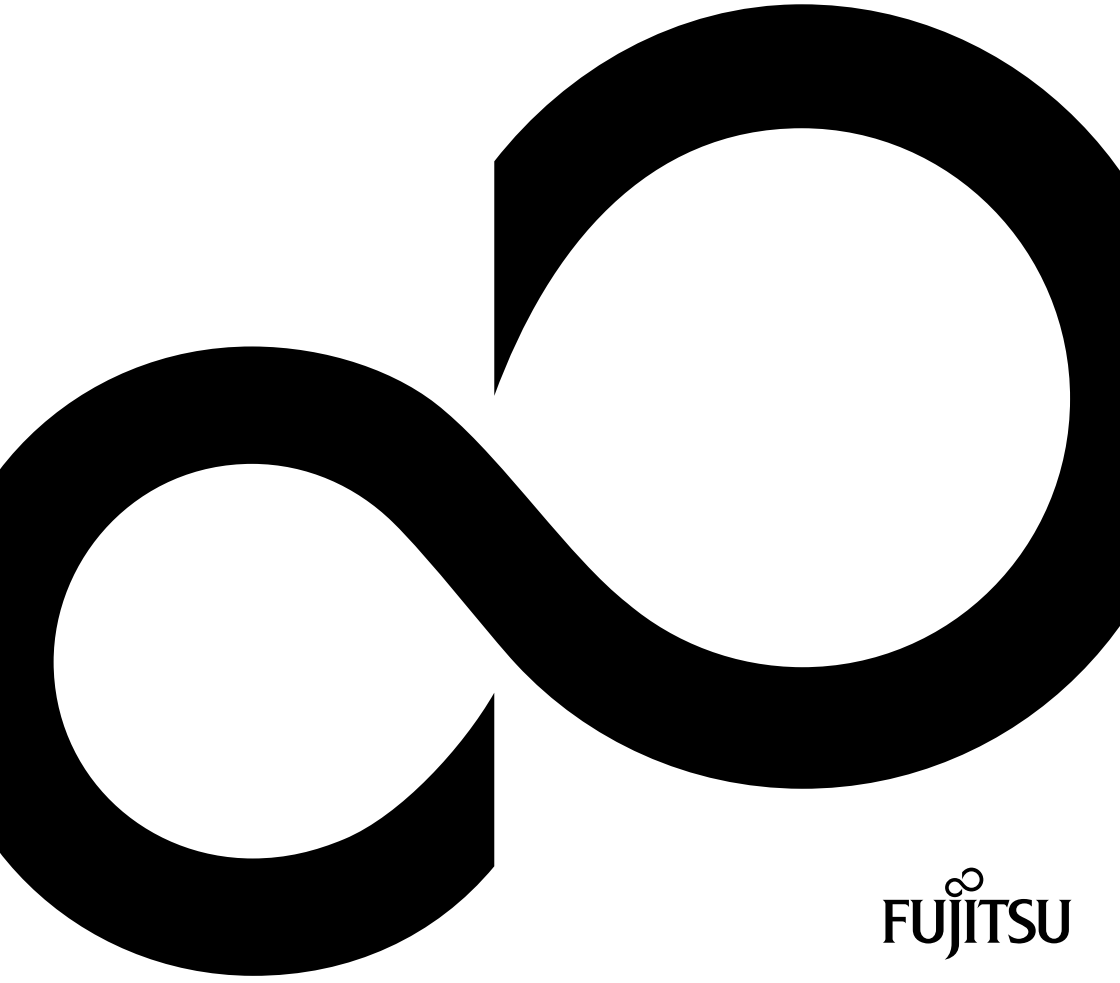
iAMT 12



FUJITSU

Thank you for buying an innovative product from Fujitsu.

The latest information about our products, tips, updates etc. can be found on the Internet at: "http://www.fujitsu.com/fts/"

You can find driver updates at: "http://support.ts.fujitsu.com/download"

Should you have any technical questions, please contact:

- our Hotline/Service Desk (see the Service Desk list or visit: "http://support.ts.fujitsu.com/contact/servicedesk")
- Your sales partner
- Your sales office

We hope you enjoy using your new Fujitsu system!

