Intel® Desktop Boards DQ67SW, DQ67EP, DQ67OW

Intel® vPro™ Technology Setup and Configuration Guide

September 2011
Part Number: G45734-001

Revision History

Revision	Revision History	Date
-001	First release of the Intel® vPro™ Technology Setup and Configuration Guide for Intel® Desktop Boards DQ67SW, DQ67EP, DQ67OW	September 2011

Contents

Revision History 2
Contents 3
Figures 3
Tables 4
Preface 5
Feature Summary 6
1. Intel® vPro™ Technology Setup and Configuration 7
1.1 BIOS Setup 7
1.1.1 Overview 7
1.1.2 Entering BIOS Setup 7
1.1.3 BIOS Setup – Configuration Menu 8
1.1.4 BIOS Setup – Security Menu 10
1.1.5 BIOS Setup – Intel® ME Menu 11
1.2 Intel® AMT – Quick Configuration: Local 22
1.3 Intel AMT – Remote Configuration, TLS-PSK 24
1.4 Intel AMT – Remote Configuration, TLS-PKI 25
1.5 Intel AMT Configuration – Host Based Configuration 25
1.6 Fast Call for Help (FCFH) 25
1.7 KVM Remote Control 27
1.8 Intel® Identity Protection Technology (Intel® IPT) 29
1.9 BIOS Maintenance Mode 30
2. References 33

Figures

Figure 1. Intel® Desktop Boards POST Screen 7
Figure 2. BIOS Setup - Main Menu 8
Figure 3. BIOS Setup - Configuration Menu 9
Figure 4. BIOS Setup - Configuration 9
Figure 5. BIOS Setup - Security Menu 10
Figure 6. BIOS Setup – Intel® ME Menu 11
Figure 7. Intel ME - Main Menu 12
Figure 8. Intel ME – Intel ME Configuration 13
Figure 9. Intel ME - Intel AMT Configuration 14
Figure 10. Remote Setup and Configuration - Main Screen 15
Figure 11. Intel AMT TLS with PKI Provisioning Options 16
Figure 12. Intel AMT Permanent Certificate Manager 16
Figure 13. Intel AMT TLS with PSK Provisioning Identifier (PID) 17

Figure 14. Intel AMT TLS with PSK Provisioning Passphrase (PPS) 17
Figure 15. Intel AMT - Local Configuration 18
Figure 16. Intel AMT - Local Configuration, IPV4 Configuration Options 19
Figure 17. Intel AMT - Local Configuration, IPV6 Configuration Options 19
Figure 18. Intel AMT - SOL/IDE-R Configuration 20
Figure 19. Intel AMT KVM Remote Control Configuration 21
Figure 20. Intel AMT - Configuring Computer Name 22
Figure 21. MEINFO Output - Intel AMT Defaults 23
Figure 22. MEINFO Output - Local Configuration 23
Figure 23. Intel AMT - TLS with PSK One Touch Configuration 24
Figure 24. FCFH Header Locations 25
Figure 25. Fast Call for Help Alert Screen 26
Figure 26. VNC Viewer+ Console Remote Login 27
Figure 27. Intel AMT Client Screen Showing KVM Remote Control Access Code 27
Figure 28. VNC Viewer+ Management Console Access Code Screen 28
Figure 29. VNC Viewer+ Management Console View 28
Figure 30. Symantec VIP Access Security Credential 29
Figure 31. VASCO DIGIPASS for Web Security Credential 29
Figure 32. BIOS Maintenance Intel AMT Reset to Defaults 30
Figure 33. Intel AMT Reset in Progress 31
Figure 34. Intel AMT Reset Complete 31
Figure 35. BIOS_CFG and MEBX_RST Header Locations 32

Tables

Table 1. Feature Summary 6
Table 2. Location of Intel vPro Technology Features in BIOS Setup 7

Preface

This Setup and Configuration Guide specifies the steps necessary for enabling the different features of Intel® vPro™ technology for the Intel® Desktop Boards DQ67SW, DQ67EP and DQ67OW. 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 Boards DQ67SW, DQ67EP and DQ67OW 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

Ch 1 A description of the supported hardware and Intel vPro technology features of the Intel Desktop Boards DQ67SW, DQ67EP and DQ67OW, plus BIOS Setup details for Intel vPro technology and Intel® Active Management Technology (Intel® AMT)

Ch 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.

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 Boards DQ67SW, DQ67EP and DQ67OW support the Intel® Core™ i3, Intel® Core™ i5, Intel® Core™ i7, and Intel® Xeon® E3 processor families in the LGA1155 package. They use the Intel® Q67 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) 7.0
	Intel® Trusted Execution Technology (Intel® TXT)
	Fast Call For Help (FCFH)
	KVM Remote Control
	Intel® Virtualization Technology (Intel® VT)
	Intel® Virtualization for Directed I/O (Intel® VT-d)
	Trusted Platform Module (TPM)
	Intel® Identity Protection Technology (Intel® IPT)

Table 1. Feature Summary

Note: Intel® Active Management Technology requires one of the following Intel® Core™ i5 vPro™ and Intel® Core™ i7 vPro™ processors: Intel® Core™ i5-2390T, Intel® Core™ i5-2400, Intel® Core™ i5-2400S, Intel® Core™ i5-2500, Intel® Core™ i5-2500S, Intel® Core™ i5-2500T, Intel® Core™ i7-2600, or Intel ® Core™ i7-2600S processor. In addition, the following Intel® Xeon® E3 processors support Intel AMT functionality: Intel® Xeon® E3-1220, Intel® Xeon® E3-1220L, Intel® Xeon® E3-1225, Intel® Xeon® E3-1230, and Intel® Xeon® E3-1235 processors. Other Intel® Core™ processors will provide Intel® Standard Manageability only.

