AMT 6.0: The IT Technician enables Intel® AMT in Enterprise Mode. 9. The IT Technician enters the PID and PPS into the Intel® AMT subsystem and other necessary data, via the BIOS configuration UI. 11. The IT Technician powers-down the platform and distributes it to the end-user. For additional Setup and Configuration options refer to Intel® Active Management Technology Remote Configuration Section.					
CCG01000 15431	Setup and Configuration wired Exit Un-configured (Pre-AMT 6.0 applicable to Enterprise mode only)	The Intel® AMT FW shall exit from un-configured state only after all the following conditions are met. - Bios has set the UUID value. - Administrator default password has been modified (either by a user or through an OEM image). - PPS and PID values have been stored - Once the above conditions are met the FW Configuration state shall be ''In-Configuration'' Note: Remote configuration is an exception to this requirement.	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15899	Setup and Configuration wired Exit Un-configured for Manual Setup and configuration (PRE-AMT6 applicable to SMB mode only)	The Intel® AMT FW shall exit from un-configured state only after all the following conditions are met. - Bios has set the UUID value. - Administrator default password has been modified (either by a user or through an OEM image). - Pre AMT 6.0: Configuration Complete for ''Small Business'' Mode. - In AMT 6.0: in order to complete Setup and Configuration it is necessary to activate the network access via MEBx or select Manual configuration for USB key.	No	No	No	No	No
CCG01000 15898	Setup and Configuration wired Exit Un-configured starting AMT 6.0	The Intel® AMT FW shall exit from un-configured state only after all the following conditions are met. Common requirements: - Administrator default password has been modified (either by a user or through an OEM image).	Yes	Yes	No	Yes	Yes
CCG01000 15430	Setup and Configuration wired Un-Configuring	The FW shall be able to move to Un-Configured state according to user command.	Yes	Yes	No	Yes	Yes
CCG01000 15429	Setup and Configuration Legacy Vs Normal Mode	The FW shall provide a configurable parameter to allow an administrator to select whether the machine should be configured as an Intel® AMT 1.0 device compatible or as a Intel® AMT 2.6-4.0 device. This option can only be set during configuration. The default value shall indicate the device should work in normal mode. The parameter can be configured through the MEBx. See the Compatibility and Interoperability section for the features set of which is supported in each mode.	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15428	Setup and Configuration AMT systems	For platform SKUs with Intel® AMT, operational power states are controlled by an Intel® ME power policy. a. The default factory setting can be configured using manufacturing tools. b. During the configuration process, the Configuration Server is allowed to issue a power policy to the Intel® AMT subsystem which will define the power states in which Intel® ME will be operational.	Yes	Yes	No	Yes	Yes
CCG01000 15366	Un-configuring Intel® AMT without password using the RTC battery clear method	To fully unconfigure an Intel® AMT system without a password the RTCRST# signal on the PCH must be asserted. The recommended method is to use a CMOS reset jumper (removing the RTC battery is an additional option.) The Intel® AMT system will unconfigure itself and restore the factory defaults. All stored information will be cleared, the MEBx password will be reset and any PSK information in the fixed.	Yes	Yes	No	Yes	Yes
CCG01000 15318	Methods of Setup and Configuration wired Initial Mode	When the Intel® AMT FW is in an un-configured state the following methods of configuration shall be supported: - Through the MEBx or custom BIOS screens - USB Key methods of provisioning - Remote Configuration methods - Intel® AMT OEM tools** ** This is not for the end user	Yes	Yes	No	Yes	Yes
CCG01000 15157	TLS PSK ciphers used	Crypto enabled: - TLS_PSK_WITH_AES_128_CBC_SHA - TLS_PSK_WITH_RC4_128_SHA Crypto disabled: - TLS_PSK_WITH_NULL_SHA	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14729	Allowed commands during provisioning	Only system settings commands will be allowed during in-provisioning mode: - Users and permissions - Network configuration (TCP/IP settings, wireless profiles,802.1x, EAC) - Security configuration (TLS, Kerberos, certificates) - Power policies - Time - Provisioning settings (for future provisioning).	No	No	No	No	No
CCG01000 14728	Interface with ME applications	The provisioning service shall keep a database of all ME applications in the system. For this purpose, the prov. service shall expose register-app/unregister-app commands to ME applications. When an ME application initializes or is being provisioned (if applicable), it must register itself in the provisioning service database. When an ME application is uninitialized or is being unprovisioned, it must unregister itself from the provisioning service database.	Yes	Yes	No	Yes	Yes
CCG01000 14727	System unprovisioning and effects on ME applications	System unprovisioning: When the system settings are being unprovisioned (the system admin sending a system unprovisioning command), the provisioning service will first send a request to registered ME applications to unprovision their own settings. An application can refuse with a ''not ready'' status. In this case, an error is returned to the system unprovisioning command.	Yes	Yes	No	Yes	Yes
CCG01000 14726	System unprovisioning: applications not ready	System unprovisioning: In case of a system unprovisioning error because of applications not being ready, an API will be available for the system admin to query which applications are not ready and why.	Yes	Yes	No	Yes	Yes
CCG01000 14725	Physical/force system unprovisioning	When the system is being physically unprovisioned (CMOS clear or BIOS unconfigure), a force-unprovision event is sent to the applications. The applications must unprovision themselves (or just be aware that the system is being unprovisioned) and cannot fail the system unprovisioning.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14724	Provisioning in Sx states	Provisioning in Sx states is supported according to the chosen power packages (when Intel® ME is operational).	Yes	Yes	No	Yes	Yes
CCG01000 14723	ME applications provisioning/unprovisioning	ME applications MAY expose APIs to allow provisioning and unprovisioning of their application-specific data.	Yes	Yes	No	Yes	Yes
CCG01000 14722	Intel® AMT disabling	The Intel® AMT disabling leads to Intel® AMT settings unprovisioning.	Yes	Yes	No	Yes	Yes
CCG01000 15897	Intel® ME out of the box discovery	Unconfigured Intel® ME systems in H0 state with configured host IPv4 address, shall respond to RMCP pings. This is to allow discovering of Intel® ME capable systems on the network prior to Intel® ME Setup and Configuration, regardless of a local agent being present.	Yes	Yes	No	Yes	Yes

3.3.11.1 Intel® Active Management Technology Setup and Configuration MEBX requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14721	SMBIOS table to ME provisioning client	In addition to the BIOS tables that MEBX sends to the AMT MEI client (as in previous products), it shall send the UUID to ME provisioning MEI client.	Yes	Yes	No	Yes	Yes
CCG01000 14720	MEBX menu and naming changes	MEBX menu structure and naming shall change to reflect provisioning of ME (instead of Intel® AMT in previous products).	Yes	Yes	No	Yes	Yes

3.3.12 Intel® Active Management Technology Remote Configuration

Remote Configuration (RCFG) allows IT departments to use TLS-PKI to deploy Intel® AMT client platforms directly into an enterprise network environment, without additional configuration at IT staging area, while maintaining secure connection.

In Automatic Setup and Configuration mode there are two methods for Setup and Configuration: TLS-PSK and TLS-PKI (a.ka. RCFG). This section describes the requirements for TLS-PKI. For TLS-PSK requirements, refer to Intel® Active Management Technology Setup and Configuration Section.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15896	One-touch TLS-PKI configuration	Intel recommends using TLS-PSK or TLS-PKI with pre-configured DNS suffix or provisioning server FQDN during setup and configuration (via the MEBx or USB key). Note: These values can also be configured through OEM tools.	Yes	Yes	No	Yes	Yes
CCG01000 15364	Remote Configuration vs. One Touch TLS-PSK configuration	- Intel will provide methods and options for both zero-touch and one-touch configuration, but it shall be the OEM's/ODM's choice to pick the default option during manufacturing, or the choice of IT post-manufacturing-	Yes	Yes	No	Yes	Yes
CCG01000 15363	Remote Configuration Root Certificate Management - Post configuration interface	Customers shall be given the option to mark any one hash as the one selected for configuration from the network interfaces (post configuration). Such a marking enhances the security of the mechanism because it prevents the adversary from obtaining a certificate from any of the listed trusted CA's, and forces him to get a certificate from the marked CA only Customers shall be given an the option to add/delete entries in the list from network interfaces (post configuration)	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15362	Remote Configuration Root Certificate Hash Management - Un- configuration	Partial un- configuration shall not affect the certificate Hash Full un-configuration shall enable all factory default hashes and remove customized hashes. For additional details refer to Firmware Variable Structures for Intel® Management Engine and Intel® Active Management Technology 6.0	Yes	Yes	No	Yes	Yes
CCG01000 15361	Remote Configuration Root Certificate Management - Customizing the Certificate Hash	Intel® AMT shall provide an option to customers/IT to add at least 3 entries to the cert hash table. This gives a minimum acceptable flexibility to customers to customize Intel® AMT based on their PKI environment. Intel® AMT will also provide space for at least 30 entries pre-bundled in the platform at the mfg floor, thus making space for overall 33 entries at least.	Yes	Yes	No	Yes	Yes
CCG01000 15360	Remote Configuration OEM Requirements - Setting RTC Time	The OEM should configure the correct value of time in the RTC. This is to enable certificate validation during PKI based configuration methods.	Yes	Yes	No	Yes	Yes
CCG01000 15359	Remote Configuration OEM Requirements - Root Certificate Management (pre-AMT 6.0)	The OEM/ODM must place SHA-1 hashes (160 bits) of one or more root public key certificates in the Intel® AMT flash (as factory defaults) - Intel will provide a minimum set of such certificate hashes to the OEM and suggest to OEM's that they include these certificate hashes in the flash. - The OEM may optionally choose the certificate hashes to include in the flash depending on its preferences of partner CA's, partner ITO's, partner ISV's. This list of hashes is the same in all platforms on the standard manufacturing line. These certificates could be from any of the following: - Commercial 3rd party CA's, e.g. Verisign - IT Outsourcers, e.g. EDS, IBM Global Services - ISV's, e.g. Microsoft, Altiris, etc. - Any other source the OEM/ODM deems fit	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15895	Remote Configuration OEM Requirements - Root Certificate Management (starting AMT 6.0)	In addition to the "Remote Configuration OEM Requirements - Root Certificate Management (pre-AMT 6.0)" requirement, the OEM/ODM may also place SHA-2 hashes in the Intel® ME flash image. Starting AMT 7.0, OEM can edit/add/remove only 1 hash from the default hashes list (hash #19) and also edit/add/remove all 3 customized hashes (hashes #20-22). All other hashes (#0-18 and #23-32) can't be edit/add/remove by anyone besides Intel.	Yes	Yes	No	Yes	Yes
CCG01000 15358	Remote Configuration OEM Requirements - Manageability Mode	Remote Configuration will only be available if Intel® AMT is shipped with "Manageability Mode" = AMT.	No	No	No	No	No
CCG01000 15357	Remote Configuration Network Configuration Requirements	Remote Configuration Static IP methods will not be supported.	Yes	Yes	No	Yes	Yes
CCG01000 15040	Simplified handling of certificates for specified Top Level Domains	The Intel® AMT validation criteria for SSL certificates issued under predefined Top - Level Domains (TLDs) will be successful upon a matched in one level below the TLD between the CN value and the DNS information. For details see the Intel® Active Management Technology (Intel® AMT) - PKI-CH in Manufacturing Technical White Paper.	Yes	Yes	No	Yes	Yes
CCG01000 15894	Supporting wild-card certificates for remote configuration	The firmware will allow use of wild-card certificates for remote configuration. This applies to certificates where the CN's lowest level is a wild-card (e.g., *.intel.com).	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015181	Multiple Domain Certificates (a.k.a. Unified Communication Certificates - UCC) support	Provide support for Multiple Domain Certificates which allows customers with multiple sub-domains to purchase a single SSL certificate issued to multiple DNS names, using the dNSName type in the subject alternate name extension (SAN).	Yes	Yes	No	Yes	Yes

3.3.13 Intel® Active Management Technology USB Key Setup and Configuration

USB Configuration is a one-touch configuration solution using a USB flash device to deliver Setup and Configuration information to the client machines

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015317	Basic USB Setup and Configuration	System can read information off of a USB key inserted into the system to configure the username, password, PID and PPS	Yes	Yes	No	Yes	Yes
CCG0100015316	Extended USB Configuration	To add to the usability of the USB Setup and Configuration model, all configurations available to the MEBx must be made available to be configured via the USB Key unless explicitly noted otherwise. For additional details refer to ''Intel® Management Engine USB Key Local Provisioning Architecture Specification''	Yes	Yes	No	Yes	Yes

3.3.14 Intel® Active Management Technology Host Based Setup and Configuration

Host Based Setup and Configuration is a local configuration solution using a local SW to deliver Setup and Configuration information to the client machines authenticating using local machine administrative credentials. Host based Setup and Configuration enables:

OS administrators to turn on Intel® vPro and set the initial AMT Admin password when MEbx password isn't previously set.

Enable all WSMAN operations to pass through the local interface. Operations will still require authentication to ME using existing ACL. Expose ACL table that allows enabling/disabling local and remote interfaces

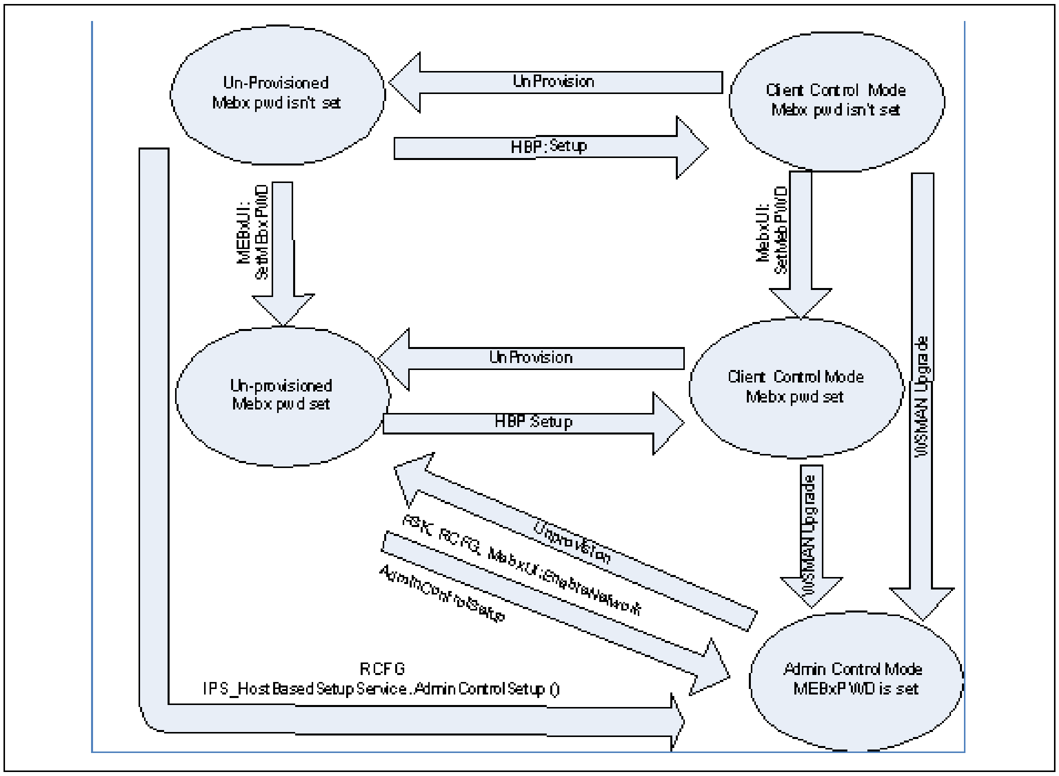


Figure 2 Configuration modes state diagram

Following table depicts the main feature changes between these modes:

	Client Control Configuration Mode	Admin Control Configuration Mode
System Defense	Disabled	Enabled
User Consent for redirection operations	Required for All operations	Programmatically modifiable possible options are: None, KVM only, All ops
Auditor consent to un-provision	Not Supported, (security consideration)	Supported
Programmatically change MEBx PWD	Not Supported (security consideration)	Supported
Security Principles authorized to unprovision AMT	Local Windows Administrators AMT Administrators	AMT administrators

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 08541	OEM Permanent disable HBP	OEM can permanently disable Client Control Configuration Mode by setting appropriate flag in the FW image	No	No	No	No	Yes
CCG01000 08542	HBP temporary Programmatic disable	OEM or IT can programmatically disable the Client Control configuration mode by executing the WS-MAN command. There is no SW programmable method to reverse this operation. However full Unconfigure will reset Client Control Mode availability back to OEM factory default	No	No	No	No	Yes
CCG01000 08543	Host Based Setup and configuration control by OS credential	Host based setup can be performed only by users who have admin privileges on the local OS. Note: if the setup method is called while AMT is disabled, the method will also enable AMT (similar to the behavior of StartConfiguration HECI command).	No	No	No	No	Yes
CCG01000 08545	Entering provisioning certificate chain for host admin and upgrade flow	Both host-based admin setup and upgrade from client control mode to Admin mode APIs will require a trusted certificate chain to validate the identity of the provisioning entity.	No	No	No	No	Yes
CCG01000 08546	HBP functionality limitations	When AMT is configured in Client Control configuration mode, FW should block the following functionality : o System Defense o Manipulation of RCFG and PSK information o Manipulation of User Consent settings o Un-consented KVM or IDER sessions o Un-consented setting of Boot Options	No	No	No	No	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100008547	Client Control Configuration Mode	FW shall provide a method that will allow local configuration solution, using a local SW to deliver Setup and Configuration information to the client machines , Without touching the machine or providing additional credentials besides the OS admin credentials. This mode of configuration will be named "Client Control Configuration Mode"	No	No	No	No	Yes
CCG0100008548	User consent limitation in client control mode	When In Client control mode and if redirection sessions are enabled, user consent will be required for the following operations: -Using Serial Over LAN to redirect BIOS screens and OS Boot text screens -IDE-Redirect -KVM -Remotely setting BIOS boot options -Changing boot sources for remote boot (e.g. causing a boot from PXE) The user consent screen will be shared with existing KVM screen if Sprite is supported, otherwise MEBx will display a screen on the next boot	No	No	No	No	Yes
CCG0100008549	Transition from Client Control Mode to Admin Control Mode Configuration	When AMT is pre-provisioned in Client control mode, FW shall support upgrade an AMT machine provisioned in Client Control mode to Admin Control mode without performing unprovisioning and potentially losing data.	No	No	No	No	Yes

3.3.15 Intel® Active Management Technology System Defense Network Protection and Agent Presence

System Defense monitors incoming and outgoing packets. Based on policies defined by the IT administrator System Defense can take actions such as blocking a specific type of packet. System Defense also will take action if a pre-defined agent has been removed from the system, implying an application issue or tampering. The configuration must be tamper proof.

System Defense behavior is determined by the policies that an IT administrator sets during initial setup and configuration. These policies can be modified by IT subsequently by using the remote OOB interface. The user of the machine cannot add or change any of the policies.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015075	System Defense Traffic Control Policy Settings	At the configuration state, IT Administrator shall pre-configure the system with policies. a. IT administrator shall define the System Defense policies they will store and those they will also activate. b. These policies will remain dormant until a certain point where IT administrator would like to activate them.	Yes	Yes	Yes	Yes	Yes
CCG0100015068	System Defense Traffic Control OOB	IT administrator shall use the OOB interface to change the System Defense policies at any time after configuration completes. Note: Only Wired features are supported in Intel® AMT 5.0.	Yes	Yes	Yes	Yes	Yes
CCG0100015058	System Defense Traffic Control	The IT administrator shall be able to turn on and off policies that the user previously configured and stored as settings in NVM. The System Defense feature shall scan packets according to packet detection configuration set by a remote configuration application or at configuration time.	Yes	Yes	Yes	Yes	Yes
CCG0100015048	System Defense Packet detection.	The System Defense feature shall scan packets according to packet detection configuration set by a remote configuration application or at configuration time.	Yes	Yes	Yes	Yes	Yes
CCG0100015047	System Defense Action Policy	The FW shall take an Action if the packet detection logics shows a match (i.e. a suspicious packet or activity has been detected). The choices that may be defined for Action Policies are: - No forward traffic. - Block traffic - Block specific packets. - Limit traffic - Limitation means the FW shall allow the first N packets matching the filter with in the timer count of one second. After N number of packets or after the one second counter (which ever one comes first), Intel AMT shall block all packets matching this filter.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		At the beginning of the next second, the counter gets reset and the block of the filter is removed. Limitations \ Note: Traffic limitation is only to be used on connectionless protocols such as UDP or TCP connection requests. Whoever configures the policy is responsible for applying this restriction. The FW shall not apply any rule checking on bandwidth limitation filters.					
CCG01000 15046	System Defense Overlapping Filter Policy	The IT administrator shall provide a priority field associated with each System Defense policy, the priority shall be used to instruct the HW when a packet matches 2 or more System Defense filters. At that point, the FW shall apply the 2 policies into the System Defense HW. In order to prevent conflicts between policies the priority is used. So if there is a conflict of policies, the higher priority policy shall be used.	Yes	Yes	Yes	Yes	Yes
CCG01000 15045	System Defense Notification Policy	The FW shall provide a parameter to set Notification : - No action. - Send WS-eventing - Send PET - Log event - Combination of the last two options	Yes	Yes	Yes	Yes	Yes
CCG01000 15044	System Defense Revoking Action Policy	Once an Action Policy has been applied it can be revoked only by issuing a command from a remote configuration application, or by the Agent Presence.	Yes	Yes	Yes	Yes	Yes
CCG01000 15035	System Defense StartUp	When the FW starts up it shall configure the selected System Defense HW policy stored in the NVM into the HW (and into the WLAN FW). In other words policies are persistent. Note: Only Wired features are supported in Intel® AMT 5.0.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15034	System Defense Configuration Store	When the FW receives a configuration from a remote application via the OOB interface, the FW shall store this information in the NVM, in other words policy configuration is persistent.	Yes	Yes	Yes	Yes	Yes
CCG01000 15028	System Defense Configuration Privacy	The FW shall prevent any host application from reading, changing or adding any of the System Defense configurations whether they are stored in the NVM or reside in volatile memory.	Yes	Yes	Yes	Yes	Yes
CCG01000 15017	System Defense DHCP	When the Host IP is acquired using the DHCP protocol the FW shall monitor the host IP address and adjust the System Defense filters accordingly to that IP address The FW shall apply this mechanism whenever a new System Defense policy is set or whenever the IP address has changed. This will affect address-spoofing.	Yes	Yes	Yes	Yes	Yes
CCG01000 15009	System Defense Agent Presence	The System Defense feature shall notify the IT administrator when a SW agent is installed and that it has started running. IT administrator may want to receive notification whenever specific applications have started running. This is mainly important for diagnostics or making sure that a remote installation has succeeded. Limitation \ Note: The application is responsible for registering itself within the FW.	Yes	Yes	Yes	Yes	Yes
CCG01000 15008	System Defense Agent Absence	When the FW detects the agent has failed to load or has crashed the FW shall : - Execute the action policy configured. - Execute the notification policy configured. Limitation \ Note: The FW can not detect if the application is running properly or if the application is not a malicious application.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15007	System Defense Agent WD Remote Registration	When a remote application sends agent presence configuration information the FW shall: a. Store the configuration to the NVM and b. Activate agent presence detection logic	Yes	Yes	Yes	Yes	Yes
CCG010001 5006	System Defense Agent Presence Local Registration	When a local application sends agent presence configuration information the FW shall activate the watchdog and will not store any information in NVM. A local application is using the host interface which is less secure then the OOB. Therefore we must prevent host applications from controlling System Defense. Limitations \ Note: Activation policy configuration is not allowed when using local registration.	Yes	Yes	Yes	Yes	Yes
CCG01000 15005	System Defense Agent Presence Configuration Security	The FW shall prevent any local application from changing any agent presence configuration set by a remote application.	Yes	Yes	Yes	Yes	Yes
CCG01000 15004	System Defense Agent Presence Stop	The FW shall reset agent presence tracking in the following cases : a. The BIOS has started its boot. b. System state has changed from S0 to Sx. c. OS was unloaded and system state is still S0. d. The system has crashed. The FW may apply a different HW policy during OS initialization, based on Remote configuration. In order to avoid false alarm of agent presence the FW must stop monitoring the agents when the OS is not running. The FW should be able to apply a HW policy while a pre-defined SW agent is not running, including the time when the OS is initializing.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15003	System Defense Policy Definition	System Defense HW Policy constitutes of the following: a. Tx Policy: i. Anti-Spoofing Filter. ii. Set of HW filters and associated HW counters. iii. Overlapping match priority. iv. Else Filter. b. Rx Policy: i. Set of HW Filters and associated HW counters. ii. Overlapping match priority. iii. Else Filter. System Defense FW Policy constitutes the following: c. Tx Policy i. Anti Spoofing enabled / disabled. ii. Set of FW Filters. iii. Overlap Priority. d. Rx Policy i. Set of FW Filters. ii. Overlap Priority. e. Base Heuristics i. Enable/disable each heuristic ii. Parameters for slow heuristic (time-window, port threshold, overall threshold). iii. Action (one of the following) - System Defense policy to activate - send alert - Block all outgoing traffic - Block all outgoing traffic from the port the worm was detected. FW Filter constitutes of either a static HW System Defense filter or a bandwidth limitation filter.	Yes	Yes	Yes	Yes	Yes
CCG01000 15605	System Defense Wireless	a. System defense shall be supported in wireless via the host SW. c. CPU utilization hit will not exceed 10%.	No	Yes	No	No	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015604	System Defense Wireless and Wired	There will be two policies - one for the wired connection and the other for the wireless connection. Both will be applied regardless of the actual active interface on the host.	No	Yes	No	No	Yes
CCG0100015603	System Defense Notification Events	The following System Defense events shall be supported - System Defense Alert - System Defense Rate Limit	Yes	Yes	Yes	Yes	Yes
CCG0100015602	System Defense Overlapping Filter Policy (fixed)	When there is a conflict between 2 filters configured simultaneously, one configured to block a packet, and the other one configured to pass that packet, the "block" filter will take precedence.	Yes	Yes	Yes	Yes	Yes
CCG0100015601	System Defense Overlapping Policies	The IT administrator shall setup different filter policies, each configuring a set of filters. Each policy should be provided with a Policy Precedence field. In case multiple policies are being activated simultaneously, the policy with the highest precedence value takes effect (policies with the same precedence are chosen arbitrarily, therefore it is not recommended to use the same precedence).	Yes	Yes	Yes	Yes	Yes
CCG0100015474	System Defense operation outside the organization	Once system was detected to be outside the organization System Defense policies will be removed from that interface	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15453	System Defense Packet scanning filters IPv4	System Defense maximum of packet scanning capabilities: a. 30 Transmit IPv4 filters (27 if Base Heuristics is supported). b. 31 Receive IPv4 filters c. 1 Else filter for Transmit and 1 else filter for receive Limitations \ Notes : - The logic for a proper use of the filters must be managed by the remote application. The FW shall not apply any rule checking on the policies set from remote. It is expected that the ISV application shall have the proper logic to manage the filters. - When 802.1X is enabled the FW shall use one of the TX System Defense filters for its usage reducing the number of available filters by 1.	Yes	Yes	Yes	Yes	Yes
CCG01000 15452	System Defense Packet scanning filters IPv6	System Defense maximum of packet scanning capabilities: a. 30 Transmit IPv6 filters (27 if Base Heuristics is supported or 29 if Auto IP is enabled in consumer SKU). b. 31 Receive IPv6 filters c. 1 Else filter for Transmit and 1 else filter for receive Limitations \ Notes : - The logic for a proper use of the filters must be managed by the remote application. The FW shall not apply any rule checking on the policies set from remote. - It is expected that the ISV application shall have the proper logic to manage the filters. Each filter can be IPv4 or IPv6 or both if the filter is layer 4 or layer 3. - If Base Heuristics feature is active, the FW will use 3 of the TX System Defense filters to support the heuristics, reducing the number of available Tx filters to 27.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15037	System Defense Policy Timeout Parameter	Each policy will have a configurable timeout parameter. When a SD policy is activated, Intel® AMT will read the timeout value and maintain the policy as active until the policy has expired. There will be a configurable default policy that can be set. Timeout parameter size is a 2 byte positive integer the timeout parameter will be counted in minutes. The default timeout should be set to 0 In the event the timeout parameter is set to 0 the policy is deemed as a permanent policy and will not expire When a policy timeout occurs, the Intel® AMT machine will either: - Revert back to the default policy that was configured. - If no default policy was configured then the policy will just be removed and no new policy will be set.	Yes	Yes	Yes	Yes	Yes

