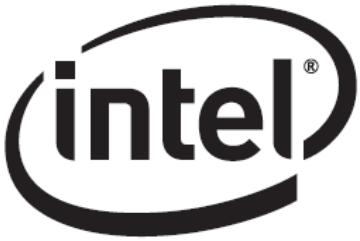

Intel® Desktop Board DQ57TM

Intel® vPro™ Technology Setup and Configuration Guide

July 2010
Order Number: G12102-001

Revision History

Revision	Revision History	Date
-001	First release of the Intel® vPro™ Technology Setup and Configuration Guide for Intel® Desktop Board DQ57TM	July 2010

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.

All Intel® desktop boards are evaluated as Information Technology Equipment (I.T.E.) for use in personal computers (PC) for installation in homes, offices, schools, computer rooms, and similar locations. The suitability of this product for other PC or embedded non-PC applications or other environments, such as medical, industrial, alarm systems, test equipment, etc. may not be supported without further evaluation by Intel.

Intel Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights.

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.

Intel desktop boards 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 before placing your product order.

Copies of documents which have an ordering number and are referenced in this document, or other Intel literature, may be obtained from:

Intel Corporation
P.O. Box 5937
Denver, CO 80217-9808

or call in North America 1-800-548-4725, Europe 44-0-1793-431-155, France 44-0-1793-421-777, Germany 44-0-1793-421-333, other Countries 708-296-9333.

Intel, Intel Core, and Intel vPro are trademarks of Intel Corporation in the U.S. and other countries.

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

Copyright © 2010 Intel Corporation. All rights reserved.

Contents

Figures

Tables

Preface

This Setup and Configuration Guide specifies the steps necessary for enabling the different features of Intel® vPro™ technology for the Intel® Desktop Board DQ57TM. It does not cover the various third-party software applications that take advantage of these features.

Intended Audience

This Guide is intended to provide detailed, technical information about the Intel Desktop Board DQ57TM and its components to the vendors, system integrators, and other engineers and technicians who need this level of information. It is specifically *not* intended for general audiences.

What This Document Contains

Chapter Description

1 A description of the supported hardware and Intel vPro technology features of the Intel Desktop Board DQ57TM and BIOS Setup details for Intel vPro technology and Intel® Active Management Technology (Intel® AMT)

2 References

Typographical Conventions

This section contains information about the conventions used in this specification. Not all of these symbols and abbreviations appear in all specifications of this type.

Other Common Notation

BIOS	Basic Input/Output System
DDR	Double Data Rate
DIMM	Dual In-line Memory Module
ECC	Error-Correcting Code
GB	Gigabyte (1,073,741,824 bytes)
GB/s	Gigabytes per second
Gb/s	Gigabits per second
KB	Kilobyte (1024 bytes)
Kbit	Kilobit (1024 bits)
kbits/s	1000 bits per second
KVM	Keyboard Video Mouse
LGA	Land Grid Array
MB	Megabyte (1,048,576 bytes)
MB/s	Megabytes per second
Mbit	Megabit (1,048,576 bits)
Mbits/s	Megabits per second
POST	Power On Self Test
UEFI	Unified Extensible Firmware Interface
VNC	Virtual Network Computing
xxh	An address or data value ending with a lowercase h indicates a hexadecimal value.

Feature Summary

Intel Desktop Board DQ57TM supports the Intel® Core™ i3, Intel® Core™ i5 and Intel® Core™ i7 processors in the LGA1156 package. It uses the Intel® Q57 Express Chipset to provide the latest in remote management via Intel® vPro™ technology. Table 1 summarizes the major Intel vPro technology features of the board.

Intel® vPro™ Technology	Intel® Active Management Technology (Intel® AMT) 6.0
	Intel® Trusted Execution Technology (Intel® TXT)
	Intel® Remote PC Assist (Intel® RPAT)
	Intel® KVM Remote Control
	Intel® Virtualization Technology (Intel® VT)
	Intel® Virtualization for Directed I/O (Intel® VT-d)
	Trusted Platform Module (TPM)

Table 1. Feature Summary

Note: Intel® Active Management Technology requires one of the following Intel® Core™ vPro™ processors: Intel® Core™ i5-650, Intel® Core™ i5-660, Intel® Core™ i5-670, Intel® Core™ i5-680, Intel® Core™ i7-860, Intel ® Core™ i7-860s, or Intel® Core™ i7-870 processor. Other Intel® Core™ processors will provide Intel® Standard Manageability only. In addition, only the Intel Core vPro processors with integrated Intel® HD graphics will support Intel® KVM Remote Control.

1. Intel® vPro™ Technology Setup and Configuration

1.1 BIOS Setup

1.1.1 Overview

The Intel Desktop Board DQ57TM BIOS interface is based upon the UEFI specification. As a result, most of the Intel® vPro™ technology features are accessed from the BIOS Setup screens. The menus of interest to the Intel vPro technology user are *Configuration*, *Security* and *Intel® Management Engine (Intel® ME)*. Table 2 lists the BIOS setup locations for setting the different features of Intel vPro technology.

Intel® vPro™ Technology Feature	BIOS Setup Menu
Trusted Platform Module (TPM)	Configuration / On-Board Devices
Intel Virtualization Technology (Intel VT)	Security
Intel Trusted Execution Technology (Intel TXT)	Security
Intel VT for Directed I/O (Intel VT-d)	Security
Intel Active Management Technology (Intel® AMT)	Intel ME

Table 2. Location of Intel vPro Technology Features in BIOS Setup

1.1.2 Entering BIOS Setup

To enter BIOS Setup, the user must press [F2] during the POST screen displayed shortly after power is applied to the board, as shown in Figure 1.

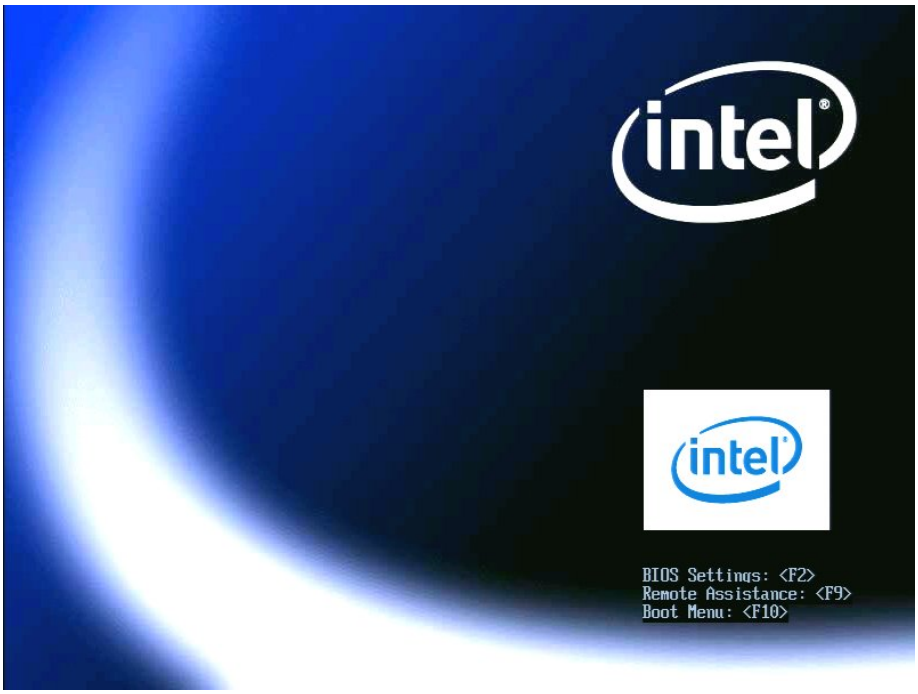

Figure 1. Intel Desktop Board DQ57TM POST Screen

Upon entering BIOS Setup, the user will be presented the BIOS Setup Main menu screen as shown in Figure 2.

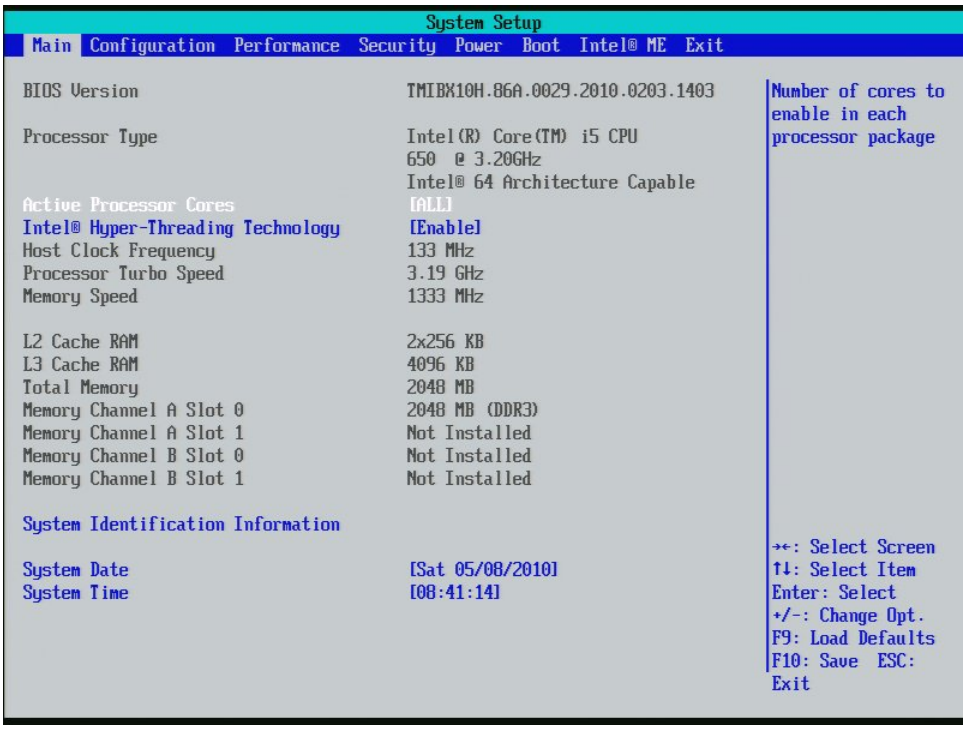

Figure 2. BIOS Setup - Main Menu

1.1.3 BIOS Setup – Configuration Menu

The Configuration Menu, shown in Figure 3, contains settings for On-Board Devices, as well as access to the system Event Log.

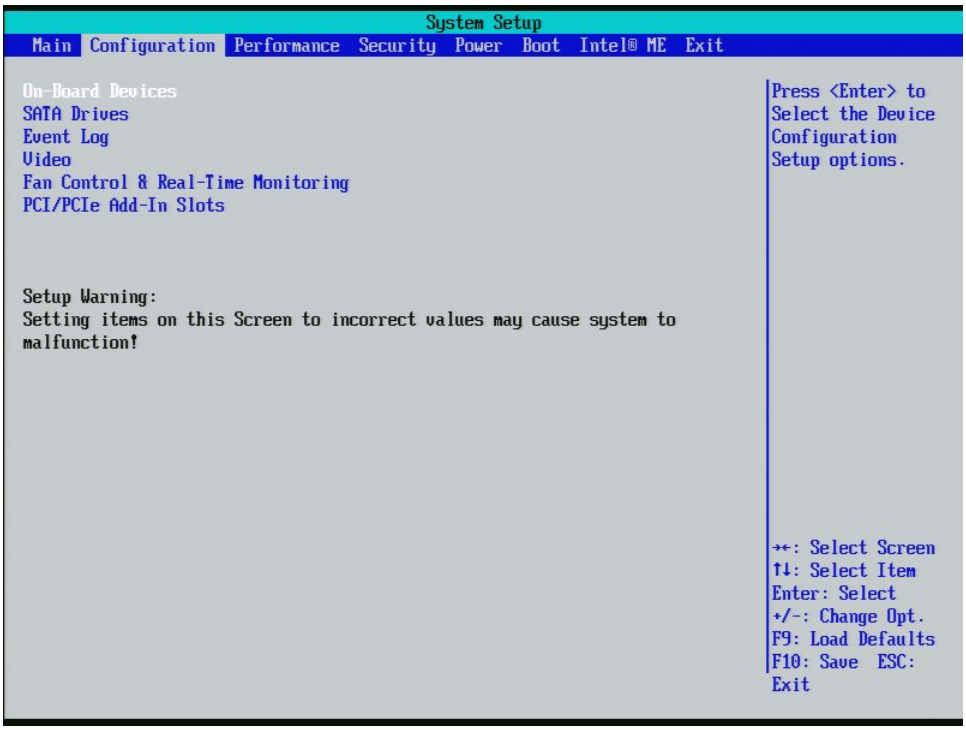

Figure 3. BIOS Setup - Configuration Menu

TPM is enabled or disabled by means of the Configuration / On-Board Devices menu as shown in Figure 4.