Published by / Contact address in EU
Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Straße 8
80807 Munich, Germany

http://www.fujitsu.com/fts/

Publication Date
08/2018

Order No.: A26361-K333-Z321-1-7419, edition 5

iAMT 12

Operating Manual

Remarks

Notes on the product description are consistent with the design specifications from Fujitsu and are made available for comparison purposes. The actual results may differ due to several factors. Technical data is subject to change without notification. Fujitsu does not accept any responsibility for technical or editorial errors or omissions.

Trademarks

Fujitsu and the Fujitsu logo are registered trademarks of Fujitsu Limited or its subsidiaries in the United States and other countries.

Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries

Intel, the Intel logo, Intel® Core, Intel® Centrino and Intel® vPro are trademarks or registered trademarks of Intel Corporation.

All other trademarks mentioned here are the property of their particular owner.

Inhalt

Darstellungsmittel

	kennzeichnet Hinweise, bei deren Nichtbeachtung Ihre Gesundheit, die Funktionsfähigkeit Ihres Geräts oder die Sicherheit Ihrer Daten gefährdet sind. Die Gewährleistung erlischt, wenn Sie durch Nichtbeachtung dieser Hinweise Defekte am Gerät verursachen
	kennzeichnet wichtige Informationen für den sachgerechten Umgang mit dem Gerät
►	kennzeichnet einen Arbeitsschritt, den Sie ausführen müssen
↳	kennzeichnet ein Resultat
`Diese Schrift`	kennzeichnet Eingaben, die Sie mit der Tastatur in einem Programm-Dialog oder in einer Kommandozeile vornehmen, z. B. Ihr Passwort (**`Name123`**) oder einen Befehl, um ein Programm zu starten (**`start.exe`**)
`Diese Schrift`	kennzeichnet Informationen, die von einem Programm am Bildschirm ausgegeben werden, z. B.: `Die Installation ist abgeschlossen!`
Diese Schrift	kennzeichnet • Begriffe und Texte in einer Softwareoberfläche, z. B.: Klicken Sie auf *Speichern*. • Namen von Programmen oder Dateien, z. B. *Windows* oder *setup.exe*.
"Diese Schrift"	kennzeichnet • Querverweise auf einen anderen Abschnitt z. B. "Sicherheitshinweise" • Querverweise auf eine externe Quelle, z. B. eine Webadresse: Lesen Sie weiter auf "http://www.fujitsu.com/fts" • Namen von CDs, DVDs sowie Bezeichnungen und Titel von anderen Materialien, z. B.: "CD/DVD Drivers & Utilities" oder Handbuch "Sicherheit/Regularien"
Taste	kennzeichnet eine Taste auf der Tastatur, z. B: F10
Diese Schrift	kennzeichnet Begriffe und Texte, die betont oder hervorgehoben werden, z. B.: **Gerät nicht ausschalten**

Intel® Active Management Technology

Die Intel-Technologie "Active Management Technology" / "iAMT" bietet Ihnen die Möglichkeit, Rechner mit *iAMT* in unterschiedlichen Systemzuständen fernzuverwalten. So besteht sogar bei beschädigter Festplatte oder defektem Betriebssystem auf einem *iAMT*-Client die Möglichkeit, via Fernwartung auf den Rechner zuzugreifen und Diagnosen durchzuführen, das System wiederherzustellen oder dessen Hardware zu verwalten.

Die *iAMT*-Technologie ist in der Hardware und Firmware des Rechners integriert. Für den Systemzugriff bedient sich die Lösung der Out-of-Band-Kommunikation (OOB-Kommunikation) und ist dabei unabhängig vom Status des Betriebssystems und auch davon, ob der Rechner ein- oder ausgeschaltet ist.

Voraussetzung für die Nutzung der *iAMT*-Technologie:

- der Rechner muss mit dem Netzwerk verbunden sein
- der Rechner muss mit dem Stromnetz verbunden bzw. der Akku muss ausreichend geladen sein
- um die 0-Watt-Funktion und die Manageability-Funktionen gleichzeitig nutzen zu können, müssen sie im BIOS Setup ein Manageability-Intervall einstellen, in dem der Rechner mit dem Stromnetz verbunden ist

Im 0-Watt-Betrieb sind die Manageability-Funktionen ausgeschaltet.

Weitere Informationen finden Sie im Intel vPro™ Expert Center: "http://www.intel.com/go/vproexpert"

Systemvoraussetzungen

Client-Rechner mit iAMT

Weitere Informationen zur *iAMT*-Unterstützung, entnehmen Sie bitte dem Datenblatt Ihres Rechners.