Note: Of the Intel processors listed above, only the Intel Core i5 and Intel Core i7 vPro processors and Intel Xeon E3 processors with integrated Intel® HD graphics will support KVM Remote Control; discrete graphics are not supported. All Intel Core i5 and Intel Core i7 vPro processors listed above and Intel Xeon E3-1225, Intel Xeon E3-1235 processors have integrated Intel HD graphics.

1. Intel® vPro™ Technology Setup and Configuration

1.1 BIOS Setup

1.1.1 Overview

The Intel Desktop Boards DQ67SW, DQ67EP and DQ67OW BIOS interface is based upon the UEFI specification. As a result, 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.

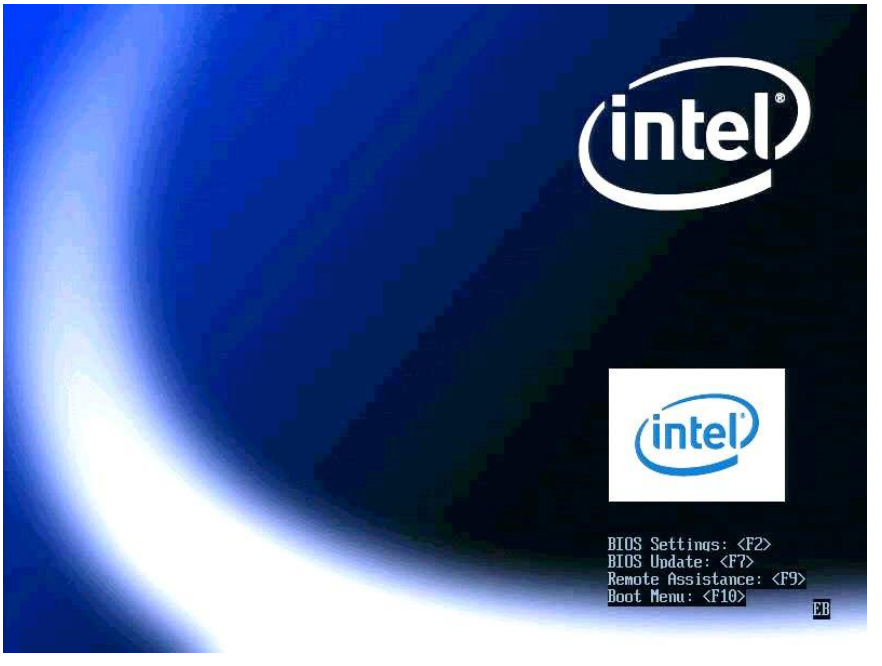


Figure 1. Intel® Desktop Boards POST Screen

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

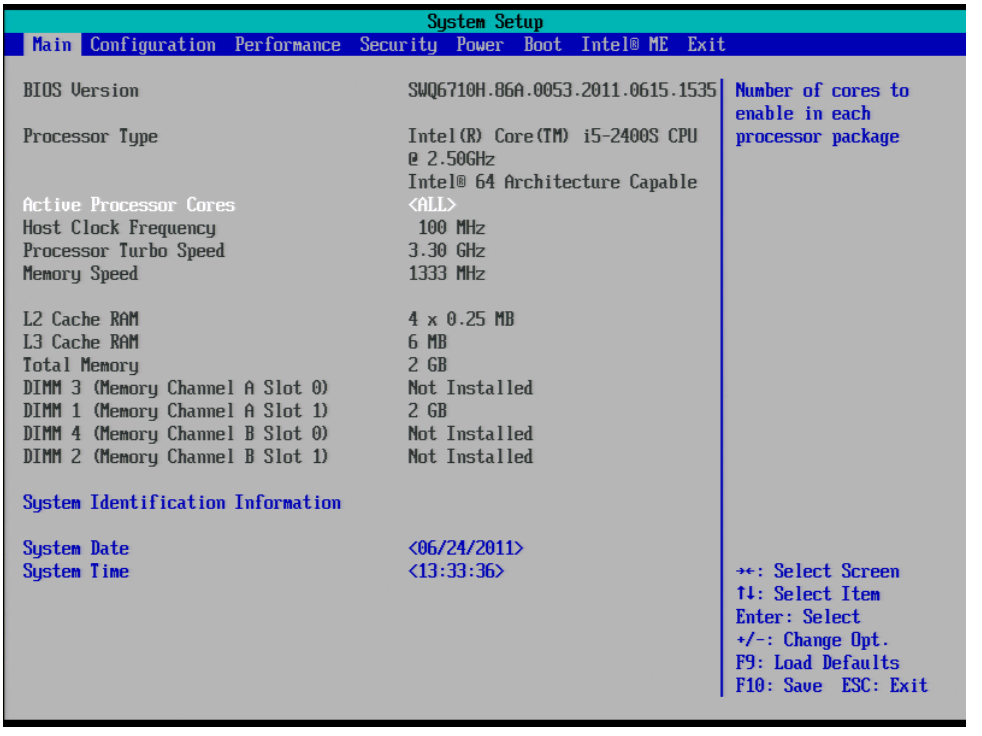


Figure 2. BIOS Setup - Main Menu

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.