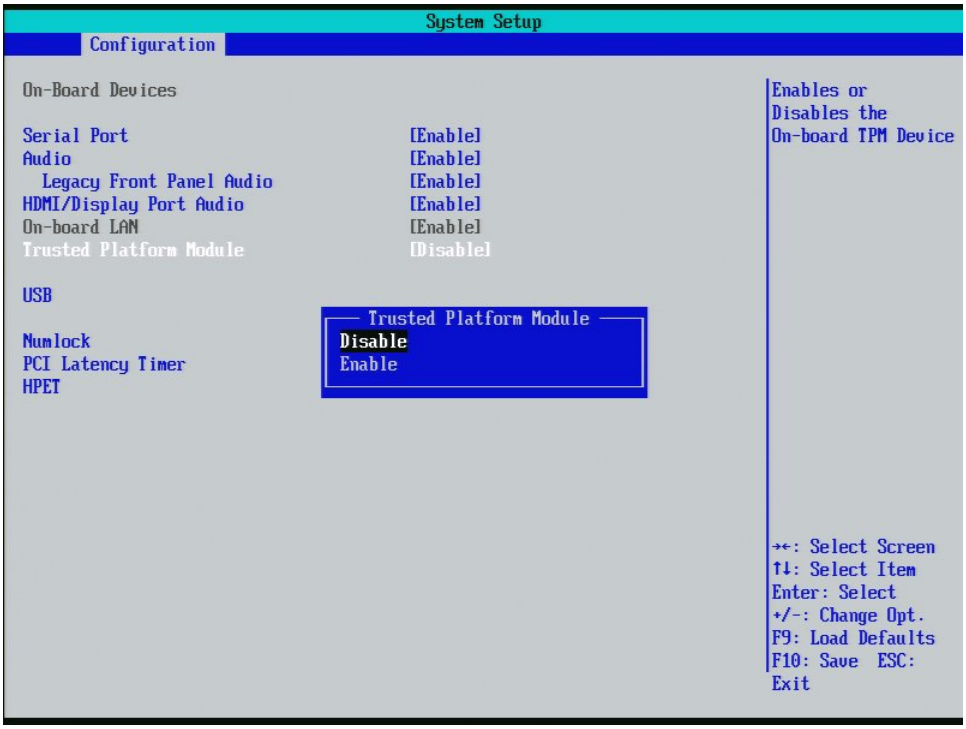

Figure 4. BIOS Setup - Configuration

In the Event Log screen, shown in Figure 5, the user can enable or disable Memory Correction.

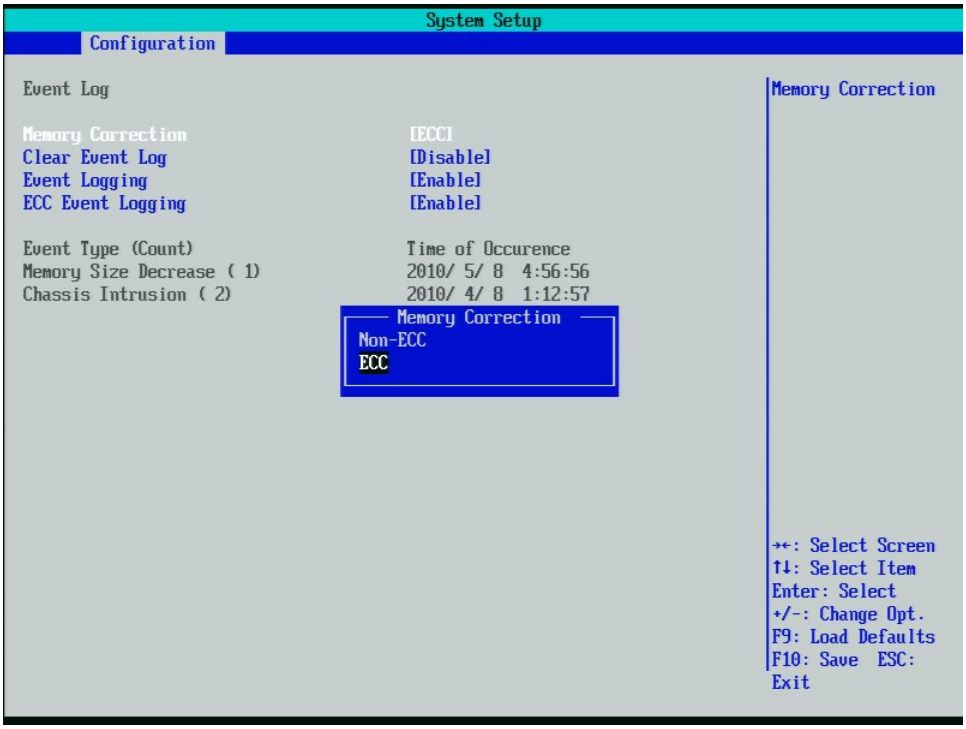

Figure 5. BIOS Setup - ECC Memory Correction

Note: Memory Correction requires the use of Intel® Xeon™ 3400-series processors and unbuffered ECC DDR3 DIMMs. This will result in Standard Manageability level of remote management features.

1.1.4 BIOS Setup – Security Menu

Figure 6 displays the Security menu. This menu gives you access to virtualization-related features such as Intel VT, Intel TXT and Intel VT-d. It also allows you to set passwords for platform- and hard drive-level security and to control the Execute Disable Bit (XD) technology and Chassis Intrusion features.

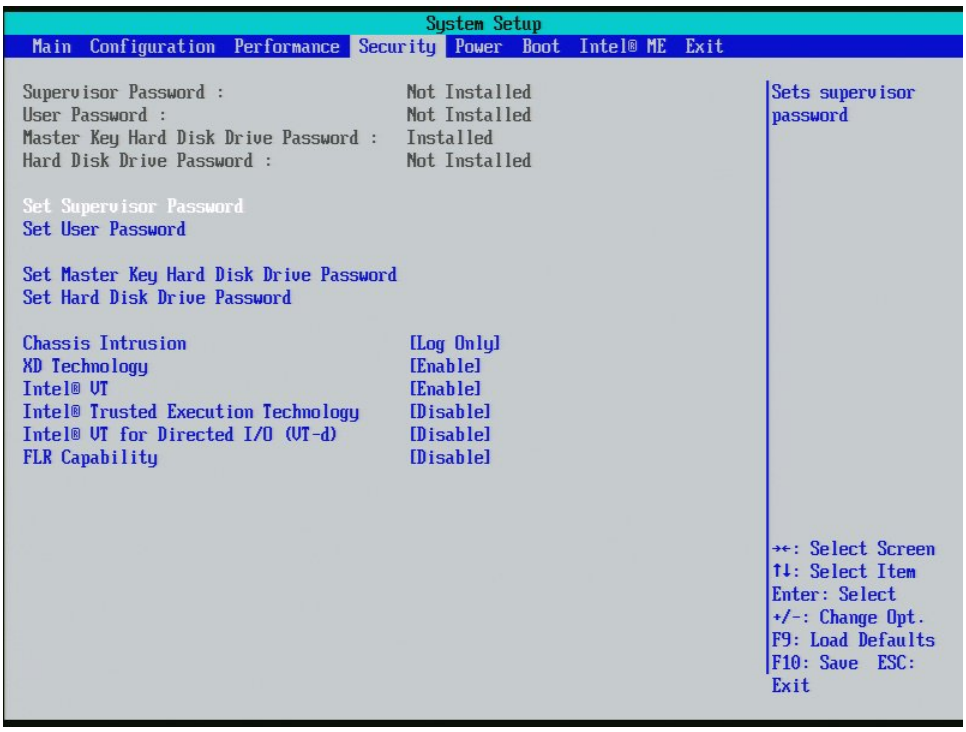

Figure 6. BIOS Setup - Security Menu

Note: Intel VT must be enabled before Intel TXT. Once Intel TXT is enabled, the user cannot disable Intel VT unless Intel TXT is disabled first.

Note: Setting the Master Key Hard Disk Drive Password will not enable Hard Disk Drive password security. Only by setting the Hard Disk Drive Password will the system pause during boot to ask for a password. At that time either the Hard Disk Drive Password or the Master Key Password (if set) will allow the system to proceed.

Note: The Supervisor Password controls access to the BIOS Setup menus. The User Password controls booting the platform and is separate from the Hard Disk Drive Password. The User Password is stored in the Intel Desktop Board DQ57TM non-volatile RAM and stays with the platform, whereas the Hard Disk Drive Password is stored directly on the HDD and is portable with it.

1.1.5 BIOS Setup – Intel® ME Menu

When first accessing the Intel ME menu, the user will be asked to change the default password of "*admin*". The new password must be at least eight characters long and be composed of upper- and lower-case letters, numbers and symbols (excluding colon, comma and double quotes). Figure 7 illustrates the initial Intel ME menu.

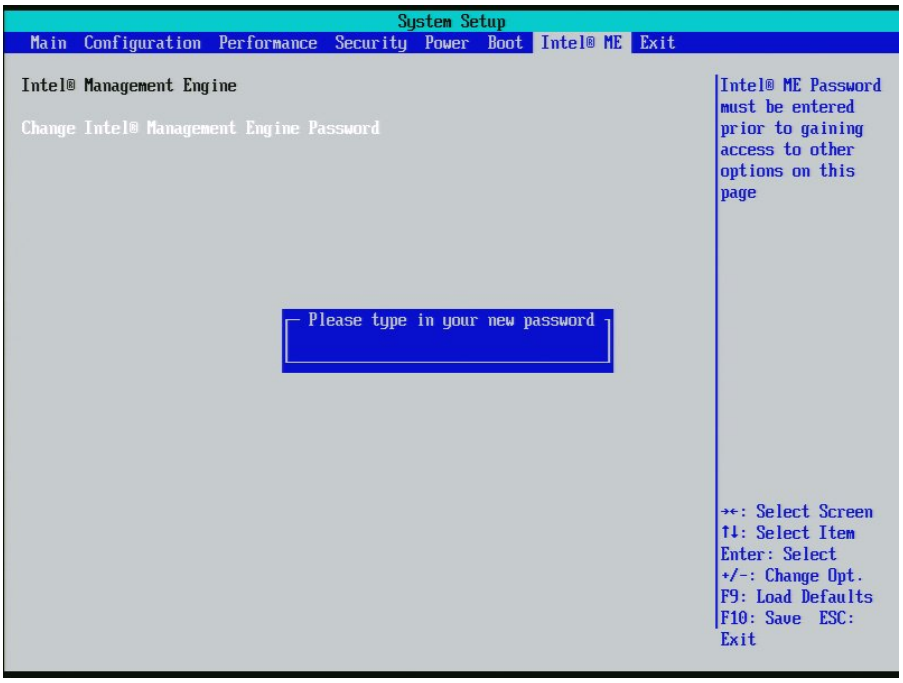

Figure 7. BIOS Setup – Intel® ME Menu

Once the administrator password is set, the user is presented the Intel ME main menu, shown in Figure 8.