Hardware	• Integrierte *iAMT*-Funktion und LAN-Anschluss • Rechner (mit *iAMT*) ans Netzwerk angeschlossen
Software	Keine besonderen Voraussetzungen

Administrator-Rechner

Hardware	• LAN-Anschluss • Rechner im Netzwerk angemeldet
Software	• Windows • *iAMT*-fähige Management-Software

Funktionsübersicht

Einige der Funktionen müssen vor einer Verwendung konfiguriert werden.

Setup und Konfiguration

Installation und Vorbereitung des *iAMT*-Clients, um *iAMT*-Funktionen ausführen zu können.

Real Time Inventory

Die grundlegenden Inventar-Daten der Hardware stehen in unterschiedlichen Systemzuständen zur Verfügung. Unter anderem sind dies Informationen zum Mainboard, zum Prozessor- und Speicherausbau sowie zu den eingebauten Festplatten und optischen Laufwerken.

Eventlog

Die Systemüberwachung wird unabhängig vom Zustand auf dem *iAMT*-Client ausgewertet. Vorkonfigurierte Alarme werden ggf. standardisiert an eine entsprechend konfigurierte Administrator-Konsole gesendet.

Serial over LAN

Um BIOS-Einstellungen zu ändern, kann von einer Administrator-Konsole während des Boot-Vorgangs der Bildschirm und die Tastatur des *iAMT*-Clients übernommen werden (ANSI-Terminal, nur Textmodus).

Die BIOS-Eingabemaske kann während der Fernwartung für den lokalen Anwender gesperrt sein.

KVM (Keyboard, Video, Maus)

KVM erlaubt die Fernsteuerung des Rechners über Maus und Tastatur auf den Rechner schon beim Bootvorgang auch wenn sich das System in einem undefinierten Zustand befindet. Der Bildschirminhalt des ferngesteuerten Rechner wird angezeigt. Damit kann z.B. auch die Installation des Betriebssystems ferngesteuert werden. Es ist keine zusätzliche Software auf dem Client erforderlich. Voraussetzung für KVM ist eine aktive, integrierte Grafik und vPro™ System, das den vPro™ Anforderungen genügt.

Remote Alarm Clock

Ein Rechner kann mit dieser Funktion zu einer vordefinierten Zeit aufgeweckt werden. Da der PC der aktive Teil ist, ist die Funktion auch außerhalb eines Firmennetzwerkes (z. B. Heimarbeitsplätzen) verfügbar. Die Funktion kann zentral über die Management-Software programmiert werden, falls die Management-Software diese Funktion unterstützt.

Storage Redirection

Mit der Storage Redirection Technologie können entsprechend der iAMT-Generation entweder USB- oder IDE-Laufwerke (Floppy, CD, DVD und ISO-Image) auf den *iAMT*-Client "gespiegelt" werden. Der *iAMT*-Client sieht diese Laufwerke als lokale Laufwerke. So kann z. B. der *iAMT*-Client mit dem Image auf einer bootbaren CD/DVD im Laufwerk des Administrator-Rechners gestartet werden.

NVRAM

Basis-Inventar-Daten, Eventkonfigurationen und frei formatierbare nutzerabhängige Daten (z. B. Software Inventory, Bilder, Dateien usw.) werden in einem nicht flüchtigen Speicher (non volatile RAM = NVRAM) gespeichert.

Power State Management - Remote on/off

Von der Administrator-Konsole aus kann der *iAMT*-Client gestartet, beendet oder ein Beenden/Starten-Zyklus durchgeführt werden (auch wenn z. B. das Betriebssystem nicht mehr reagiert).

Das System wird ohne Vorwarnung für den Anwender gestoppt.

System Defence

iAMT erkennt am Netzwerk-Traffic ob evtl. ein Virenbefall vorliegt, z. B. anhand der Anzahl abgehender E-Mails pro Minute. Wird ein potentieller Virenbefall erkannt, kann der Rechner vom Netzwerk isoliert werden. Der Zugriff per Remote Control ist aber weiterhin möglich.

Agent Presence

Mit dieser Funktion können wichtige Dienste (z. B. von Virenscannern) bei der *iAMT*-Firmware zur Überwachung registriert werden. Wird ein überwachter Dienst versehentlich gestoppt oder gelöscht, sendet *iAMT* eine Alarmmeldung an den Administrator.

Audit Log

Alle sicherheitsrelevanten OOB-Aktionen des Administrators werden protokolliert.