3.3.16 Intel® Active Management Technology Audit Log

The Audit Log is a mechanism which allows certain transactions on Intel® AMT clients to be reviewed by an Administrator holding the Auditor role in an enterprise.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15315	Audit Log	Intel® AMT shall have an Audit Log which records functions acted upon the Intel® AMT Subsystem	Yes	Yes	Yes	Yes	Yes
CCG01000 15314	Wrap log option	When the Audit Log is full the audit log should have the option to allow the action to occur and wrap recoding of the event	Yes	Yes	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15313	Audit Log actions when log is full	The Audit Log shall support the following actions upon receiving a new action in the event the log is full: - Allow the action to occur and do not log the event - Do not allow the action to occur until the log is cleared and return an error message	Yes	Yes	Yes	Yes	Yes
CCG01000 15312	Audit Log information	The Audit Log shall contain the following information - The user which initiated the action - The time and date stamp in which the action occurred - The action attempted	Yes	Yes	Yes	Yes	Yes
CCG01000 15311	Audit Log EOI API	The Audit Log will be accessible with EOI APIs	Yes	Yes	Yes	Yes	Yes
CCG01000 15310	Audit Log WS-MAN API	The Audit Log will be accessible with WS-MAN APIs	Yes	Yes	Yes	Yes	Yes
CCG01000 15309	Audit Log size	The Audit Log shall be able to record ~1000 entries, depending on individual entry size	Yes	Yes	Yes	Yes	Yes
CCG01000 15308	Audit Viewer realm	An Audit Log viewer realm shall be created to which Administrators have access by default	Yes	Yes	Yes	Yes	Yes
CCG01000 15307	Auditing Realm	A new security realm shall be defined for the sole purpose of Auditing. Administrators will not have access to the Auditing realm	Yes	Yes	Yes	Yes	Yes
CCG01000 15306	Policy based logging	Audit Log shall Log only the events it is configured to log by a Policy	Yes	Yes	Yes	Yes	Yes
CCG01000 15305	Audit Log persistence during firmware update	The Audit Log shall persist through all firmware updates	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15304	Emergency UnProvisioning	There shall exist a mean to unprovision a system in case the Audit Log has entries and the unprovisioning permissions are unavailable. This method is only executed on the local system; however it will not require any physical changes such as battery removal or jumpers. If this method is an enablement issue to the BIOS it must be in the BIOS writers guide as a mandatory implementation. It will also be included in any compliancy tools and testing	Yes	Yes	Yes	Yes	Yes

3.3.17 Intel® Active Management Technology NVM ISV Storage

The Non Volatile Memory ISV storage shall by used by ISV to store their asset management information in an Intel® AMT system. They will retrieve the information securely via OOB regardless of OS and system state. This feature increases the reliability of SW asset management.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15002	Storage NVM Sections	The Intel® Management Engine Firmware shall protect its private data in NVM from access by any host application. This protection shall be implemented internally by The Intel® Management Engine. Nothing shall be required from BIOS for this protection. The FW/HW is using the NVM for its own usage and shall protect integrity and privacy by ensuring no external application accesses it.	Yes	Yes	Yes	Yes	Yes
CCG01000 15001	Storage Local Interface	The FW shall expose a host interface for an ISV application to store information in the NVM area.	Yes	Yes	Yes	Yes	Yes
CCG01000 15000	Storage Remote Interface	The FW shall expose a remote OOB interface for an ISV management application to retrieve information in the NVM area.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14999	Storage Partner Area	The FW shall provide NVM partner area for the exclusive use of Intel factory partner ISVs. Limitations \ Note: There is no guarantee that an Intel Factory partner shall receive a specific allocation.	Yes	Yes	Yes	Yes	Yes
CCG01000 14998	Storage Partner Allocation Algorithm	When a partner ISV application tries to allocate NVM storage the FW shall check the storage availability according to the following algorithm : Check that the allocation request does not exceed the allowed limit for that application. If there is no room left there the FW shall return an error code.	Yes	Yes	Yes	Yes	Yes
CCG01000 14997	Storage Non Partner Allocation Algorithm	When a non partner ISV application requests storage the FW shall check availability according to the following algorithm: a. Check that there is room in the non Partner NVM area. b. Check for specific application NVM area limit c. If there is no room left the FW shall return an error code. Note: By default, the non partner NVM area size is set to 0. Non-partner location is intended to be a NVM section that could be used by those ISVs that are smaller or niche, or OEMs that have applications which are adjacent to Intel® AMT 6.0.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14996	Storage Default Factory Storage allocation	The FW default NVM allocations shall be according to the below table. The overhead per ISV is the amount of memory allocated for managing the storage and cannot be used by the ISV for storage purposes. - Partner Size: 192 KB (48KB/partner * 4 partners) - Overhead per ISV=32 KB - Overhead per EIT SW=4KB OEM may change some of the settings during the configuration stage or after the configuration stage using OOB interface (See requirement Storage Configurable Parameters)	Yes	Yes	Yes	Yes	Yes
CCG01000 14995	Storage Configurable Parameters	When a remote configuration application changes the below parameters via the OOB interface the FW shall : a. Check that the parameters are within allowed range. b. Update the configured parameters. Configurable parameters are: (i) Maximum Total Partner area size in Kbytes. (ii) Maximum allocation size for non partner area in Kbytes. - This is set to 0 by default. Note: Up to 24 partners are supported Limitations \ Note : It is expected that OEMs / IT will configure the NVM parameters in such a way that it shall exceed the total available physical storage area. When this situation occurs and an application requests additional storage the FW shall refuse to allocation request.	Yes	Yes	Yes	Yes	Yes
CCG01000 14994	Storage Physical Space Limitation	When an ISV application requests storage allocation and all the physical storage is already allocated the FW shall fail the request. This shall apply to both partner and non partner ISV applications.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14993	Storage Block Allocation	When a 3rd party application requests storage allocation the FW shall allocate the memory in chunks that are multiple of 4Kbytes each.	Yes	Yes	Yes	Yes	Yes
CCG01000 14992	Storage Block DeAllocation	When a 3rd party application requests storage de-allocation, the FW shall : a. Check that the block is owned by the requesting 3rd Party b. Mark the allocated storage as free for further usage. c. Erase its content If the 3rd party application does not own the block the FW shall return an error code and disregard the command.	Yes	Yes	Yes	Yes	Yes
CCG01000 14991	Storage Flash Wear-out	When a 3rd party agent tries to write to the NVM the FW shall protect the flash from being worn out. The algorithm will prevent any block from an average re- write of more than 40 times in a 24 hour period, over long period of times. This algorithm is FLASH specific and dependant on the list of supported FLASH parts.	Yes	Yes	Yes	Yes	Yes
CCG01000 15451	Storage Non Partner area	The FW shall provide NVM storage for non partner ISV applications, if the non partner NVM area size is manually set by a storage administrator to a size > 0 (by default the non partner NVM area size is set to 0). Limitations \ Note: There is no restriction on the usage of this area and applications can allocate storage on first come first serve basis.	Yes	Yes	Yes	Yes	Yes
CCG01000 15450	Storage Minimum Block Size	The SW shall support block allocation smaller than 4 K byte.	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14719	Factory Partner List	There shall be a Factory Partner Access List (FPACL), which contains entries for application Partners that have established a contractual arrangement with Intel to include the entries for their applications into the Storage Manager at the Intel factory (Factory Application ID, Total Allocation Size). The FPACL shall support a minimum of 48 entries.	Yes	Yes	Yes	Yes	Yes
CCG01000 14718	Application Registration List	There shall be an Application Registration List (ARL), which contains entries for each application currently registered with an Intel® AMT instance. The ARL shall support a minimum of 8 entries	Yes	Yes	Yes	Yes	Yes
CCG01000 14717	Application Registration	Applications shall use to the Storage Registration commands to register with an Intel® AMT instance (and create a corresponding ARL entry) If an application presents a Factory Application ID, which is found in the FPACL, then the Partner Application Registration is used; otherwise, the Non-Partner Application Registration is used.	Yes	Yes	Yes	Yes	Yes
CCG01000 14716	Partner Application Registration	In response to providing the following valid information, a ARL entry is created for the Application with corresponding Handle, which is returned to the Application. Subsequently, the Application may allocate Storage from the Partner area of the NVM. For Partner Registration, the Application must provide the following information:- - Factory Application ID - Vendor Name - Application Name - Enterprise Name - UUID	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14715	Non-Partner Application Registration	In response to providing the following valid information, a ARL entry is created for the Application with corresponding Handle, which is returned to the Application. Subsequently, the Application may allocate Storage from the Non-Partner area of the NVM. For Partner Registration, the Application must provide the following information:- - Vendor Name - Application Name - Enterprise Name - UUID	Yes	Yes	Yes	Yes	Yes
CCG01000 14714	Storage Command Security	The Storage Command Interface shall support Registration, Administrative, and Storage commands. To provide operational traceability to storage administrators, access to Storage Administrative command shall be controlled by an authentication realm separate from other access administrative realms. To facilitate some operational scenarios (e.g. local agent access to Storage) separate authentication realms shall be defined for the local host interface and the network interface to control access to the Registration and Storage commands. These realms can be optionally specified at storage session start-up for Registration and Storage commands to be passed over each interface.	Yes	Yes	Yes	Yes	Yes
CCG01000 15709	HW Asset Information	HW Asset information about an AMT machine will not be cleared after un-provisioning; this information will be saved when un-provisioning from an AMT manageability mode. HW Asset information is cleared on un-configure.	Yes	Yes	Yes	Yes	Yes

3.3.18 Intel® Active Management Technology Connection model & OOB

This section defines the connection model between the Intel® Management Engine Firmware and its managing console and the OOB mechanism to support it.

There are few main options:

- A server model where the Intel® Management Engine Firmware is reactive and the managing console is initiating the connection.
- A client initiated model is where the Intel® Management Engine Firmware is the initiating side and the console acts as a server.
- Remote connection where the Intel® Management Engine Firmware and the managing console are not sharing the same intranet and need to create a connection across the global network.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14989	Connect Network Security	The FW shall support network security During the configuration process the IT shall chose whether to enable or disable network security.	Yes	Yes	Yes	Yes	Yes
CCG01000 14988	Connect Network Security Algorithms	When network security is activated the FW shall implement the following network security mechanisms : Apply TLS v1 encryption and authentication to all traffic except the PET packets. The following algorithms are supported : - RSA(1024)-AES-128-CBC-SHA1 - RSA(1024)-RC4-128-SHA1 - RSA(1536)-AES-128-CBC-SHA1 - RSA(1536)-RC4-128-SHA1 and RSA(2048)-AES-128-CBC-SHA1 - RSA(2048)-RC4-128-SHA1	Yes	Yes	Yes	Yes	Yes
CCG01000 14987	Connect Network Security Algorithms: Controlled Countries	For SKUs targeted for controlled countries where encryption is not permitted, the following TLS v1 cipher-suite should be provided: - RSA(1024)-NULL-SHA1 - RSA(1536)-NULL-SHA1 - RSA(2048)-NULL-SHA1	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14986	Connect Network Presence	When the FW is connected to the Network (The link of the network interface is up) the FW shall maintain its IP presence in the following manner : a. Implement DHCP client protocol to receive an IP address (if configured for DHCP mode). b. Register within the DNS server, through the use of DHCP options. c. Respond to incoming ARP requests. Limitations \ Note : When the Host operating system is up and running the FW shall not implement the DHCP protocol but shall update its IP according to the host DHCP stack. When the Host operating system is up and running the FW shall not respond to ARP requests.	Yes	Yes	Yes	Yes	Yes
CCG01000 15893	Connect Network Presence: Presence notifications - FW support for Presence WS-Event	Intel® ME FW will support a new WS-Event Presence event (defined below). The event notifications will include the following arguments: 1. The FQDN of the ME subsystem 2. The FQDN of the Host 3. The list of ME configured IPv4 and IPv6 addresses 4. System UUID 5. Whether the system is connected to the local network. Other types of connectivity such as via VPN may be added in the future. 6. System state (S0 or Sx) Intel® ME FW will send these notifications upon occurrence of one of the following events: 1. Change to ME FQDN 2. Change in Host FQDN 3. Change or renew of IP address configuration 4. Periodic notification. The interval is configurable by the WSMAN API. The default interval 0. A value of 0 disables this feature.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		Note1: It is important to avoid a situation where all systems on a network are sending the periodic notification together. This should be achieved by a random delay before sending the first periodic notification. Note 2: When FW exits from MOFF or when there a link re-connected the FW network stack renews its network configuration and a WS-Event Presence event will be sent to notify the change.					
CCG01000 15892	Connect Network Presence: Presence notifications Support for ME Wake on LAN	If Intel® ME power package supports Wake on LAN and there are subscribers for the Presence WS-Event then FW should wake when the next periodic notification time arrives in order to send the Presence notification and then return to MOFF	Yes	Yes	No	Yes	Yes
CCG01000 15891	Connect Network Presence: Presence Notification Configuration	FW will support the following configuration options for the presence notifications (over WSMAN): 1. Periodic Update Interval (default 0). The units are minutes with minimum interval of 15 minutes (so that when in Sx the platform will not wake the host too frequently).	Yes	Yes	No	Yes	Yes
CCG01000 15890	Connect Network Presence: Presence notifications in un-provisioned states	Partial and Full Un-provisioning: FW will delete the WS-Event presence subscriptions upon full or partial un-provision and will not be discoverable via the presence events.	Yes	Yes	No	Yes	Yes
CCG01000 15889	Connect Network Presence: Support for additional subscribers	FW is required to support 4 additional subscribers (currently FW supports a maximum of 6 subscribers as the number of event filters)	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14985	Connect IPPorts Usage	The FW shall use IP ports pre-assigned to it by IANA for : - Legacy SoL/IDER secure - 16995 - Legacy SoL/IDER non-secure - 16994 - HTTP Server - 16992 - HTTPS Server - 16993 - WS-MAN port - 664 (secure), 623 (non-secure) - VNC port - 5900 These ports shall be consumed by the FW and will not be transferred to the host SW. Other ports shall be transferred to the Host OS.	Yes	Yes	Yes	Yes	Yes
CCG01000 14984	Connect Host Interface Host OS SW	When the OS is running the FW shall respond to SOAP commands and to a limited number of buffered commands. When the FW is configured to secure the host interface channel, it will respond to similar security protocols as defined for the network interface. Limitations \ Note: The FW shall assume OS is running when the BIOS starts the OS boot.	Yes	Yes	Yes	Yes	Yes
CCG01000 14983	Connect Host Interface HostBIOS	When the system is in S0 and PCI reset has occurred the FW shall accept BIOS commands via the host interface.	Yes	Yes	Yes	Yes	Yes
CCG01000 14982	Connect Server Connection	The FW shall operate as server providing a passive interface for management application. This connection can be used for both local and remote connection. For the remote connection it is expected that the console has the ability to open a secure connection into the managed system intranet using any kind of tunneling mechanism.	Yes	Yes	Yes	Yes	Yes
CCG01000 15613	DHCP discovery packet	The DHCP fields transmitted during power up are - FW hostname value - Domain name - Ethernet MAC address	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15612	DHCP request packet	The client FQDN value is transmitted with the value computed by concatenating the FW hostname, a period and the domain name configured during Setup and Configuration. Note: If no value is configured for the domain name, then revert to using only the FW hostname value. If the FQDN is changed by the IT then the TLS certificate and Kerberos* credential are no longer valid and must be re-configured. Note: For shared IP configuration if the host name or domain name of the host changes this requires re-configuring AMT with a new TLS certificate and Kerberos* Credentials.	Yes	Yes	Yes	Yes	Yes
CCG01000 15888	Connect Network Presence DNS - Intel® ME dedicated FQDN	Intel® ME FW will support using a dedicated FQDN that is not shared with the host. When setting a host name and domain name in FW it is required to specify whether the FQDN is shared or dedicated. The WSMAN, AMTHI (MEBx and USBKey) and Web UI are required to be updated to support this new configuration option. When configured with a dedicated FQDN FW will still share its IPv4 address with the host. The FWwill maintain the A and AAAA records in DNS for the dedicated FQDN when the DDNS Update client is enabled.	Yes	Yes	No	Yes	Yes
CCG01000 15887	Connect Network Presence DNS - Dynamic DNS Registration client in FW	Intel® ME FW will support a Dynamic DNS Update client (RFC 2136 and 1035) that will register the ME FQDN in the Corporate DNS. The DDNS Update client will be active under the following conditions: 1. Its state is set to enabled (default) 2. The platform is provisioned for Corporate (DDNS Update is never operable in Pre or In provisioning states or on consumer platforms)	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		3. The fully qualified domain name was provisioned in FW. If just a host name is configured then FW will not perform a DDNS Update. The default for DDNS Update should be disabled (since legacy ISV SW cannot disable it). DDNS Update client supported transport: 1. Supports UDP and not TCP 2. Supports both IPv4 and IPv6					
CCG01000 15885	Connect Network Presence DNS - Dynamic DNS Registration client in FW supported RRs (Resource Records)	The Dynamic DNS Update client in Intel® ME FW supports registration of RRs in DNS for both dynamic and manually configured IP addresses for the following RR types: A RR for shared IPv4 address and shared FQDN A RR for shared IPv4 address and dedicated FQDN A RR for static IPv4 address and dedicated FQDN. AAAA RR for dedicated IPv6 addresses and dedicated FQDN Note 1: FW does not support registration of PTR RRs.for IPv4 or IPv6 addresses Note 2: FW does not support update of A RR for static IP and shared FQDN	Yes	Yes	No	Yes	Yes
CCG01000 15884	Connect Network Presence DNS - Dynamic DNS Registration for shared FQDN	FW supports DDNS Update for shared FQDN with the following limitations: 1. There is no additional plug-in card besides the ME network interfaces on the system. 2. Both interfaces LAN and WLAN are using DHCP configuration	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		3. DDNS Update is only active when there is no lease maintained by the Host on any interface (wired or wireless). 5. When the host is actively maintaining the DNS registration it A RR the FW will periodically check whether the A RRs are up to date and if not FW will send a DDNS Update to refresh the Host FQDN A RRs in DNS.. In this case FW only sends ADD requests with no DELETE requests. 6. When FW detects that the FQDN changed FW does not delete RRs for the previous FQDN from DNS but the new FQDN RRs are updated by FW. It is assumed that the host handles removing the RR set for the previous FQDN.					
CCG01000 15883	Connect Network Presence DNS - Dynamic DNS Registration client in FW configuration options - WSMAN/WebUI	W will support the following configuration options in WSMAN and WebUI: 1. Enable/disable of the DNS Update client. Default is disabled. 2. The TTL value of the registered DNS RRs. Default is 15 min or 1/3 of lease time for DHCP (MSFT default is 20 min) -- not required in WebUI. Note: This applies only to WSMAN. 3. The periodic update interval default is 24 hours (MSFT default). A value of 0 disables the DDNS update refresh. The minimum value for the periodic refresh interval is 20 minutes. 4. Whether the FQDN set in FW is shared with the host or dedicated. Default is shared.	Yes	Yes	No	Yes	Yes
CCG01000 15882	Connect Network Presence DNS - Dynamic DNS Registration client in FW configuration options MEBx and USBKey	FW will support the following configuration options in AMTHI (pre-boot): 1. Enable/disable of the DNS Update client. Default is disabled. 2. Whether the FQDN set in FW is shared with the host or dedicated, Default is shared.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15881	Connect Network Presence DNS - Dynamic DNS Registration of Host VPN IP address for ME dedicated FQDN	When FW is configured with a dedicated FQDN, DDNS update is enabled and FW is using the Host VPN for connectivity into the corporate network (in cases that the environment detection determines that all interfaces are outside the Enterprise or FW could not find SOA/NS for the zone), then if the FW DDNS Update client is enabled FW will request that the LMS register the ME FQDN with the host VPN IPv4/IPv6 addresses in DNS. (Note that this might not be possible for all types of VPNs).	Yes	Yes	No	Yes	Yes
CCG01000 15600	Connect Link Selection	Dependent on policy setting, FW can support up to two interfaces (wired and wireless) simultaneously running with an IP for each connection that can be used when the host's network interfaces are down. Policy can prohibit one of the interfaces from being used.	No	Yes	No	No	Yes
CCG01000 15599	Connect Remote Bidirectional	All Intel® AMT client and server features should be available in remote connection both client and server features.	Yes	Yes	Yes	Yes	Yes
CCG01000 15598	Connect User Notification	The FW shall provide a notification interface to local host SW, for the purpose of notifying end users when critical System Defense policies, limiting the users networking capabilities have been applied by the FW.	Yes	Yes	Yes	Yes	Yes
CCG01000 15597	Connect User Notification Interfaces (SOAP only)	User notification shall be provided through dedicated SOAP API	No	No	No	No	No
CCG01000 15880	Connect User Notification Interfaces (WS only)	User notification shall be provided through WS-Eventing API	Yes	Yes	Yes	Yes	Yes
CCG01000 15483	Intel® AMT Network Presence in DNS through DHCP FQDN option (81)	Persistence of the Intel® ME PC DNS entry while the Intel® ME PC OS is off, sleeping, or non-functional, and the ME sub-system is operable, using the DHCP FQDN Option. The implementation will support the DHCP - RFC 4702 standard. Pre-AMT6: Intel® ME shall use the DHCP FDQN Option (81) to request that the DHCP server use DDNS to update the DNS Entry corresponding to the FDQN with the IP Address assigned by the	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		DHCP Server. In AMT6: - If the Intel® ME DDNS Update state was not set by the configuration SW or manually via MEBx/USBKey then Intel® ME implements Pre-AMT6 behavior. - If the Intel® ME DDNS Update is disabled by the configuration SW or manually via MEBx/USBKey then Intel® ME will not include the DHCP FQDN option in DHCP packets sent by FW. - If the Intel® ME DDNS Update is enabled by the configuration SW or manually via MEBx/USBKey then Intel® ME will use the DHCP FQDN option to request that the DHCP client (Intel® ME) will use DDNS Update to update the forward DNS Entry corresponding to the FDQN. The DHCP server will update the reverse lookup. The hostname value used for host record registration (in DHCP FQDN option or DDNS Update) will be the concatenation of the hostname field value, a period (''.''), and the domain name field value. In Pre-AMT6 or when Intel® ME DDNS Update state is not set: If the domain name field value is null or blank, the hostname value used in the DHCP FQDN option for host record registration will be the value of the hostname. In AMT6: When DDNS Update is enabled it is required that the domain name field be configured for thehost record registration to succeed.					