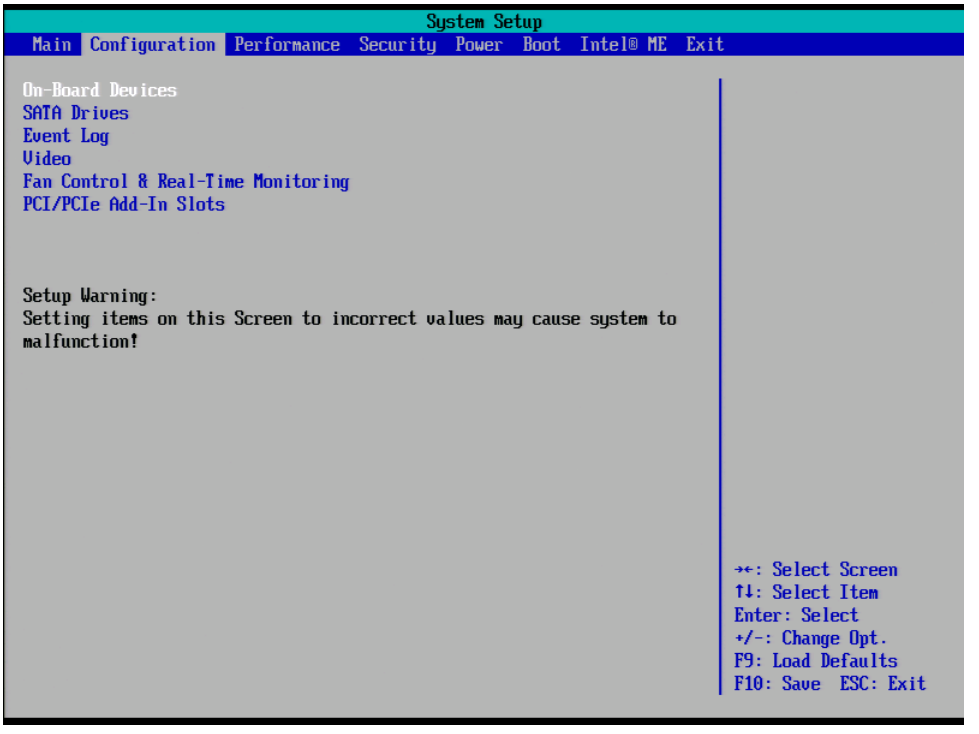


Figure 3. BIOS Setup - Configuration Menu

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

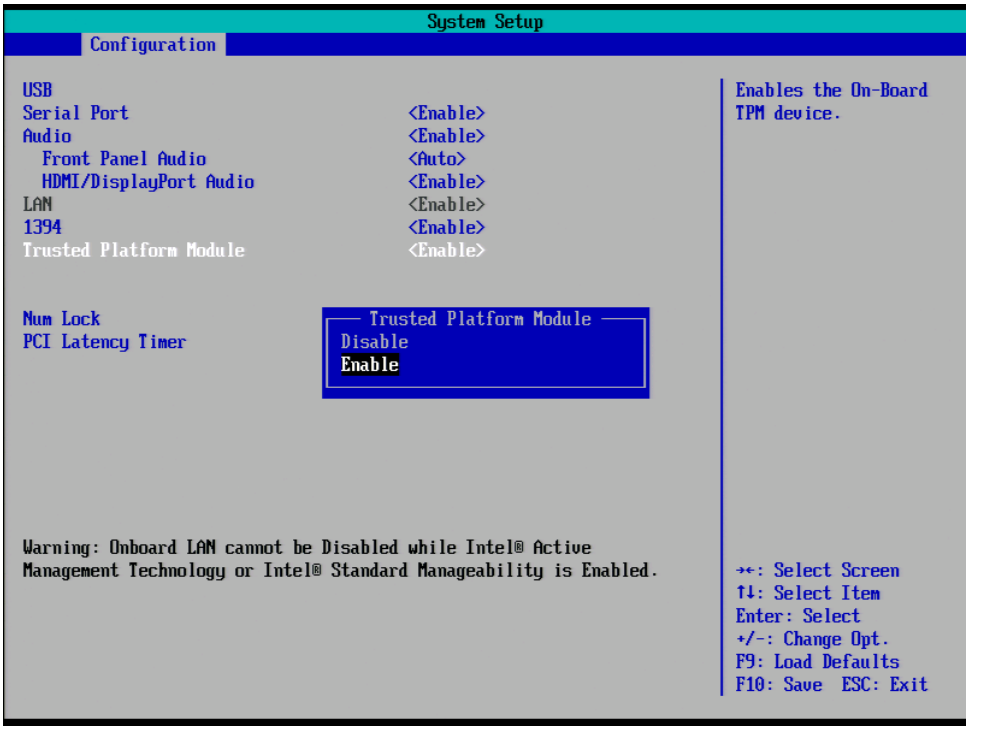


Figure 4. BIOS Setup - Configuration

1.1.4 BIOS Setup – Security Menu

Figure 5 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.