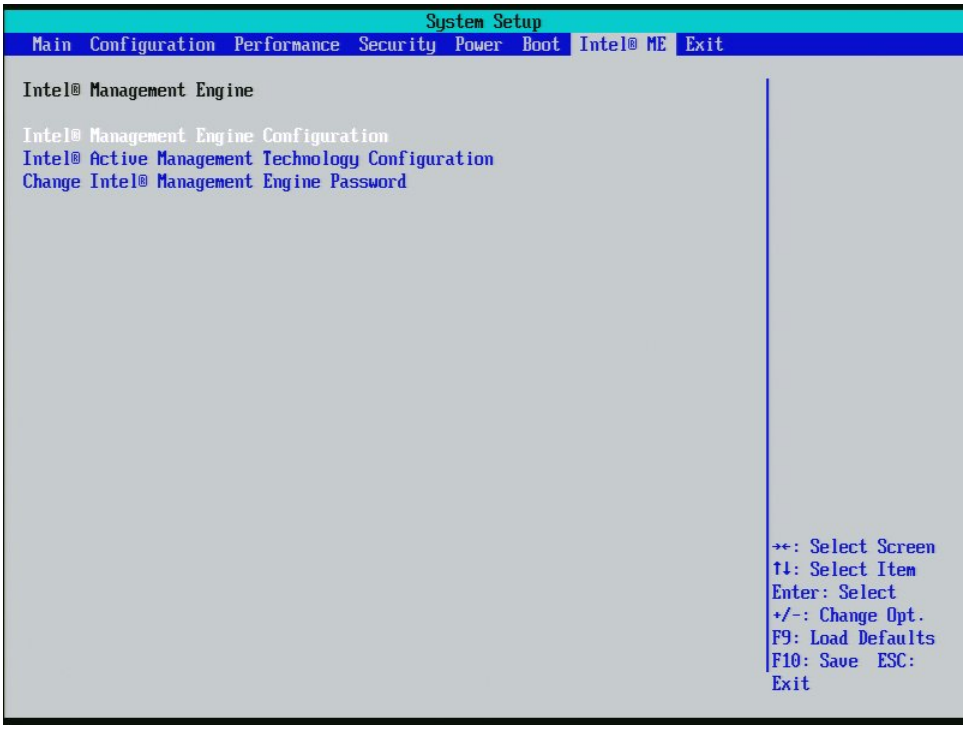

Figure 8. Intel ME - Main Menu

1.1.5.1 Intel ME – Intel ME Configuration

Under the Intel ME Configuration menu, the user will be able to disable Intel AMT (enabled by default); select the Intel ME Power Policy; and set the Idle Timeout, the amount of time, in seconds, Intel ME must be idle before it will enter its lowest-power state (valid values are from 1 – 65535). These options are shown in Figure 9.

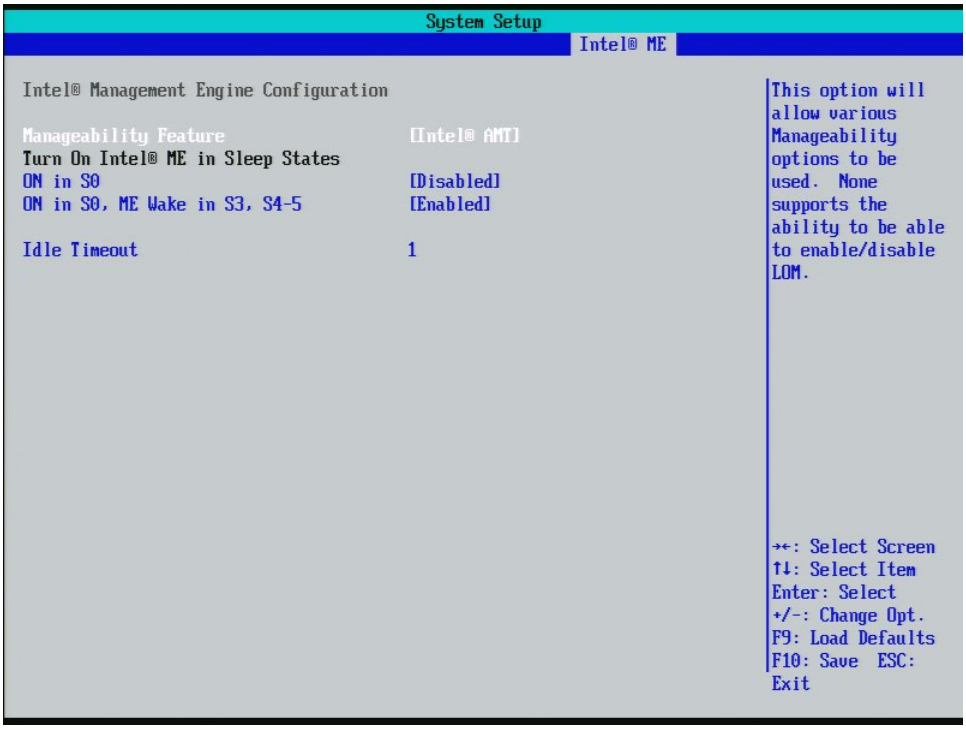

Figure 9. Intel ME – Intel ME Configuration

> Note: If Intel AMT is enabled, on-board LAN (found under BIOS Setup - Configuration / On-Board Devices) cannot be disabled. See Figure 4.

Choosing Power Policy 1 (On in S0) effectively disables Intel AMT Out-of-Band (OOB) operation. Power Policy 2 (On in S0, ME Wake in S3, S4-S5) allows Intel ME and Intel AMT to operate when the system is turned off or in a standby state. After the Idle Timeout timer has expired, Intel ME will enter its lowest power state, but can be awakened by network traffic directed at the Intel ME without waking the entire system.

> Note: Actual time required before Intel ME will enter into its lowest power state is approximately Idle Timeout + 1½ minutes.

1.1.5.2 Intel® ME – Intel® AMT Configuration

Figure 10 displays the main Intel AMT Configuration screen. From here, the user can select the Setup and Configuration (Provisioning) Mode as well as reset Intel AMT back to factory defaults (except the Intel ME administrator password).

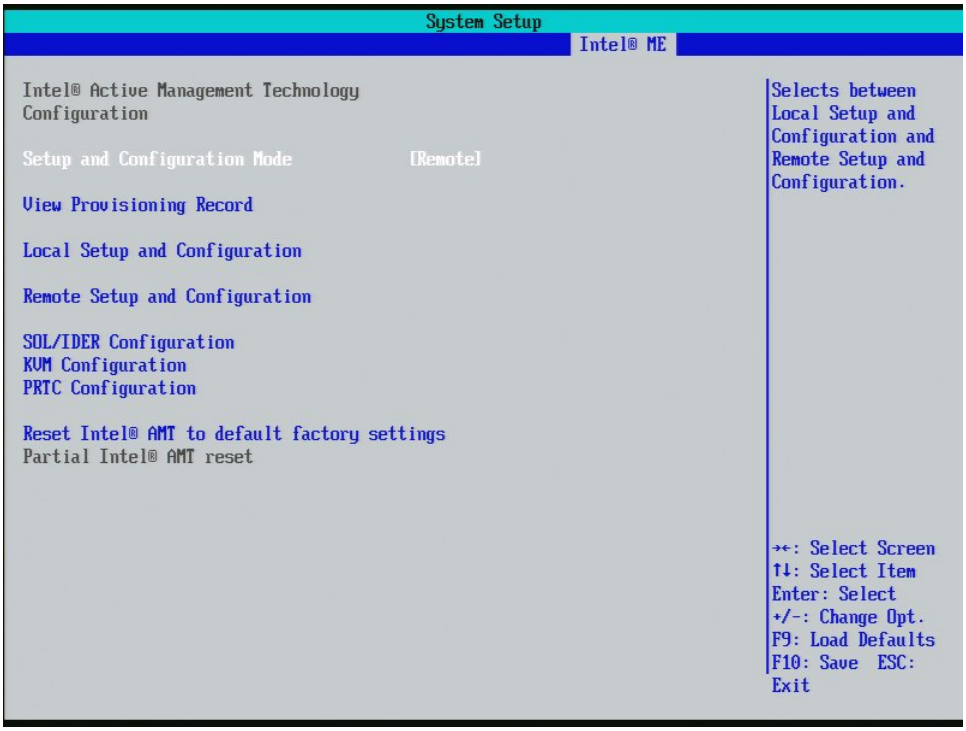

Figure 10. Intel ME - Intel AMT Configuration

1.1.5.2.1 Intel AMT Configuration – Remote Configuration

Once the user selects the provisioning mode to use, the detailed settings of these modes can be viewed and configured. Figure 11 shows the details of Remote Setup and Configuration Mode (previously known as Enterprise, or Standard/Advanced, Provisioning).

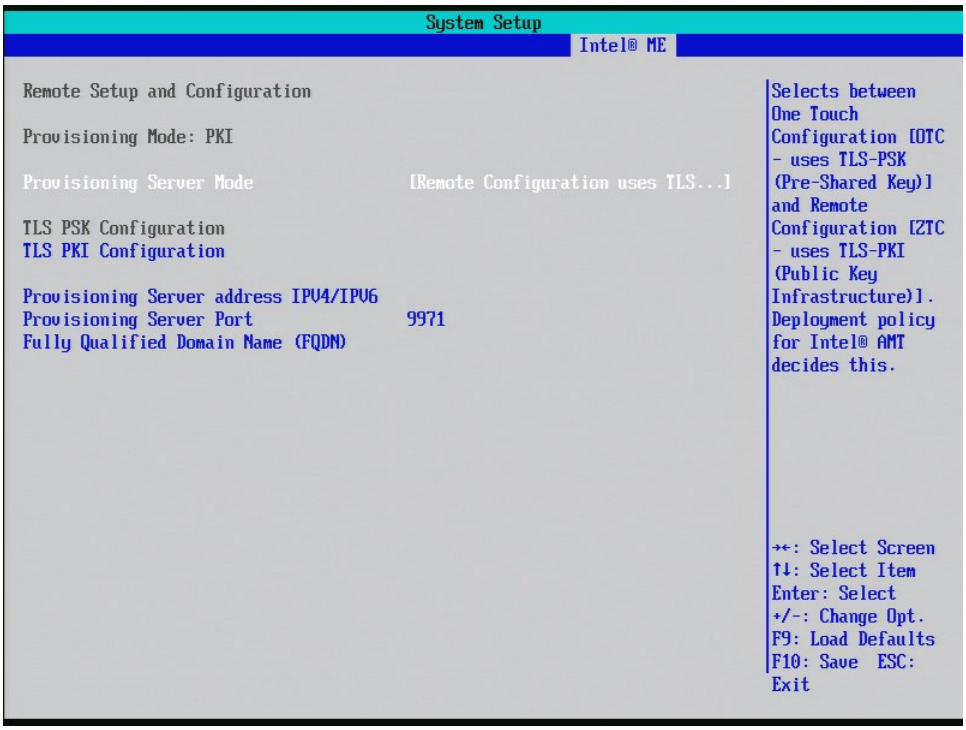

Figure 11. Remote Setup and Configuration - Main Screen

From this screen the user can select whether to use TLS (Transport Layer Security) with PKI (Public Key Infrastructure), also known as Zero Touch, Bare-metal or Remote Configuration; or TLS with PSK (Pre-shared Key), which can be used with a USB flash drive for One Touch Configuration.

Other options available from the Remote Setup and Configuration screen allow the user to assign an IP address to the Provisioning Server (either IPV4 or IPV6), change from the default Server Port of 9971, or provide a Fully Qualified Domain Name (FQDN) for the Provisioning Server to enhance enterprise security.

1.1.5.2.1.1 Remote Configuration – TLS with PKI

Figure 12 shows the options for TLS with PKI configuration. Figure 13 follows with a view of Permanent Certificate Manager; the User Certificate Manager operates in a similar manner.