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15482	Memory initialization by host BIOS	When FW is unable to initialize the host system memory under the following scenarios: - BIOS boot-block flash memory is corrupted - CPU is dead or missing from socket - No memory is present in the DIMM sockets It shall log an error message into the flash and send appropriate PET alert to pre-defined management console.	Yes	Yes	Yes	Yes	Yes
CCG01000 15473	SMI to Intel® Management Engine Alerting Protocol	Define an SMI to ME alerting protocol to be used across a Intel® AMT Management Interface.	Yes	Yes	Yes	Yes	Yes
CCG01000 15471	Support 2nd Intel® MEI in OS	Add an OS 2nd Intel® MEI client of the 2nd Intel® MEI driver, and send messages between SMI and ME. This can be a fixed address client, or connection based.	Yes	Yes	Yes	Yes	Yes
CCG01000 15470	Alerting across 2nd Intel® MEI	Add support in the ASF & AMT Compatibility Modules for sending alert events and LAN link up / down events from ME to host through the 2nd Intel® MEI client	Yes	Yes	Yes	Yes	Yes
CCG01000 15449	Connect IPV4 Static IP Mode	The FW shall provide an option to configure the LAN interface to operate with Static IP configuration. Note 1: Intel® ME FW LAN address and host address configuration method must match: both must use either static IP or DHCP. Configuring Intel® ME FW LAN to use static IP and configuring the host to use dynamic IP (or vice versa) is an invalid configuration. Note 2: If both Intel® ME FW and the host use static IP, the static IP addresses must be different, in order to prevent address collision.	Yes	Yes	Yes	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 55541	Connect IPV4 shared Static IP Mode	The FW shall provide an option to configure the LAN interface to operate with shared Static IP configuration that can be synchronized with the Host IP. Note 1: Intel® ME FW LAN address and host address will be synchronized from Host IP. Note 2: When FW is set to "shared static IP", FW should implement same logic as shared DHCP for responding to ARP and ping. Note 3: Static IP mode can have the following modes: o Not applicable – when using DHCP o Shared static IP that should be synchronized by UNS o Shared static IP that should not be synchronized by UNS o Dedicated static IP	No	No	No	Yes	Yes
CCG01000 15434	ISV Enablement SSL VPN HTTP payload	The SSL VPN Gateway will be able to pass the following HTTP payload from AMT remote client to the management server: - SOAP 1.2 request/response - Binary data over HTTP.	No	No	No	No	No
CCG01000 15433	ISV Enablement SSL VPN Single Sign On	The SSL VPN Gateway Single Sign On (SSO) shall support the following authentication methods for the internal connection to the management server: - HTTP Basic/Digest Authentication - Support for Kerberos* Client that enables authentication based on AD credentials. Note: these are the maximum security requirement supported by AMT; there is no demand from ISV to support all of them.	No	No	No	No	No
CCG01000 15303	Connect MAC & IP Address Sharing	The FW shall share the MAC of the host regardless of DHCP or Static mode.	Yes	Yes	Yes	Yes	Yes
CCG01000 15302	Static AMT IP and Host OS IP may be the same	Since Intel® AMT and the Host OS will now share a MAC, the static IP of Intel® AMT and the Host OS may now be a supported configuration.	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15301	Firmware Connection Initiation Logic	The FW shall initiate a client connection when the FW is connected to the network. - This logic shall apply to both a local or remote connection. - The Initiation periodic time shall be set at Configuration time.	No	No	No	No	No
CCG01000 15300	Timeout Connection Initiation Logic	The FW shall initiate a client connection when the connection initiation time expires. - This logic shall apply to both a local or remote connection. - The Initiation periodic time shall be set at Configuration time.	No	No	No	No	No
CCG01000 15299	System Defense Connection Initiation Logic	The FW shall initiate a client connection when a System Defense event occurs - This logic shall apply to both a local or remote connection. - The Initiation periodic time shall be set at Configuration time.	No	No	No	No	No
CCG01000 15298	User Initiated Connection Initiation Logic	The FW shall initiate a client connection when the user triggers client initiated support from BIOS. - This logic shall apply to both a local or remote connection. - The Initiation periodic time shall be set at Configuration time.	No	No	No	No	No
CCG01000 15173	CPU Missing Alert	The ME FW should send an alert if the CPU has been removed in either a G3 or Sx state	Yes	Yes	Yes	Yes	Yes
CCG01000 15042	Link-related PET Events must identify the affected interface	Link UP PET events must now contain the following data: - Entity Instance of Link-up Event. - The IP address of the Link up Event LAN interface - Vendor ID and Entity ID must be added to the EventData field at the Link-up event	Yes	Yes	Yes	Yes	Yes
CCG01000 14713	Manageability VPN	The Intel® AMT FW shall support identical functionality through a VPN tunnel as it does over a local connection. The network infrastructure must support ME access of the VPN for both incoming and outgoing traffic on the Intel® AMT IANA ports.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15799	Dual Interface	Intel® AMT shall support both wired and wireless interface on the same subnet	No	No	No	No	No

3.3.19 Intel® Active Management Technology Connection Model for Remote Access & Client Initiated Connection

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15435	Connect Remote Access detection DNS Method	If user configures FW to use the DNS detection method then the FW shall detect whether it is operating remote to the enterprise based on: The FW shall compare the DNS domain passed from the DHCP server during the DHCP handshake (DHCP option 15) to a pre-configured set of Enterprise DNS suffixes. If the local DNS value does not match, the FW shall operate in remote access mode..	Yes	Yes	Yes	Yes	Yes
CCG01000 15432	Connect Remote Access Server Operations	When operating remote to the enterprise the FW shall disable its Server based operation for the network interface. Server operation from the host shall be supported.	Yes	Yes	Yes	Yes	Yes
CCG01000 15350	Host VPN feature Support	The following operations shall be supported when connecting to a management console via host VPN: - WS-MAN interface commands - EOI(SOAP) interface commands - PET and WS events Unsupported operations: - Redirection protocol messages for SOL and IDER - In AMT 6.0: KVM redirection Host VPN when the Intel® AMT device is configured to operate in either static IP	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15349	Host VPN Feature Enable	An Intel® AMT Admin level command will allow remote admin to enable or disable host VPN route, the default state is DISABLED	Yes	Yes	Yes	Yes	Yes
CCG01000 15348	Accepting remote connection from a host VPN route	Intel® AMT will accept an incoming connection from a host VPN route, when all of the below conditions are met: - The LMS has signaled that it has access to the enterprise network. - The Host VPN route is enabled, as defined in the new AMTNI command above.	Yes	Yes	Yes	Yes	Yes

3.3.20 Intel® Active Management Technology Client Initiated Remote Access

Starting with Intel® AMT 4.0, Intel® AMT supports User-Initiated Healing and Scheduled Maintenance use case scenarios that enables an end-user to trigger a manageability OOB connection from the Intel® AMT client to the manageability information structure.

The Healing use case can occur when the Intel® AMT client connects to the Enterprise or Small Medium Business network from the inside, using local access, or from outside, by means of remote access. This connection enables IT manageability tools to diagnose and heal the Client.

The Scheduled Maintenance use case can occur when the Intel® AMT client connects to the Enterprise or Small Medium Business network from the inside, using local access, or from outside, by means of remote access. This connection enables IT manageability tools to perform regular maintenance activities on the Client.

Intel® AMT 4.0/5.0 supported only wired Client Initiated Remote Access. Intel® AMT 6.0 introduces support for WLAN Client Initiated Remote Access as well.

3.3.20.1 General Requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15172	Client initiated Remote Access	Client initiated Remote Access	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15171	Client initiated connection Triggering	All Intel® AMT features are supported in a client-initiated model	Yes	Yes	Yes	Yes	Yes
CCG01000 15170	Availability of Client initiated Connection	There are two methods of end use triggering: - BIOS Screen - Intel® AMT SW Agent in the host OS (For example: Intel® tray icon APP). The method of end use triggering is dependent upon the health state of the Client Host OS.	Yes	Yes	Yes	Yes	Yes
CCG01000 15169	Client initiated OOB connection- Post conditions	To enable an end-user to initiate a healing session the following must be in place: - An Intel® AMT FW Client that receives a MEI command to trigger OOB connection. - An MEBx BIOS screen that enables an end user to enter during the BIOS boot process and request the triggering of the Healing use case, which in turn sends a MEI trigger command to the Intel® AMT FW. - An Intel® AMT OS Agent dialog box that enables the end user to place a request for triggering the Healing use case, which also sends a MEI trigger command to the Intel® AMT FW. - A mechanism for identifying whether the platform it is located inside or outside the corporate network, and triggering the Remote access or ICC-like connectivity mode accordingly. - Crypto must be enabled	Yes	Yes	Yes	Yes	Yes
CCG01000 15168	Connection Initiation Logic	The FW shall initiate a client connection when the following occurs : - The FW is connected to the network. - The connection initiation time has expired. - User triggered client initiated support from BIOS or Intel® AMT OS agent - This logic shall apply to both a local or remote connection. - The Initiation periodic time shall be set Intel® AMT Configuration time.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15167	End-User Screen	A new BIOS screen must be created for the BIOS Boot use case. The BIOS screen does not require that the end user have specific credentials such as a BIOS or MEBx user name and password. There are two options for the BIOS screen: - A new OEM BIOS Activate Healing Process screen for the end user. Such a screen is created by the OEM to conform with other OEM BIOS screens. The BIOS passes the trigger from the BIOS screen to MEBx in the form of a new parameter in the MEBx parameter frame or alternative API mechanism. - A new MEBx Activate Healing Process screen for the end user. As is the case with the OEM process, the end user does not require specific credentials in order to access this screen.	Yes	Yes	Yes	Yes	Yes
CCG01000 15166	Intel® Management and Security Status for End-User Control	For the Host OS case, a new dialog box is added to Intel® Management and Security Status. Upon opening the tray, the user sees an option for activating the healing process. This dialog box displays text that explains the Healing process to the end user, along with a button for triggering the process. This dialog box works in a fashion similar to that of the OEB/MEBx screen described above. Furthermore, the dialog box must allow OEM customization and localization, as is required with the Intel® Management and Security Status.	Yes	Yes	Yes	Yes	Yes
CCG01000 15165	Intel® AMT HECI Client	Upon receiving a MEI command, the Client triggers one of the following two actions, according to the current user initiation policy and the Intel® AMT Client location (inside or outside Enterprise network). - Start the Remote Access connection - Trigger an Intermittent Connection Computing (ICC) Healing mode.	Yes	Yes	Yes	Yes	Yes

3.3.20.2 Intel® Management Engine BIOS Extension Module (Intel® MEBx)

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015652	Trigger method	MEBx traps CTRL-ALT-F1 through entire period MEBx is running, and displays message ''Press and hold CTRL-ALT-F1 to enter Intel® Remote PC Assist Wizard''. MEBx must not support the above if RPAT capability bit is not enabled or firmware has completed Setup and Configuration	Yes	Yes	Yes	No	No
CCG0100015651	Localization	MEBx must support localization, at least on EFI BIOS version of MEBx. Localization will follow language(s) supported by the OEM's BIOS that ships with the PC. OEM configures the supported language(s) in MEBx at time of inclusion.	No	No	No	No	No
CCG0100015650	Connectivity Errors	MEBx must call HostCheckNetworkStatus AMTHI command before proceeding with Wizard. If error, must display Connectivity Error screen, with description, possible resolutions (e.g. check cable) and Intel support phone numbers.	Yes	Yes	Yes	Yes	Yes
CCG0100015649	Welcome, Privacy and Terms of Use, and Service Enable Screen	MEBx must display a welcome screen with legal privacy message and options for end user to opt in or opt out. MEBx will only display one time, if user opts in. MEBx should support scroll-like mechanism to support longer privacy policy message.	Yes	Yes	Yes	Yes	Yes

3.3.20.3 Intel® Management and Security Status Icon

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15636	Localization	All end user visible user interfaces must be localized.	Yes	Yes	Yes	Yes	Yes
CCG01000 15635	OS hot key support	Two software agents, (IMSS and Intel® RPAT client user interface agent) capable of trapping CTRL+ALT+F1 hot key, can coexist on the platform simultaneously and register for trapping the hot key event. The following requirements must be met by each of the software agents. Intel® RPAT UI agent requirements: Intel® RPAT UI agent will register for CTRL+ALT+F1 hot key in user's operating system under the following conditions: - If the system is not provisioned and the platform is Intel® RPAT capable - the Intel® RPAT UI will register for CTLR+ALT+F1 hot key, will trap the event and open an Intel® RPAT session when the hot key is pressed by the user.	Yes	Yes	Yes	No	No

3.3.20.4 Intel® AMT WLAN Client Initiated Remote Access

This section refers to Intel® AMT WLAN on Mobile platforms only.

This section specifies the requirements for WLAN Remote Access support. Host SW is Intel application that is responsible for WLAN connection management (Intel® PROset).

3.3.20.4.1 Intel® AMT FW for WLAN Remote Access

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15541	WLAN Profiles Access Policy	The Intel® Management Engine Firmware shall prohibit access to local profiles from remote and vise versa (Local applications shall not access remote profiles). Access to profiles includes enumeration, retrieval and deletion of a profile.	N/A	Yes	N/A	Yes	Yes
CCG01000 14712	WLAN User Profiles Mgmt	The Intel® Management Engine Firmware shall provide Applications running on Host with the functionality to Add, delete, update and enumerate user WLAN profiles (using Local Manageability Service). The API shall be provided by WSMAN interface. Profiles that are added by local application are used by host and Intel® Management Engine for establishing WLAN connection.	N/A	Yes	N/A	Yes	Yes
CCG01000 14711	WLAN User Profiles validity	Only valid user profiles shall be accepted by WLAN FW: Open (without encryption), Open - WEP, WPA-PSK (CCMP, TKIP)- RSN-PSK (CCMP, TKIP)	N/A	Yes	N/A	Yes	Yes
CCG01000 14710	WLAN IT Profiles Mgmt	The Intel® Management Engine Firmware shall provide Applications running on Host with the functionality to Add, delete, update and enumerate IT WLAN profiles (using Local Manageability Service). The API shall be provided by WSMAN interface. Profiles that are added by local application are used by host and Intel® Management Engine for establishing WLAN connection.	N/A	Yes	N/A	Yes	Yes
CCG01000 14709	WLAN IT Profiles validity	Only valid IT profiles shall be accepted by WLAN FW: WPA-PSK (CCMP, TKIP)-RSN-PSK (CCMP, TKIP)-WPA-802.1x - RSN-802.1x	N/A	Yes	N/A	Yes	Yes
CCG01000 14708	WLAN IT Profiles Access Policy	The Intel® Management Engine Firmware shall prohibit altering or deleting IT profiles by user.	N/A	Yes	N/A	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14707	WLAN Local Profiles Number	The WLAN stack SHALL support 8 BSS profiles for local management, stored in FLASH, prioritized by preference. Remark: The profile's priority is used to determine the order for choosing the WLAN network to connect to.	N/A	Yes	N/A	Yes	Yes
CCG01000 14706	Unprovisioning event	Upon unprovisioning event, both remote and local profile databases should be cleared.	N/A	Yes	N/A	Yes	Yes
CCG01000 14705	WLAN MAC User Profiles Encryption	The Intel® Management Engine Firmware stack shall support the following encryption mechanism: - WEP - TKIP - CCMP - No encription	N/A	Yes	N/A	Yes	Yes
CCG01000 14704	WLAN MAC User Profiles Authentication	The Intel® Management Engine Firmware stack shall support the following Authentication mechanism: Open, WPA and WPA2	N/A	Yes	N/A	Yes	Yes
CCG01000 14703	WLAN default link policy	WLAN link should be enabled by default in The Intel® Management Engine Firmware (S0 only)	N/A	Yes	N/A	Yes	Yes
CCG01000 14702	Wireless Profile synchronization enablement state changed event	FW requirement: Intel® Management Engine Firmware should issue Wireless Profile synchronization enablement state changed event to local SW. SW requirement: The locals SW should register for this event in Intel® Management Engine Firmware. When local SW receives this event, it should be written to Windows Event log	N/A	Yes	N/A	Yes	Yes
CCG01000 15879	WLAN Link Sensitive for User-Initiated: Inside Corporate Network	When User-Initiated is requested within the corporate environment, ME FW should assume control of WLAN (using link sensitive). Control should be released when PET / WS-Event is broadcast successfully, or when ME otherwise gives up on transmitting the PET / WS-Event.	N/A	No	N/A	Yes	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15878	WLAN Link Sensitive for User-Initiated: Outside Corporate Network	After User-Initiated is requested outside the corporate environment, ME FW may need to assume control of WLAN on any opening of a relevant tunnel to MPS (using link sensitive). Control should be released when user-initiated tunnel to MPS is closed for any reason.	N/A	No	N/A	Yes	No
CCG01000 19861	Link Control definition	For all ME network interfaces: - Host link control: The host controls the link attributes (e.g WLAN association), and both host and ME traffic can pass over the link. - ME link control: ME controls the link attributes (e.g. WLAN association), and ME traffic can pass over the link. - Host + ME link control: There are no issues of link attribute control, and both host and ME traffic can pass over the link.	N/A	Yes	N/A	Yes	Yes
CCG01000 19862	Link Preference Definition	For all ME network interfaces: - Host link preference: A link has host control as long as ME identifies a functional host driver over that link's interface. Otherwise, ME takes control over that link - though this taking over is not guaranteed to be immediate. If ME has control and identifies that host driver has resumed operation, ME relinquishes link control back to host. - ME link preference: ME takes control of the link, regardless of host driver status. Note: - ME does not relinquish control to host as long as the timeout hasn't expired. - The link survives host resets, host power-ups, and host driver disabling. - The link is guaranteed to survive power-down and power-cycle reset transitions in case those occur during a redirection session. - Host + ME link preference: has the same meaning as host + ME link control. Note:	N/A	Yes	N/A	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		- The link survives host resets, host power-ups, and host driver disabling. - The link is guaranteed to survive power-down and power-cycle reset transitions in case those occur during a redirection session.					
CCG01000 19863	Link reference with no wireless host driver	A user initiated wireless Fast Call for Help without a functional wireless host driver will result in the WLAN link preference changing to ME link preference. If no further action is taken, the link preference will return to Host link preference after a predefined timeout.	N/A	Yes	N/A	Yes	Yes
CCG01000 19864	Link control and link preference support	LAN supports only Host + ME link control and link preference. WLAN does not support the Host + ME link control and link preference. The default wireless link preference is the Host link preference	N/A	Yes	N/A	Yes	Yes
CCG01000 19865	Setting the link preference - KVM	When using KVM, the link preference can be set on a specific ME network interface. ME FW will return the link preference and the link control on a specific ME network interface when queried	N/A	Yes	N/A	Yes	Yes
CCG01000 19866	Setting the link preference - SOL/IDER	When using SOL/IDER, the link preference can be set on a specific ME network interface. ME FW will return the link preference and the link control on a specific ME network interface when queried	N/A	No	N/A	Yes	No
CCG01000 19867	Network Interface Priority	When possible, Remote Access from outside the organization will be invoked on the wired interface. Only if there is no IP address the session will be invoked on the wireless interface.	N/A	Yes	N/A	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 19868	Link Toggles During Remote Access (all network interfaces)	Remote Access sessions will maintain the connection in case there was a link toggle (link up link down) that did not cause an IP change. In case of a link toggle event that does trigger an IP change, the session will disconnect and the ME FW will automatically reestablish a new Remote Access session.	N/A	Yes	N/A	Yes	Yes

3.3.20.4.2 Host SW for WLAN Remote Access

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14700	Profiles synchronization enablement	Intel® PROSet shall provide mechanism for the user to enable/disable profile synchronization. Default before provisioning is enabled	N/A	Yes	N/A	Yes	Yes
CCG01000 14699	User profile synchronization acceptance	Intel® PROSet shall provide mechanism for user to Accept/Reject user profile synchronization on per profile basis if profile sync is enabled in ME FW Default is enabled	N/A	Yes	N/A	Yes	Yes
CCG01000 14698	User profile synchronization	If profile synchronization is enabled by Admin, PROset shall synchronize a User profile once it is successfully connected, saved in host profile store and accepted by the user.	N/A	Yes	N/A	Yes	Yes
CCG01000 14697	User profile synchronization privacy	For user profile synchronization, Intel® PROSet shall provide <appropriate> warning message to address the privacy concern.	N/A	Yes	N/A	Yes	Yes
CCG01000 14696	Admin profile synchronization	If profile synchronization is enabled by IT Admin, Intel® PROSet shall synchronize 16 IT WPA-PSK/ WPA2-PSK IT profiles with Intel® Management Engine Firmware whenever profile is applied & associated	N/A	Yes	N/A	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14694	IT profiles HTTP digest authentication with AMT	Intel® PROSet shall authenticate with AMT using the credentials and authentication method specified by an IT Administrator as defined in the document '' Intel® Active Management Technology -- Network Interface Guide'' version 3.0.01 & CIRA SAS	N/A	Yes	N/A	Yes	Yes
CCG01000 14693	User profiles HTTP digest authentication with AMT	Intel® PROSet shall use OSAdmin credentials	N/A	Yes	N/A	Yes	Yes
CCG01000 14691	Admin credentials configuration	Intel® PROSet shall provide UI mechanism for an IT Administrator to configure Username/password that shall be used to authenticate with Intel® Management Engine Firmware.	N/A	Yes	N/A	Yes	Yes
CCG01000 14690	Profile synchronization interface	Intel® PROSet application shall use DMTF WSMAN wireless profile for profile sync with Intel® Management Engine Firmware.	N/A	Yes	N/A	Yes	Yes