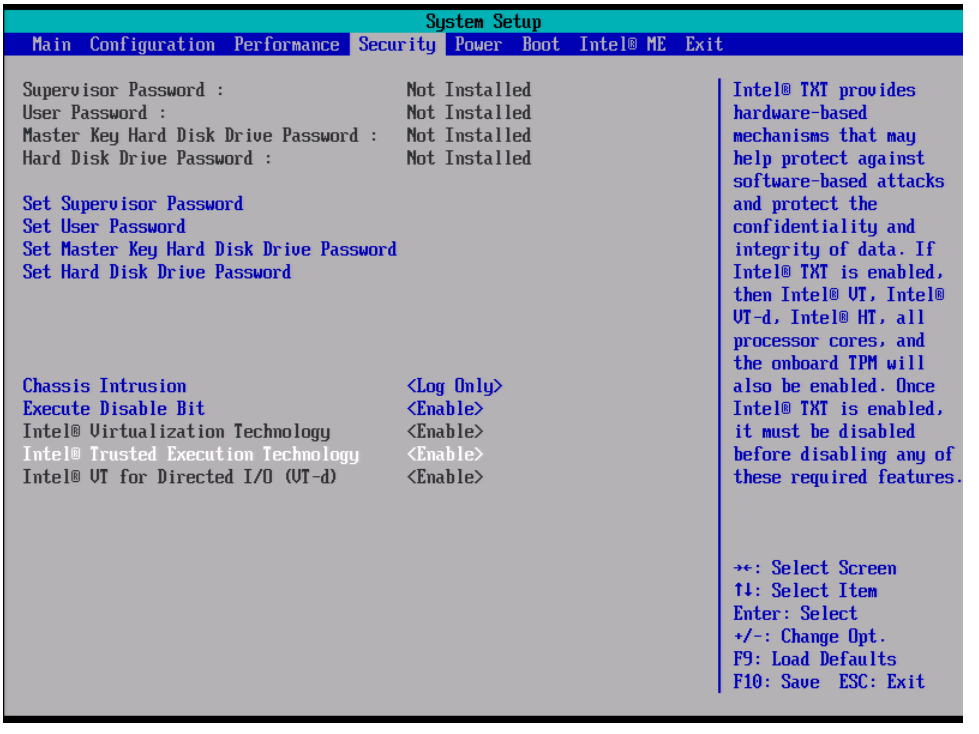


Figure 5. BIOS Setup - Security Menu

Note: Intel VT and Intel VT-d must be enabled before Intel TXT. Once Intel TXT is enabled, the user cannot disable Intel VT or Intel VT-d 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 Boards DQ67SW, DQ67EP and DQ67OW 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.

Note: The Hard Disk Drive Password is only functional for hard drives connected to SATA port 0.

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 6 illustrates the initial Intel ME menu.

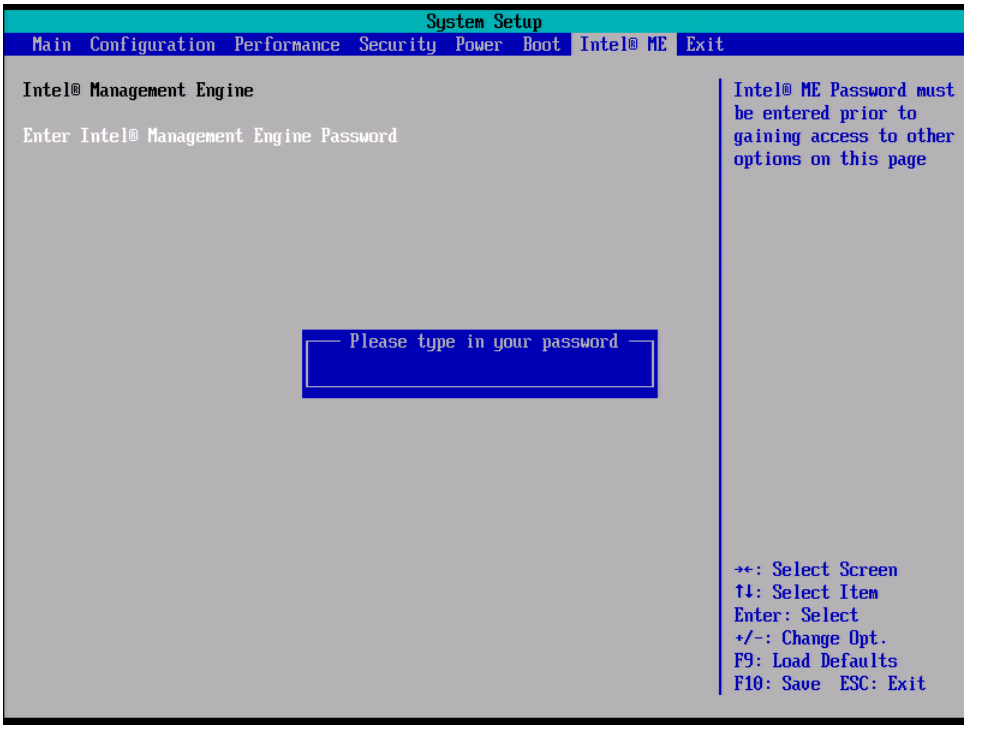


Figure 6. BIOS Setup – Intel® ME Menu

Once the administrator password is set, the user is presented the Intel ME main menu, shown in Figure 7.

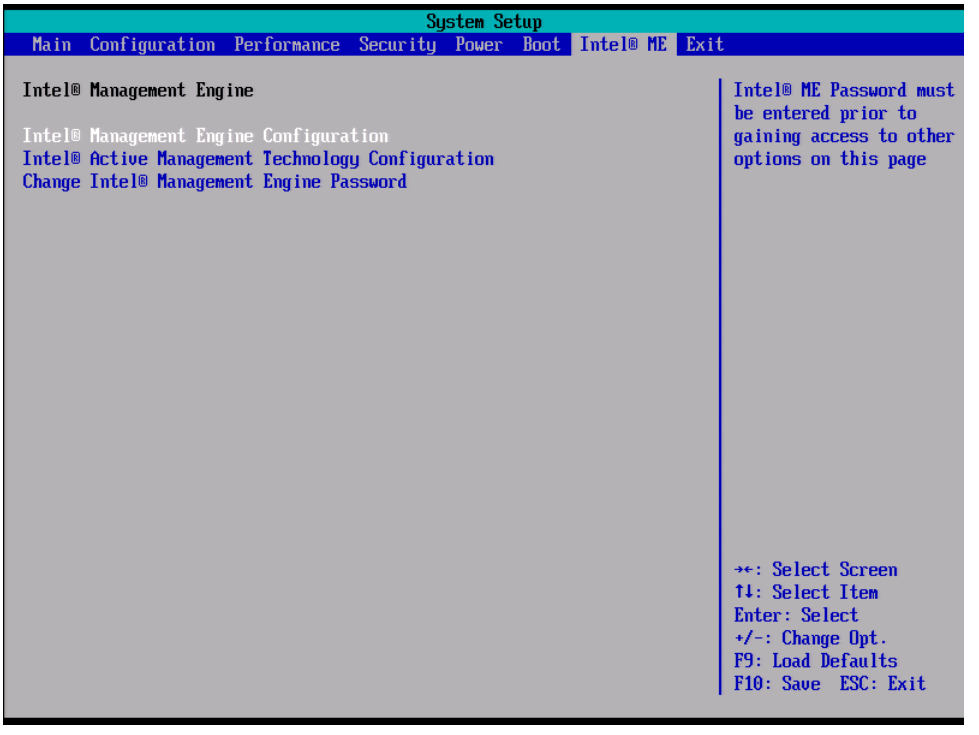


Figure 7. Intel ME - Main Menu

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 8.