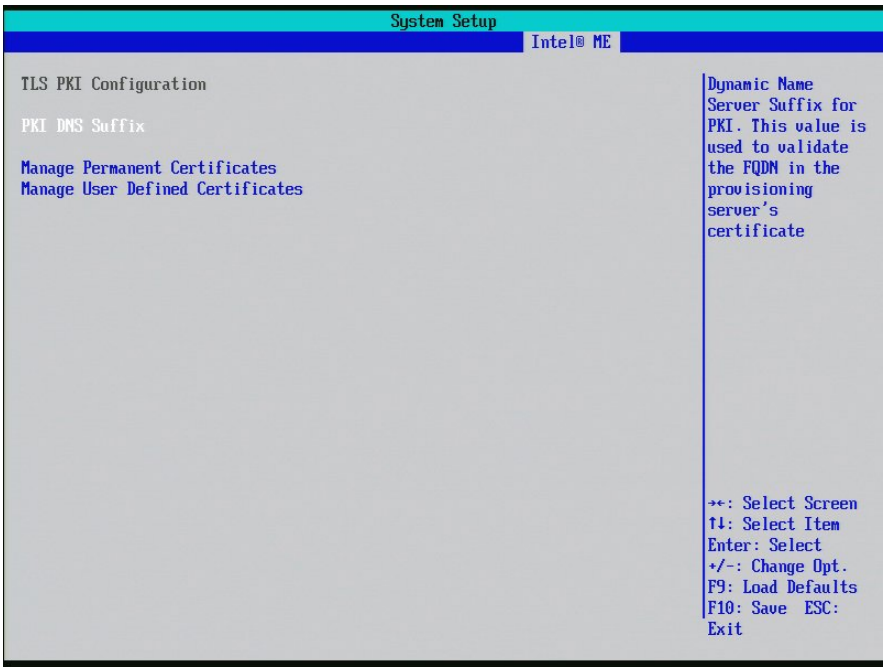

Figure 12. Intel AMT TLS with PKI Provisioning Options

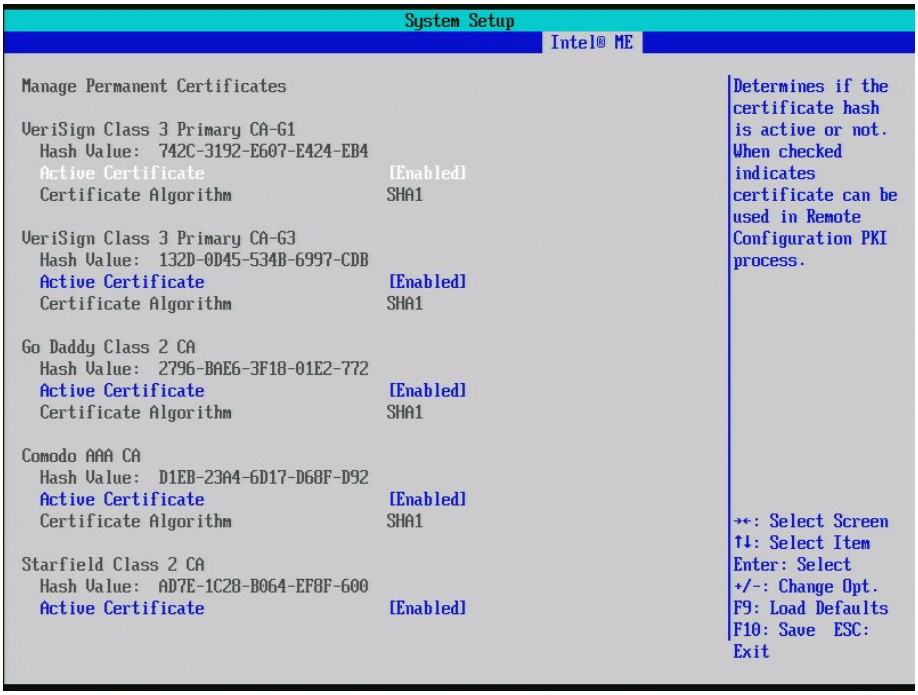

Figure 13. Intel AMT Permanent Certificate Manager

1.1.5.2.1.2 Remote Configuration – TLS with PSK

For TLS with PSK, the options are shown in Figure 14. The Provisioning Identifier (PID) is an eight-character string formatted as two quartets separated by a dash.

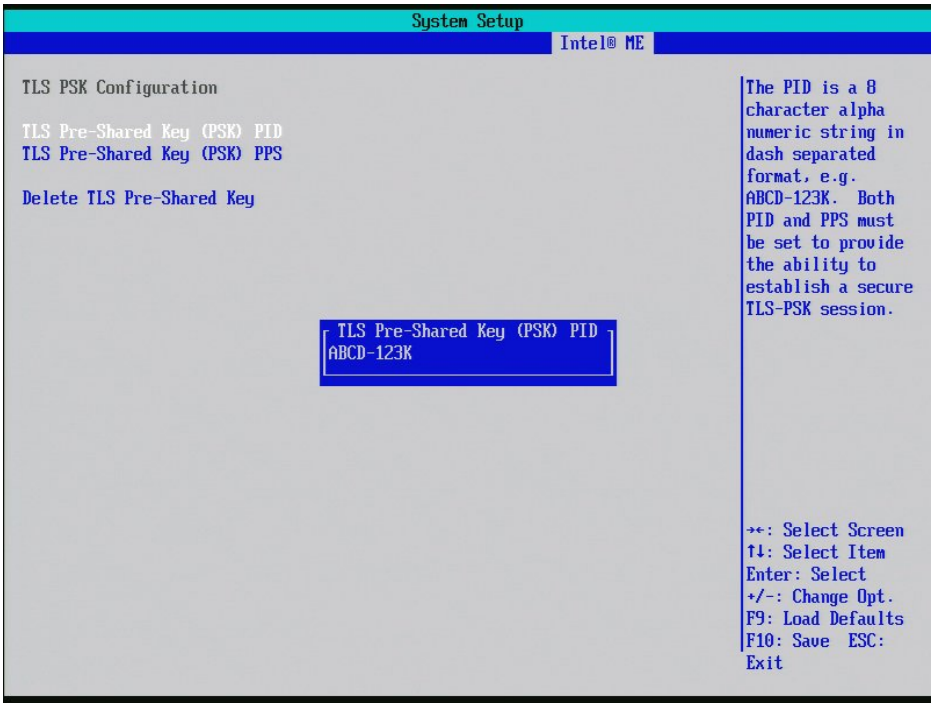

Figure 14. Intel AMT TLS with PSK Provisioning Identifier (PID)

The Provisioning Passphrase (PPS) similarly is a 32-character string formatted as eight quartets separated by dashes, as shown in Figure 15.

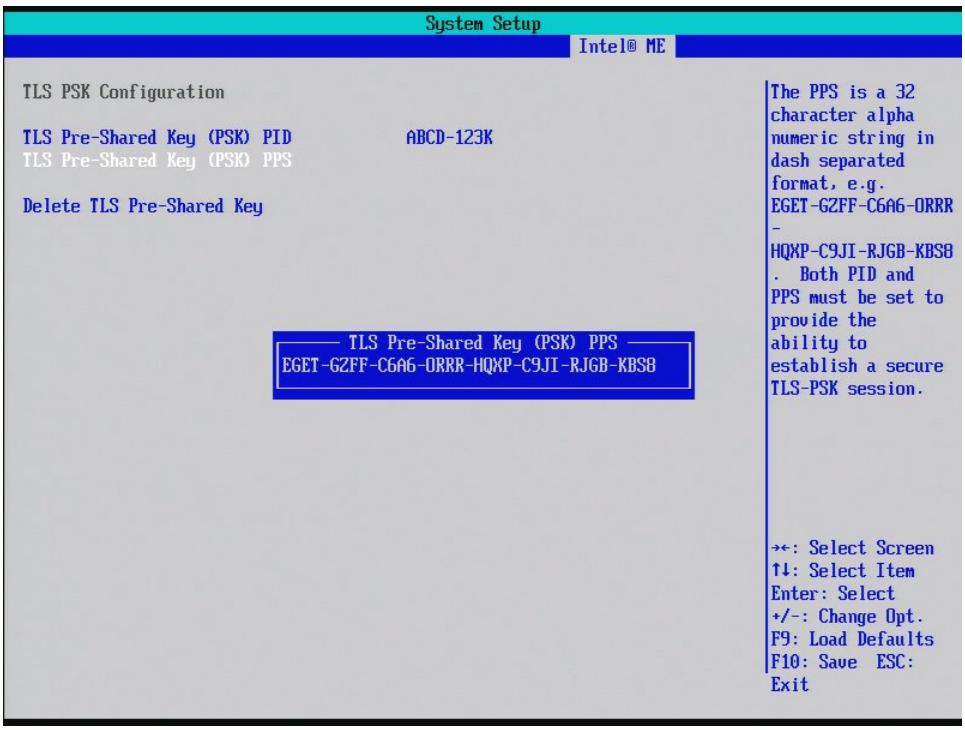

Figure 15. Intel AMT TLS with PSK Provisioning Passphrase (PPS)

1.1.5.2.2 Intel® AMT Configuration – Local Configuration

As can be seen from Figure 16 through Figure 18, the user can manually set Computer and Domain Name in the Local Setup and Configuration screen (previously known as SMB/Small-Medium Business Mode). The user can also choose to: share the Management Engine's FQDN with the operating system (IPV6 does not allow FQDN sharing if DDNS is enabled); allow dynamic updates to the DNS (Domain Name System); and configure the IPV4 or IPV6 TCP/IP protocols. Default is set to IPV4, with DHCP enabled.