3.3.21 Intel® Active Management Technology Wireless OOB Management

The 802.11 Wireless LAN Package includes all of the elements necessary to provide out-of-band networking over the IEEE 802.11 standard in order to support Intel® AMT network operations.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15164	Wireless Enabled Features	The wireless stack shall support the following Intel® Active Management Technology features: - Web access - Asset management - SOL/IDE-R - System Defense - 3PDS - Remote Connectivity - KVM Note: Certain features are limited or implemented differently due to differences in wireless vs. wired operations	No	Yes	No	Yes	Yes
CCG01000 15163	Wireless Stack Operations	Establishment and persistence of secure and authenticated 802.11 link. This includes deployment of an 802.1X EAP protocols. Maintenance of the wireless link while the Intel® AMT PC OS is off, sleeping, or non-functional.	No	Yes	No	Yes	Yes
CCG01000 15162	Wireless support for Intel® AMT	Wireless support is composed of: - The 802.11 Wireless Stack package, a part of the Intel® AMT FW - The Wireless Intel® AMT Support SW Package running on the host operating system, consisting of the Intel® AMT-enabled Host Wireless Driver and Host Wireless Configuration Application - A communication and synchronization mechanism between the entities. Both packages communicate using Hardware Assistant Protocol (HAP) based on WLAN NIC HW, and Shared Memory accessible from ME by GP DMA.	No	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15161	WLAN NIC Ownership	Intel® AMT sends and receives Out-of-Band (OOB) traffic over the wireless NIC AMT any powered system state: - When the PC is on (S0) and uses the wireless NIC for wireless management traffic; - When Host PC is not using the wireless NIC because it is in one of S3-S5 power states; - When PC is AMT S0 power state but host does not use wireless NIC due to some problem (disabled/crashed).	No	Yes	No	Yes	Yes
CCG01000 15160	Manageability/Wireless Coexistence	The major system states from Manageability/Wireless coexistence point of view include: - Wireless NIC is not used. This situation happens when Intel® AMT is disabled. - Only Intel® AMT uses wireless NIC. This is the case when Management sub-system is ON but host is off or malfunctioned or does not use wireless LAN. Another use case is when Intel® AMT takes over NIC in order to preserve wireless link unbroken when some link-sensitive Intel® AMT flow is activated. In this mode all traffic between NIC and Upper MAC is redirected to M-Link bus. - Only host uses wireless NIC. The state occurs when Intel® AMT is off while host is up and uses wireless NIC. In this case all the Upper MAC traffic is send over PCI-E bus. Both host and Manageability use wireless NIC. In this case, Host WLAN Driver is used as a router for Manageability data traffic. The Host Driver also takes responsibility for Manageability Upper MAC activities. Management Sub-system does not access the NIC directly in this state.	No	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15159	WLAN NIC Drivers	According to the above state, WLAN NIC may serve needs of either host OS or Manageability Engine or both of them together. AMT any specific moment only one or both is defined as a WLAN NIC owner. Both owner and slave drivers should: - Configure the WLAN NIC over appropriate configuration space (PCI-e for host /M-Link for ME). - Change appropriate WLAN NIC power state (D-State for host, DM-State for ME) - Communicate one with the other via HAP. - Receive interrupts caused by NIC state change. In addition, only owner can and should: - Reset the WLAN NIC. - Download microcode to the NIC and check it's healthy by checking the microcode watchdog. - Send/receive traffic and control data to/from NIC. - Handle RF Kill and CT Kill events	No	Yes	No	Yes	Yes
CCG01000 15158	WLAN Networks	In Remote Connectivity scenarios, Intel® AMT supports the following Wi-Fi security communication methods to establish a connection with a WLAN Access Point (AP): - Open Networks - WEP - WPA - Personal - WPA2 - Personal	No	Yes	No	Yes	Yes
CCG01000 15877	WLAN Profile Sync Policies Intel Default	The default policy for WLAN profile sync is enabled before provisioning, disabled after.	No	Yes	No	Yes	Yes
CCG01000 15876	WLAN Riding of Host Connection	ME will ride any BSS connection established by host, without performing ME WLAN profile match.	Yes	Yes	No	Yes	Yes
CCG01000 15875	WLAN Stack Operation regardless of MNG mode	If present in the FW SKU, the WLAN stack must be operable regardless of MNG mode -- specifically, for any MNG mode even if different from ''AMT''.	No	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15874	WLAN Stack Operation in non-enterprise environments	WLAN stack architecture must not assume the presence of an IT and an enterprise provisioning process, i.e it should be operable also in non-IT environments and in cases where there is no post-production provisioning process.	No	Yes	No	Yes	Yes
CCG01000 15873	WLAN Connection Activation only by ME app requirements.	WLAN connection should only be activated when appropriate ME application or ME Common Services module requires it, i.e not rely only on some given policy (e.g system states).	No	Yes	No	Yes	Yes
CCG01000 15872	WLAN activation by user / admin action.	WLAN connection should not be activated without some explicit configuration/action by a user/admin (e.g ME app admin configuration or user-initiated trigger).	No	Yes	No	Yes	Yes
CCG01000 15871	WLAN CIRA Operation regardless of MNG mode	If present in the FW SKU, WLAN CIRA must be operable regardless of MNG mode -- specifically, for any MNG mode even if different from "AMT".	No	Yes	No	Yes	Yes
CCG01000 15870	WLAN CIRA Operation in non-enterprise environments	If present in the FW SKU, WLAN CIRA architecture must not assume the presence of an IT and an enterprise provisioning process, i.e it should be operable also in non-IT environments and in cases where there is no post-production provisioning process.	No	Yes	No	Yes	Yes
CCG01000 15869	WLAN Unprovisioning Event	The determining unprovisioning event for WLAN shall be ME common services unprovisioning (rather than AMT unprovisioning).	No	Yes	No	Yes	Yes
CCG01000 15868	WLAN Profile Sync Enabling According to ME Apps	WLAN Profile sync can be activated on a given platform only if that platform has a SKU containing an ME FW application requiring such sync.	No	Yes	No	Yes	Yes
CCG01000 15867	Intelligent Link Management	Link manager shall not automatically activate a link only based on the link policy. Instead, it shall only activate a link if both the link policy enables the link's interface AND there is an application which requires the use of that link.	No	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15866	WLAN link activity	WLAN link shall be considered active if ME uses it for any traffic, including for scanning.	No	Yes	No	Yes	Yes
CCG01000 15865	ME Wake On Link	In Sx, ME shall not wake on link-related events if the link is not active in Sx. WLAN-related events are ME Wake On WLAN packet and periodic wake for WLAN re-association. LAN-related events are ME Wake On LAN packet and link change event.	No	Yes	No	Yes	Yes
CCG01000 15864	Interface for App Need for Link	Link Manager shall expose an interface, internal to FW, which allows applications to declare that they require a certain link interface to become active.	No	Yes	No	Yes	Yes
CCG01000 15863	AMT Need for Active WLAN link	AMT requires an active WLAN link only if it is fully provisioned (i.e CS is provisioned and manageability mode is AMT).	No	Yes	No	Yes	Yes
CCG01000 15862	WLAN Profile Sync Policies	The FW shall contain two policies: Sync of IT (admin) profiles (enabled / disabled). Sync of user profiles (enabled / disabled).	No	Yes	No	Yes	Yes
CCG01000 15861	WLAN Profile Sync Policies	Policies regarding WLAN profile sync should be held in FW, should be readable by local and remote interfaces, and should be configurable by remote interfaces. The ability to read from local should be independent of ME Core Services provisioning state. On ME Core Services unprovisioning, policies should return to factory defaults. FW should also send an event when the policies change.	No	Yes	No	Yes	Yes
CCG01000 15860	WLAN Profile Sync -- SCS	SCS should allow IT admin to configure the local WLAN profile sync policies.	No	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15859	WLAN Profile Sync Policies Status -- Connection Managers (documentation)	The white-paper for connection managers wishing to support profile sync should include guidelines along the following lines: 1) ''The connection manager should ask ME whether profile sync is enabled, rather than holding a static policy in software.'' 2) ''The connection manager should follow events sent from the FW regarding profile sync policy change''.	No	Yes	No	Yes	Yes
CCG01000 15858	WLAN Core Service Provsioning Status	FW needs to send a user-notification when the WLAN core service provisioning is done, and allow reading the status of WLAN core service provisioning state.	No	Yes	No	Yes	Yes
CCG01000 15857	WLAN Core Service Provsioning Status Collection -- Connection Managers (documentation)	The white-paper for connection managers wishing to support profile sync should include guidelines along the following lines: ''The connection manager should ask ME regarding the WLAN Core Service provisioning state, and follow events regarding change of that state.''	No	Yes	No	Yes	Yes
CCG01000 15856	WLAN uCode Image and Core Services Provisioning	A valid uCode image should be present in the system at the moment of ME core services provisioning done.	No	Yes	No	Yes	Yes
CCG01000 15855	WLAN Removal of WebUI Support outside of AMT	WLAN must not allow a WebUI display of its settings outside of AMT.	No	Yes	No	Yes	Yes

3.3.22 Supported Power Transitions

Supported Power Transitions	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
G3/MOff to S0/M0	Y	Y	Y	Y	Y
S3/MOff to S0/M0	Y	Y	Y	Y	Y
S3/MOff to S3/M3	Y	Y	Y	Y	Y
S3/M3 to S3/M-Off	Y	Y	Y	Y	Y
S4,5/M-Off (with ME WOL) to S4,5/M3	Y	Y	Y	Y	Y

Supported Power Transitions	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
S4,5/M-Off (w/o ME WOL) to S4,5/M3	Y	Y	Y	Y	Y
S0/M0 to S3/M-Off	Y	Y	Y	Y	Y
S0/M0 to S3/M3	Y	Y	Y	Y	Y
S0/M0 to S4,5/M3	Y	Y	Y	Y	Y
S0/M0 to S4,5/M-Off (with ME WOL)	Y	Y	Y	Y	Y
S0/M0 to S4,5/M-Off (w/o ME WOL)	Y	Y	Y	Y	Y
S3/M3 to S0/M0	Y	Y	Y	Y	Y
S4,5/M3 to S4,5/M-Off (w/o ME WOL)	Y	Y	Y	Y	Y
S4,5/M3 to S4,5/M-Off (with ME WOL)	Y	Y	Y	Y	Y
S4,5/M-Off to S0/M0 (with ME WOL)	Y	Y	Y	Y	Y
S4,5/M-Off to S0/M0 (w/o ME WOL)	Y	Y	Y	Y	Y

NOTES:

1. M3 state is a new state introduced in the Intel® 5 Series Chipset Family (Ibex Peak). In pre-Ibex Peak generations, the same functionality was provided by the M1 state.

3.3.23 Intel® Active Management Technology Firmware Update

Firmware Update mode is a special mode provided by Intel® AMT firmware to download a new FW code off the network or from the local host into the flash device. To avoid a risk of unintentionally updating FW, the access to update should be transmitted over a secure channel and with certain basic authentication credentials. FW update process is essential for distributing new FW images with bug fixes. It is not allowed to update to images of different product generations (e.g. Intel® AMT 1.0 image with Intel® AMT 2.0/2.1 image and vice versa).

It should be noted that Intel® AMT Firmware is supported through ME general mechanisms and not through AMT.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14675	Intel® Management Engine Firmware Update versioning	FW update shall implement versioning range validity. An unmatched version image must not be updated into the flash.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15854	Intel® Management Engine Firmware Update requests OEM ID	FW update shall require an OEM ID to be entered if the Intel default of 0X0 has been changed during manufacturing. The FW shall verify that the ID is one of the options below: - The same OEM ID present on the pre-update image - An Intel default ID that allows update on all OEM systems	Yes	Yes	Yes	Yes	Yes
CCG01000 14664	Intel® Management Engine Firmware Update remote	Limitation \ Note: - Remote FW update must be done in S0 and via a host application - Recovery from flash contamination (power loss during the image write to flash) is not supported over network interface see FWUpdate recovery.	No	No	No	No	No
CCG01000 14654	Intel® Management Engine Firmware Update local	Intel® AMT FW shall implement FW Update process via the host (Intel® MEI) interface. - ME Firmware Local Update must be enabled in the MEBx. - The Intel® MEI driver must be installed.	Yes	Yes	Yes	Yes	Yes
CCG01000 14652	Intel® Management Engine Firmware Update Local Policy	Intel® AMT FW shall have administrative policy to enable / disable local host update. The policy shall be set at Intel® AMT configuration.	Yes	Yes	Yes	No	No
CCG01000 15798	Intel® Management Engine Firmware Update Secure	Intel® AMT FW shall implement FW Update process securely via the Intel® LMS interface. - In the MEBx, Intel® AMT must be selected in the Manageability Feature Selection menu. - In the Intel® AMT Configuration menu (in the MEBx), Local Firmware Update must be enabled. - The Intel® AMT LMS must be installed.	Yes	Yes	Yes	No	No
CCG01000 14641	Intel® Management Engine Firmware Update Initiation	Intel ® AMT FW update initiation shall use HTTP.	Yes	Yes	Yes	No	No
CCG01000 14630	Intel® Management Engine Firmware Update security	Intel ® AMT FW update initiation and download shall support security using TLS protocol.	Yes	Yes	Yes	No	No
CCG01000 14620	Intel® Management Engine Firmware Update Download protocol	The Intel ® ME FW shall download the code image using HTTP (SOAP or HTML) protocol.	Yes	Yes	Yes	No	No

ID	Requirements	Detailed Description	Intel[®] AMT 6.0 Desktop	Intel[®] AMT 6.0 Mobile	Intel[®] AMT 6.0 Consumer	Intel[®] AMT 7.0 Desktop	Intel[®] AMT 7.0 Mobile
CCG01000 14619	Intel® Management Engine Firmware Update Code image Verification	The Intel ® AMT FW shall verify the image content by doing authenticity check against the image signature.	Yes	Yes	Yes	Yes	Yes
CCG01000 14618	Intel® Management Engine Firmware Update Success Completion	When FW Update flow successfully completes, the Intel ® AMT FW shall send success alert notification. Limitation \ Note: The alert notification is only supported for network FW updates and not for local-Intel® MEI.	Yes	Yes	Yes	Yes	Yes
CCG01000 14617	Intel® Management Engine Firmware Update Fail Completion	When FW Update flow fails to complete, the Intel® AMT FW shall send failure alert notification. Intel® AMT FW shall keep using the old FW image when the update process ''failed to complete'' and the flash has not been contaminated (wrong version, bad integrity, etc.). In case of flash contamination (some of the data has been written into the flash), the FW shall work according to the Recovery process (FWUpdate recovery) Limitation \ Note: The alert notification is only supported for network/LMS FW updates and not for local.	Yes	Yes	Yes	Yes	Yes
CCG01000 14616	Intel® Management Engine Firmware Update Self Update	FWUpdate shall support updating FWUpdate code itself.	No	No	No	No	No
CCG01000 14615	Intel® Management Engine Firmware Update recovery condition	When flash contamination (power loss during the image write to flash) happens during normal FW update process the Intel® AMT FW shall move to Recovery mode.	Yes	Yes	Yes	Yes	Yes
CCG01000 14614	Intel® Management Engine Firmware Update recovery	In recover mode Intel® AMT FW shall implement recovery process of downloading new FW code image via the host interface (Intel® MEI).	Yes	Yes	Yes	Yes	Yes
CCG01000 14613	Intel® Management Engine Firmware Update recovery security	Intel® AMT FW recovery process shall be done via the host interface (Intel® MEI) using non-secure protocol.	Yes	Yes	Yes	Yes	Yes
CCG01000 14611	Intel® Management Engine Firmware Update Multiple SKUs	FW Update shall check that the image is compatible to the platform SKU according to versioning validity range. Each platform SKU will have its own version valid range.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14610	Intel® Management Engine Firmware Update Persistent data	The FW Update process shall not change any of the data that is saved on the NVM (3PDS , System Defense filters , ACLs , event log, HW Asset, etc).	Yes	Yes	Yes	Yes	Yes
CCG01000 14609	Intel® Management Engine Firmware Update Backwards compatibility	The Intel® AMT FW shall refuse to update to an Intel® AMT 1.0/2.0 flash image.	Yes	Yes	Yes	Yes	Yes
CCG01000 15517	Intel® Management Engine Firmware Localization	All user-visible strings should be in a format and location to enable easy localization. The FW Update tool will be English-only - any OEM or ISV can redistribute it in localized form.	Yes	Yes	Yes	Yes	Yes
CCG01000 15297	FWDowngradePolicy	The firmware will maintain a setting (Allowed or Not allowed) as to whether the firmware may be downgraded, this can be set by the OEM, and configured by provisioning or the MEBx.	No	No	No	No	No
CCG01000 15853	Flash lock override	-> Intel® ME FW shall expose an MEI lock-override mechanism interface that will override the flash lock -> An NVAR mechanism shall be exposed to allow the OEM to enable/disable the MEI flash lock-override mechanism An MEI override lock-out command shall be available for BIOS BIOS to lock and unlock the MEI override mechanism interface	Yes	Yes	Yes	Yes	Yes
CCG01000 15852	Flash lock override availability	-> MEI lock-override mechanism interface shall always be available when Intel® ME is in manufacturing mode -> MEI interface shall be available post manufacturing mode under the following conditions: -> EOP message has not been sent -> MEI override lock-out command has not been received -> The MEI command to allow host access to the ME region of flash will return an error after the MEI override lock-out command has been received	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14524	Graph of allowed FW updates	The image of each FW version V shall contain in its manifest: - A FW versions graph descriptor. The graph contains only undirected (bi-directional) edges, where an edge between two versions indicates that bug fixes have been merged from one of the versions to the other. The descriptor itself shall contain only the list of edges. - A black-list - listing all FW versions that V is aware of, for which a FW update from V to those versions is prohibited. Size of descriptor and black list combined shall not exceed 1K total.	No	No	No	Yes	Yes
CCG01000 14533	FW downgrade file	ME FW shall allow reading the current FW code through HECI.	No	No	No	Yes	Yes
CCG01000 14523	Migration cases	When updating from FW version V to FW version U, a named variable X may require migration if any of the following is true: - X is supported by V and not by U (variable removal). - X is supported by U and not by V (variable addition). - X is supported by both V and U, but its format (e.g. C structure) is different between V and U (variable format change). - X is supported by both V and U, but a value for X that is supported by V is not supported by U (variable value removal). Note that this is a special case where the update from V to U may not always be supported, or the firmware may behave differently after the update due to data loss. Also note that if variable X is tied to another variable Y in a manner where the value removal of X may create an illegal combination with Y's value, it is up to the migration code to try and handle these cases. - X is supported by both V and U, but a value for X that is supported by U is not supported by V (variable value addition).	No	No	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14526	Migration logic location	If a FW update from version V to version U is allowed and FW version V is newer (i.e U's FW version graph is a subset of V's FW version graph), FW version V must also contain all required migration logic to / from FW version U's variables	No	No	No	Yes	Yes
CCG01000 14530	Fault tolerant data migration	On update from FW version V to FW version U, any data migration invoked by FW version U must be fault tolerant. If a power loss occurs during the migration, on next ME init the migration must start over again until completion, taking into account that some of the data may already have been migrated (the migration logic is responsible for that).	No	No	No	Yes	Yes

3.3.24 Intel® Active Management Technology Identity, Credential, and Access Control

Identity, Credentials, and Access Control are critical components and building blocks of any security product design. These requirements define the security properties of an Intel® AMT / Intel® Management Engine system, and direct the security protocols, algorithms and system behavior.

These requirements also help reach a common understanding on security perimeter around our product, with Cisco, Enterprises IT departments, OEMs and other customers.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15588	Credential Identity Binding	AMT shall be configured with appropriate identity, which is bound to the platform identity. The platform identity will also delegate identity to the host(s) on the same platform.	No	No	No	No	No
CCG01000 15587	Credential Distinct	Host and AMT shall maintain separate and distinct set of credentials, for a dual-MAC mode. For single MAC mode, the same credentials may be used to access the WLAN/LANs.	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15586	Credential Management	AMT shall allow remote updates, revocation, and installation of credentials.	No	No	No	No	No
CCG01000 15585	Credential Enforcement	AMT shall have a clear cut-over policy and mechanism for the use of new credentials.	No	No	No	No	No
CCG01000 15584	Credential No User Interaction	AMT shall be configured with credentials whose use does not require any interactive session with users.	No	No	No	No	No
CCG01000 15583	Credential Selection	AMT may support selection of credentials, based on (1) Protocol (2) Administrative domain.	No	No	No	No	No
CCG01000 15582	Credential Multiple	Depending on IT policy, administrative domain, and security protocols, AMT may be configured with more than one credential.	No	No	No	No	No
CCG01000 15581	Credential Admin Domain	AMT may distinguish between different administrative domains.	No	No	No	No	No
CCG01000 15580	Credential Access Policy	AMT may store and apply specific access and policy profiles, when connecting through different administrative domains.	No	No	No	No	No
CCG01000 15579	Credential No Security	AMT shall connect to LAN/WLAN networks which do not support link security.	No	No	No	No	No
CCG01000 15578	Credential Hotspot	AMT may be configured with appropriate credentials to connect to the hotspot WLAN.	No	No	No	No	No
CCG01000 15518	Environment Detection	List of DNS names or Any DNS (*.*) must be configured in initial configuration time. In case of a DNS mismatch Intel® AMT will close its HTTP port and disable the System Defense policies enforcement. System must differentiate between the two interfaces Wired and Wireless with detecting and enforcing the behavior Limitations: In Case of static IP no detection will take place. Note: Only Wired features are supported in Intel® AMT 3.0.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14686	Remote Access Detection Trust Method	An IT can configure environment detection to operate in secure mode. In this mode, the IT must provide a list of HTTPS servers, known to be accessible only within the enterprise Intranet. Each entry in the list must contain the FQDN of the server. The SSL Server certificate of the server must be rooted with a root of trust cert, trusted by AMT.SDK	No	No	No	No	No

3.3.25 802.1x

802.1x authentication is required in order to allow Intel® AMT to connect to the network when the local IT policy is to use 802.1x. 802.1x is widely used in wireless networks, and in some wired networks.

802.1x is also a building block for the NAC feature.

Note: Only Wired features are supported in Intel® AMT 3.0 and 5.0. Those requirements for AMT 3.0 and 5.0 with a "Y" in the column refer to wired networks only.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15577	802.1x General	[802.1x] and [EAP] shall operate over both LAN and WLAN links	Yes	Yes	Yes	Yes	Yes
CCG01000 15576	802.1x EAP TLS	802.1x EAP TLS[EAP-TLS(a)] and [EAP-TLS(b)] shall be supported over the LAN and WLAN links.	Yes	Yes	Yes	Yes	Yes
CCG01000 15575	802.1x EAP TTLS	[EAP-TTLS(a)] and [EAP-TTLS(b)] shall be supported over the LAN and WLAN links - Inner method supported: MSCHAPv2.	Yes	Yes	Yes	Yes	Yes
CCG01000 15574	802.1x PEAP MSCHAP	[PEAP] & [MSCHAP-v2] shall be supported over the LAN and WLAN links.	Yes	Yes	Yes	Yes	Yes
CCG01000 15573	802.1x EAP Fast	[EAP-FAST] shall be supported over the LAN and WLAN links. Inner methods supported: EAP-GTC, MSCHAPv2,TLS.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15572	802.1x EAP GTC	{EAP-GTC} shall be supported over the LAN link.	Yes	Yes	Yes	Yes	Yes
CCG01000 15571	802.1x. No OS (For Wired also when OS is up)	The Intel® AMT FW Shall activate the 802.1x authentication protocol only: For wireless - when the host's OS is not functional and when the FW is configured to operate in shared-ip DHCP mode, the FW will not provide 802.1x when operating in Static IP mode.	Yes	Yes	Yes	Yes	Yes
CCG01000 15570	802.1x LAN Profile	The Intel® AMT FW shall support a single configuration of the 802.1x supplicant over LAN. (i.e. single EAP type with single set of credentials / certificate).	Yes	Yes	Yes	Yes	Yes
CCG01000 15569	802.1x. Remote_Config	The 802.1x configuration shall be exposed for configuration by Remote Management Application using SOAP.	Yes	Yes	Yes	Yes	Yes
CCG01000 15568	802.1x Radius Server Support	The 802.1x supplicant shall be tested with the following RADIUS servers: - Cisco* ACS v3.3, v4.0, and 4.2 - Microsoft* Radius server (MS server 2003) - Funk Odyssey* v2.01 - Devicescape - WiFi WPA2 Test Bed RADIUS Server for Linux - MeetingHouse - MDC AEGIS Server for Windows*	Yes	Yes	Yes	Yes	Yes
CCG01000 15567	802.1x AP Support	The 802.1x supplicant shall be tested with Cisco* AP1200 access point.	Yes	Yes	Yes	Yes	Yes
CCG01000 15566	802.1x Switch Support	The 802.1x supplicant shall be tested with the following switches: - Cisco* 3750 switch - HP ProCurve* 2824 switch	Yes	Yes	Yes	Yes	Yes

3.3.26 Endpoint access Control (EAC)

In the EAC usage model, a client’s access to an Enterprise is dependent on the client platform being in an acceptable state. The Enterprise determines the parameters of acceptability in the form of an Access Policy.