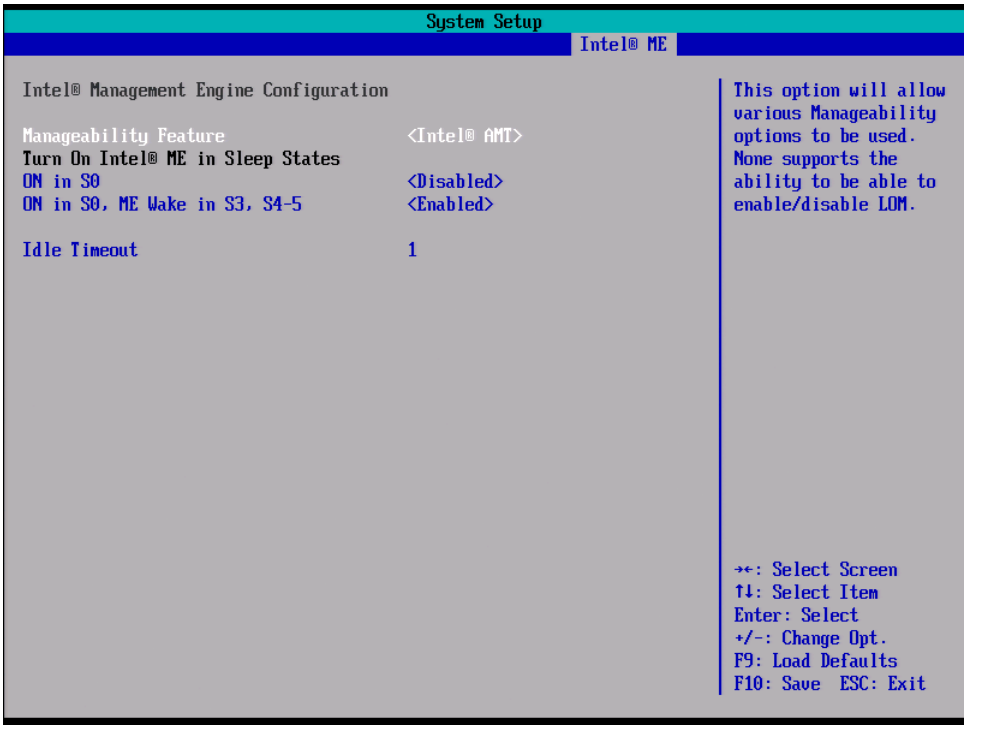


Figure 8. Intel ME – Intel ME Configuration

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 plus 1½ minutes.

1.1.5.2 Intel® ME – Intel® AMT Configuration

Figure 9 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).

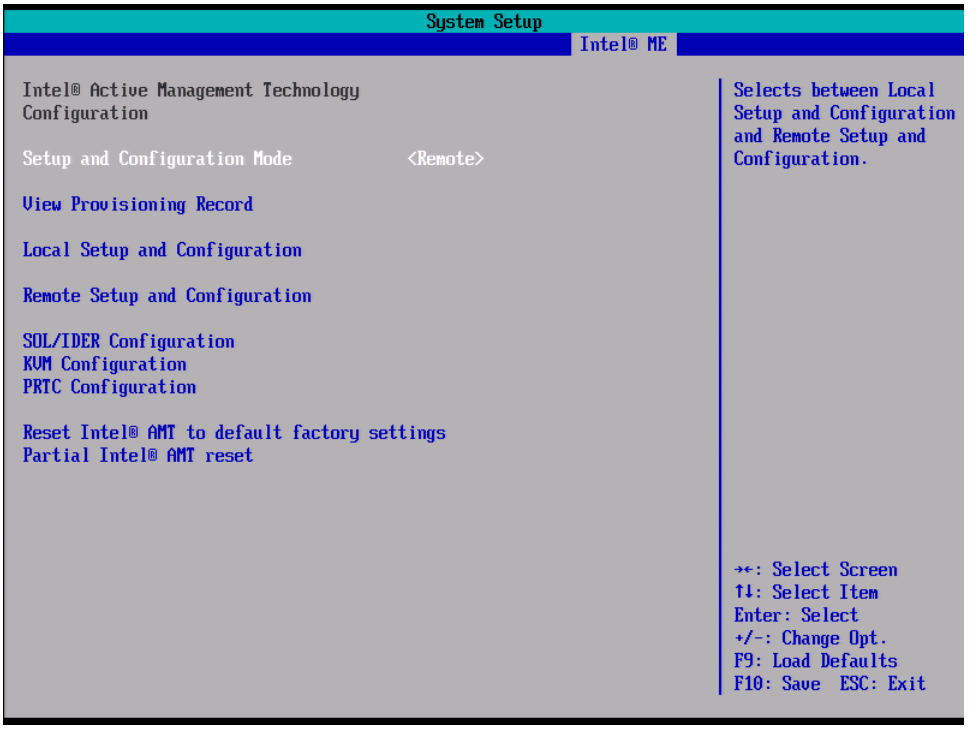


Figure 9. Intel ME - Intel AMT Configuration

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 10 shows the details of Remote Setup and Configuration Mode (previously known as Enterprise, or Standard/Advanced, Provisioning).