Remote Assistance / Client Initiated Remote Access (CIRA)

Die Funktion ist nur verfügbar, wenn diese durch den Service Provider oder Ihre EDV-Abteilung entsprechend konfiguriert wurde.

Der *iAMT*-Client baut zu Diagnose- und Wartungszwecken zu einem sog. "Managed Presence Server (MPS)"-Server eine sichere OOB-Remote-Verbindung auf. Mit dieser Verbindung kann der Client über das Internet sicher verwaltet werden. Die Verbindung erlaubt dem autorisierten Administrator den Zugriff zu allen OOB-Funktionen.

- **Fast Call for Help**
  Mit der Tastenkombination CTRL + ALT + F1 kann eine IT-Soforthilfe durch den Anwender initiiert werden. Dies funktioniert auch wenn das Betriebssystem defekt ist oder der Rechner nicht mehr startet.
- **Intel® Remote-PC-Assist-Technik (Intel® RPAT)**
  RPAT erlaubt es dem technischen Support, nach einem Fast Call for Help, eine Verbindung zum *iAMT*-Client aufzubauen, um ein Problem auf dem Rechner zu lösen.

Virtual Private Network (VPN) Support

Damit werden In-Band Zugriffe auf *iAMT*-Systeme unterstützt, die über VPN mit dem Netzwerk verbunden sind.

Measured iAMT

Alle Vorgänge der Management Engine (ME) werden überprüft. Wenn der HASH-Wert der Firmware mit einer „WhiteList“ nicht übereinstimmt, wird der Boot-Vorgang abgebrochen. Damit werden unberechtigte Patches der ME unterbunden.

Support for Microsoft Network Access Protection (MS-NAP) / Cisco Network Admission Control (Cisco NAC)

Clients, die sich an einem Netzwerk anmelden, welches durch MS-NAP oder Cisco NAC geschützt ist, werden einer Sicherheitsprüfung unterzogen, bevor sie Zugang zum Netzwerk erhalten.

Der *iAMT*-Client reagiert auf die NAP-/NAC-Anfragen des Servers und stellt sicher, dass AMT-Systeme nicht gesperrt werden.

Support for DASH 1.0/1.1/1.2

DASH (Desktop and mobile Architecture for System Hardware) ist ein DMTF-Standard. Dieser stellt Spezifikationen für das System-Management zur Optimierung des Remote-Zugriffs zur Systemüberwachung, Systemorganisation und Systemwartung dar.

Dieser Standard steht auch dann zur Verfügung, wenn das Betriebssystem nicht verfügbar ist (z. B. im Schlaf-Modus).

Weitere Informationen finden Sie im Internet unter "www.dmtf.org".

Boot Control

Ermöglicht die Remote-Auswahl des Boot-Laufwerks.

IPv6

Unterstützung der Internet Protokoll Version 6.

Alerting

System kann Alarmmeldungen, basierend auf definierten Voreinstellungen, zur Management Konsole senden.

Wireless Management in Sleep States

iAMT ist vorbereitet, um Notebooks oder Desktops mit den entsprechenden Intel-WLAN-Karten mit einem integrierten Intel-WLAN-Anschluss drahtlos zu managen.

Folgende Funktionen sind möglich:

- Remote-Boot des Computers
- Ereignisprotokolle abrufen
- BIOS-Zugriff
- Out Of Band-Alarmierung (OOB-Alarmierung)

Auf den Computer kann nur dann ferngesteuert zugegriffen werden, wenn er am Stromnetz angeschlossen oder wenn er eingeschaltet ist.

Hardwareinventory

Remote-Abfrage der Hardware-Komponenten des Systems.

Host Based Configuration (HBC)

HBC ist eine einfache Methode um AMT zu konfigurieren. Bei HBC ist für die Konfiguration kein Zertifikatserver notwendig. Die Konfigurationsdaten für AMT werden mittels einer Applikation auf dem Zielsystem während des laufenden Betriebs in die Management Engine (ME) übertragen. Dabei sind folgende Einschränkungen zu beachten:

- System Defense ist ausgeschaltet
- User Consent wird für alle Redirection Operationen und Änderungen beim Boot Prozess benötigt

Firmware Update

Das Update der Firmware wird über das *iAMT*-Setup oder eine spezielle Management-Software durchgeführt.