The main drive behind this section is to support the Cisco NAC and Microsoft NAP initiatives.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15565	NAC General	NAC shall be supported over both wired and wireless links. * Wireless not supported on desktop platforms	No	Yes	No	Yes	Yes
CCG01000 15563	NAC Access Requestor	The Intel® AMT FW shall act as a NAC access requestor when it's embedded 802.1x supplicant is the active supplicant	Yes	Yes	Yes	Yes	Yes
CCG01000 15562	NAC AMT posture	The Intel® AMT FW shall send the following information as its own and the host's posture: - AMT module image - Hardware inventory - BIOS vendor/version - Event log - IDER boot log	Yes	Yes	Yes	Yes	Yes
CCG01000 15561	NAC AMT PEP	The Intel® AMT FW shall send the following information as its own and the host's posture: - AMT module image - Hardware inventory - BIOS vendor/version - Event log - IDER boot log	No	No	No	No	No
CCG01000 15560	NAC Cisco NAC Req	The Intel® AMT FW shall conform to CCXv4-S52 - NAC requirements, with changes resulting from being an embedded supplicant rather than a host-side supplicant.	No	No	No	No	No
CCG01000 15559	NAC Cisco EAP fast NAC Req	The Intel® AMT FW shall conform to CCXv4-S58 - EAP-FAST enhancements.	No	No	No	No	No
CCG01000 15558	NAC Posture Signature	The Intel® AMT FW shall wrap the AMT posture in a secure XML envelope. The envelope shall be signed according to XML-DSIG standard, using RSA.	No	No	No	No	No
CCG01000 15557	NAC Posture Signature Verification	The Intel PDP plug-in shall verify the posture according to the shared credentials with Intel® AMT, and evaluate it according to pre-defined rules set by IT.	No	No	No	No	No
CCG01000 15556	NAC Policy Signature	The Intel PDP plug-in shall sign the NAC policy using the shared credentials and send it via the EAC inner method.	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15555	NAC Policy Signature Verification	AMT FW shall receive the policy, verify the XML security envelope, and implement the policy in System Defense filters.	No	No	No	No	No
CCG01000 15554	NAC Testing ACS Ver	AMT shall be tested with the following Cisco ACS versions: ACS v4.2	Yes	Yes	Yes	Yes	Yes
CCG01000 15553	NAC Testing CTA Ver	Intel® AMT shall be tested with Cisco CTA v2.1 (CTA is the Cisco NAC host agent)	Yes	Yes	No	Yes	Yes
CCG01000 15552	NAC Testing Switch Ver	AMT NAC agent shall support with the following Cisco switches: Cisco 3750 switch	Yes	Yes	No	Yes	Yes
CCG01000 15551	NAC Testing AP Ver	AMT NAC agent shall support the following Cisco access points: Cisco AP1200	Yes	Yes	No	Yes	Yes
CCG01000 15550	NAC configuration	NAC feature shall be configured via SOAP/WS-MAN. Configuration commands include enable/disable of the features, and credentials configuration.	Yes	Yes	No	Yes	Yes
CCG01000 15549	NAC Networking Presence Support	The Intel ® AMT FW Shall act as a NAC access requestor when it's embedded 802.1x supplicant is the active supplicant. See 802.1x PRD for more details.	No	No	No	No	No
CCG01000 15295	EAC Secure policy enforcement	When the authentication between AMT and the <EAC backend server> is completed AMT shall receive SDT Policy from the <EAC backend server>	No	No	No	No	No
CCG01000 15294	EAC alerting	When the authentication between AMT and the <EAC backend server> is completed AMT shall receive <Alert Policy> from the <EAC backend server>	No	No	No	No	No
CCG01000 15293	EAC platform policy enforcement	When the authentication between AMT and the <EAC backend server> is completed AMT shall receive <SDT Policy> from the <EAC backend server> in order to enforce network access control as defined by the system administrator	No	No	No	No	No
CCG01000 15292	NAC Version	AMT shall be conformant with NAC v2.1	No	Yes	No	No	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15291	NAC posture plug-in	When a Cisco Trusted agent starts its authentication process it shall retrieve a posture from the AMT FW for the purposes of providing AMT posture to the NAC backend.	Yes	Yes	Yes	Yes	Yes
CCG01000 15290	NAC protocols support	When the Intel® AMT exchanges posture information with the <Cisco ACS> it shall use one of the following protocols: - 802.1x - EAP over UDP.	Yes	Yes	Yes	Yes	Yes
CCG01000 15289	NAP General	Intel® AMT shall support NAP vX.X	Yes	Yes	Yes	Yes	Yes
CCG01000 15288	NAP posture plug-in	When Microsoft NAP agent starts its authentication process it shall retrieve a posture from the AMT FW for the purposes of providing AMT posture to the NAP backend.	Yes	Yes	Yes	Yes	Yes
CCG01000 15287	NAP Network presence AMT OS absent states	When the host system enters OS absent state the AMT FW must maintain its <network presence> on an <NAP enabled network>.	Yes	Yes	Yes	Yes	Yes
CCG01000 15286	NAP DHCP support	When AMT is in a NAP enabled environment it shall implement the NAP DHCP extensions in order to get its IP address	No	No	No	No	No
CCG01000 15285	NAP Linksec Support	When Microsoft NAP agent starts its authentication process it shall retrieve a posture plug-in from the AMT FW. Active Management Technology shall have the capability to interoperate with a Linksec enabled environment (IEEE 802.1AE)	No	No	No	No	No
CCG01000 15154	Usage	The feature shall be employed when a client is attempting to enable the network in AMT/OOB mode and will result in either being granted access or quarantined.	Yes	Yes	No	Yes	Yes
CCG01000 15153	NAC Network presence AMT OS absent states	When the host system enters OS absent state the AMT FW must maintain its <network presence> on an <NAC enabled network>.	Yes	Yes	Yes	Yes	Yes
CCG01000 15152	802.1x support	When the host system enters OS absent state the AMT FW must maintain its <network presence> on an <NAC enabled network>.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15151	802.1x protocols	When a Cisco Trusted agent starts its authentication process it shall retrieve a posture from the AMT FW.	Yes	Yes	Yes	Yes	Yes
CCG01000 15150	Linksec Support	When Microsoft NAP agent starts its authentication process it shall retrieve a posture from the AMT FW. Active Management Technology shall have the capability to interoperate with a Linksec enabled environment (IEEE 802.1AE)	No	No	No	No	No
CCG01000 15041	PEAPv0 support for NAP SoH	Support for NAP SoH protocol on top of PEAP v0 authentication for AMT to exchange posture/health information with NAP NPS backend server directly and get onto a NAP network OOB (when OS is not present). The NAP SoH protocol format is specified in IF-TNCCS-SOH_v1[1].0_r6.doc. Reference: https://www.trustedcomputinggroup.org /specs/TNC/IF-TNCCS-SOH_v1.0_r8.pdf	Yes	Yes	Yes	Yes	Yes

3.3.27 Intel® Active Management Technology SOL/IDE redirection

Note: This section does not include performance requirements. The performance requirements are in section 3.6 and 7.2.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15427	USB redirection	Intel® AMT will support USBr redirection	No	No	No	No	No
CCG01000 15426	No session on reset or power state transitions.	No re-start of the remote media session shall be required during a platform reset or power on/off.	No	No	No	No	No
CCG01000 15425	Re-authentication	Redirection sessions have an inactivity timeout. The user must be required to re-authenticate and re-establish a new session after a timeout.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15424	Detach & Disconnect	Detach of media redirection device must appear to the BIOS/OS as equivalent to removing media from a CDROM or super-floppy. Disconnect from remote media redirection server must appear to BIOS/OS as equivalent to removing media from a CDROM or super-floppy	Yes	Yes	Yes	Yes	Yes
CCG01000 15423	Enable/Disable redirection	The redirection interfaces must have the ability to be enable and disable (each interface alone).	Yes	Yes	Yes	Yes	Yes
CCG01000 15422	OS installation	It shall be possible to install an operating system on a bare metal (no OS present) platform using a remotely mounted device. This may also require the use of SoL to configure the OS during install.	Yes	Yes	Yes	Yes	Yes
CCG01000 15421	Boot from IDEr devices	Mounted IDEr devices shall show up in the BIOS boot order and it shall be possible to change the BIOS boot order to boot from this remote device. Depends on BIOS support.	Yes	Yes	Yes	Yes	Yes
CCG01000 15420	Redirection over WS-MAN	Intel® AMT will use WS-Man for the control flows only. The data will be transferred in TCP.	No	No	No	No	No
CCG01000 15419	Redirection over TCP	Intel® AMT will redirect all SoL/IDEr/USBr data over TCP.	No	No	No	No	No
CCG01000 15284	Redirection Support to floppy drives	Intel® AMT shall allow any Floppy devices on the management console to appear as local devices to the host BIOS and host OS.	Yes	Yes	Yes	Yes	Yes
CCG01000 15283	Redirection Support for LS-120 drives	Intel® AMT shall allow any LS-120 devices on the management console to appear as local devices to the host BIOS and host OS.	Yes	Yes	Yes	Yes	Yes
CCG01000 15282	Redirection Support for CD-ROM devices	Intel® AMT shall allow any CD-ROM devices on the management console to appear as local devices to the host BIOS and host OS. Note: DVD devices will be treated as CD-ROM devices by the host BIOS; will appear as local devices to the host BIOS and host OS.	Yes	Yes	Yes	Yes	Yes
CCG01000 15281	Redirection Support for HD images	Intel® AMT shall allow images of Hard Drive devices on the management console to appear as local devices to the host BIOS and host OS.	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15280	Redirection Support for images of all supported devices	Redirection will allow AMT to connect to images emulating any of the support devices on a remote system	Yes	Yes	Yes	Yes	Yes
CCG01000 15279	Flexible Storage of redirection images	AMT will not discriminate as to how the remote system chooses to access images which it serves for redirection. Images may be stored on any storage device exposed to the remote system operating system provided the read-write permissions are correct and the performance and latency falls within normal device usage. This storage including mapped network drives and USB storage.	No	No	No	No	No
CCG01000 15278	IDE-R / SOL capabilities advertisement	Provide a method for determining formatting of data from screen (VT-100, PC-ANSI, rows and column counts) Also if hardware does not support a type of redirection (ex. floppy) allow advertisement of that as well	Yes	Yes	Yes	Yes	Yes
CCG01000 57995	Redirection Support for DVD-R device	Intel® AMT shall allow any DVD of type DVD-R devices on the management console to appear as local devices to the host BIOS and host OS. Note: Redirected DVD image will be treated as CD-ROM devices by the host BIOS; will appear as local devices to the host BIOS and host OS.	No	No	No	Yes	Yes
CCG01000 08864	Privacy Notice during redirection session	During active redirection session (SOL, KVM-R, IDE-R) the firmware will display a visual indication on the screen at all times using ME sprite (like is done for KVM - red border, flashing icon in top right). This is visual indication only, and not opt in (i.e. no passcode box before connect).	No	No	No	Yes	Yes

3.3.28 LinkSec (802.1AE/AF)

LinkSec is a layer-2 security protocol (authentication and encryption) for wired networks. 802.1ae is the runtime authentication and encryption protocol. 802.1af is the key agreement protocol, but this standard is still in an early draft phase. Cisco has defined the SAP protocol for key agreement and it is expected that 802.1af will be very similar to SAP.

Note: Support of this feature assumes HW offload of the runtime encryption and authentication. Key agreement protocol will be done in FW or SW.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15418	Key agreement protocol - Cisco SAP	Intel® AMT will support Cisco SAP protocol for key agreement	No	No	No	No	No
CCG01000 15417	Key agreement - 802.1x	The 802.1x supplicant should derive the master session key (MSK) as a result of the EAP exchange.	No	No	No	No	No
CCG01000 15416	Key agreement protocol - 802.1af	Intel® AMT will support 802.1af key agreement protocol (reason: spec is not expected to be ready on time)	No	No	No	No	No

3.3.29 Outbreak Containment - Base Heuristics

This section specifies the outbreak containment requirements. It describes the configuration of the heuristics and the actions to take in case a worm is detected.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15415	Number of Heuristics	Intel® AMT will implement up to 2 base heuristics and 2 DoS heuristic. All heuristics may be run simultaneously. The DoS heuristics are hard coded, and automatically enabled when at least on the base heuristics is enabled.	Yes	No	Yes	Yes	No
CCG01000 15414	Base heuristics Configuration Store	When the FW receives a configuration from a remote application via the OOB interface, the FW shall store this information in the NVM, in other words policy configuration is persistent.	Yes	No	Yes	Yes	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15413	Action effectiveness	After a worm is detected it will move to another state called ''encounter'' state, the engine will stay in this state for 'x' (configurable time) seconds, as long as the worm identified it will apply the action and stay in this state, if there will be 'x' seconds of quiet it will remove the action and return to the running state, if DoS was identified it will perform the action and enter into disable state). The action will take affect until the IT administrator will update the configuration and re-enable the base heuristics engine.	Yes	No	Yes	Yes	No
CCG01000 15412	Availability	The base heuristics features will be active as long as Intel® AMT is running and the host OS is up. If the base heuristics activate an action - the action will not be removed (even when OS is down) until the IT administrator will update the configuration.	Yes	No	Yes	Yes	No
CCG01000 15411	Heuristics configuration	Intel® AMT will expose a network interface to configure the base heuristics. For each base heuristic the following parameters will be available: - enable/disable heuristic - Heuristic parameters (time-window, max unique addresses, max unique addresses per port). - Action: what Intel® AMT should do if it detects worm. - Possible actions are: - Notify management console. - Activate pre-defined System Defense policy. - Block the specific port the worm was detected on and the specific protocol TCPSyn, UDP for Tx traffic only. - Block all outgoing traffic.	Yes	No	Yes	Yes	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15410	Type of Heuristics	Intel® AMT will support only transmit heuristics. There will be no support in Receive heuristics. List of heuristics: - Fast base heuristic - time window of 10-1000 ms - Slow base heuristic - time window of 1-50 seconds. - DoS heuristic - detect if too many packets are passing the Header redirection filters and block them. - Fragmented IP heuristic - detect an Attack of fragmented IP packets and block it.	Yes	No	Yes	Yes	No
CCG01000 15409	Packets scanning	The base heuristics will scan the following outgoing packets: - All TCP packets with the SYN flag asserted. - ALL UDP packets. - The first fragment of all fragmented IP packets.	Yes	No	Yes	Yes	No
CCG01000 15277	Wireless Heuristics	Support for Heuristics over a wireless interface	No	No	No	No	No

3.3.30 Other Requirements

3.3.30.1 Network Stack Compliance

Defines the tools required for validation so that the product adheres to external specification requirements for network operation.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15818	Stack TCP/IP	The FW TCP/IP stack shall be compliant with the following RFCs - RFC 793 ''Transmission Control Protocol'' - RFC 1122 ''Host Requirements-Communications'' - RFC 1323 ''Path MTU Discovery'' - RFC 2001 ''TCP Slow Start, Congestion Avoidance, Fast Retransmit and Fast Recovery Algorithms'' Limitations \ Note : The FW stack shall not support fragmented packets Limitations \ Note : The FW stack shall not support fragmented packets	Yes	Yes	Yes	Yes	Yes
CCG01000 15817	Stack Gateways	The FW stack shall support only 1 default gateway.	Yes	Yes	Yes	Yes	Yes
CCG01000 15816	Stack Num Of IPV4 Address	The FW stack shall support 1 IPv4 address.	Yes	Yes	Yes	Yes	Yes
CCG01000 15815	Stack Max MTU Size	The MTU size the FW shall support is 1500 bytes.	Yes	Yes	Yes	Yes	Yes
CCG01000 15814	Stack Compliance tool	The FW stack shall pass IXIA ANVL TCP test suite. Limitation \ Note: The pass criteria are defined by the 3rd party providing the stack. The test results of the 3rd party must be reviewed and approved.	Yes	Yes	Yes	Yes	Yes
CCG01000 15813	Stack HTTP Browsers	The FW HTTP implementation shall be interoperable with the following web browsers: a. Internet Explorer* 6 (or latest available during Beta release) c. Firefox* Limitations \ Note: The browsers must be updated with the latest security patches and fixes.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15809	Stack Soap	FW SOAP stack shall be compliant with WS-I Basic Profile 1.1. The FW shall pass the WS-I interoperability test tools. Limitation \ Note : The pass criteria are defined by the 3rd party providing the stack. The test results of the 3rd party must be reviewed and approved.	Yes	Yes	Yes	Yes	Yes
CCG01000 15808	Stack TLS Interoperability	The FW TLS implementation shall be interoperable with the following web browsers: - Internet Explorer* 6 (or latest available during Beta release) - Firefox* Limitations \ Note: The pass criteria are defined by the 3rd party providing the stack. The test results of the 3rd party must be reviewed and approved. The browsers must be updated with the latest security patches and fixes	Yes	Yes	Yes	Yes	Yes
CCG01000 15807	Stack TLS Interoperability SSL	The FW TLS implementation shall be interoperable with the latest open SSL implementation. 3rd party vendors must supply Codenomicon* TLS test tool results.	Yes	Yes	Yes	Yes	Yes
CCG01000 15806	Stack DHCP	The FW DHCP client implementation shall be interoperable with the following DHCP server implementations: - Windows* 2003 - Cisco Switch - Latest Linux-based DNS\DHCPs (testing to be done with Open Source only)	Yes	Yes	Yes	Yes	Yes
CCG01000 15400	Stack DHCPv6	The FW DHCPv6 client implementation should be interoperable with the following DHCPv6 servers/routers: - Cisco -- server, relay -- in Cisco IPv6 router (dhcpv6 stateless configuration only) - Windows Server 2008 - Dibbler	No	No	No	No	No

3.3.31 Protected Real Time Clock (PRTC)

Intel® AMT uses the PRTC to provide time for the logging application, certificate validation, and time-driven policy execution (e.g., once a week, check for a firmware update).

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15516	Protected real time clock	Intel® AMT shall use the PRTC to provide time for: - the logging application - certificate validation - time-driven policy execution - the calculation of the DHCP lease renewal time when configured for Intel® Management Engine Wake on LAN to wake the Intel® Management Engine in time to renew the DHCP lease. For synchronizing the time on the PRTC, SNTP/NTP (Simple Network Time Protocol RFC2030/Network Time Protocol RFC 1305) like semantics are used for calculating network latencies, and resulting in high accuracy time updates (for more sensitive usage scenarios such as Kerberos*).	Yes	Yes	Yes	Yes	Yes
CCG01000 15515	Trusted time	The Intel® Management Engine shall acquire trusted time from a remote console over TLS. Limitation: This is true only when TLS is enabled at configuration time. If TLS is disabled, Intel® Management Engine will acquire time from management console after authentication with HTTP digest as defined in the ''Secure time'' requirement given below.	Yes	Yes	Yes	Yes	Yes
CCG01000 15514	Current time & Non-volatile flash memory	Once an Intel® AMT device is configured with time from a trusted time source, it will periodically place the current time in the non- volatile flash memory for ensuring that the PRTC has a time if it loses it due to loss of power.	No	No	No	No	No
CCG01000 15513	Accurate Time	PRTC acquires time using a 2 step (SNTP style) high-accuracy mechanism because the Kerberos application needs such level of accuracy.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15512	Secure Time	If TLS is disabled, ME shall acquire time from management console after authentication to Intel® AMT using HTTP Digest, before Intel® AMT allows it to update the time. Underlying TLS layer provides communication security to time update messages.	Yes	Yes	Yes	Yes	Yes

3.3.32 Installation and Upgrades

This section describes Installation and upgrades of Intel® AMT Firmware and SW.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15802	Install End user BIOS	IT Administrations or Technicians shall turn on the Intel® AMT features via the system BIOS.	Yes	Yes	Yes	Yes	Yes
CCG01000 15801	Install End user ISV app	IT Administrations or Technicians shall configure the Intel® AMT features via the user interfaces of the enabled ISV management applications.	Yes	Yes	Yes	Yes	Yes
CCG01000 15800	Install SDK master	ISVs shall use the SDK to install documentation, sample code, code libraries, WSDLs and other SDK components.	No	No	No	No	No
CCG01000 15796	Install SDK Master OS mechanism	The SDK shall install on both Linux and Windows* using the OS prescribed mechanisms	No	No	No	No	No
CCG01000 15795	Install SDK master custom	The installation shall allow for customization of installed content.	No	No	No	No	No
CCG01000 15794	Install SDK master prerequisites	The installation shall perform a check for any necessary software prerequisites and block installation with a meaningful error if prerequisites are not met.	No	No	No	No	No
CCG01000 15793	Install SDK master OS method	The installation must use installation and de-installation methods prescribed by the OS vendor.	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15792	Install SDK master update	The installation shall not require the de-installation of a previous version, but shall silently perform a de-installation, if necessary.	No	No	No	No	No
CCG01000 15791	Install SDK master uninstall	The SDK uninstall shall remove not only the software, but any changes that it introduces into the registry, so that it is removed entirely leaving no corruption or vestigial registry keys.	No	No	No	No	No
CCG01000 15790	Install SDK master errors	All error events shall generate an explanatory error message. Significant errors shall be logged in the event viewer (for Windows*) or system log (Linux and any other supported operating systems).	No	No	No	No	No
CCG01000 15789	Install SDK static build environment	The compiling instructions shall be provided by engineering to ISVs including a complete build environment description.	Yes	Yes	Yes	Yes	Yes
CCG01000 15788	Install SDK static steps	The compiling instructions shall be provided by engineering to ISVs to include exact steps known to work.	Yes	Yes	Yes	Yes	Yes
CCG01000 15787	Install SDK dynamic operating systems	The library will be portable to a variety of operating systems as specified in the OS support section.	Yes	Yes	Yes	Yes	Yes
CCG01000 15786	Install SDK dynamic link info	Linking instructions shall be provided by engineering to ISVs.	Yes	Yes	Yes	Yes	Yes
CCG01000 15785	Install SDK dynamic build environment	Instructions shall include a complete build environment description.	Yes	Yes	Yes	Yes	Yes
CCG01000 15784	Install SDK dynamic steps	Instructions shall include exact steps known to work.	Yes	Yes	Yes	Yes	Yes
CCG01000 15783	Install Firmware FPACL	Intel® AMT firmware image shall include a current set of entries in the FPACL.	Yes	Yes	Yes	Yes	Yes
CCG01000 15782	Install Firmware FPACL ISVs	Intel® AMT firmware image shall include updated FPACL entries for 32 ISVs.	Yes	Yes	Yes	Yes	Yes
CCG01000 15781	Install Firmware FPACL Apps	Intel® AMT firmware image shall include updated FPACL entries for ISV applications.	Yes	Yes	Yes	Yes	Yes
CCG01000 15780	Install Firmware username and password	Intel® AMT firmware image shall include the default security admin username and password.	Yes	Yes	Yes	Yes	Yes
CCG01000 15779	Install Installer	Intel® AMT shall be shipped and installed using RVS (Rapid validation suite).	No	No	No	No	No

3.3.33 Intel® Active Management Technology Reliability

No defined requirements Intel® AMT this time apart from the usual quality expectations for the release.

3.3.34 Intel® Active Management Technology Installer

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15511	No force reboot	Installation of the software shall not force a reboot of the operating system.	Yes	Yes	Yes	Yes	Yes
CCG01000 15510	Installation over newer files	The installation software shall not overwrite newer versions of the software without user interaction.	Yes	Yes	Yes	Yes	Yes
CCG01000 15509	Installation over older files	The installation software shall overwrite older versions of the software components with no data loss to the OS or any user notification.	Yes	Yes	Yes	Yes	Yes
CCG01000 15508	Intel® MEI Windows* Driver	Intel® MEI driver is a WDM driver, accessible only to Local System & Administrator accounts.	Yes	Yes	Yes	Yes	Yes
CCG01000 15507	Intel® MEI Windows Vista* Driver	Include support for Vista in the Intel® MEI driver.	Yes	Yes	Yes	Yes	Yes
CCG01000 15506	LMS	LMS will be installed as a service. Service properties: - LMS runs automatically after boot, before user authentication. - LMS runs as a Local System account	Yes	Yes	Yes	Yes	Yes
CCG01000 15505	Uninstall	All files installed during installation shall be removable through the Control panel Add/Remove software utility only.	Yes	Yes	Yes	Yes	Yes
CCG01000 15504	Unattended Install	Unattended Install	Yes	Yes	No	Yes	Yes
CCG01000 15503	Have-Disk install	The driver must support a have-disk installation for all supported operating systems.	Yes	Yes	Yes	Yes	Yes
CCG01000 15502	Documentation readiness	The Production Version shall not be released unless an updated License Agreement is available.	Yes	Yes	Yes	Yes	Yes
CCG01000 15501	Successful file copy	All supported file copy methods shall place all necessary files in the proper location.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15500	Name strings correct and verified	Name strings shall be written in accordance with Intel's naming standards. All strings shall be approved by Intel Legal and Marketing.	Yes	Yes	Yes	Yes	Yes
CCG01000 15499	Driver signing	The Production Version shall not be released unless the driver is accompanied by the signature file (.cat) and appears to the operating systems to have a WHQL* logo signature under all supported operating systems.	Yes	Yes	Yes	Yes	Yes
CCG01000 15498	Text strings	All text strings used with the product shall be approved by Intel Marketing, Customer Support, Localization, and Legal. (This includes Error messages, Text screen, and License agreement.)	Yes	Yes	Yes	Yes	Yes
CCG01000 15497	Product names	All product names associated with this software shall be added to the Intel Names Database for English and localization.	Yes	Yes	Yes	Yes	Yes
CCG01000 15496	Automatic reboot switch	Automatically reboots the system after installation. This flag is ignored if exact flag is specified on the command line or in the installer configuration file. This parameter works in either Silent mode or Interactive mode.	Yes	Yes	Yes	Yes	Yes
CCG01000 15495	Silent switch	Runs the Installer in silent mode. No user interface is displayed.	Yes	Yes	Yes	Yes	Yes
CCG01000 15494	Installation path switch	Installation Utility shall support the installation parameter to designate the path for the installed components. If this flag is not supplied, the default path shall be used.	Yes	Yes	Yes	Yes	Yes
CCG01000 15493	Language Switch	Installation Utility shall support installation parameter to designate which language code to invoke in setup.	Yes	Yes	Yes	Yes	Yes
CCG01000 15492	Log file path switch	The installer will support a flag which will allow for the log file path to be specified. The default location is <root>\Intel\Logs	Yes	Yes	Yes	Yes	Yes
CCG01000 15275	Installation content for all platforms	All platforms: Win Intel® MEI driver (inc. cat file)	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15274	Installation content for platforms with Intel® AMT	Platforms containing Intel® AMT: - Win SoL INF file (inc. cat file) - Win Local Management Service (LMS) - User notification Service (UNS)	Yes	Yes	Yes	Yes	Yes
CCG01000 15273	Installation content for platforms for Intel® AMT	Platforms containing Intel® AMT: - Intel® AMT Status Icon - Intel® AMT Status Icon	Yes	Yes	Yes	Yes	Yes
CCG01000 15272	Component Installer	Unified Installer: - Includes MEI driver and SOL/LMS/UNS/ IMSS/NAC plugin	Yes	Yes	Yes	Yes	Yes
CCG01000 15797	Install Intel® AMT software when devices are not enabled	Installation utility shall have a flag to the installation file to allow installation of LMS, UNS and IMSS (Services Icon) software when MEI and SOL devices have not been installed.	Yes	Yes	Yes	Yes	Yes