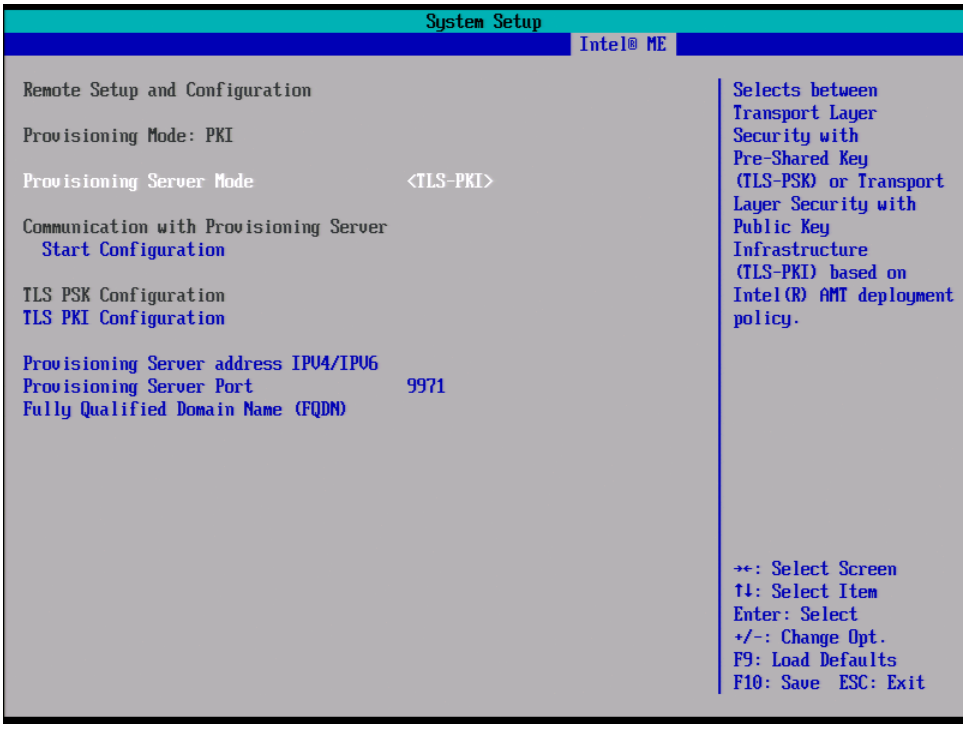


Figure 10. Remote Setup and Configuration - Main Screen

From this screen the user can select whether to use TLS (Transport Layer Security) with PKI (Public Key Infrastructure), also known as Zero Touch 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.

For this generation of Intel AMT, the Remote Configuration Service is disabled by default. As a result, Bare Metal Provisioning is no longer supported. To begin TLS with PKI remote configuration, select Start Configuration under the Communication with Provisioning Server heading. The platform will then begin to send out the "Hello Packets" necessary for Remote Configuration.

1.1.5.2.1.1 Remote Configuration – TLS with PKI

Figure 11 shows the options for TLS with PKI configuration. Figure 12 follows with a view of the Permanent Certificate Manager; the User Certificate Manager operates in a similar manner.