IPT (Identity Protection Technology)

IPT bietet eine einfache Möglichkeit um zu prüfen, ob sich ein Anwender von einem vertrauenswürdigen PC für eine Online-Transaktion anmeldet. Der One Time Code (Passwort) wird, isoliert vom System, in der Management Engine (ME) erzeugt und von einem Drittanbieter-Security-ISV (Independent Software Vendor) der Webseiten validiert.

Graceful Power Operations

Frühere AMT-Versionen unterstützten nur “hartes” Abschalten. Seit AMT9 ist nun auch ordnungsgemäßes Herunterfahren / Neu starten möglich. Falls das Betriebssystem normales Herunterfahren unterstützt, interagiert die ME FW mit dem ME-Treiber, um es zu starten. Ein Hinweis wird angezeigt und informiert den Benutzer darüber, dass eine solche Remote-Aktion eingeleitet worden ist und nun ausgeführt wird.

Unterstützte iAMT-Funktionen

Funktion	iAMT 12	iAMT 11	iAMT 10	iAMT Standard-manageability
Remote Configuration	X	X	X	X
Real Time Inventory	X	X	X	X
Eventlog	X	X	X	X
Serial over LAN	X	X	X	X
KVM	X	X	X	–
Remote Alarm Clock	X	X	X	–
Storage Redirection	USB	USB	IDER	USB(ME11) / IDER(<=ME10)
NVRAM	X	X	X	X
Remote on / off	X	X	X	X
System Defense	X	X	X	X
Agent Presence	X	X	X	X
Audit Log	X	X	X	X
Remote Assistance / Client Initated Remote Access	X (nur LIFEBOOK)	X (nur LIFEBOOK)	X (nur LIFEBOOK)	–
VPN Support	X	X	X	–
Measured iAMT	X	X	X	–
NAP Support	X	X	X	–
NAC Support	–	–	–	–
Support for DASH 1.0/1.1	X	X	X	X
Boot control	X	X	X	X
Power State Management	X	X	X	X
IP v6	X	X	X	X
Alerting	X	X	X	X
Wireless Management in Sleep States	X	X (nur LIFEBOOK)	X (nur LIFEBOOK)	–
Hardwareinventory	X	X	X	X
Host Based Configuration (HBC)	X	X	X	X
IPT	X	X	X	–
Graceful Power Operations	X	X	X	X

iAMT aktivieren

Die Einstellungen für *ME* und *iAMT* können lokal im Menü *MEBx* geändert werden.

- *ME* = Management Engine ist die zentrale Komponente von Intel AMT
- *iAMT* = die Manageability-Funktion der *ME*
- *MEBx* (**M**anageability **E**ngine **B**IOS E**x**tension) = Erweiterung des BIOS um die Eigenschaften von *ME* und *iAMT* einzustellen

MEBx aufrufen

Beim Bootvorgang erscheint am Bildschirm für ca. 2 Sekunden die Meldung:

`Press CTRL-P to enter Intel® ME Setup.`

► Drücken Sie in dieser Zeit die Tastenkombination CTRL (oder auf der deutschen Tastatur STRG) und P.

Sollte die Aufforderung nicht erscheinen, müssen sie diese erst im BIOS Setup aktivieren. Standardmäßig ist die Meldung bei Desktopsystemen und Workstation deaktiviert. Weitere Informationen erhalten Sie im BIOS Handbuch.

Beachten Sie bei der Passwortvergabe, dass im BIOS das US-amerikanische Tastaturlayout aktiviert ist. Es sind z. B. die Tasten Z und Y vertauscht.

↳ Das Passwort muss folgende Bedingungen erfüllen:

- 8 – 32 Zeichen lang
- Mindestens eine Zahl
- Mindestens ein nicht alpha-numerisches Zeichen, z.B. !,$,;
- Mindestens ein Großbuchstabe und mindestens ein Kleinbuchstabe

Folgende Zeichen dürfen nicht verwendet werden:

- , (Komma)
- ’ (Hochkomma)
- : (Doppelpunkt)

Jetzt können Sie die *iAMT*-Funktionen über das *MEBx*-Menü konfigurieren.