3.3.35 Intel® Active Management Technology Security

This section defines the security protocols and mechanisms used by the Intel® Management Engine Firmware to secure access via network, local host to critical resources such as the Intel® Management Engine Firmware code or 3DPS.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15774	Security External Interfaces	The ME shall be accessible through 3 external interfaces: - LAN Access - Local host Access via Intel® MEI HW - WLAN Interface	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15773	Security Networking Protocols	Networking Security shall be based on the following protocols: - TLS (RFC 2246) - HTTPS (RFC 2818) - for SOAP and HTML interfaces - HTTP Digest Authentication (RFC 2617) for SOL/IDER , SOAP and HTML interfaces (Hash algorithm is MD5) - PSK Ciphersuites for TLS (RFC4279) - User Authentication mechanism integrated into SoL/IDER protocols - Single sign-on with Windows* Domain Authentication to IDE-R/SoL and Intel® AMT device.	Yes	Yes	Yes	Yes	Yes
CCG01000 15772	Security Networking Protocols TLS	When TLS is enabled the following modes will be supported: - TLS Mutual Authentication - TLS Server Side authentication	Yes	Yes	Yes	Yes	Yes
CCG01000 15771	Security Networking Protocols TLS Default Configuration	When activated in Setup & Configuration the Default configuration shall be: Mutual Authentication enabled	Yes	Yes	Yes	Yes	Yes
CCG01000 15770	Security Networking Protocols TLS algorithms	The Following cipher-suites shall be supported: - TLS_RSA_WITH_AES_128_CBC_SHA - TLS_RSA_WITH_RC4_128_CBC_SHA - TLS_RSA_WITH_NULL_SHA - TLS_PSK_WITH_AES_128_CBC_SHA	Yes	Yes	Yes	Yes	Yes
CCG01000 15769	Security Networking Protocols TLS algorithms Key Size Server	For FW TLS Server Certificate: the RSA key sizes supported shall be : - 2048 bit - 1536 bit - 1024 bit	Yes	Yes	Yes	Yes	Yes
CCG01000 15768	Security Networking Protocols TLS algorithms KeySize Client	For SW entities TLS Client Certificates the RSA key sizes supported shall be : - 2048 bit - 1536 bit - 1024 bit	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15767	Security Networking Protocols TLS algorithms Crypto Fuse	When the HW Crypto Fuse is disabled, the following cipher-suite shall be supported: - TLS_RSA_WITH_NULL_SHA - TLS_PSK_WITH_NULL_SHA (during PSK provisioning) When the HW Crypto Fuse is enabled, the following cipher-suite shall be supported: - TLS_RSA_WITH_AES_128_CBC_SHA - TLS_RSA_WITH_RC4_128_CBC_SHA - TLS_RSA_WITH_AES_256_CBC_SHA - TLS_PSK_WITH_AES_128_CBC_SHA (during PSK provisioning) - TLS_PSK_WITH_RC4_128_CBC_SHA (during PSK provisioning) - TLS_PSK_WITH_AES_256_CBC_SHA (during PSK provisioning)	Yes	Yes	Yes	Yes	Yes
CCG01000 15766	Security Networking Protocols TLS Client Certificate Verification	The FW shall validate Client Certificates based on standard criteria as described in [RFC 3280] Sec. 6 Certification Path Validation, with the following modification and requirement that are further described in the sections below: - Modified certificate period validity criteria. - Additional requirement for ''Key usage'' indicating certificate was issued for the purpose of Intel® AMT. - Additional requirement on the Common Name field limiting the scope based on DNS framework.	Yes	Yes	Yes	Yes	Yes
CCG01000 15765	Security Networking Protocols TLS Client Certificate Verification Time Validity Verification	- When ME has limited notion of time, it will positively validate certificates which ''Validity End Period'' value is later then a known past date to ME. - When ME has accurate notion of time, it will validate the time period as defined in [RFC 3280]	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15764	Security Networking Protocols TLS Client Certificate Verification Enhanced Key Usage Verification	- Client Certificate sent over the Network connection the ''Enhanced Key Usage'' OID list field of the leaf certificate must contain the OID : 2.16.840.1.113741.1.2.1 - Client Certificate sent over the local host connection the ''Enhanced Key Usage'' OID list field of the leaf certificate must contain the OID 2.16.840.1.113741.1.2.2	Yes	Yes	Yes	Yes	Yes
CCG01000 15763	Security Networking Protocols TLS Client Certificate Verification FQDN Suffix	The FW Shall Validate whether or not the Common Name field of incoming certificates contains an FQDN which suffix appears in a pre-configured suffix list	Yes	Yes	Yes	Yes	Yes
CCG01000 15762	Security Networking Protocols TLS Client Certificate Verification FQDN Suffix List	The FW shall maintain an allowed FQDN Suffix list which will include 4 entries.	Yes	Yes	Yes	Yes	Yes
CCG01000 15761	Security Networking Protocols TLS Client Certificate Verification FQDN Suffix Comparison Schemes	The comparison rule will validate an incoming certificate FQDN if one of the configured suffixes is a suffix of the input up to a ''.'' notation i.e. Given the suffix: Intel.com The following FQDN are validated successfully: - Host.intel.com - Host.ger.intel.com - The following FQDN fail comparison: - Host.foo.com - Hostintel.com	Yes	Yes	Yes	Yes	Yes
CCG01000 15760	Security Networking Protocols TLS Client Certificate Verification FQDN Suffix List Default	The Default Suffix List configuration shall include a single entry depicting a suffix comprised of the Domain name part of the FW configured FQDN located in the TLS Server certificate FQDN	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15759	Security TLS Client Certificate CRL	The FW shall maintain a local database containing information on revoked certificates as set by an administrator and derived from multiple CA Certificate Revocation List (CRL). The database shall support up to 64 entries, each entry will be associated with a certificate corresponding to the certificate's Issuer CA and the Certificate's ''Serial ID''. The following indicate the limits of the CRL store: - Max of 4 URLs - Max total (NOT per URL) number of entries (i.e. serial numbers) = 64 - Total store (include the overhead for internal purposes) won't exceed 1424 bytes - Max serial number length = 20 bytes	Yes	Yes	Yes	Yes	Yes
CCG01000 15758	Security TLS Client Certificate CRL Entry Information	Each Entry in the FW CRL database shall contain the Revoked Certificate ''Serial ID'' and a reference to the CA's ''CRL Distribution Points'' string used to uniquely identify the issuer CA.	Yes	Yes	Yes	Yes	Yes
CCG01000 15757	Security Networking Protocols TLS Client Certificate Root Of Trust	The FW shall support up to 4 configurable Root of Trust certificates Each one (root certificate) is 1500 bytes at most.	Yes	Yes	Yes	Yes	Yes
CCG01000 15851	Security Networking Protocols TLS Client Certificate	The FW shall support up to 7 configurable client certificates. Each one (client certificate) is 4100 bytes at most.	Yes	Yes	Yes	Yes	Yes
CCG01000 15756	Security Networking Protocols HTTP	The client must authenticate to the FW by specifying username and password through http authentication.	Yes	Yes	Yes	Yes	Yes
CCG01000 15755	Security Networking Protocols HTTP Digest	The algorithm used for HTTP authentication is HTTP digest as defined in RFC 2617	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15754	Security Networking Protocols HTTP Digest Password Localization	The Intel® Management Engine Firmware shall maintain on NVRAM the machine specific localized password information in accordance with the http Digest RFC: MD5(<user>":"Realm":" <passwd>) The Realm field includes a relatively unique number (no need for cryptographic randomly) which is unique for the platform (not the machine UUID)	Yes	Yes	Yes	Yes	Yes
CCG01000 15753	Security Networking Access Control Password Strength	The FW shall enforce the following password policy: - Password Length: Passwords must comprise of at least 8 characters. - the following attributes must be met: At least one Digit character ('0', '1',...'9') At least one: 7-bitASCII non alpha-numeric character (e.g. '!', '$', ';') Either contains both lower-case Latin ('a', 'b',...,'z') and upper case Latin ('A', 'B',...'Z') or password contain non ASCII characters (UTF+0080 and above).	Yes	Yes	Yes	Yes	Yes
CCG01000 15752	Security Networking Access Control Realms	When a user is accessing the FW interfaces the FW shall check if the user has the appropriate realm access rights. The following set of realms for networking access are defined, each External Interface (Local host and LAN) maintains a different set or realms: - AMTAdmin - HWAsset - RemoteControl - Storage - EventManager - StorageAdmin - System Defense - AgentPresence - SoL/IDER - Network time - General info - FW update - common user - Audit Log	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15751	Security Networking Access Control Intrusion Protection	The FW shall provide a mechanism to mitigate online password attacks, the mechanism shall effectively slow down attacks to 1 try per minute.	Yes	Yes	Yes	Yes	Yes
CCG01000 15750	Security Networking Access Control Intrusion Notification	The FW shall log and alert administrators of invalid login attempts.	Yes	Yes	Yes	Yes	Yes
CCG01000 15749	Security External Interfaces TLS Configuration	AMT will provide a single administrator capability to enable or disable TLS for both the LAN and host access networking interfaces.	Yes	Yes	Yes	Yes	Yes
CCG01000 15748	Security External Interfaces TLS Configuration Default Value	The Default TLS configuration factory settings shall be TLS disabled.	Yes	Yes	Yes	Yes	Yes
CCG01000 15747	Security External Interfaces LAN Access Supported Features	The following Features shall be supported: - AMT Administration - Remote Control - SoL/IDER - ISV Storage - ISV Storage Admin - EventManager - FW Update - System Defense - AgentPresence -Remote Console only - Hardware Asset - GeneralInfo	Yes	Yes	Yes	Yes	Yes
CCG01000 15746	Security External Interfaces Host Access OS State Separation	The FW shall maintain the following OS States: - Pre-OS - for Bios code access - OS - for OS application access The FW shall Provide different access levels for each state as defined in items below.	Yes	Yes	Yes	Yes	Yes
CCG01000 15745	Security External Interfaces Host Access Bios Access	For Pre- Os State Bios level access shall be protected through the Bios extension. The FW shall provide an authentication function over the Intel® Management Engine Interface, allowing the ME Bios extension to authenticate users.	Yes	Yes	Yes	Yes	Yes
CCG01000 15744	Security External Interfaces Host Access Bios Access Authentication Credentials	The FW shall provide an ACL dedicated for local Bios access.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15743	Security External Interfaces Host Access Bios Access Authentication	The FW shall accept interactive Bios level commands only after successful authentication.	Yes	Yes	Yes	Yes	Yes
CCG01000 15742	Security External Interfaces Host Access Bios Access login Limit	The FW will limit login access to protect against local access dictionary attacks. A platform reboot should reset the protection state.	Yes	Yes	Yes	Yes	Yes
CCG01000 15741	Security External Interfaces Host Access BIOS Access Supported Features	In Pre-Os State, the following capabilities shall be provided: - Network configuration - Network Admin ACL setup - Bios Admin setup	Yes	Yes	Yes	Yes	Yes
CCG01000 15740	Security External Interfaces Host Access Bios Access Intel® AMT Redirection Control	The FW shall provide a control to disable the following features through the Bios access interface: - SoL/IDER	Yes	Yes	Yes	Yes	Yes
CCG01000 15739	Security Application Admin Feature Control Network Interface	The FW Shall Provide an admin level control to disable / enable the following features through the network interface: - Web-UI - SoL/IDER	Yes	Yes	Yes	Yes	Yes
CCG01000 15738	Security Application Admin Feature Control Network Interface Defaults (legacy)	- Web-UI enabled when configured in SMB mode and disabled in Enterprise mode. - SoL/IDER enabled when configured in SMB mode and disable in Enterprise mode.	No	No	No	No	No
CCG01000 15850	Security Application Admin Feature Control Network Interface Defaults when Setup and Configuration is completed	- Web-UI is enabled - If SoL/IDER/KVM are not disabled through MEBx, their network interface default is Enabled - Note: In order to maintain security, although the default is enabled, the Listener ports of the redirection will have to be explicitly opened for redirection sessions to take place.	Yes	Yes	Yes	Yes	Yes
CCG01000 15737	Security Application Admin Feature Control SOL/IDER control	For SoL/IDER to be enabled both the network control switch and the Bios control switch should be enabled	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15736	Security Application ACL Configuration Command	The SOAP command shall provide remote entity the capability to send password information in localized manner: Send Localized Password H(A1) value, per Sec 3.2.2.2 of RFC 2617	Yes	Yes	Yes	Yes	Yes
CCG01000 15735	Security Flash Code Image Authentication	Flash Code image shall be digitally sighed by Intel and authenticated by the ROM FW. If authentication fails the ROM shall refuse to run the flash code	Yes	Yes	Yes	Yes	Yes
CCG01000 15734	Security Flash 3DPS Privacy	The 3DPS storage shall not implement any confidentiality mechanisms. The impact is that : - All content in 3DPS is not encrypted and can be locally accessed by any application running on the local host - ISV application have to perform their own confidentiality algorithms (such as encryption) if they see the need. - A local host application can erase any content from the 3PDS.	Yes	Yes	Yes	Yes	Yes
CCG01000 15733	Security Configuration	Configuration can be executed in an open network environment using the TLS protocol with Pre-Shared Key (PSK) cipher suite (TLS PSK WITH AES 128 SDC SHA), outlined in TLS-PSK Internet Draft (draft-ietf-tls-psk-07.txt). Configuration in open network can also be with TLS-PKI in the case of ZTC (also known as RCFG). Using Zero Touch Configuration requires using TLS/PKI for Setup and configuration. For more information please refer to Remote Setup and configuration section in this document. Intel recommends using TLS/PSK or TLS/PKI with pre-configured domain name through the MEBx (or USB key) at Setup and configuration	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15732	Security Lost Password	The FW shall not allow changing its configuration state without the correct user name password. Limitation \ Note : If the IT administrator looses or forgets password, ME must be un-configured through the local MEBx screens and all data is lost	Yes	Yes	Yes	Yes	Yes
CCG01000 15731	Security System Defense Security	The FW shall enable the System Defense feature only if mutual authentication security is applied to the network security protocol.	No	No	No	No	No
CCG01000 15730	Security External Cert	The Software, Firmware and Hardware running together must be certified by an external security expert company. Note: External companies have the ability to examine and certify the SW, FW and HW to determine if vulnerabilities exist. A certification of this type lowers the risk of security vulnerability.	Yes	Yes	Yes	Yes	Yes
CCG01000 15729	Security Allowed Char Set	The FW shall support 7 bit ASCII characters in the range of 32 to 126 decimal for user name and password. Limitation: FW shall not support ':', ' " ' and ',' characters for all usernames and passwords. For passwords, the following characters will also not be allowed: '<', '>', '&', space.	Yes	Yes	Yes	Yes	Yes
CCG01000 15610	HTTP Support	- The Intel® AMT applications and samples shall support HTTP digest. - The Intel® AMT applications and samples shall fail to perform HTTP basic authentication.	Yes	Yes	Yes	Yes	Yes
CCG01000 15609	IDER Session Log	The FW shall hold a cyclic log of 16 IDER session entries. Each entry will hold the following data: - Timestamp in seconds from (1/1/1970) - Remote console IP address - Remote console TCP port	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15608	IDER Session log interface	The log interface shall return: - Up to 16 entries of IDER sessions - Index which points to the last valid entry in the log + 1 - Wrap-around flag, indicating there were more than 16 IDER sessions. The log contains only the latest 16 sessions.	Yes	Yes	Yes	Yes	Yes
CCG01000 15607	ISVS registration Protocol and AES	The FW shall communicate to the library according to the AES_IV vector: - If keys are encrypted, it will contain the actual value based on SNPR protocol. - If keys are not encrypted, AES_IV will be set to 0. Note: The FW shall use the encryption, unless the crypto fuse is disabled.	Yes	Yes	Yes	Yes	Yes
CCG01000 15520	Certificate storing	The FW will store at most 4 certificates for the 802.1x profiles (3 for wireless, 1 for wired profile) each certificate size is 4100 bytes at most.	Yes	Yes	Yes	Yes	Yes
CCG01000 15519	Security TLS Client Certificate Verification	The FW shall implement the following Standard Verification criteria: - Client certificate is a leaf of a configured root of trust. - All certificates in the chain are currently valid based on time. - Each certificate in the chain correctly signs its immediate leaf. - Certificate does not appear in the configured CRL - Intel® AMT specific criteria: - DN Qualifier field includes the string ''Intel® AMT Host'' - For FW TLS client Certificate: the RSA key sizes supported shall be : 2048 bit	No	No	No	No	No
CCG01000 15491	Security Networking Kerberos* Protocols	The client must authenticate to the FW by supplying a Kerberos ticket obtained from the Windows* KDC. The initial authentication to the Microsoft Windows* domain should have happened by specifying the Windows* username and password by the client.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15490	IT administrator Automatic authenticate	An IT administrator logged into the Microsoft Windows* domain using his username (i.e. domain\username e.g. amr\john) and password, shall be able to automatically authenticate to Intel® AMT devices.	Yes	Yes	Yes	Yes	Yes
CCG01000 15489	IT administrator group membership	An IT administrator shall be allowed or denied privileges to manage an Intel® AMT device, based on his membership to a Group in Active Directory.	Yes	Yes	Yes	Yes	Yes
CCG01000 15488	IT administrator & ACL	Intel® AMT devices should be able to ascertain the identity of the administrator attempting to gain access to the Intel® AMT system, and be able to apply access control for that user governed by the Access Control List (ACL) located within an Intel® AMT device.	Yes	Yes	Yes	Yes	Yes
CCG01000 15487	Authentication protocol	Authentication shall only be via the Kerberos protocol, as implemented in Windows* 2000 and later operating systems. Hence the Kerberos KDC will be the one as implemented by Windows* 2000 and later versions of the OS (e.g. Windows* 2003, Windows Vista*, etc). Credential Caching SHALL be supported	Yes	Yes	Yes	Yes	Yes
CCG01000 15486	Symmetric encryption protocol	The desired symmetric encryption protocol for Kerberos* is RC4-HMAC (where HMAC is MD5 based).	Yes	Yes	Yes	Yes	Yes
CCG01000 15485	Kerberos* Protocols supported	The following protocols shall be supported: a. Kerberos* v5 - RFC4120 b. Kerberos* v5 over GSS-API Mechanism - RFC4121 c. GSS-API SPNEGO Mechanism - RFC4178 d. SPNEGO over HTTP e. Support "Authorization: Kerberos" and "Authorization: Negotiate" - RFC 4559	Yes	Yes	Yes	Yes	Yes
CCG01000 15399	HTTP Client Support	The Intel® AMT HTTP client will support: - Digest Authentication or SPNEGO Kerberos for all other client initiated connections.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15398	Security External Interfaces LAN Access Supported Features	The following Features shall be supported: - AMT Administration - Remote Control - SoL/IDER - ISV Storage - ISV Storage Admin - EventManager - FW Update - System Defense - AgentPresence -Remote Console only - WAsset - Network time - General Info - CommonUser - AuditLog	Yes	Yes	Yes	Yes	Yes
CCG01000 15370	Hardware TRNG seeds	Intel® AMT will use the hardware TRNG unit to generate seeds for the pseudo random number generator.	Yes	Yes	Yes	Yes	Yes
CCG01000 15369	Memory alias check	A memory alias check will be performed before Intel® AMT gets loaded.	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15368	Blob data protection	Intel® AMT data that is considered secret will be protected before storing in flash, according to the following list: - Integrity + Anti Replay protection - Admin authentication: username, (digested) password - Network: client auth enabled - User authentication: username, (digested) password - User authorization: user/kerb, permissions, realms list - Kerberos data: SPN string, type, realname, encryption type, clock tolerance, with exception of master key - Certificates data: with exception of private RSA keys. - RCFG: root certificates hashes; Provisioning Server (PS) FQDN; PKI DNS suffix; Remote Configuration enabled flag - Encryption + Integrity + Anti Replay protection - Provisioning: PID, PPS - PRNG: Power up counter, seed. - Kerberos data: master key - Certificates data: private RSA keys.	Yes	Yes	Yes	Yes	Yes
CCG01000 15356	Intel® Management Engine Temporary Disable mode through setting the ''Flash Descriptor Security Override'' jumper	When the ''Flash Descriptor Override Pin-Strap'' (ICH hardware feature) is set, the ME firmware shall be put into a temporarily disabled state. In this state, the OEM can safely reprogram the ME flash region from the host system.	Yes	Yes	Yes	Yes	Yes
CCG01000 15271	Security Flash Code Image Access	Flash code image can be overridden or updated locally via non secure host interface when the FW is in recovery mode	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15476	Support of PKCS#10 certification request	The Intel® AMT Firmware should provide a "PKCS#10 certification request" queried by the network interface, to allow issuing a certificate for its key pair. This is useful in this scenario usage: - Reissuing certificate in case of certificate expiration/revocation - Reissuing certificate in case of CA change/update Support for PKCS#10 certification request should be available as soon as the Intel® AMT is set with RSA key pair.	Yes	Yes	Yes	Yes	Yes

3.3.35.1 Certificate Revocation Support

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14685	Certificate RevocationSupport	Intel® AMT must provide the functionality to verify certificates revocation status presented for the following services: - IRA: MPS SSL Server cert - Enterprise TLS mode : SSL Client Cert - Client Initiated: SSL Server cert	No	No	No	No	No
CCG01000 14684	Certificate revocation operation	For each service, the IT must be able to configure revocation behavior: - Revocation check not required - Perform revocation only if certificate includes revocation status check support. - Revocation check mandatory	No	No	No	No	No
CCG01000 14683	OCSP Support	AMT must support OCSP, [RFC 2560] AMT must support HTTP as the transport layer for OCSP. AMT must adhere to the OCSP format specified in :draft-ietf-pkix-lightweight-ocsp-profile-11.txt	No	No	No	No	No

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14682	CRL	AMT must support Certificate Revocation List method [RFC 3280]	No	No	No	No	No

3.3.36 Intel® Active Management Technology Naming Requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14681	MEI nomenclature	The following should use MEI nomenclature (replaces HECI that was used in previous generations): - Marketing documents - Customer collateral - User-visible strings (SDK API, MEBx, error messages)	Yes	Yes	Yes	Yes	Yes

3.3.37 Web GUI Requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15270	Web GUI	Intel® AMT systems have a Web GUI interface which is available by making an HTTP request from a standard web browser to the port which AMT is configured for.	Yes	Yes	Yes	Yes	Yes
CCG01000 15269	Browser Support	The Web GUI shall function properly when viewed with the following Web Browsers (however not to the exclusion of unlisted browsers) - Internet Explorer 6 - Internet Explorer 7	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15268	Wireless Profile Configuration	Wireless profiles may be configured through the Web GUI	No	Yes	No	No	Yes
CCG01000 15266	Remote Control	Remote Control operations can be articulated through the Web GUI	Yes	Yes	Yes	Yes	Yes
CCG01000 15267	HW Asset Information	HW Asset information may be viewed through the Web GUI	Yes	Yes	Yes	Yes	Yes
CCG01000 18906	CPT Browser Support	The Web GUI shall function properly when viewed with the following Web Browsers (however not to the exclusion of unlisted browsers): - Internet Explorer 6 - Internet Explorer 7 - Internet Explorer 8 - Firefox	No	No	No	Yes	Yes

3.3.38 Asset Management

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15265	Asset Management Support	Intel® AMT will support Asset Management where during boot AMT will acquire hardware information from the BIOS and make this available to ISV applications through AMT interfaces	No	Yes	No	Yes	Yes

§

4 Other Requirements

4.1 Certification Requirements

OEM system certification requirement to get Microsoft logo.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15778	WHQL standards	The driver shall - Pass Microsoft's Device Test Kit HCTs for all supported Windows operating systems and supported Codec's. - Receive a Microsoft Windows* WHQL Certification for following operating systems as given in the ''Operating system support'' section. Note: Any exceptions shall be noted in the release notes.	Yes	Yes	Yes	Yes	Yes
CCG01000 15777	WHQL standards	The driver shall pass Microsoft's System Test Kit on a CRB (Intel® 965 Express Chipset Family).	Yes	Yes	Yes	Yes	Yes
CCG01000 15776	WHQL tests	No failures of the Microsoft Windows* Certified program for System and Device Tests shall be ignored. A Waiver or Contingency must be obtained from Microsoft for any failures of the Microsoft Windows* Certified program for System and Device Tests prior to Production Version release.	Yes	Yes	Yes	Yes	Yes
CCG01000 15775	Driver signing	The Production Version shall not be released unless - The driver is accompanied by the signature file (.cat) and - Appears to the operating systems to have a WHQL logo signature under all supported operating systems.	Yes	Yes	Yes	Yes	Yes
CCG01000 15524	WHQL Certification	Intel® MEI, SoL drivers must be certified by Microsoft with production hardware.	Yes	Yes	Yes	Yes	Yes

4.2 Compatibility and Interoperability

4.2.1 Compatibility between different generations of SW/FW components

This section defines the compatibility between the different generations of Intel® AMT implementations.
In general, generations following the Intel® AMT 1.0 prior to Intel® AMT 4.0 version had an Intel® AMT 1.0 compatibility mode. This mode won't be supported for Intel® AMT 4.0 and future versions. In general, Intel® AMT generations are compatible (meaning that Intel® AMT 2.0 consoles will be able to configure Intel® AMT 2.0-features on Intel® AMT 2.6 / 3.0 machines).