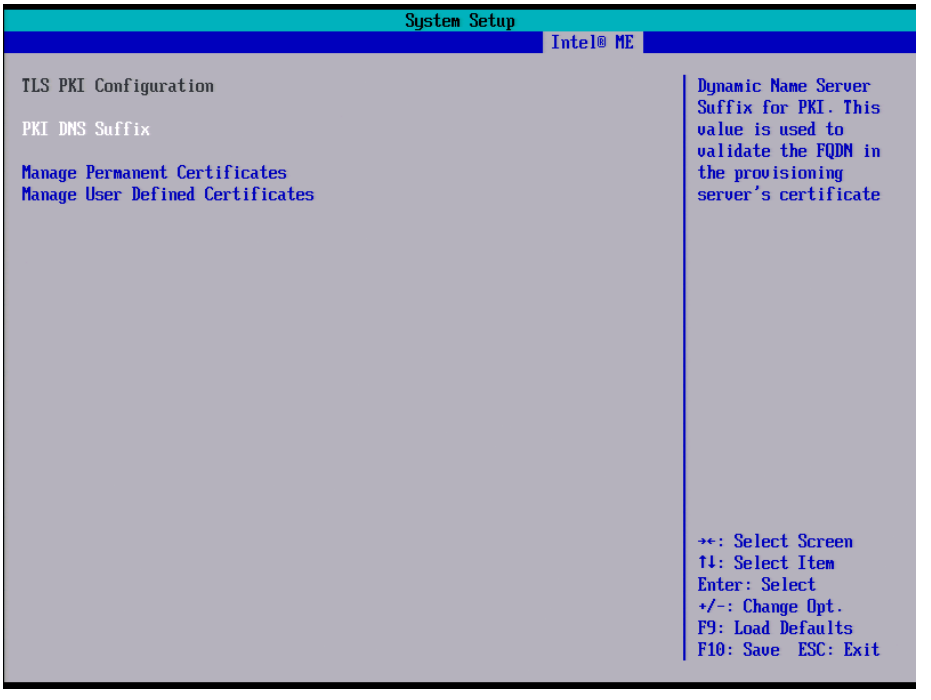


Figure 11. Intel AMT TLS with PKI Provisioning Options

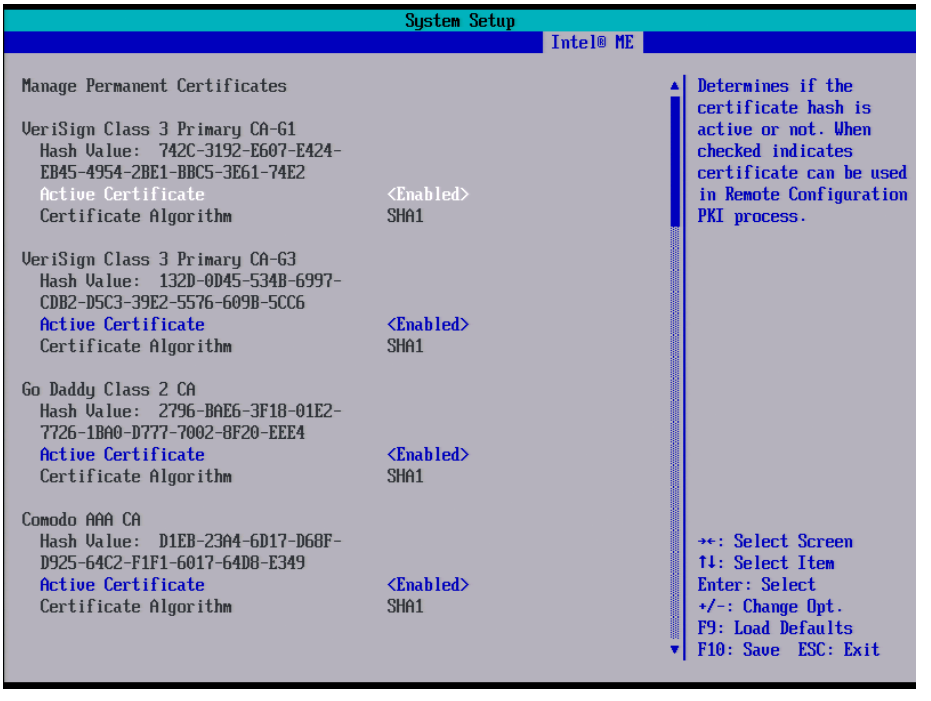


Figure 12. Intel AMT Permanent Certificate Manager

1.1.5.2.1.2 Remote Configuration – TLS with PSK

For TLS with PSK, the options are shown in Figure 13. The Provisioning Identifier (PID) is an eight-character string formatted as two quartets separated by a dash.

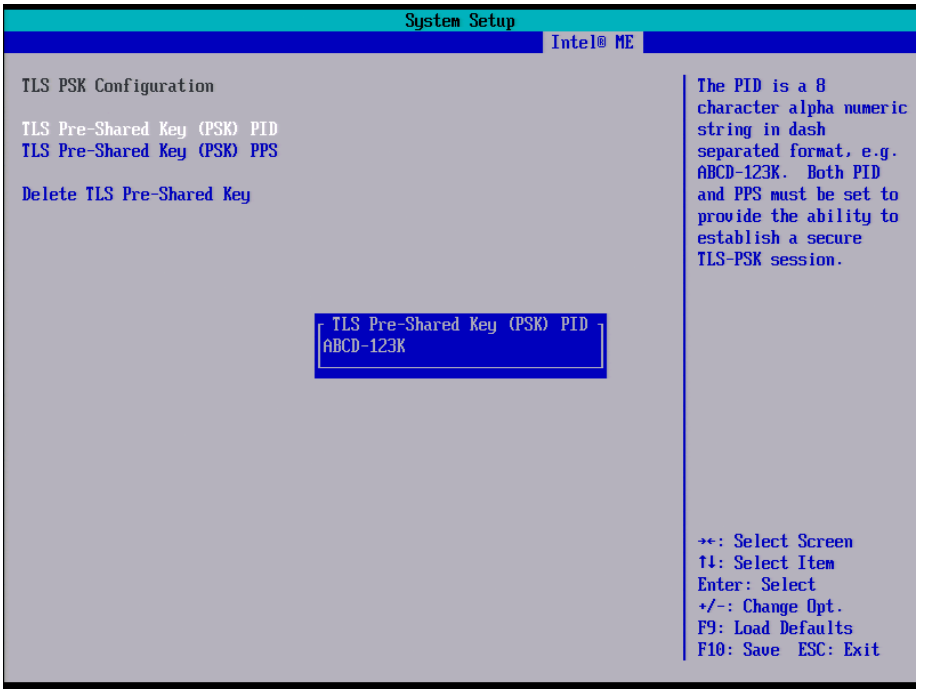


Figure 13. Intel AMT TLS with PSK Provisioning Identifier (PID)

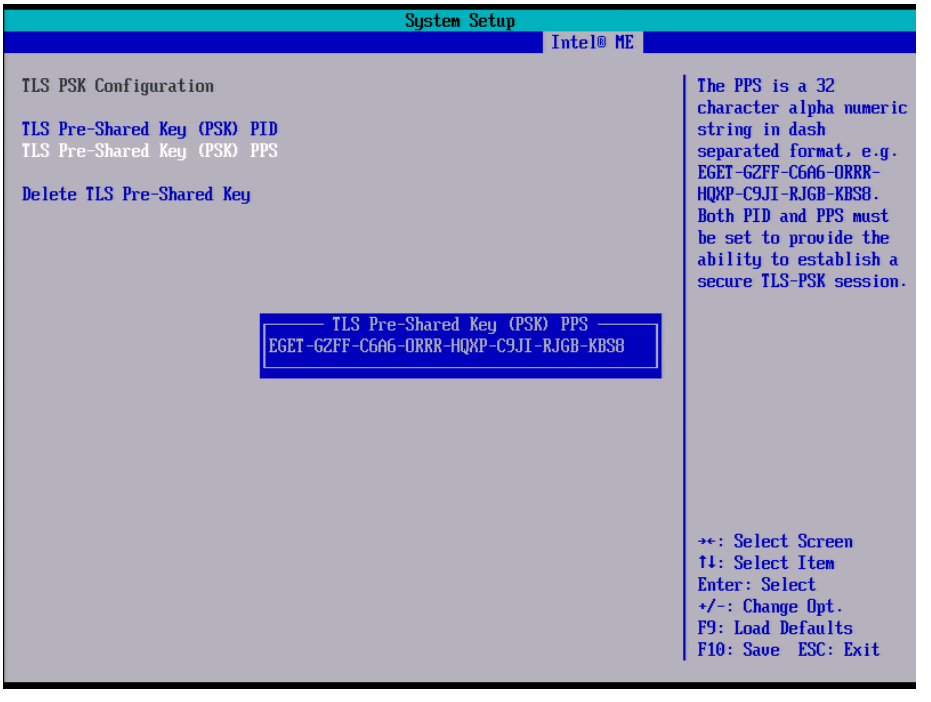


Figure 14. Intel AMT TLS with PSK Provisioning Passphrase (PPS)