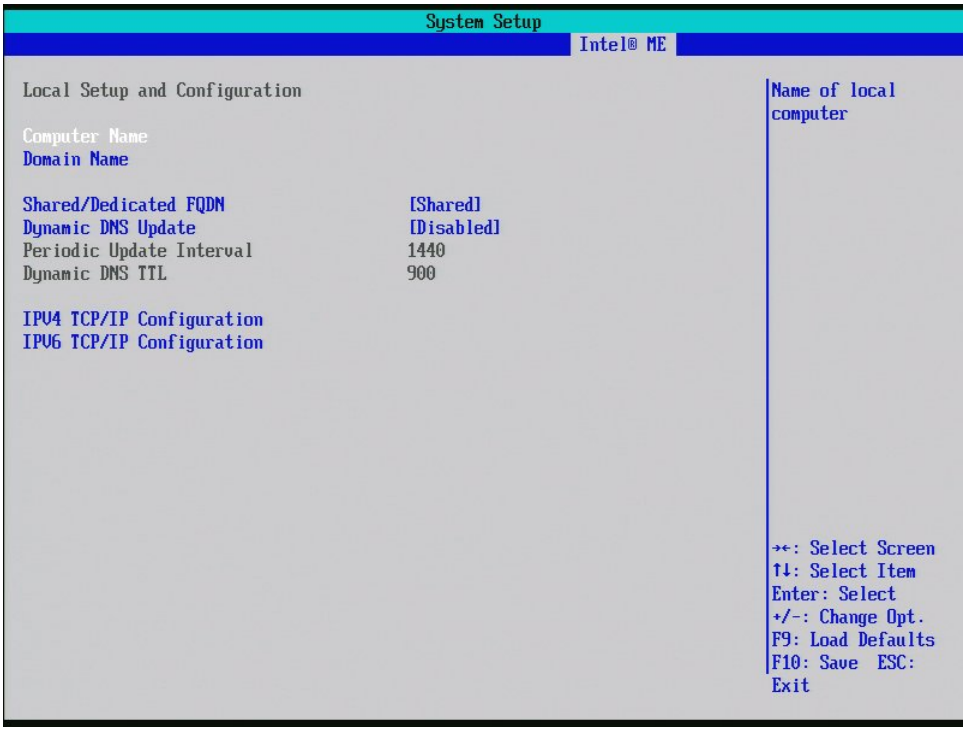

Figure 16. Intel AMT - Local Configuration

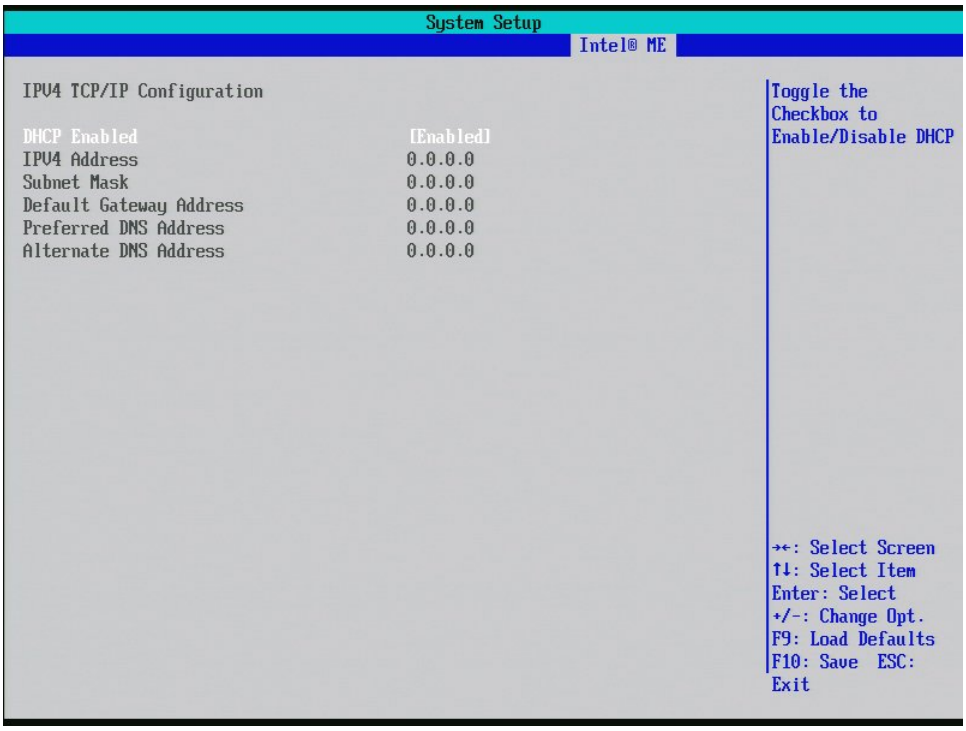

Figure 17. Intel AMT - Local Configuration, IPV4 Configuration Options

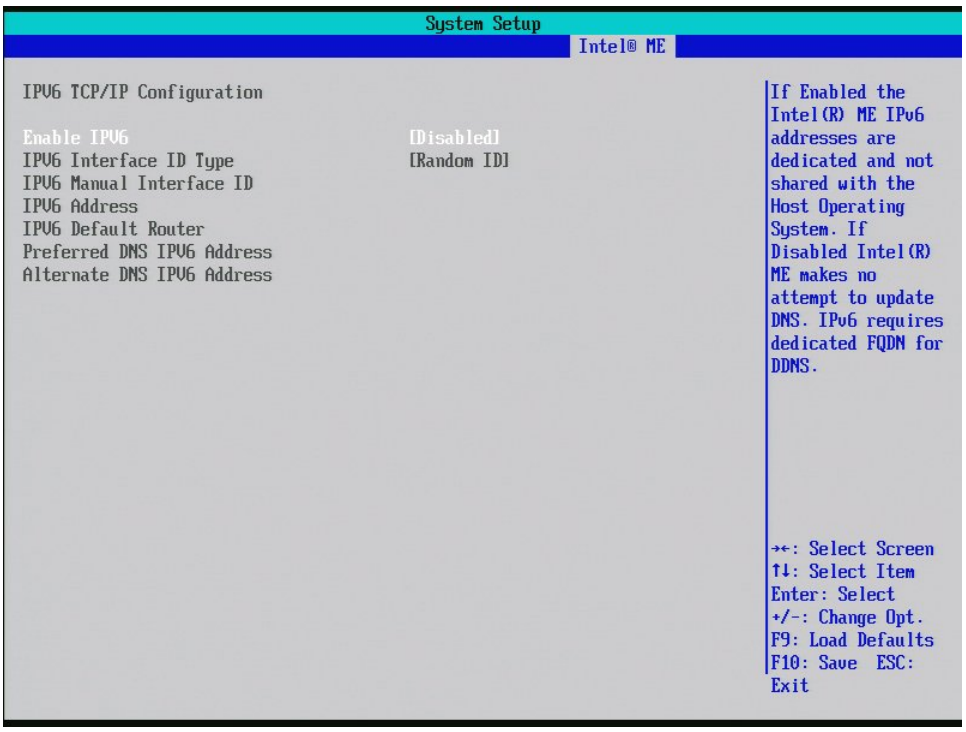

Figure 18. Intel AMT - Local Configuration, IPV6 Configuration Options

1.1.5.2.3 Intel AMT Configuration – Other Options

The following screens highlight several of the common features of Intel AMT provisioning. These include: SOL/IDE-R (Serial-over-LAN/IDE-Redirection) configuration in Figure 19; Intel® KVM (Keyboard Video Mouse) Remote Control Configuration in Figure 20; as well as PRTC (Protected Real Time Clock).

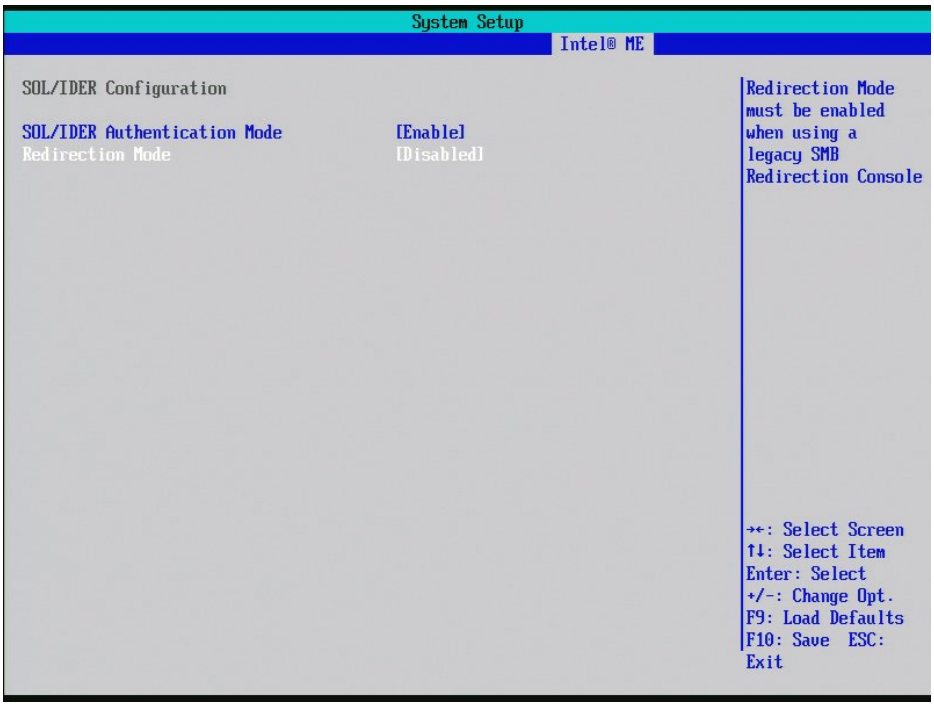

Figure 19. Intel AMT - SOL/IDE-R Configuration

New for Intel AMT 6.0 is the Redirection Mode setting under SOL/IDE-R, as highlighted in Figure 19. Legacy platforms (Intel AMT 5.0 and earlier) require specific port initialization commands whenever performing redirection operations which were eliminated for Intel AMT 6.0. Enabling this mode allows the use of Intel AMT 5.0 (and earlier) management consoles with this platform.

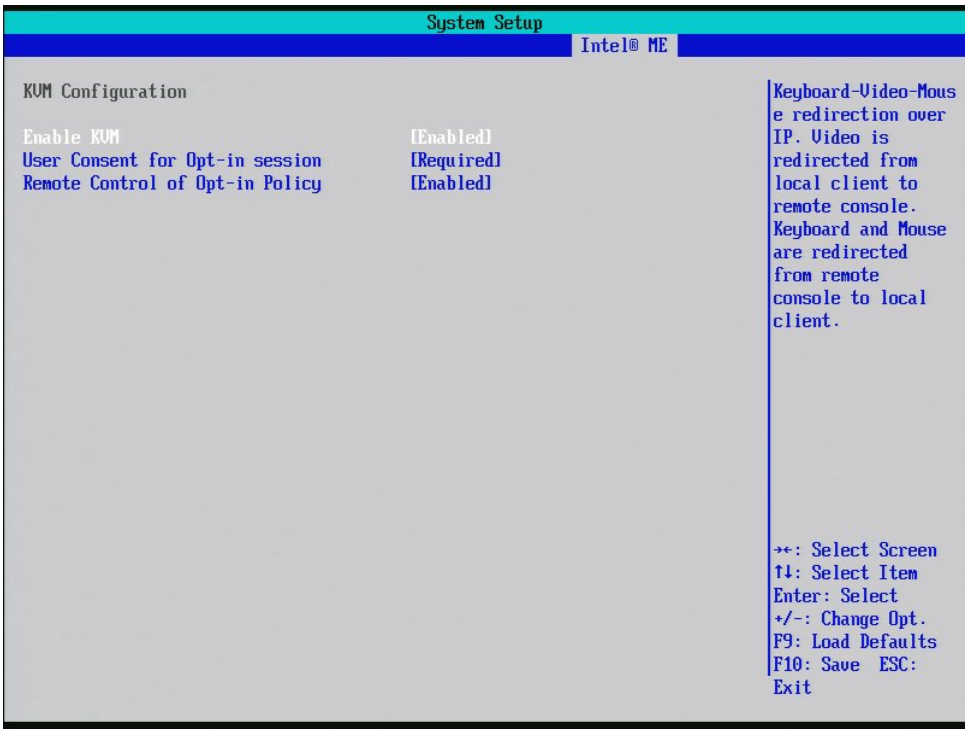

Figure 20. Intel AMT IntelKVM Remote Control Configuration

As shown in Figure 20, the options for Intel KVM Remote Control not only include enabling and disabling the Intel KVM Remote Control feature, but also include the ability to set the level of user-controlled security. The user has the ability to allow Intel KVM Remote Control usage with or without user intervention, and to allow a remote user, such as IT personnel, to set this policy. These features provide greater flexibility to allow platform maintenance to be performed after hours when no user is present.

1.2 Intel AMT – Local Configuration

As described in the previous sections, Intel AMT Setup and Configuration is divided into two provisioning modes: **Local** (aka SMB or Basic) and **Remote** (aka Enterprise or Standard/Advanced). To provision Intel Desktop Board DQ57TM in Local Mode, the user needs to simply enter the Local Setup and Configuration page under Intel ME in BIOS Setup and set the Computer Name, as shown in Figure 21. As the platform is already set for IPV4 and DHCP as defaults, no other settings are necessary. F10 Save and Exit will finish the Local Setup and Configuration process. Once the platform reaches the end of POST, the process will be complete. The platform may reboot a few times as it populates the firmware's SMBIOS tables with the updated information.

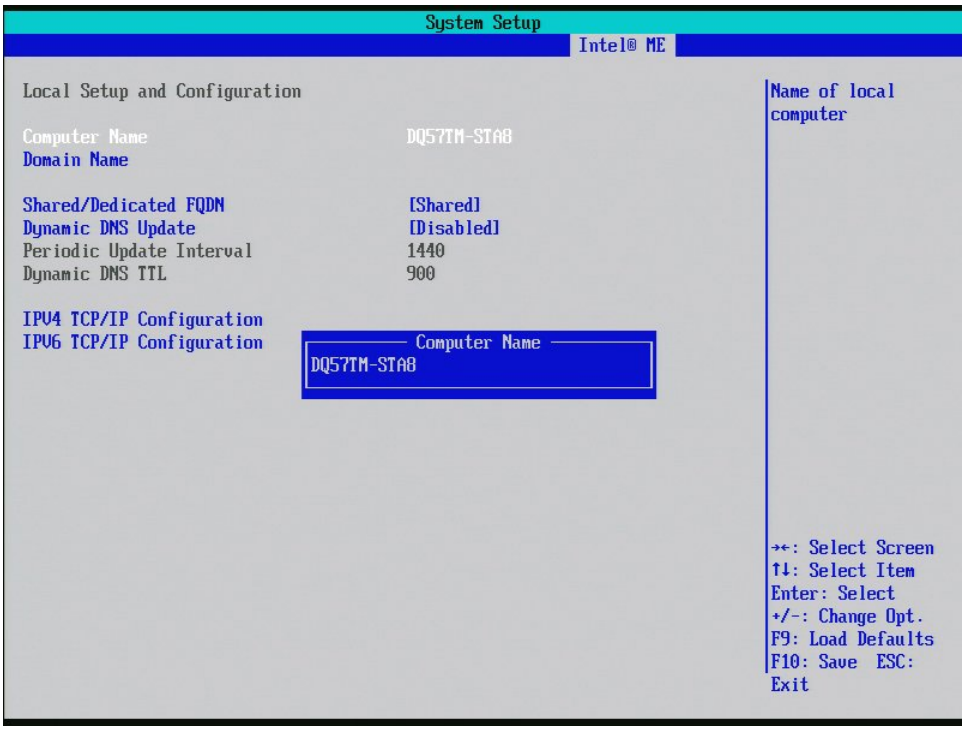

Figure 21. Intel AMT - Configuring Computer Name

Figure 22 and Figure 23 show the results of the MEINFO utility before and after Local Configuration.

```
Last ME reset reason:                  Firmware reset
System UUID:                           6071483b-e142-df11-9559-7071bc0ba73c
MAC Address:                           70-71-bc-0b-a7-3c
Configuration state:                   In process
IPv4 Address:                          192.168.7.14
IPv6 Enablement:                       Disabled
BIOS and GbE Config Lock:              Enabled
Host Read Access to ME:                Disabled
Host Write Access to ME:               Disabled
SPI Flash ID #1:                       EF4017
SPI Flash ID VSCC #1:                  20052005
BIOS boot State:                       Post Boot
Provisioning Mode:                     PKI
FWU Override Counter:                  Always
FWU Override Qualifier:                Always
Local FWUpdate:                        Enabled
Secure FWUpdate:                       Enabled
OEM Id:                                00000000-0000-0000-0000-000000000000
Capability Licensing Service:          Enabled
Capability Licensing Service Status:   Permit info not available
Override to RPAT-c SKU:                Not Set
FW behavior on Flash Descriptor Override Pin-Strap: Halt


C:\>_
```

Figure 22. MEINFO Output - Intel AMT Defaults

```
Last ME reset reason:                  Firmware reset
System UUID:                           6071483b-e142-df11-9559-7071bc0ba73c
MAC Address:                           70-71-bc-0b-a7-3c
Configuration state:                   Completed
IPv4 Address:                          192.168.7.14
IPv6 Enablement:                       Disabled
BIOS and GbE Config Lock:              Enabled
Host Read Access to ME:                Disabled
Host Write Access to ME:               Disabled
SPI Flash ID #1:                       EF4017
SPI Flash ID VSCC #1:                  20052005
BIOS boot State:                       Post Boot
Provisioning Mode:                     Unknown
FWU Override Counter:                  Always
FWU Override Qualifier:                Always
Local FWUpdate:                        Enabled
Secure FWUpdate:                       Enabled
OEM Id:                                00000000-0000-0000-0000-000000000000
Capability Licensing Service:          Enabled
Capability Licensing Service Status:   Permit info not available
Override to RPAT-c SKU:                Not Set
FW behavior on Flash Descriptor Override Pin-Strap: Halt


C:\>_
```

Figure 23. MEINFO Output - Local Configuration

The platform is now ready for remote management.