Eine ausführliche Beschreibung aller Menüpunkte des *MEBx*-Menüs für die aktuelle *AMT*-Version finden Sie in der Intel-Dokumentation Intel® Management Engine BIOS Extension: "http://communities.intel.com/community/openportit/vproexpert?view=documents"

Allgemeine Sicherheitsvorkehrungen

Bei allen Systemen, die noch nicht für iAMT-Management konfiguriert wurden bzw. nicht für iAMT-Management vorgesehen sind, ist das Standard-ME-Passwort aktiv. Es wird empfohlen, das Standard-ME-Passwort vor dem produktiven Einsatz der Systeme zu ändern und ein sicheres BIOS-Admin-Passwort zu vergeben, um das Zurücksetzen der iAMT-Konfiguration abzusichern.

Um einen unrechtmäßigen Zugriff zu unterbinden, wurden bei Client-Systemen ab AMT 11 zwei zusätzliche BIOS-Menüs unter *Advanced ->AMT Configuration* integriert:

- Ausführen der MEBx (CTRL + P), wie im Kapitel "MEBx aufrufen", Seite 10 - Deutsch beschrieben.
- USB Provisioning

  Provisionierungsmethode, bei der ein lokal am System angeschlossener USB-Key mit Konfigurierungsdaten für iAMT verwendet wird.

Das Ausschalten dieser Funktionen und die Absicherung des BIOS-Setup per Admin-Kennwort schützen vor unrechtmäßigem lokalem Zugriff bei Systemen, die nicht für iAMT-Management konfiguriert bzw. vorgesehen sind.

Eine detaillierte Beschreibung zu diesen Menüs finden Sie im BIOS-Handbuch.

Contents

Notational conventions

	Pay particular attention to text marked with this symbol. Failure to observe these warnings could pose a risk to health, damage the device or lead to loss of data. The warranty will be invalidated if the device becomes defective through failure to observe these warnings.
	Indicates important information for the proper use of the device.
►	Indicates an activity that must be performed
↳	Indicates a result
`This font`	indicates data entered using the keyboard in a program dialogue or at the command line, e.g. your password (**`Name123`**) or a command used to start a program (**`start.exe`**)
`This font`	indicates information that is displayed on the screen by a program, e.g.: `Installation is complete.`
This font	indicates • terms and texts used in a software interface, e.g.: Click on *Save* • names of programs or files, e.g. *Windows* or *setup.exe*.
"This font"	indicates • cross-references to another section, e.g. "Safety information" • cross-references to an external source, e.g. a web address: For more information, go to "http://www.fujitsu.com/fts/" • Names of CDs, DVDs and titles or designations for other materials, e.g.: "CD/DVD Drivers & Utilities" or "Safety/Regulations" manual
Key	indicates a key on the keyboard, e.g: F10
This font	indicates terms and texts that are emphasised or highlighted, e.g.: **Do not switch off the device**

Intel® Active Management Technology

Intel's "Active Management Technology" / "iAMT" allows computers with *iAMT* to be remotely administered in various system modes. Even if the hard disk on an *iAMT* client is damaged or the operating system is faulty, it is possible to gain remote maintenance access to the computer to carry out diagnostics, system recovery or hardware management.

The *iAMT* technology is integrated into the computer's hardware and firmware. System access is granted via Out of Band (OOB) communication; this is independent of the status of the operating system and of whether or not the computer is switched on.

Requirements for using *iAMT* technology:

- The computer must be connected to the network
- The computer must be connected to the power supply or the rechargeable battery must be adequately charged
- To use the 0-Watt function and the manageability functions at the same time, you must set a Manageability Interval in the BIOS Setup while the computer is connected to mains power.

In 0-Watt mode the manageability functions are switched off.

For further information visit the Intel vPro™ Expert Center: "http://www.intel.com/go/vproexpert"

System requirements

Client computer with iAMT

For further information on *iAMT* support, please refer to the datasheet for your computer.

Hardware	• Integrated *iAMT* function and LAN port • Computer (with *iAMT*) connected to the network
Software	No special requirements

Administrator computer

Hardware	• LAN port • Computer logged on to network
Software	• Windows • *iAMT*-capable management software

Function overview

Some of the functions must be configured before use.

Setup and Configuration

Installation and initialisation of the *iAMT* client, to allow *iAMT* functions to be performed.

Real time inventory

The basic hardware inventory data is available in various system states. This includes information relating to the main board, processor, memory and installed hard disks and optical drives.

Event log

System monitoring is evaluated regardless of the status on the *iAMT* client. Where required, pre-configured alarms are sent in a standard way to a suitably configured administrator console.

Serial over LAN

In order to change BIOS settings, an administrator console can take over the screen and keyboard of the *iAMT* client during the boot-up process (ANSI terminal, text mode only).