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15728	Compatibility Intel ® AMT 1.0 / Intel ® AMT 2.0/2.1 FW Mode	The Intel® AMT 2.5 / 3.0/ 4.0 FW shall implement ''Intel® AMT 1.0 FW mode''. In this mode the FW shall : - Implement Network security as in Intel® AMT 1.0 FW - Support host interface backwards compatible to Intel® AMT 1.0 / 2.0 via Intel® MEI. - Support only Intel® AMT 1.0 feature set. No support for System Defense, Agent Presence or any other new Intel® AMT 2.6 - 4.0 features.	No	No	No	No	No
CCG01000 15727	Compatibility Local Host ISV SW	Compatibility of local host ISV application shall comply with the following: - Intel® AMT 1.0 platform will only support Intel® AMT 1.0 ISV APP - Intel® AMT 2.0-4.0 platform will only support Intel® AMT 2.0-4.0 ISV APP - Intel® AMT 2.0-4.0 platform (''Intel® AMT 1.0 mode'') will support both Intel® AMT 1.0 ISV APP and Intel® AMT 2.0-3.0 ISV APP Note: Intel® AMT 2.6 - 4.0 ISV APP is an application that uses the new Intel® AMT 2.6 - 4.0 interface through the LMS.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15726	Compatibility Intel® Management Engine Firmware Enterprise Console Security	Intel® AMT 1.0 and Intel® AMT 2.0-4.0 network security mechanisms shall be compatible. Exception: When Mutual authentication is enabled on an Intel® AMT 2.6 - 6.0 machine an Intel® AMT 1.0 console cannot communicate with that machine.	Yes	Yes	Yes	Yes	Yes
CCG01000 15725	Compatibility Intel® Management Engine Firmware Enterprise Console	Compatibility of remote enterprise management console and FW shall comply with the following. - Intel® AMT 1.0 platform will only support Intel® AMT 1.0 ISV APP - Intel® AMT 2.0-6.0 platform will only support Intel® AMT 2.0-6.0 ISV APP - Intel® AMT 2.0-6.0 platform (''Intel® AMT 1.0 mode'') will support both Intel® AMT 1.0 ISV APP and Intel® AMT 2.0-6.0 ISV APP Limitations : - Intel® AMT 1.0 console can communicate with an Intel® AMT 2.6 / 6.0 FW only if it is configured to work in ''Intel® AMT 1.0 security mode'' - The above restriction applies only if network security is turned on. (Note: pre AMT 6.0 this was applicable only to Enterprise Mode) Intel® AMT 2.6 / 6.0 consoles must add specific code in order to distinguish between Intel® AMT 1.0 and Intel® AMT 2.6 / 6.0 systems.	Yes	Yes	Yes	Yes	Yes
CCG01000 15724	Compatibility Intel® Management Engine Firmware Configuration Server	Compatibility of configuration server and FW shall comply with the following: - Intel® AMT 1.0 configuration server can configure Intel® AMT 2.6 - 6.0 FW to work only in Intel® AMT 1.0 mode when mutual authentication is not enabled. - Intel® AMT 2.6 - 6.0 configuration servers must add specific code in order to distinguish between Intel® AMT 1.0 and Intel® AMT 2.6 / 6.0 system.	No	No	No	No	No
CCG01000 15723	Compatibility SDK Lib API	The Intel® AMT 2.6 - 6.0 SDK lib shall be backwards compatible with Intel® AMT 1.0 / 2.0 APIs.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15722	Compatibility ISV Storage	ISV storage interface in the local host shall be backwards compatible to Intel® AMT 1.0 / 2.0.	Yes	Yes	Yes	Yes	Yes
CCG01000 15721	Compatibility Host IFC Driver	The Intel® AMT 2.6 - 6.0 Host interface driver (Intel® MEI driver) shall support only Intel® AMT 2.6 - 6.0 platforms.	Yes	Yes	Yes	Yes	Yes
CCG01000 15720	Compatibility Intel® Management Engine Firmware Update	Compatibility of FW Update utility shall comply with the following: - Intel® AMT 1.0 FW update utility shall only be supported with Intel® AMT 1.0 FW - Intel® AMT 2.0-6.0 FW update utility shall only be supported with Intel® AMT 2.0-6.0 FW	Yes	Yes	Yes	Yes	Yes
CCG01000 15475	AMT based Memory Error Reporting	If an error occurs and bring-up is unable to get ME UMA initialized, it shall log the error to the flash.	Yes	Yes	Yes	Yes	Yes
CCG01000 15456	Enable Intel® AMT features in all authentication modes	System Defense and Agent Presence shall work in all authentication modes.	Yes	Yes	Yes	Yes	Yes
CCG01000 15455	ASF based Memory Error Reporting	If an error occurs and Bring-up is unable to get ME UMA initialized, it should send an ASF PET on the network.	Yes	Yes	Yes	Yes	Yes
CCG01000 15454	ASF based Memory Error Reporting	If an error occurs and Bring-up is unable to get ME UMA initialized, it should send an ASF PET on the network.	Yes	Yes	Yes	Yes	Yes
CCG01000 15264	AMT Mode Identification	A management console must be able to determine which version of AMT is running, what mode it is in for backward compatibility , what connection interface it is using (EOI, WS-MAN DMWG 1.0)	Yes	Yes	Yes	Yes	Yes

- XML will be used as the automation interface to the Intel® AMT data and methods.
- Must be OS independent; built on IA Platform resources (processor, chipset, BIOS, LAN controllers)
- HTTP and XML transaction must support SSL client and server side authentication.
- Must have option to interface with an enterprise PKI.
- Remote Boot capability must provide server-side authentication
- Must have option to integrate with Active Directory, Novell, and Linux authentication directories (RADIUS).

4.2.2 DMWG 1.0 Support

This section defines requirements for support of the DMWG 1.0 specification.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15187	DMWG 1.0 Profile support	The ME Firmware shall support the mandatory elements specified by the final release version 1.0 of the following profiles: - Base Desktop and Mobile Profile (DSP 1058). Defines the objects, associations, properties, and operations that are used to describe and manipulate a managed desktop or mobile computer system. - Boot Control Profile (DSP 1012). Defines the objects, associations, properties, and operations that are used to describe and manipulate the boot options of a managed desktop or mobile computer system. - CPU Profile (DSP 1022). Defines the objects, associations, properties, and operations that are used to describe and manipulate the processor(s) of a managed desktop or mobile computer system. - Fan Profile (DSP 1013). Defines the objects, associations, properties, and operations that are used to describe and manipulate fans in a managed desktop or mobile computer system. - Physical Asset Profile (DSP 1011). Defines the objects, associations, properties, and operations that are used to describe and manipulate the physical assets in a managed desktop or mobile computer system. This profile focuses on the information required to replace or assess the value of the elements of the managed system, as opposed to their operational characteristics. - Power State Management Profile (DSP 1027). Defines the objects, associations, properties, and operations that are used to describe and manipulate the power state of a managed desktop or mobile computer system.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		- Power Supply Profile (DSP 1015). Defines the objects, associations, properties, and operations that are used to describe and manipulate the power supply of a managed desktop or mobile computer system. - Sensors Profile (DSP 1009). Defines the objects, associations, properties, and operations that are used to describe and manipulate sensors in a managed desktop or mobile computer system. - Software Inventory Profile (DSP 1023). Defines the objects, associations, properties, and operations that are used to describe and manipulate software or firmware in a managed desktop or mobile computer system. - System Memory Profile (DSP 1026). Defines the objects, associations, properties, and operations that are used to describe and the memory of a managed desktop or mobile computer system. - Simple Identity Management Profile (DSP 1034). The information in this specification should be sufficient for a provider or consumer of this data to identify unambiguously the classes, properties, methods, and values that shall be instantiated and manipulated to represent and manage a chassis manager that is modeled using the DMTF Common Information Model (CIM) core and extended model definitions. - Profile Registration Profile (DSP 1033). defines the classes used to describe the DMTF profile registration and the version information of the profiles advertised as implemented for a managed system and components of the system. - Role Based Authorization Profile (DSP 1039). Defines the classes used to describe role-based authorization in a managed system. Also included are descriptions of the relationship between the authorization and authentication for a managed system, and the DMTF profile version information.					

4.3 User Interface (UI) Requirements

4.3.1 User Interface Requirements

This section describes the requirements for the various Intel® AMT components (FW, SW) that have user interfaces.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15719	Setup and Configuration arguments	The Setup and configuration application shall recognize both forward slashes and dashes as argument switches.	Yes	Yes	Yes	Yes	Yes
CCG01000 15718	Setup and Configuration Command Line	The Setup and configuration application shall operate in a command line environment with NO GUI.	Yes	Yes	Yes	Yes	Yes
CCG01000 15717	Web Interface (WebUI)	The Intel® AMT HTTP Interface shall contain all of the features required in the 06 Intel® AMT PRD.	Yes	Yes	Yes	Yes	Yes
CCG01000 15716	Connect HTTP Server	The FW shall provide an HTTP web browser UI that implements the following control pages : - System information - Event log - Network configuration - Remote control operations - including boot options. - Users administration - FW update (versions prior to Intel® AMT 4.0 only) Limitation \ Note: The Web pages will not to be localized only English shall be supported.	Yes	Yes	Yes	Yes	Yes
CCG01000 15523	SDK Documentation Language	The SDK shall be written in English and shall NOT be translated.	Yes	Yes	Yes	Yes	Yes
CCG01000 15522	SDK Documentation Format Style Guide	The SDK shall use the accepted Intel technical documentation template for all documents.	Yes	Yes	Yes	Yes	Yes
CCG01000 15521	SDK Documentation Style Guide	The SDK authors shall agree on a technical publications style guide and conform to said guide.	Yes	Yes	Yes	Yes	Yes
CCG01000 15382	Setup and Configuration arguments	The Configuration application shall recognize both forward slashes and dashes as argument switches.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15381	Setup and Configuration Command Line	The Configuration application shall operate in a command line environment with NO GUI.	Yes	Yes	Yes	Yes	Yes

4.3.2 UI Standards

The UI is for IT developers and ISV developers of management applications. The standards of the UI will match that of production quality Intel® PROSet drivers.

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15715	UI Standards HTML	The SDK shall use PDF format for documentation.	No	Yes	No	No	Yes
CCG01000 15714	UI Standards CI	The UIs shall conform to CI 162, a US government directive for handicapped/color blind people.	Yes	Yes	Yes	Yes	Yes

4.3.3 UI Compatibilities and Other UI Requirements

The UI of Intel® AMT 2.6 / 3.0 does not need to be compatible with Windows* XP Explorer UI. The UI needs to be easily integrated into the Windows*based code of the management application consoles. This requirement is to provide ease of integration for the server side (console) code of Intel® AMT 2.6 / 3.0.
A browser UI needs to be easily used by IT developers who develop custom management applications. The UI should work with Windows* XP Explorer coding, format and styles.

4.4 Internationalization and Localization Requirements

4.4.1 Internationalized components

Specify product components that require internationalization so that they will run in a foreign language based OS, or localization to have the software operate in the user's preferred language

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15627	Internationalization of Intel® Management Engine Firmware	Intel® AMT FW shall not be localized	No	No	No	No	No
CCG01000 15626	Internationalization SW not supported	The following Intel® AMT SW shall be not be localized: Platform system software and ISV software both for IT user group. This includes LMS and UNS.	No	No	No	No	No
CCG01000 15625	Export requirements	Intel® AMT shall comply with export requirements for encryption. Note: France has an encryption requirement.	Yes	Yes	Yes	Yes	Yes
CCG01000 15624	Software Help	The Intel® AMT Software shall display help.	Yes	Yes	Yes	Yes	Yes
CCG01000 15623	Installation program	The Intel® AMT Software installation program shall be localized.	Yes	Yes	Yes	Yes	Yes
CCG01000 15622	Internationalization Support	The Intel® AMT Software installation programs shall be localized in the following languages: o ENG - English o CHS - Chinese Simplified o CHT - Chinese Traditional o DEU - German o ESP - Spanish o FRA - French o JPN - Japanese o KOR - Korean o PTB - Brazilian Portuguese o ARA - Arabic o CSY - Czech o DAN - Danish o ELL - Greek o FIN - Finnish o HEB - Hebrew o HUN - Hungarian o ITA - Italian o NLD - Dutch o NOR - Norwegian o PLK - Polish o PTG - Portuguese - Portugal	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		o RSU - Russian o SKY - Slovak o SLV - Slovenian o SVE - Swedish o THA - Thai o TRK - Turkish					
CCG01000 15621	Localized operating systems support	The Intel® AMT Software shall operate correctly on supported localized operation systems.	Yes	Yes	Yes	Yes	Yes
CCG01000 15620	Product names	All product and feature names must be added to the Intel Legal Names database before they shall be implemented into the localized resource files.	Yes	Yes	Yes	Yes	Yes
CCG01000 15332	Localization Ready	MEBx must be ready for localization Note: Localization for specific regions is not part of this requirement, this requirement covers code readiness	No	No	No	No	No
CCG01000 15263	Internationalization readiness of the MEBx	MEBx shall be localization ready and OEMs who wish to internationalize their MEBx shall be enabled to do so	No	No	No	No	No
CCG01000 15078	Intel® Management and Security Status Localization	The Intel® Management and Security Status will be localized so that users who do not understand English will understand the message Languages: Chinese(T), Chinese(S), German, Spanish, French, Japanese, Korean, Brazilian Portuguese, Arabic, Czech, Danish, Greek, Finnish, Hebrew, Italian, Hungarian, Dutch, Norwegian, Polish, Portuguese-Portugal, Russian, Slovak, Slovenian, Swedish, Thai, Turkish	Yes	Yes	Yes	Yes	Yes
CCG01000 15077	MEI/LMS installer Localization	MEI/LMS installer will be localized so that users who do not understand English will understand the message Languages: Chinese(T), Chinese(S), German, Spanish, French, Japanese, Korean, Brazilian Portuguese, Arabic, Czech, Danish, Greek, Finnish, Hebrew, Italian, Hungarian, Dutch, Norwegian, Polish, Portuguese-Portugal, Russian, Slovak, Slovenian, Swedish, Thai, Turkish	Yes	Yes	Yes	Yes	Yes

4.5 Legal Requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15619	Legal Trademark	All documents shall be reviewed by a Certified Content Editor as well as Intel Legal for correct trademarks and disclaimer usage prior to document external release.	Yes	Yes	Yes	Yes	Yes
CCG01000 15618	Legal Encryption	Intel® AMT shall use TLS-PSK encryption during configuration. There are no new encryption capabilities in Intel® AMT 2.5 / 3.0 beyond what Intel® AMT 2.0 delivers	Yes	Yes	Yes	Yes	Yes
CCG01000 15617	Legal License	The installer shall contain the Legal license requirement for end user install and silent install.	Yes	Yes	Yes	Yes	Yes
CCG01000 15616	Legal Agreement	Legal Agreement is needed to be in place to release the driver to ISVs.	Yes	Yes	Yes	Yes	Yes
CCG01000 15615	Product Name	The legal product shall be Intel® Active Management Technology (Intel® AMT).	Yes	Yes	Yes	Yes	Yes
CCG01000 15614	Name strings correct and verified	All name strings shall be approved by Intel Legal and Marketing.	Yes	Yes	Yes	Yes	Yes
CCG01000 15484	Tool distribution and agreement	The tool will be distributed to OEMs under contract: 1) A standard contract has to be prepared which will name - Intel Corporation - OEM Content outline: - Due to OEM requirement for open-network configuration and OEM pre-configuration Intel implements a custom flow - OEM agrees to - Keep the AMTNVMCustomize tool tools confidential - Give each end-user corporation a distinct password, distinct certificate, distinct PID/PPS - Keep the passwords, certificates and the PID/PPS confidential - Oblige the end-customer corporations to keep the password, certificates, PID/PPS confidential	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		- If OEM pre-configuration not implemented, oblige the end-customer corporations to change the password on a closed network 2) The OEM acknowledges that failure to follow any of these directives may result in Intel® AMT machines being ''hijacked'' and permanently inactivated by attackers					

§

5 Intel® Active Management Software Requirements

5.1 Intel® Active Management Technology Software

The section describes all the Intel® AMT software products which Intel will develop and will be released on the product CD, as part of the platform software, or used for internal validation. The SW product components are 1) special drivers for managing the various AMT functions of the AMT device (host interface, IDE redirection and SOL redirection). 2) An Intel® AMT manageability service application that the various ISV applications will communicate with when accessing the AMT device. See the Intel® AMT SDK section for software developed specifically for ISV development purposes.

Note: Microsoft .NET Framework 3.5 is a prerequisite for running Intel® AMT SW (specifically for running the Intel® Management and Security Status application).

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14969	SW Host Operating System	All the SW components which run on the Intel® AMT machine (''host side'') shall run on specified operating systems. See section Operating Systems Supported.	Yes	Yes	Yes	Yes	Yes
CCG01000 15592	SW.NAC.posture plug-in	AMT Posture plug-in (host SW). This module shall collect the AMT posture, send it via the NAC tunnel in EAP-TLV format, receive the policy and send it to AMT. The AMT posture will include this information: - AMT version - AMT standalone (Boolean) - Security parameters: TLS state, interfaces enabled/disabled, Setup and Configuration state, etc. - BIOS and platform information - Boot log - IDER log	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15591	SW.NAC.PDP plug in	AMT Policy Decision Point (PDP) plug-in (remote SW). This module shall receive the posture, authenticate AMT using the XML security envelope, retrieve the appropriate policy, wrap it in XML security envelope, and return it to the PDP.	Yes	Yes	Yes	Yes	Yes
CCG01000 15262	Intel® ME Deliverable: MEI Driver	An interface from the Host OS to the ME. Previously named the HECI Driver (Host Embedded Controller Interface)	Yes	Yes	Yes	Yes	Yes
CCG01000 15261	Intel® AMT Deliverable: LMS	Local Management Service for Windows Operating Systems	Yes	Yes	Yes	Yes	Yes
CCG01000 15260	Intel® AMT Deliverable: Linux IDE-R Driver	A driver for the IDE-R PCIM device for Linux Operating Systems	No	No	No	No	No
CCG01000 15259	Intel® AMT Deliverable: Win SoL INF File	An INF file for the serial PCIM device for Windows	Yes	Yes	Yes	Yes	Yes
CCG01000 15258	Intel® ME Deliverable: Local FW Update	A tool for local updates of the ME Firmware	Yes	Yes	Yes	Yes	Yes
CCG01000 15257	Intel® AMT Deliverable: Setup and Configuration Server	A Windows server for setup and configuration of Intel® AMT which detects AMT clients, maintains a database of systems and configures them for use in enterprise environments.	Yes	Yes	Yes	Yes	Yes
CCG01000 15256	Intel® AMT Deliverable: Intel® AMT Management and Security Status	A Windows systray Icon and Control Panel Interface for AMT Local User notifications	Yes	Yes	Yes	Yes	Yes
CCG01000 15255	Intel® AMT Manageability presence Server	A Server for the enterprise that allows remote access to Intel® AMT clients to be managed	Yes	Yes	Yes	Yes	Yes
CCG01000 15254	Intel® AMT Deliverable: Manufacturing & Validation Tools	Manufacturing and Validation tools for Intel® AMT	Yes	Yes	Yes	Yes	Yes
CCG01000 15253	NAP SHA	An SHA (System health application) that will collect the AMT posture and send to the NAP agent	Yes	Yes	Yes	Yes	Yes
CCG01000 15252	NAP SHV	A System Health Validator that will communicate with the NAP server (NPS) and return the policy to the MPS.	Yes	Yes	Yes	Yes	Yes
CCG01000 15849	AMT software size in kit	The AMT SW can take up to 60 MB in the kit.	N/A	N/A	N/A	N/A	N/A
CCG01000 15848	AMT software size on disk	The AMT SW can take up to 50 MB on the platform's disk after installation.	N/A	N/A	N/A	N/A	N/A

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15847	Loading time for AMT services	The LMS and UNS services should be in Started state from the moment the user receives control of the platform and startup applications are running. A normal user's experience should not be adversely affected (in a way noticeable by the user) while the services are loading.	N/A	N/A	N/A	N/A	N/A

5.2 Intel® Active Management Technology LMS

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14978	SW Local Management Service Secured Channel	The communication between an ISV agent (which runs on a machine which Intel® AMT resides on, aka host machine) and the AMT device will be done via secured channel. This channel will be http over TLS. Therefore a dedicated Intel® AMT service (daemon) shall run on each AMT machine in order to provide this secured channel.	Yes	Yes	Yes	Yes	Yes
CCG01000 14977	Local Mgmt Service Supported Operating Systems	This Local service shall support the operating systems as specified in the host OS section Operating Systems Supported.	Yes	Yes	Yes	Yes	Yes
CCG01000 15594	SW Local Management Service Interface Server	The Local AMT management service will support TCP sessions, initiated by the local host SW targeted to the AMT device.	Yes	Yes	Yes	Yes	Yes
CCG01000 15593	SW Local Management Service Interface Client	The Local AMT management service will support TCP sessions, initiated by the AMT device targeted to local host agents.	Yes	Yes	Yes	Yes	Yes
CCG01000 15347	Local Management Service network detection	The LMS service shall be able to determine if the client is connected to an enterprise network, either via a VPN or a 3rd party interface.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15346	Local Management Service VPN tunneling	When the LMS service determines that the client is connected to an enterprise. Note that Intel® AMT will only accept connection sent from LMS, if Intel® AMT has no direct connection to the enterprise.	Yes	Yes	Yes	Yes	Yes
CCG01000 15345	LMS enterprise connectivity detection	LMS will decide whether a given interface (virtual or physical) is connected to an enterprise network based on the following criteria: LMS queries Intel® AMT for the set of pre-defined enterprise DNS suffix list. LMS compares the DNS suffix information provided by the local DHCP server (provided by IP helper API in windows), with the list received from Intel® AMT, if there is a match LMS assumes the interface is connected to an enterprise network.	Yes	Yes	Yes	Yes	Yes
CCG01000 15251	Local Mgmt Service Supported Devices	This Local service Provided with the Intel® AMT package shall support Intel® AMT 4.0 device only.	No	Yes	No	No	Yes
CCG01000 15250	Ports	The LMS will listen on the TCP/TLS ports of Intel® AMT and will forward the communication to the Intel® AMT device via the MEI driver	Yes	Yes	Yes	Yes	Yes
CCG01000 15249	Protocol	The LMS will communicate with Intel® AMT as defined in [AMTHI]	Yes	Yes	Yes	Yes	Yes
CCG01000 15846	LMS maximum used memory	The LMS will use a maximum of 10MB of system memory (RAM)	Yes	Yes	Yes	Yes	Yes

5.3 Intel® AMT and Intel® ME Drivers

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14976	Intel® MEI driver Mediator	The Intel® MEI driver shall be the mediator between the Local Management service application and the Intel® AMT FW. This driver shall run on the Intel® AMT machine. It will transfer messages from the local service to the FW and in the opposite direction as well. The Intel® MEI driver will serve only once the OS is up.	Yes	Yes	Yes	Yes	Yes
CCG01000 14975	Intel® MEI driver Certification	The Windows* Intel® MEI driver shall pass WHQL certification on the Windows*operating systems as defined in the section Operating Systems Supported. The certification shall be a general device certification. Note that early versions of the drivers (pre-production) are not signed/certified.	Yes	Yes	Yes	Yes	Yes
CCG01000 14974	Intel® MEI driver OS Support	The Intel® MEI driver shall support the operating systems as specified in the section Operating Systems Supported.	Yes	Yes	Yes	Yes	Yes
CCG01000 14973	Intel® MEI driver OS Up Indication	The Intel® MEI driver shall implement a mechanism for detecting OS hangs and notify the FW. Limitation: On Windows Vista* there will be a special mechanism for identification of OS state. The Intel® MEI driver and the FW shall utilize this mechanism.	Yes	Yes	Yes	Yes	Yes
CCG01000 14972	Intel® MEI driver Supported Interfaces	The Intel® MEI driver will communicate with the FW according to the Intel® MEI interface Hardware Programming Specification doc and will communicate with Intel® AMT service according to Intel® MEI driver interface which is described in the Intel® MEI driver design doc.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 14971	IDER Driver	The SW shall provide PCI IDE driver supporting Intel® AMT IDE for the Linux kernel 2.4.x and above. Limitation: Limited to the list of Linux operating systems as defined in the section Operating Systems Supported. Assumption: In Windows*, there is no need to any specific driver file for supporting AMT IDE, since the Windows* IPCI DE driver will support Intel® AMT IDE by default.	No	No	No	No	No
CCG01000 14970	SOL Driver	The SW shall provide driver installation files supporting Intel® AMT for the Windows* operating systems which will utilize communications port COM4. Limitation: Limited to the list of Windows* operating systems as defined in the section Operating Systems Supported. Note: the COM port assignments are static and cannot be changed. Assumption: For Linux, there is no need to any specific driver file for supporting Intel® AMT comm. port, since the Linux comm. port driver will support this device by default.	Yes	Yes	Yes	Yes	Yes
CCG01000 15050	Manual COM port registration	The SOL driver installer shall allow the user to manually choose the Windows COM port on which the SOL device operates	Yes	Yes	Yes	Yes	Yes