1.3 Intel AMT – Remote Configuration, TLS-PSK

Intel AMT Remote Configuration using TLS with PSK can be configured manually as shown in Section 1.1.5.2.1.2 and Figure 14 and Figure 15, or the user can insert a USB flash drive containing a SETUP.BIN file created by a Setup and Configuration Server (SCS). This method of provisioning is known as One Touch Configuration.

> Note: The SCS is also the source of the PSK PID and PSK PPS keys shown in Section 1.1.5.2.1.2. Details of how to use this and other Remote Configuration methods can be found in the documentation of your SCS or management application and are beyond the scope of this document.

The results of Intel Desktop Board DQ57TM encountering a USB flash drive with a valid SETUP.BIN at startup is shown in Figure 24. At this point the user presses "Y" and the platform will complete TLS with PSK One Touch configuration.

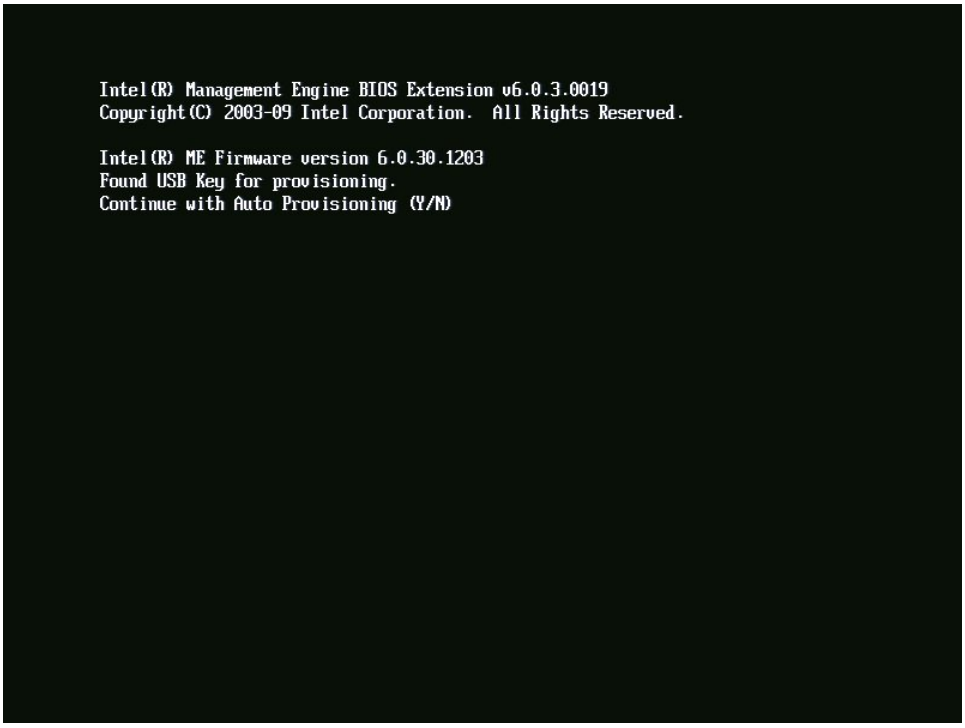

Figure 24. Intel AMT - TLS with PSK One Touch Configuration

1.4 Intel AMT – Remote Configuration, TLS-PKI

TLS with PKI configuration requires a provisioning server configured with an Intel AMT Remote Configuration certificate that is rooted in one of the pre-installed permanent certificates. This method of configuration is shown in Section 1.1.5.2.1.1 and Figure 12 and Figure 13.

> Note: Details of how to use this and other Remote Configuration methods can be found in the documentation of your SCS or management application and are beyond the scope of this document.

1.5 Intel® Remote PC Assist Technology (Intel® RPAT)

Intel Remote PC Assist Technology, or Intel® RPAT, requires no configuration out of the box. The user has three methods to activate: 1) F9 key, 2) Intel RPAT header, and 3) Intel RPAT client agent.

During the initial POST screen, remote assistance can be accessed by repeatedly pressing the F9 key while the "Remote Assistance: F9" message is displayed on the screen (see Figure 1). The user may also choose to connect a momentary switch to the IRPAT header located on the board's edge near the PCI slot, as illustrated in Figure 25. When depressed, access to remote assistance will occur on the next system boot. When triggered successfully, both of these methods will launch the Remote PC Assist Wizard, as seen in Figure 26.

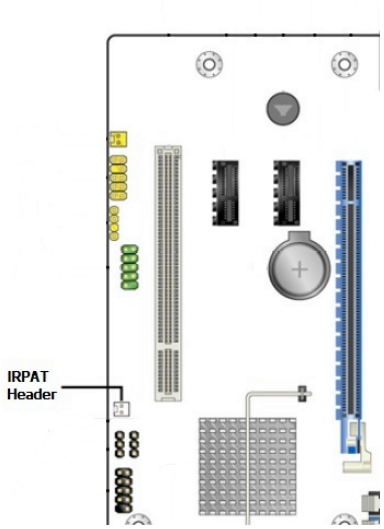

Figure 25. Intel RPAT Header Location

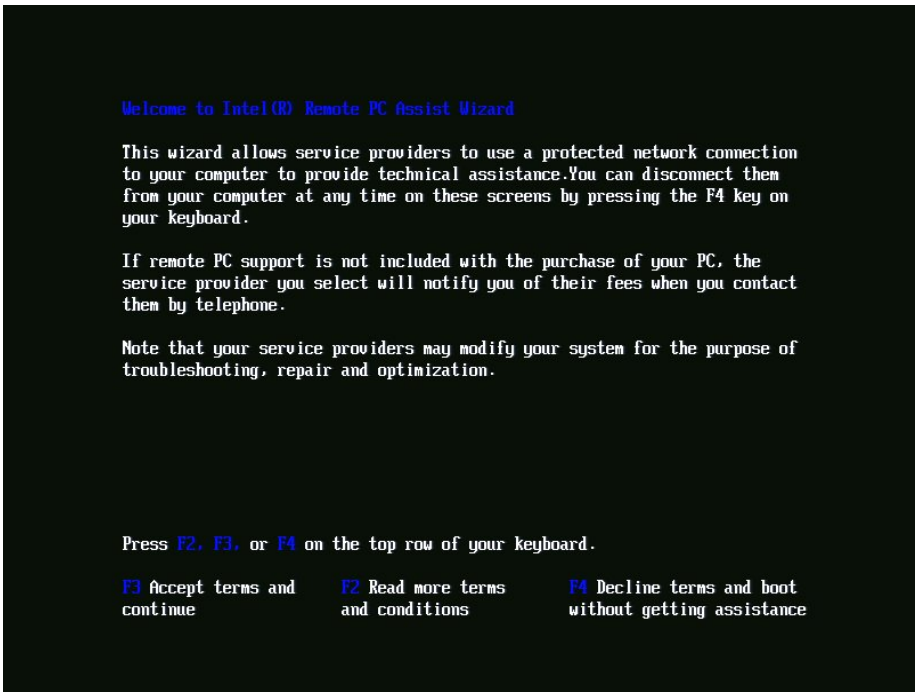

Figure 26. Intel(R) Remote PC Assist Wizard

From this screen the user would press F3 to accept terms and continue. The next screen requests a 12-digit session code. This code is provided by the contracted service provider and entered by the user, see example shown in Figure 27.

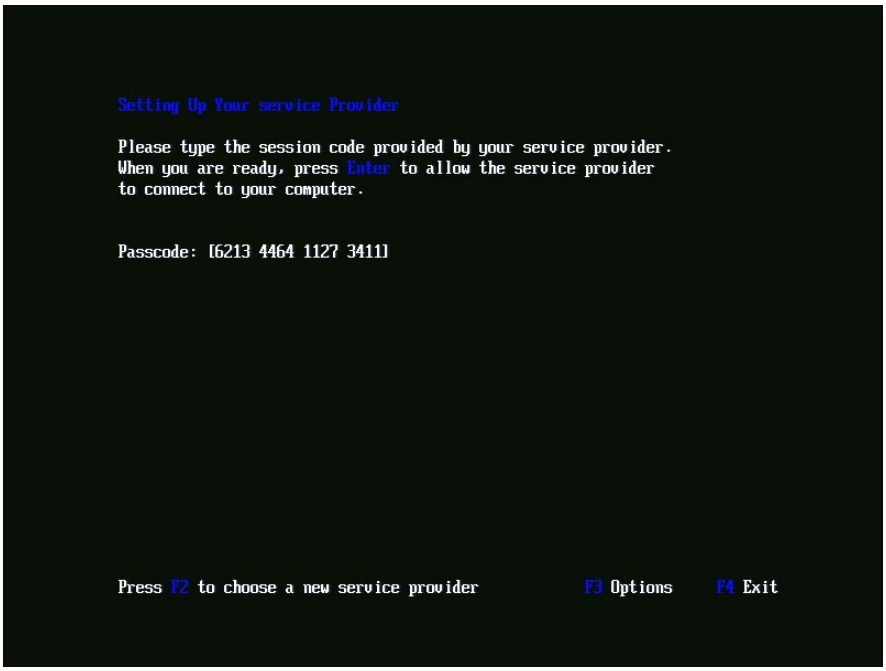

Figure 27. Intel RPAT Wizard Session Code

If a successful connection is made to the service provider, the screen shown in Figure 28 will display.

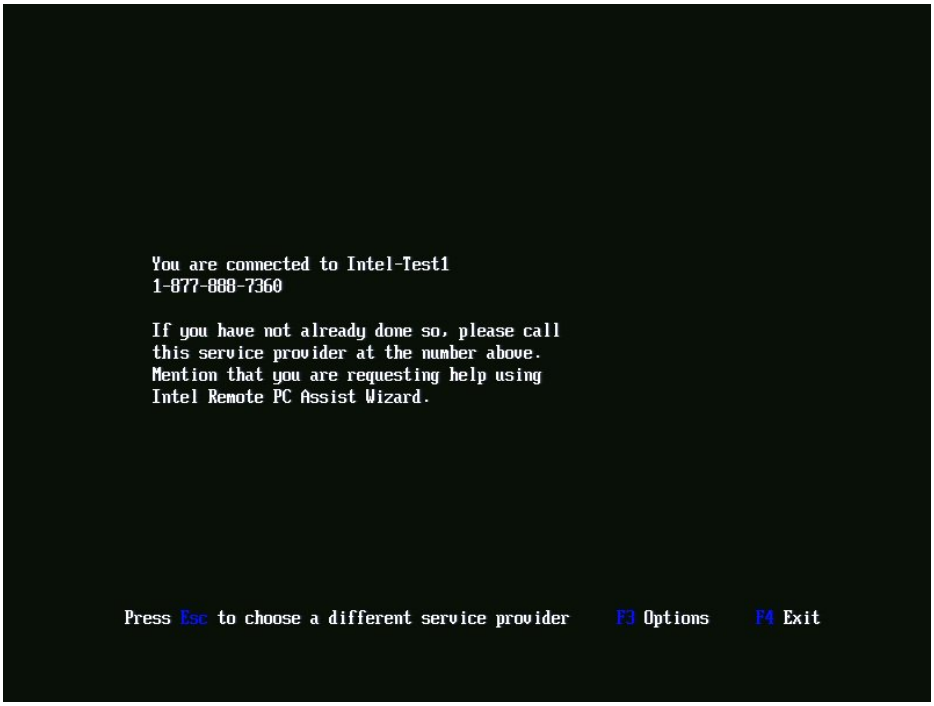

Figure 28. Intel RPAT Wizard Successful Connection

Alternatively, Intel RPAT may be accessed from the user's Windows* operating system environment by using the Intel RPAT Client Agent, provided by LogMeIn* and available for download from the Intel® Remote PC Assist Technology website listed in the reference section of this document. Figure 29 through Figure 32 show the process of connecting to a service provider using the Intel RPAT Client Agent.