The BIOS input mask can be disabled for local users during remote access maintenance.

KVM (Keyboard, Video, Mouse)

KVM allows remote access to the computer via mouse and keyboard including during the boot process, even if the system is in an undefined state. The screen content of the remotely controlled computer is displayed. In this way it is even possible to install the operating system remotely. No additional software is needed on the client. KVM requires an active, integrated graphics and vPro™ system which meets the vPro™ requirements.

Remote alarm clock

This function allows a computer to be woken up at a predetermined time. Since the PC is the active element, this function can also be accessed from outside a corporate network (from a home workstation, for example). The function can be programmed centrally via the management software, provided the management software supports this function.

Storage Redirection

Storage Redirection technology allows USB or IDE drives (floppy, CD, DVD and ISO image) to be "mirrored" on the *iAMT* client, according to the iAMT generation. The *iAMT* client sees these drives as local drives. This means, for example, that the *iAMT* client can be started using an image on a bootable CD/DVD located in a drive on the administrator computer.

NVRAM

Basic inventory data, event configurations and freely-formattable, user-dependent data (e.g. software inventory, images, files etc.) can be saved in non-volatile memory (non-volatile RAM = NVRAM).

Power State Management - Remote on/off

Working from the administrator console, the *iAMT* client can be started or stopped, or a stop/start cycle can be performed (even if the operating system is no longer responding, for example).

The system will be stopped for the users, without prior warning.

System Defense

iAMT detects any virus attack in the network traffic, for example based on the number of outgoing e-mails per minute. If a potential virus attack is recognised, the computer can be isolated from the network. Remote control access remains possible, however.

Agent presence

This function can be used to register important services (e.g. virus scanners) for monitoring on the *iAMT* firmware. If a monitored service is accidentally stopped or deleted, *iAMT* sends an alarm message to the administrator.

Audit log

All security-related OOB actions of the administrator are logged.

Remote Assistance / Client Initiated Remote Access (CIRA)

This function is only available if it has been appropriately configured by the service provider or your IT department.

The *iAMT* client establishes a secure OOB remote connection to a "Managed Presence Server (MPS)" for diagnosis and maintenance purposes. This connection allows the client to be administered securely over the Internet. The connection allows the authorised administrator access to all OOB functions.

- **Fast Call for Help**
  The key combination CTRL + ALT + F1 can be used to ask for immediate help. This works even if the operating system is faulty or the computer will not start.
- **Intel® Remote PC Assist Technology (Intel® RPAT)**
  After a Fast Call for Help, RPAT allows technical support to establish a connection with the *iAMT* client in order to resolve a problem on the computer.

Virtual Private Network (VPN) Support

This supports in-band accesses to *iAMT* systems which are connected to the network via VPN.

Measured iAMT

All processes of the management engine (ME) are checked. If the HASH values of the firmware do not agree with a "whitelist", the boot process will be terminated. This blocks unauthorised ME patches.

Support for Microsoft Network Access Protection (MS-NAP) / Cisco Network Admission Control (Cisco NAC)

Clients which log into a network which is protected by MS-NAP or Cisco NAC will undergo a security test before they are granted access to the network.

The *iAMT* client reacts to the NAP/NAC queries from the server and ensures that AMT systems are not blocked.

Support for DASH 1.0/1.1/1.2

DASH (Desktop and mobile Architecture for System Hardware) is a DMTF standard. It provides specifications for system management used to optimise remote access for system monitoring, system organization and system maintenance.

This standard remains available even when the operating system is not available (e.g. in sleep mode).

You will find more information on the following website: "www.dmtf.org".

Boot Control

Allows the boot drive to be selected remotely.

IPv6

Support for Internet Protocol version 6.

Alerting

The system can send alarm messages based on pre-defined settings to the management console.

Wireless Management in Sleep States

iAMT is prepared for wireless management of notebooks or desktops with corresponding Intel WLAN cards with an integrated Intel WLAN port.

The following functions are possible:

- Boot the computer remotely
- Call up event logs
- BIOS access
- Out Of Band (OOB) alarms

The computer can only be remotely accessed if it is connected to mains power or if it is switched on.

Hardware inventory

Remote querying of the hardware components of the system.