5.4 Local User Notification Service

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15248	SW Local User Notification Service	A service shall exist that will register to Intel® ME Eventing Service and will log events in the Windows event log	Yes	Yes	Yes	Yes	Yes
CCG01000 15247	UNS service	UNS will be implemented as a system service	Yes	Yes	Yes	Yes	Yes
CCG01000 15246	SW User Notification Service Interface (SOAP)_	The UNS will implement a SOAP server. It will talk to Intel AMT via LMS	No	No	No	No	No
CCG01000 15845	SW User Notification Service Interface (WS)	The UNS will implement a WS-Eventing server. It will talk to Intel® ME Eventing Service via LMS	Yes	Yes	Yes	Yes	Yes
CCG01000 15245	HW support	The UNS for each generation shall support only the hardware for that generation's chipset	Yes	Yes	Yes	Yes	Yes
CCG01000 15244	UNS Supported Operating Systems	This Local service shall support the operating systems as specified in the host OS section Operating Systems Supported.	Yes	Yes	Yes	Yes	Yes
CCG01000 15243	UNS authentication methods - Legacy	The UNS will by default authenticate to the Intel® ME Eventing Service device using anonymous login	No	No	No	Yes	Yes
CCG01000 15242	UNS credentials	The UNS will be able to register with Intel® ME Eventing Service with TLS on or off and with mutual authentication on or off.	Yes	Yes	Yes	Yes	Yes
CCG01000 15241	UNS Credentials configuration	UNS will supply a method of configuring the credentials and storing them encrypted	Yes	Yes	Yes	Yes	Yes
CCG01000 15240	UNS EAC notification	Upon event that causes change in posture UNS shall call the functions of NAC/NAP for change in posture notification	Yes	Yes	Yes	Yes	Yes
CCG01000 15844	UNS maximum used memory	The UNS will use a maximum of 10MB of system memory (RAM)	Yes	Yes	Yes	Yes	Yes
CCG01000 15843	UNS not writing errors when AMT is unprovisioned or disabled.	The UNS should NOT write subscription errors to the Event Viewer when AMT is unprovisioned or disabled.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15840	Capture event for contracts updated	UNS must register for (when UNS running) and receive (when sent by firmware) new event from firmware, which is sent when connection failure occurs due to contracts having been updated when the PC was offline. Firmware will update the contracts, store locally and then send this event. UNS must make this event available to other applications in the OS via the OS event log interface.	Yes	Yes	No	Yes	Yes
CCG01000 79533	UNS synchronization of static IP addresses.	When IPSyncEnabled=TRUE, UNS will monitor the Windows IP Configuration on the LAN interface and will automatically update the AMT IP configuration to either static IP or dynamic. For static IP UNS will configure all the AMT IP settings with the current Windows IP settings.	No	No	No	Yes	Yes

5.5 NAC SW Components

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15239	NAC plug-in module	Intel shall provide a software module that serves as a plug-in to Cisco's CTA client software.	Yes	Yes	Yes	Yes	Yes
CCG01000 15238	NAC plug-in implementation	The NAC plugin will implement the functions as described in the Cisco* CTA SDK.	Yes	Yes	Yes	Yes	Yes
CCG01000 15237	NAC plugin	The Intel NAC PP will work in SOAP/WSMAN/TLS/TCP/mutual authentication modes. Credentials will be kept encrypted in the registry.	Yes	Yes	Yes	Yes	Yes
CCG01000 15236	NAC credentials configuration	The NAC PP will include a program that will allow setting the credentials to the EAC realm and saving them encrypted in the registry.	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15235	NAC plugin OS support	The NAC plugin shall support the operating systems as specified in the host OS section Operating Systems Supported.	Yes	Yes	Yes	Yes	Yes
CCG01000 15234	NAC ACS back-end verifier	Intel shall provide documentation and sample code supporting ISVs in creating Verifier products integrated into Cisco's ACS back-end server. This documentation shall provide the security validation method of the Intel® AMT posture signature and provide Posture format and details.	Yes	Yes	Yes	Yes	Yes
CCG01000 15233	NAC PVS user interface	The Intel Sample code will allow simple configuration of validation parameters	Yes	Yes	Yes	Yes	Yes
CCG01000 15232	NAC PVS protocol	The NAC PVS sample code will implement the HCAP protocol to communicate with the Cisco ACS	Yes	Yes	Yes	Yes	Yes
CCG01000 15231	NAC PVS OS support	The NAC PVS sample code will run on Windows Server 2003	Yes	Yes	Yes	Yes	Yes
CCG01000 15186	Request to allow retrieving NAC posture locally without HTTP authentication.	The requested change is to allow anonymous HTTP access for retrieving the NAC posture from the FW. The posture itself does not contain any confidential information. Note: this has no affect on the TLS layer: if TLS is used by the FW, it will still be used from NAC.	Yes	Yes	Yes	Yes	Yes
CCG01000 15185	Support Cisco Compliance Certification for AMT FW Embedded NAC trust agent	This RCR covers Cisco request for AMT FW Trust Agent Certification and CCX compliance in order for AMT platforms to work seamlessly OOB in Cisco NAC environment (wired & wireless).	Yes	Yes	Yes	Yes	Yes
CCG01000 15183	Support for EAP-TLS as inner method of EAP-FAST	Support for EAP-TLS as inner method of EAP-FAST in AMT FW to work in seamlessly OOB in Cisco NAC environment (wired & wireless)	Yes	Yes	Yes	Yes	Yes
CCG01000 15184	Support for PXE remote boot with AMT FW Embedded 802.1x/NAC trust agent	Add support for PXE remote boot with AMT FW Embedded 802.1x/NAC trust agent in order for AMT/vPro platforms to work seamlessly with PXE remote boot OOB in 802.1x/NAC environment (wired only).	Yes	Yes	Yes	Yes	Yes

5.6 NAP SW Components

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15230	NAP SHA module	Intel shall provide a software module that serves as a SHA plugin to the NAP agent.	Yes	Yes	Yes	Yes	Yes
CCG01000 15229	NAP SHA implementation	The NAP SHA will implement the functions as described in Microsoft platform SDK.	Yes	Yes	Yes	Yes	Yes
CCG01000 15228	NAP SHA	The Intel NAP SHA will work in SOAP/WSMAN/TLS/TCP/mutual authentication modes. Credentials will be kept encrypted in the registry.	Yes	Yes	Yes	Yes	Yes
CCG01000 15227	NAP SHA credentials configuration	The NAP SHA will include a program that will allow setting the credentials to the EAC realm and saving them encrypted in the registry. The registry location may be the same used for NAC.	Yes	Yes	Yes	Yes	Yes
CCG01000 15226	NAP SHA OS support	The NAP SHA shall support the operating systems specified in the host OS section Operating Systems Supported and that include the Microsoft NAP agent. The OS currently supported are Windows* XP and Windows Vista*.	Yes	Yes	Yes	Yes	Yes
CCG01000 15225	NAP SHV back-end verifier	Intel shall provide documentation and sample code supporting ISVs in creating Verifier products integrated into Microsoft's NPS back-end server. This documentation shall provide the security validation method of the Intel® AMT posture signature and provide Posture format and details.	Yes	Yes	Yes	Yes	Yes
CCG01000 15224	NAP SHV Posture Signature Verification	The Intel SHV shall verify the posture according to the shared credentials with AMT, and evaluate it according to pre-defined rules set by IT	Yes	Yes	Yes	Yes	Yes
CCG01000 15223	NAP SHV user interface	The Intel Sample code will allow simple configuration of validation parameters	Yes	Yes	Yes	Yes	Yes
CCG01000 15222	NAP SHV implementation	The NAP SHV sample code will implement the API as defined in the Microsoft SDK	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15221	NAP SHV OS support	The NAP SHV sample code will run on Windows Vista* Server.	Yes	Yes	Yes	Yes	Yes

5.7 NAP SHV Product Requirements

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15030	SHV.Product	Intel provided product SHV plugin to NPS for verification of Intel® AMT SoH	Yes	Yes	Yes	Yes	Yes
CCG01000 15029	SHV.OS	Operating System Support: Windows Vista* Server	Yes	Yes	Yes	Yes	Yes
CCG01000 15027	SHV.Interfaces	- SHV will implement the following interfaces to talk to NPS: INapComponentConfig INapComponentInfo INapSystemHealthValidator - SHV will use the following interfaces: INapSoHConstructor <http://msdn2.microsoft.com/en-us/library/aa369520.aspx> INapSoHProcessor <http://msdn2.microsoft.com/en-us/library/aa369527.aspx> INapSystemHealthValidationRequest INapServerCallback <http://msdn2.microsoft.com/en-us/library/aa369499.aspx>	Yes	Yes	Yes	Yes	Yes
CCG01000 15026	SHV.performance	No explicit requirements	Yes	Yes	Yes	Yes	Yes
CCG01000 15025	SHV.availability	Must be always available	Yes	Yes	Yes	Yes	Yes
CCG01000 15024	SHV.Logging	- Errors in SHV will be written to windows event log - SHV will log all interactions with machines in database and/or file (configurable by user)	Yes	Yes	Yes	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15023	SHV.GUI	SHV will provide GUI for management & configuration. Configuration items are: - Logging - Plugin for certificate retrieval - Policy GUI will allow configuring the policy SHV will provide GUI for management & configuration. Configuration items are: - Logging - Plugin for certificate retrieval - Policy GUI will allow configuring the policy	Yes	Yes	Yes	Yes	Yes
CCG01000 15022	SHV.Policy	- Rules in syntax <,>,=,<>, and, or, not, in GUI - Script - Rules per types. - DLL?	Yes	Yes	Yes	Yes	Yes
CCG01000 15021	SHV.Compatibility	SHV will handle and display unknown parameters as binary data to allow compatibility with future posture with current feature set	Yes	Yes	Yes	Yes	Yes
CCG01000 15020	SHV.Signature validation	SHV will verify the signature of the posture and allow this as field in policy	Yes	Yes	Yes	Yes	Yes
CCG01000 15019	SHV.CLI	No CLI will be provided	Yes	Yes	Yes	Yes	Yes
CCG01000 15018	SHV.Install	SHV will include installer for product. SHV will be installed as services.	Yes	Yes	Yes	Yes	Yes
CCG01000 15016	SHV.Documentation	SHV will include product level documentation that will cover: - Installation - Configuration - Policy definition - Sample posture Sample script & dll for policy definition	Yes	Yes	Yes	Yes	Yes
CCG01000 15015	SHV.Localization	SHV will not be localized. Will support only English.	Yes	Yes	Yes	Yes	Yes
CCG01000 15014	SHV.Help	Help will not be provided. This is covered by documentation.	Yes	Yes	Yes	Yes	Yes
CCG01000 15013	SHV.Source	SHV full source code will be provided in SDK.	Yes	Yes	Yes	Yes	Yes

5.8 Intel® Management and Security Status Icon and Application for Intel® AMT

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15220	System Notification Icon	Provide an icon in the System Notification area for supported Windows Operating Systems and SKUs that depict the state of ME components and applications: ME Services, AMT.	Yes	Yes	No	Yes	Yes
CCG01000 15839	ME Services Events	- Intel® ME configured - Intel® ME unconfigured	Yes	Yes	No	Yes	Yes
CCG01000 15219	Communication	The icon and application can communicate with Intel® AMT via the Intel® MEI. No authentication or encryption is used for this communication as none of the information transmitted is sensitive.	Yes	Yes	No	Yes	Yes
CCG01000 15218	Graphic Quality	The Manageability Icon, the Right Click Menu, Notification bubbles and the application should have an appearance that is comparable to Windows Vista style graphics. - A UI that integrates properly with Aero - Windows that function with Aero Glass enabled - Icons that thematically fit in with other vista icon styles - Scalable Icons	Yes	Yes	No	Yes	Yes
CCG01000 15217	First Run after Enable/Disable	Upon First Run after one, or more, of Intel® AMT Technology transfers either from Enabled to Disabled, or from Disabled to Enabled, the Icon shall display a "Notification Bubble". This does not occur every time the computer starts up, Notification will appear for each user every time Intel® AMT changes from Disabled to Enabled, or from Enabled to Disabled. The notification bubble will contain the text: "Intel® Management and Security Status notification. Click here for details."	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		When disabling ME or when application is running without drivers, all status information will show "Information Unavailable" and only "General" and "Advanced" tabs will be shown. The application will contain an "Enable User Notification" checkbox to allow user control of this notification bubble. This option will be selected by default. - OEMs may configure the icon to enable\disable user notification which will serve as a default selection for the user. o The user may override the OEM configuration from the application. This Notification shall address the legal requirements of notifying the user about privacy.					
CCG01000 15711	Icon State - Enabled	The Icon's appearance will be ''Enabled'' when running on a ME SKU/platform.	Yes	Yes	No	Yes	Yes
CCG01000 15710	Icon State - Disabled	The Icon shall change appearance to "Disabled" when running on a non ME sku/platform.	Yes	Yes	No	Yes	Yes
CCG01000 15215	Follow Windows Vista* User Experience Guidelines	Microsoft provides guidelines for implementing icons in the System Notification area. The requirements in this section are written to follow these guidelines, additionally architecture and engineering decisions should reference these published guidelines.	Yes	Yes	No	Yes	Yes
CCG01000 15214	Application	A Windows application in supported Windows Operating systems, which is invoked by the tray icon or through the "Program Files" menu. The application contains ME Services and AMT information as well as notification configuration options. The application is present regardless of whether or not Intel® AMT or Intel® ME are enabled on the system.	Yes	Yes	No	Yes	Yes
CCG01000 15213	Exiting Icon	Upon exit the user is prompted whether or not they wish this icon to appear at startup, and that if they choose not to load it, they may re-enable it any time in the Application.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015212	Hover	Displays a Tooltip with the icon name	Yes	Yes	No	Yes	Yes
CCG0100015211	Left Click Action	Same Functionality as Right Click Action	Yes	Yes	No	Yes	Yes
CCG0100015210	Right Click Action	Right Clicking the icon displays a pop-up menu which contains the following: - Open - shows the Manageability Application - Exit - Stop KVM session (if KVM is connected)	Yes	Yes	No	Yes	Yes
CCG0100015209	Double Click Action	Double clicking the icon opens the Manageability Application.	Yes	Yes	No	Yes	Yes
CCG0100015208	User notification	A corner pop-up or ''Notification bubble'' may be used for events when the icon must notify the user. The pop-up must have an X in the upper right hand corner to dismiss it. - KVM Session start/end will stay on until dismissed by the user - KVM Session start will be automatically replaced by KVM session end. - All other notifications should time out in no longer than 10 seconds when system is active When KVM notification is displayed, no other notifications will be displayed to the user (the event will appear in the event history). When displaying a non KVM user notification and more than one notification is queued; notification text will be general such as: ''Intel® Management and Security Status detected several events. Click here to display them'' The icon in the system notification area may change its appearance to notify the user of events. Once explicitly viewed, icon must return to its normal state	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15207	No unnecessary notifications	At no point shall the icon on startup or during runtime make any notification to the user unless such a valid event has occurred. This means no display of ''Welcome'' messages.	Yes	Yes	No	Yes	Yes
CCG01000 15206	Helpful and understandable messages	All messages to the user must be clear, contain all the information required to understand the event, as well as pointers to required actions when appropriate	Yes	Yes	No	Yes	Yes
CCG01000 15203	AMT Events	- Intel® AMT Disabled - Intel® AMT Enabled - SOL session opened - SOL sessions closed - IDER session opened - IDER session closed - System Defense activated - System Defense deactivated - Intel® AMT remote power control operation has occurred - KVM_CLOSE_CONTENT_MSG - KVM_ENABLED - KVM_DISABLED - KVM_SESSION_INITIATED - KVM_SESSION_STARTED - KVM_SESSION_ENDED	Yes	Yes	No	Yes	Yes
CCG01000 15202	On Startup	Default: - OEMs may configure the icon to always appear\not appear (application will run in background) which will serve as a default selection for the user. o The user may override the OEM configuration from the application. The manageability icon will not appear and the process will end itself on startup when running on no ME sku (consumer sku) or when running without drivers/ME disabled.	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015201	Application Help	Help Menu of Manageability Application contains information about Intel® ME, Intel® AMT. - A description of the Status Icon/App purpose - Directions pointing to user guide for more information on operation (installed on platform under IMSS installation directory) - A URL pointing to the privacy statement on the Intel website: www.intel.com. The listed URL can be updated by OEMs. NOTE: URL must be validated to a location that will remain supported across generations.	Yes	Yes	No	Yes	Yes
CCG0100015199	Application Information	Opening the application opens a window that displays the following information (NOTE: Final wording in UI may vary, that is a UI design consideration.) - Intel logo - should be modifiable by OEM to be replaced by OEM logo instead - "General" tab with the following data: o Intel® AMT -- not shown for sku with no AMT: Enabled | Disabled| Information Unavailable (no drivers) o Event History: Will show all event covered in CCG0100015203 Toggle on and off notification / startup options	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG01000 15708	Application Information -- Intel® AMT Tab	The application shall contain a selectable tab for Intel® AMT with the following data: -> System Defense Status: Enabled | Disabled | information Unavailable (when no drivers or AMT disabled) -> Request Assistance section: o AMT Status Enabled | Disabled | Information Unavailable (when no drivers or AMT disabled) o Call for help: Connected to Enterprise (CILA) | Connected Outside Enterprise (CIRA) | Disconnected o Connect | Disconnect support session button for KVM/IDE-R/SOL o Configure KVM Disconnection Hot-Key	Yes	Yes	No	Yes	Yes
CCG01000 15837	Application Information- Intel® Manageability Engine	The application shall contain a selectable tab for Intel® ME (named "Advanced") with the following data: -> Status: Configured | Not Configured | Not Detected (??) o Configure ME [output] messages language (match user regional settings by default) and message screen size. -> The Intel ME tab will allow opening Network Information for each interface: o Mode: Static | DHCP o For wireless display whether AMT is configured for wireless o Link Status: Up | Down ???? o IP information (IPV4 and IPV6) o MAC information	Yes	Yes	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100014628	Remote Access	Application should indicate the status of a Remote Access (CIRA (Fast call for help), SOL, IDE-R and KVM) connection (or whether Remote Access is not configured). Where possible by the FW Remote Access configuration, the Icon should allow the user to initiate (or terminate) a Remote Access connection.	Yes	Yes	No	Yes	Yes
CCG0100015036	Intel® Management and Security Status Icon for End-User Control	For the Host OS case, a new dialog box is added to Intel® Management and Security Status. Upon opening the tray, the user sees an option for activating the healing process. This dialog box displays text that explains the Healing process to the end user, along with a button for triggering the process. This dialog box works in a fashion similar to that of the OEB/MEBx screen. Furthermore, the dialog box must allow OEM customization and localization, as is required with the Management and Security Status icon.	Yes	Yes	No	Yes	Yes
CCG0100015836	IMSS maximum used memory	The IMSS will use a maximum of 30MB of system memory (RAM)	Yes	Yes	Yes	Yes	Yes
CCG0100015835	IMSS query frequency	Intel® Management and Security Status queries the system and updates its information (including CIRA information) once every 10 seconds.	N/A	N/A	N/A	N/A	N/A

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100015834	Behavior when no .NET	When the user executes Drivers/SW installer on platform Drivers/SW installer shall verify .NET FW version installed on the platform. - 1. .NET FW version >= 3.5 - a. Drivers/SW installer shall install IMSS application. - 2. .NET FW version >= 2.0 - a. Installer shall notify user a newer .NET FW installation exists and recommend to upgrade .NET FW on platform - b. Drivers/SW installer shall install IMSS application. - 3. .NET FW version < 2.0 / not installed on platform - a. Installer shall notify user that .NET FW 3.5 must be installed on platform for IMSS to function properly. - b. IMSS shall not be installed. - c. All other drivers/SW shall be installed	N/A	N/A	N/A	N/A	N/A
CCG0100079534	IMSS indication that WiFi is unavailable to host	1) Whenever IMSS detects that WLAN has ME preference activated, it shall show a pop-up box that will allow the end-user to click it. The pop-up box shall indicate to user that WiFi is unavailable to host because it is being used for system heal purposes. 2) Whenever IMSS detects that WLAN has Host preference activated, it shall not show the pop-up. 3) If end-user clicks the pop-up box, IMSS shall open up its GUI and provide the user an option to send to ME a command to move WLAN to host link preference using a button for return control. 4) Network information window shall display the WLAN link control (OS / Intel ME), WLAN link preference (OS / Intel ME).	No	No	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100079535	IMSS support for User Consent Privacy - pop-ups	1. IMSS to have a Balloon for the "Timeout inactivity ended" event. 2. Update text of KVM and IDER "Session Ended" balloons, with info on the inactivity timer start.	No	No	No	Yes	Yes
CCG0100079536	IMSS support for User Consent Privacy - event history	Log Inactivity timer period "start" and "End" events.	No	No	No	Yes	Yes
CCG0100079537	IMSS support for User Consent Privacy - Advanced tab information	User Consent Policy info to be displayed in "Advanced Tab".	No	No	No	Yes	Yes
CCG0100079538	IMSS support for User Consent Privacy - Taskbar Icon	Display the animation icon as long as a remedy session is in progress (in 6.0 animated icon is used while KVM session is in progress)	No	No	No	Yes	Yes
CCG0100079539	IMSS support for User Consent Privacy - Session Termination	1. IMSS to provide user with an option to terminate "remedy session" AND/OR SOL session throughout its lifetime: i. Start time: User Consent sprite displayed. ii. End-time timeout expired. 2. Using UNS, terminate all current active sessions: KVM, IDER, SOL and inactivity timer. 3. The termination logic, doesn"t depend on the User Consent policy (i.e. None), it will always try to terminate all active sessions.	No	No	No	Yes	Yes
CCG0100079540	IMSS Application Information - Extended System Details	There shall be an option within the IMSS User Interface that will allow the user to view a System Report. The report will be launched from the "Extended System Details" button within the "Advanced" tab. This report will be shown as Windows System Information format (NFO file). There shall be an option that will allow the user to save the System Report to a file. There will be an option to export the report in text format. The default save location for this file shall be TEMP folder. User will also have the option to save to any location.	No	No	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
CCG0100079541	IMSS 'Extended System Details' - Report contents	The Intel ME System Report shall contain text describing the system's AMT/ME device drivers and configuration. Host Information: Operating System Name Operating System Version System Name System Manufacturer System Model Processor BIOS Version LAN DeviceID LAN Driver Wireless DeviceID Wireless Driver Version Intel® ME Information: ME Control Mode Provisioning Mode BIOS boot State Last ME reset reason System UUID FW Capabilities Intel® Active Management Technology Intel® AMT State Intel® AMT Status CIRA Connection Status Intel® Anti-Theft Technology PC Protection Intel® AT State Intel® AT Status Intel® Capability Licensing Service Protect Audio Video Path Local FWUpdate Power Policy: Cryptography Support Componets information MEBx Version FW Version UNS Version	No	No	No	Yes	Yes

ID	Requirements	Detailed Description	Intel® AMT 6.0 Desktop	Intel® AMT 6.0 Mobile	Intel® AMT 6.0 Consumer	Intel® AMT 7.0 Desktop	Intel® AMT 7.0 Mobile
		LMS Version MEI Driver Version Network information Lan MAC Address Lan Configuration state Link Status					
CCG01000 79542	IMSS Level III SSKU Manageability Upgrade	IMSS should display any MNG state before and after Level III MNG upgrade	No	No	No	Yes	Yes
CCG01000 79543	IMSS Display AT-p	IMSS should scan host platform and display Intel® AT capable message when AT is present - IMSS should collect AT activation status and displays summary to End User - IMSS should redirect non-activated AT platform end user to approved AT provider list (List is Hosted on Intel Web Site)	No	No	No	Yes	Yes

5.9 Manageability Presence Server

Remote access describes the ability for the enterprise admin that is within an organization to manage Intel® AMT systems that are outside the organization (behind firewalls, NAT, etc.). The technical solution involves a vPro enabled gateway that serves as a proxy between the management consoles and the remote Intel® AMT systems.

Detailed MPS requirements are being handled elsewhere.

5.10 Intel® Active Management Technology Setup and Configuration Server

The Intel® Active Management Technology (Intel® AMT) Setup and Configuration Server (SCS) is provided to help ISVs integrate the Intel® AMT setup and configuration process into their management applications. This SDK provides the ISV the necessary documentation, APIs, sample code, libraries, and tools that can take advantage of this technology.

Detailed SCS requirements are being handled elsewhere.

5.11 Intel® Active Management Technology SDK

The Intel® Active Management Technology (Intel® AMT) tools in the Intel® AMT Software Development Kits are provided to help ISVs integrate asset control, Out-of-Band management and System Defense features into their software applications. This SDK provides the ISV the necessary documentation, APIs, sample code, and tools that can take advantage of this technology. There are two types of SDK partner and non-partner. The non-partner SDK is a sub-set of the partner SDK. Where appropriate, non-partner SDK requirements will be called out separately. These SDKs provide the necessary interface information as well as the ability to test the functionality that the ISVs will add to their applications.

Detailed SDK requirements are being handled elsewhere.

§

6 Default Root Certificate Hashes

The firmware shall include the following certificate hashes by default:

- GoDaddy
- Starfield*
- Comodo
- Verisign* (including the Verisign G3 and Class 3 G2 root certificate)

  Starting Intel® AMT 6.1 VeriSign Class 3 G1.5 and G5 root certificates

§

7 Related Documents

This section contains a list of documents (Product Requirement Documents and others) for components that are related to or referenced by this document.

Document Name	Doc #
Intel® Anti-Theft Technology - PC Protection Calpella Platform PRD (AT)	Anacapa# 27431
Intel® AMT 7.0 and Intel® Management Engine Tools PRD	Anacapa# 28538
Intel Upgrade Service Platform PRD	CDI# 443653
Intel RST 10.0 – Technical Product Specification Differences Document	CDI# 446846
Firmware Variable Structures for Intel® Management Engine and Intel® Active Management Technology 7.0	Anacapa# 28662
Intel® Management Engine Firmware – Collateral Forecast	CDI #447228
PKI-CH in Manufacturing for Systems Enabled with Intel® Active Management Technology (Intel® AMT)	CDI# 357645