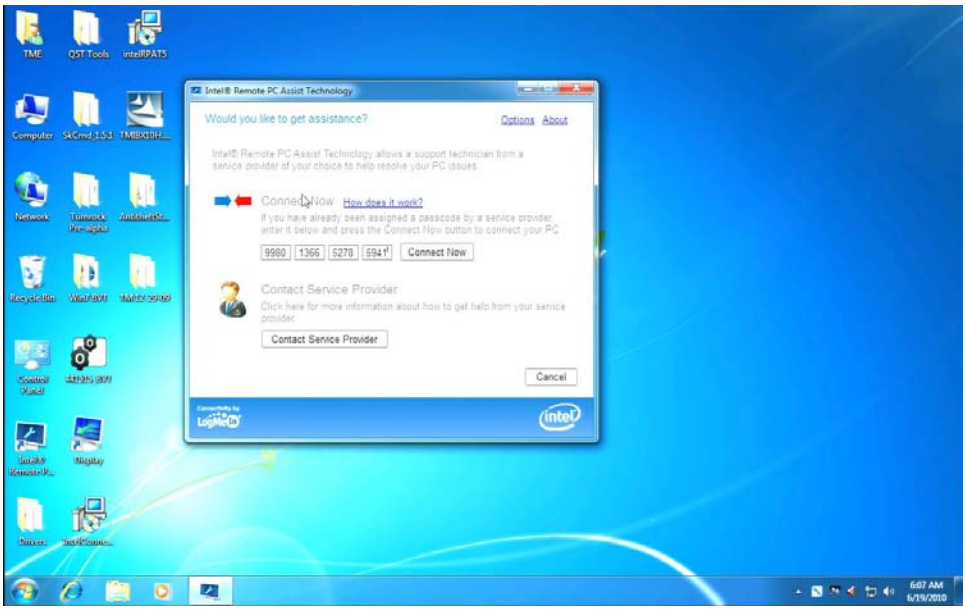

Figure 29. Intel RPAT Client Agent Contact Service Provider

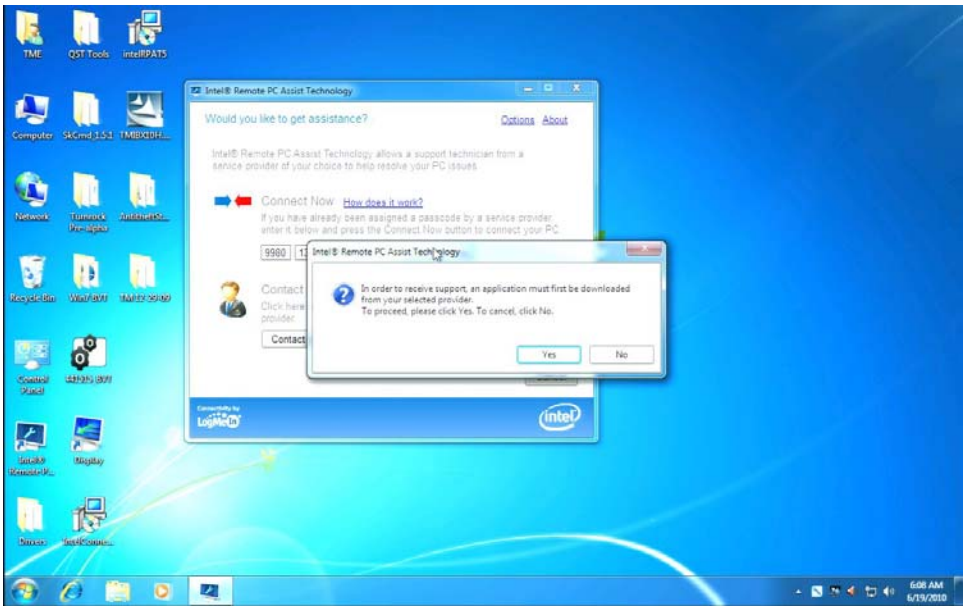

Figure 30. Intel RPAT Client Agent Download Request

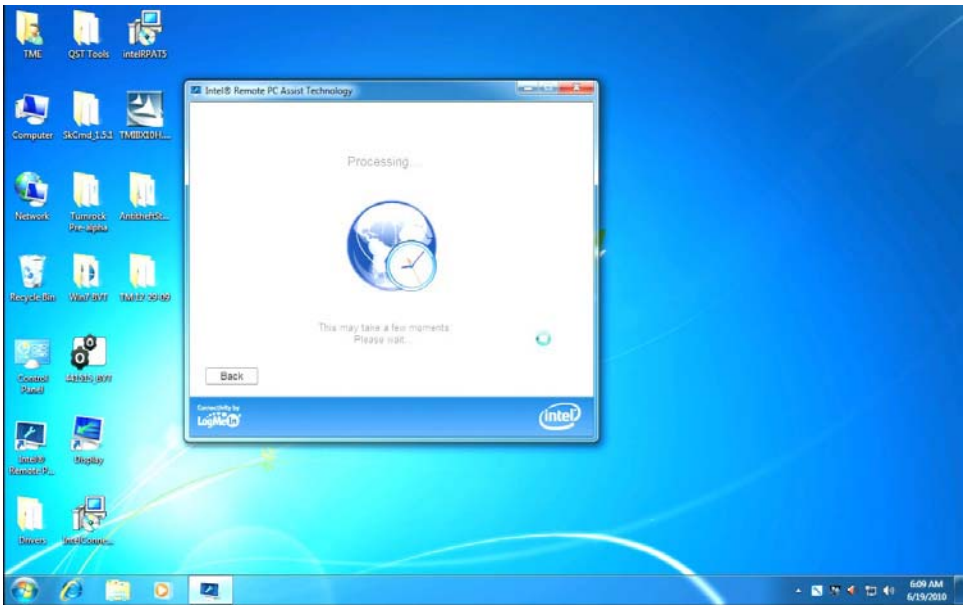

Figure 31. Intel RPAT Client Agent Wait Screen

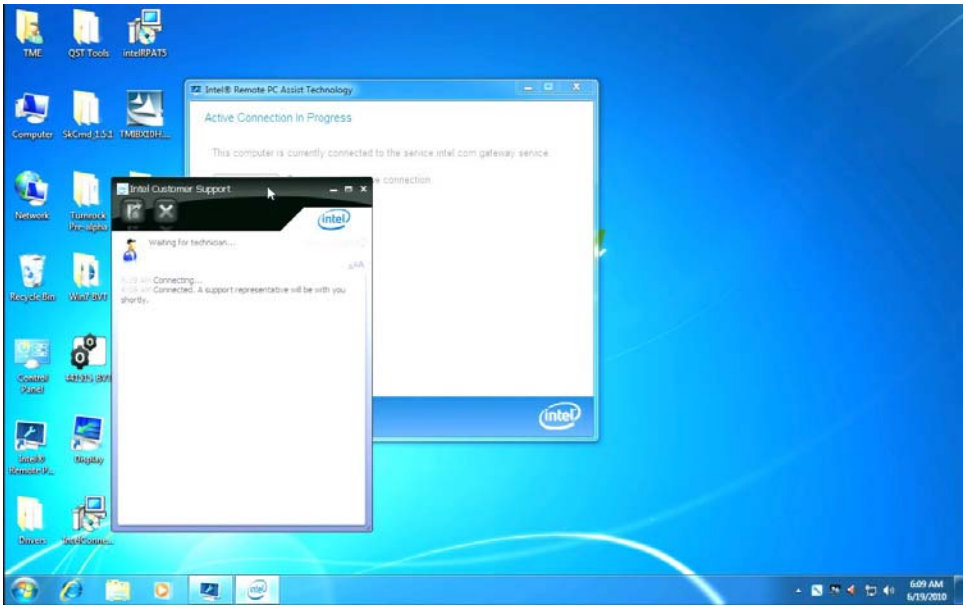

Figure 32. Intel RPAT Client Agent Successful Connection

1.6 Intel® KVM Remote Control

Intel® KVM Remote Control is available on Intel vPro Q57 Express Chipset-based desktop boards that contain 2010 Intel Core vPro processors with integrated Intel HD Graphics.

Note: Intel KVM Remote Control is not supported on platforms with discrete graphics.

Note: For the purposes of this guide, the Intel AMT client system is provisioned in Local (SMB) mode.

If using VNC Viewer+* as the remote management console, the user enters the IP address of the client, as shown in Figure 33. For Authentication, use the Intel AMT administrator (*admin*) password. On the client system, a six-digit access code will appear (Figure 34). This is used in the VNC Viewer+ console to gain access (Figure 35). Figure 36 shows the view of the Intel AMT client as seen from the VNC Viewer+ console.