Host Based Configuration (HBC)

HBC is a simple method for configuring AMT. With HBC, a certificate server is not necessary for the configuration. The configuration data for AMT is transferred into the Management Engine (ME) using an application on the target system while the machine is operating. The following limitations must be considered here:

- System Defense is switched off
- User Consent is needed for all redirection operations and changes during the boot process

Firmware Update

The firmware is updated via the *iAMT* setup or using special management software.

IPT (Identity Protection Technology)

IPT is an easy way of checking if a user is using a trustworthy PC to log in for an online transaction. The One Time Code (password) is generated in the Management Engine (ME), isolated from the system, and validated by a third-party security ISV (Independent Software Vendor) of the website.

Graceful Power Operations

Earlier AMT versions support only “hard” power operations. Since AMT9 graceful power operations will be available. If the OS supports graceful power operations, the ME FW interacts with the ME driver to initiate it. A notification is displayed informing the user that a remote power operation was triggered and now is executed.

Supported iAMT functions

Function	iAMT 12	iAMT 11	iAMT 10	iAMT Standard manageability
Remote Configuration	X	X	X	X
Real time inventory	X	X	X	X
Event log	X	X	X	X
Serial over LAN	X	X	X	X
KVM	X	X	X	–
Remote alarm clock	X	X	X	–
Storage Redirection	USB	USB	IDER	USB(ME11) / IDER(<=ME10)
NVRAM	X	X	X	X
Remote on/ off	X	X	X	X
System Defense	X	X	X	X
Agent presence	X	X	X	X
Audit log	X	X	X	X
Remote Assistance / Client Initiated Remote Access	X (LIFEBOOK only)	X (LIFEBOOK only)	X (LIFEBOOK only)	–
VPN support	X	X	X	–
Measured iAMT	X	X	X	–
NAP support	X	X	X	–
NAC support	–	–	–	–
Support for DASH 1.0/1.1	X	X	X	X
Boot control	X	X	X	X
Power State Management	X	X	X	X
IP v6	X	X	X	X
Alerting	X	X	X	X
Wireless Management in Sleep States	X	X (LIFEBOOK only)	X (LIFEBOOK only)	–
Hardware inventory	X	X	X	X
Host Based Configuration (HBC)	X	X	X	X
IPT	X	X	X	–
Graceful Power Operations	X	X	X	X

Enable iAMT

The settings for *ME* and *iAMT* can be changed locally in the *MEBx* menu.

- *ME* = Management Engine is the central component of Intel AMT
- *iAMT* = the manageability function of *ME*
- *MEBx* (**M**anageability **E**ngine **BI**OS E**x**tension) = extension of the BIOS for setting the properties of *ME* and *iAMT*

Calling MEBx

During the boot process, the following message appears on the monitor for about 2 seconds:

`Press CTRL-P to enter Intel® ME Setup.`

► During this time, press the key combination CTRL (or on a German keyboard STRG) and P.
If the request does not appear, you must first enable it in the BIOS Setup. On desktop systems and workstations, the message is disabled by default. Please refer to the BIOS Manual for more information.

When assigning passwords, be aware that the US American keyboard layout is enabled in the BIOS. For example, the Z and Y keys are switched.

↳ The password must meet the following criteria:
- 8 – 32 characters long
- At least one character must be a number
- There must be at least one non-alphanumeric character such as !,$,;
- There must be at least one upper-case and at least one lower-case character

The following characters may not be used:
- , (comma)
- ’ (apostrophe)
- : (colon)

You can now configure the *iAMT* functions via the *MEBx* menu.

You will find a comprehensive description of all the items in the *MEBx* menus for the current *AMT* version in the Intel documentation, Intel® Management Engine BIOS Extension: "http://communities.intel.com/community/openportit/vproexpert?view=documents"

General safety precautions

For all systems that have not yet been configured for iAMT management or which are not intended for iAMT management, the default ME password is active. It is recommended that you change the default ME password before live use of the systems and assign a secure BIOS admin password, to prevent resetting of the iAMT configuration.

To prevent unauthorized access, two additional BIOS menus have been integrated under *Advanced ->AMT Configuration* in client systems with AMT 11:

- Run MEBx (CTRL + P), as described in chapter "Calling MEBx", Page 10 - English.
- USB Provisioning

  Provisioning method in which a locally connected USB key with configuration data is used for iAMT.

Deactivation of these functions and protection of the BIOS setup with an admin password offers protection against unauthorised local access on systems not configured or intended for iAMT management

For a detailed description of these menus, see the BIOS manual.