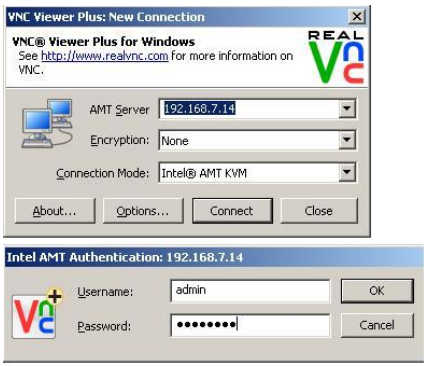

Figure 33. VNC Viewer+ Console Remote Login

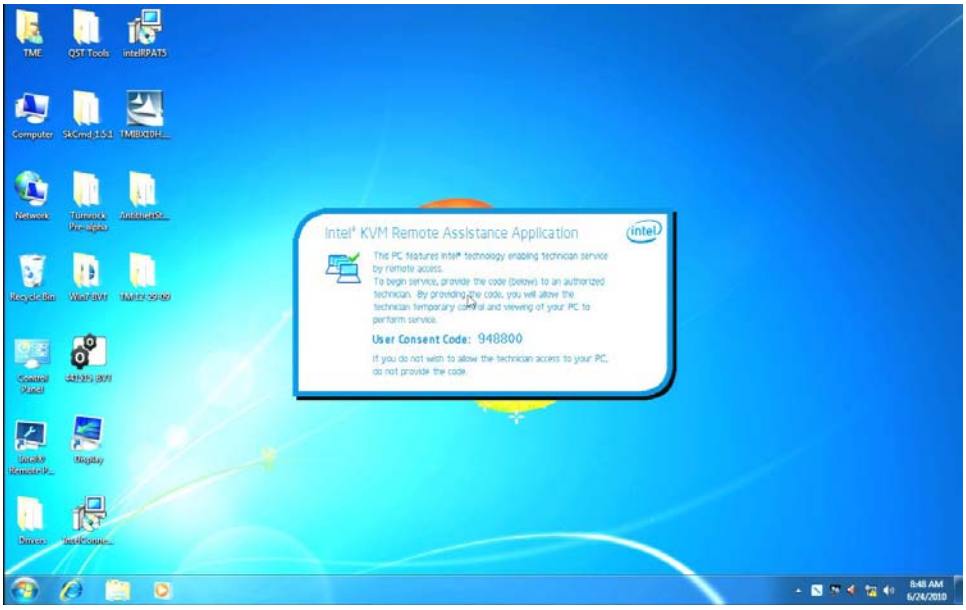

Figure 34. Intel AMT Client Screen Showing Intel KVM Remote Control Access Code

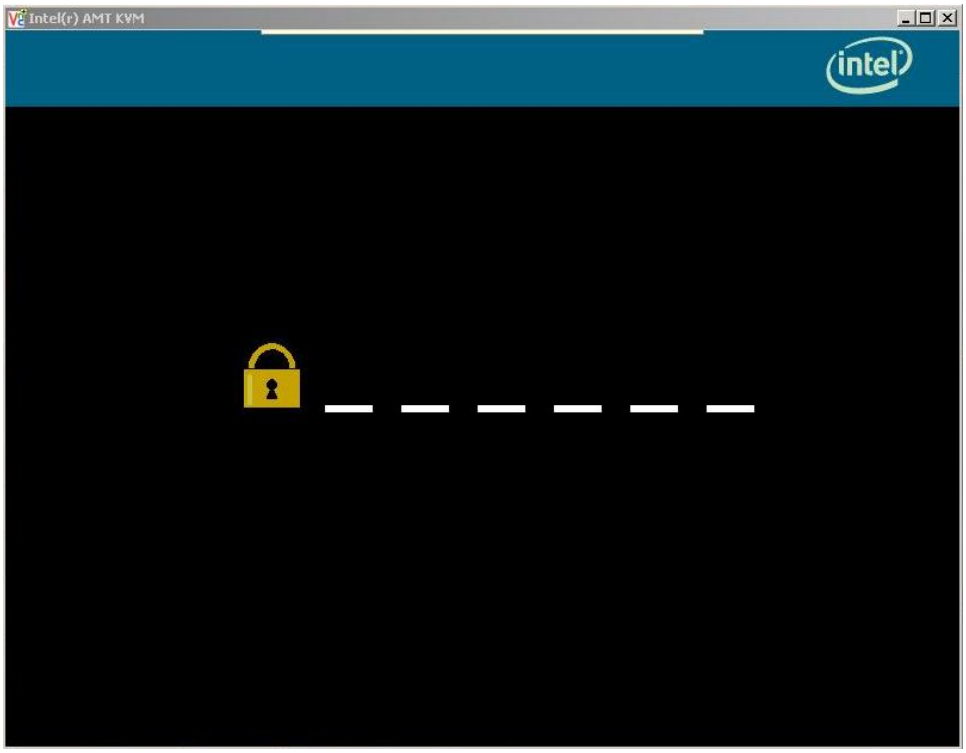

Figure 35. VNC Viewer+ Management Console Access Code Screen

Figure 36. VNC Viewer+ Management Console View

1.7 BIOS Maintenance Mode

A quick way to reset Intel AMT to default settings (including the Intel ME *admin* password) is to enter BIOS Maintenance Mode. This is done by moving the BIOS_CFG jumper from the Normal to the Config position and powering on the board (see Figure 40 for location). From the BIOS Maintenance screen, select "Reset Intel® AMT to default factory settings" as displayed in Figure 37 and press "Y".

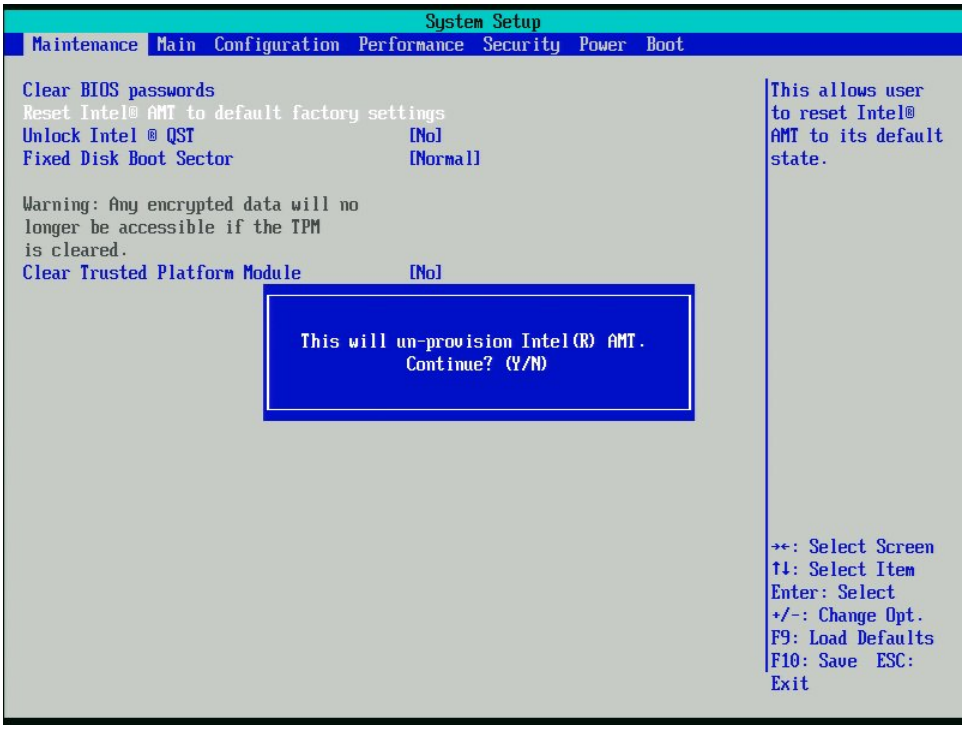

Figure 37. BIOS Maintenance Intel AMT Reset to Defaults

During reset, the screen of Figure 38 is shown. Once finished, the user will receive the notification shown in Figure 39. The user must then save and exit BIOS Setup, power off the system and restore the BIOS_CFG jumper back to the Normal position. These steps are necessary for proper reset of Intel AMT.

One other way to reset Intel AMT back to defaults is to use the CLEAR_CMOS header. First, the user must remove all power from the board. A jumper is then placed for 5 seconds shorting pins 1 and 2 of the CLEAR_CMOS header. It is imperative that the jumper is removed before power is reapplied to the board. Failure to do so may cause damage to the board and/or its firmware.

> **Caution:** Do not apply board power with a jumper in place on pins 1 and 2 on the CLEAR_CMOS header. Doing so may cause damage to the board and/or its firmware.

The BIOS_CFG and CLEAR_CMOS headers are shown in Figure 40.

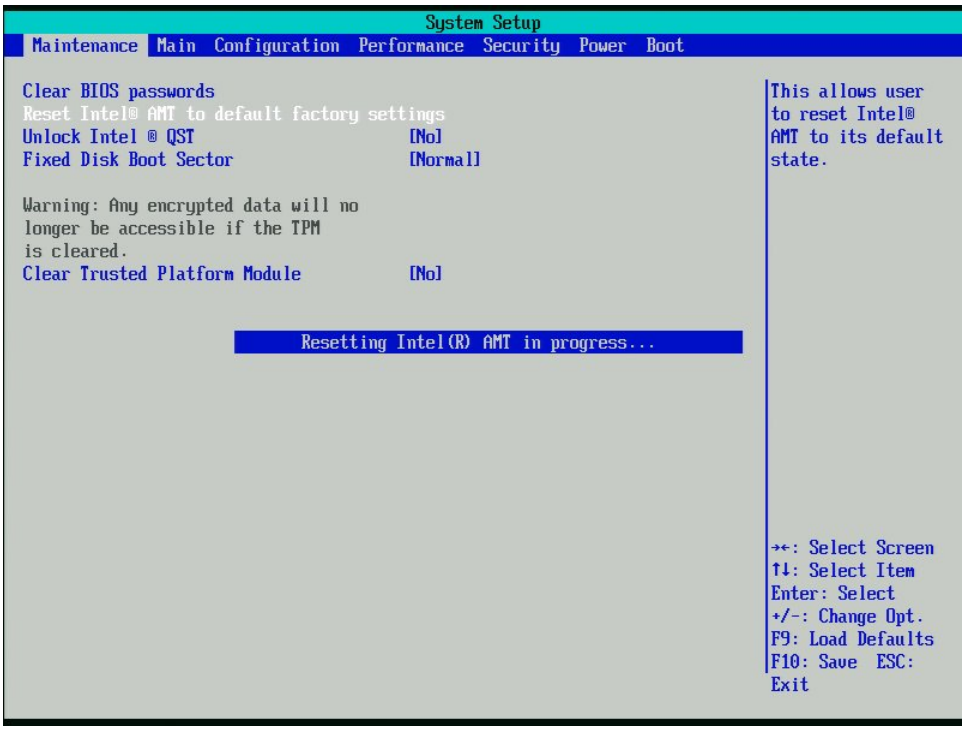

Figure 38. Intel AMT Reset in Progress

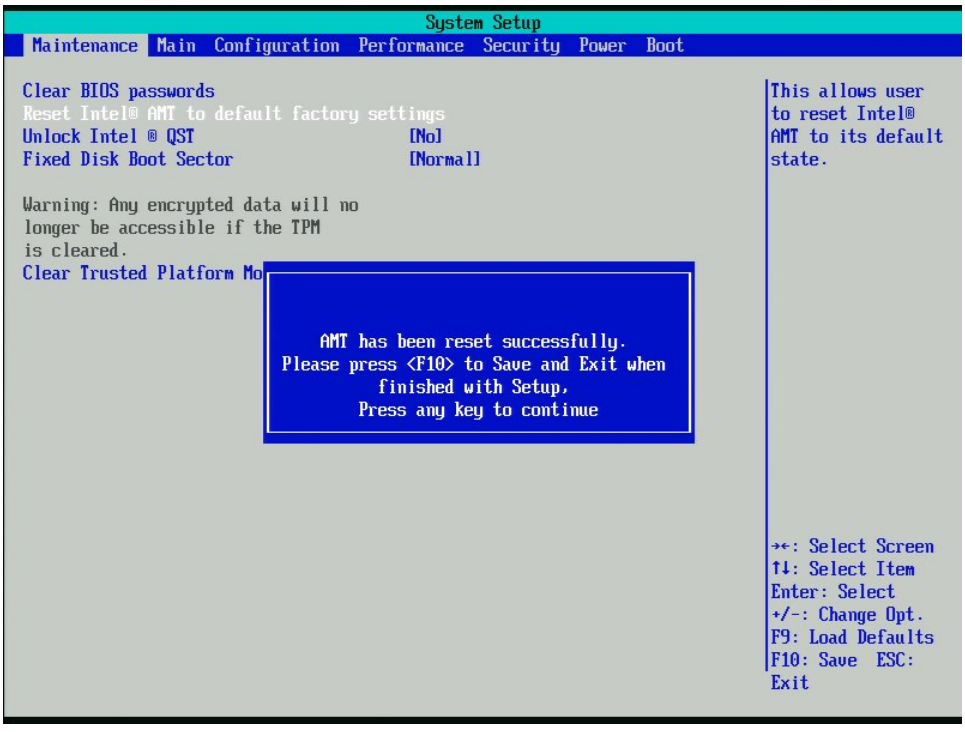

Figure 39. Intel AMT Reset Complete

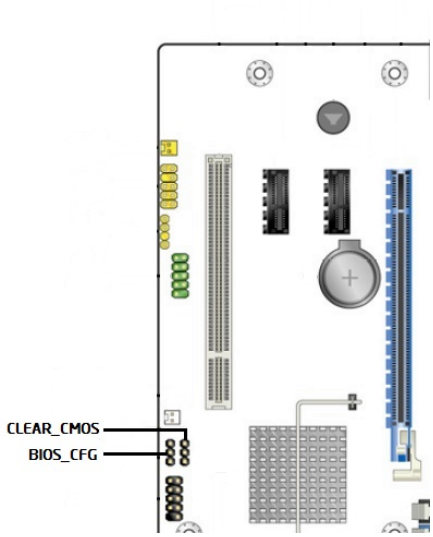

Figure 40. BIOS_CFG and CLEAR_CMOS Header Locations

2. References

http://download.intel.com/technology/vpro/Whitepaper_AllNew2010IntelCorevProProcessors.pdf for a complete list of Intel vPro features for 2010. Not all 2010 Intel vPro technology features may be supported on the Intel Desktop Board DQ57TM.

http://www.intel.com/technology/security/downloads/TrustedExec_Overview.pdf for an overview of Intel TXT.

http://www.intel.com/technology/virtualization/index.htm?iid=tech_vpro_body_vt for an overview of Intel VT.

http://www.intel.com/technology/xdbit/index.htm?iid=tech_vpro_body_edb for more information on Execute Disable Bit .

http://software.intel.com/en-us/articles/intel-virtualization-technology-for-directed-io-vt-d-enhancing-intel-platforms-for-efficient-virtualization-of-io-devices/ for more on Intel VT-d.

http://www.intel.com/technology/product/remotepcassist.htm for more information on Intel Remote PC Assist and download of the Intel RPAT Client Agent.