1.1.5.2.2 Intel AMT Configuration – Local Configuration

As can be seen from Figure 15 through Figure 17, 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.

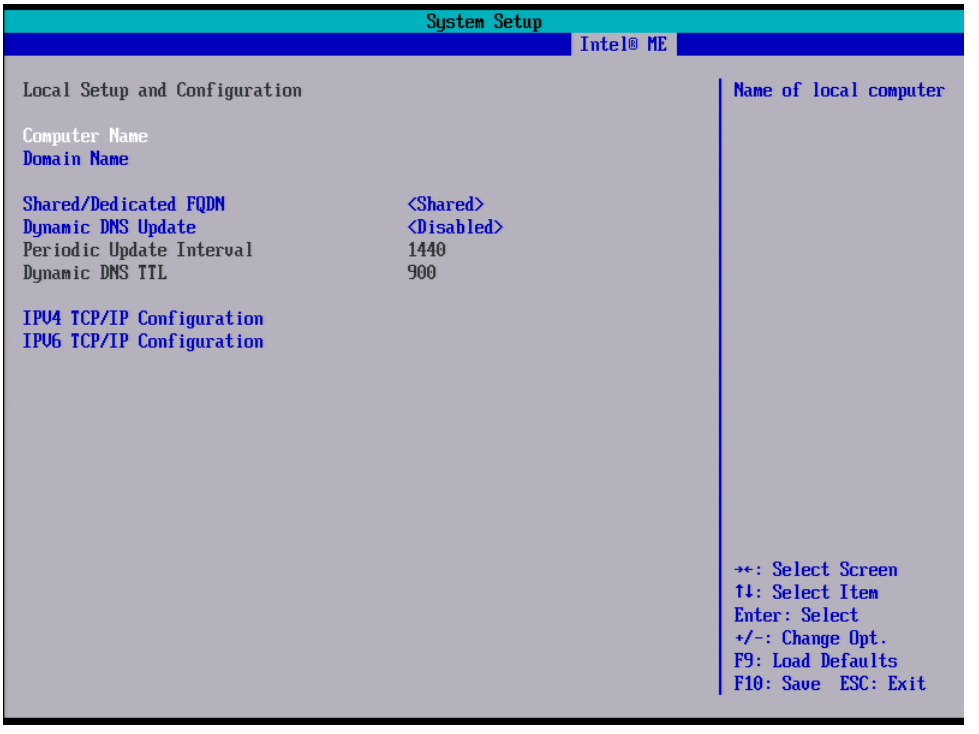


Figure 15. Intel AMT - Local Configuration

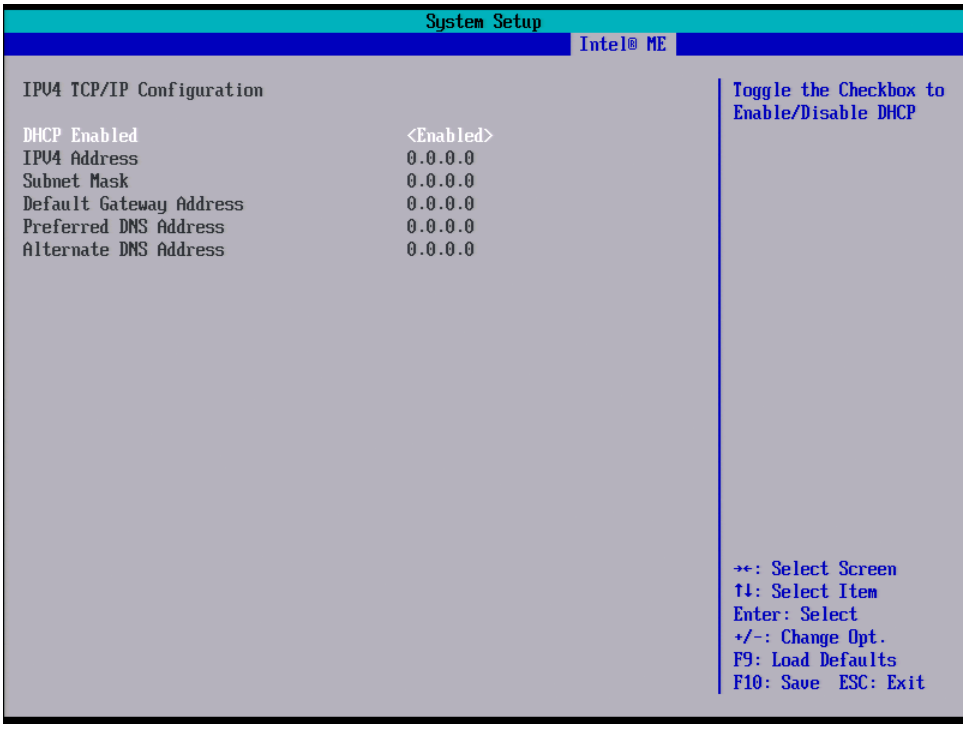


Figure 16. Intel AMT - Local Configuration, IPV4 Configuration Options

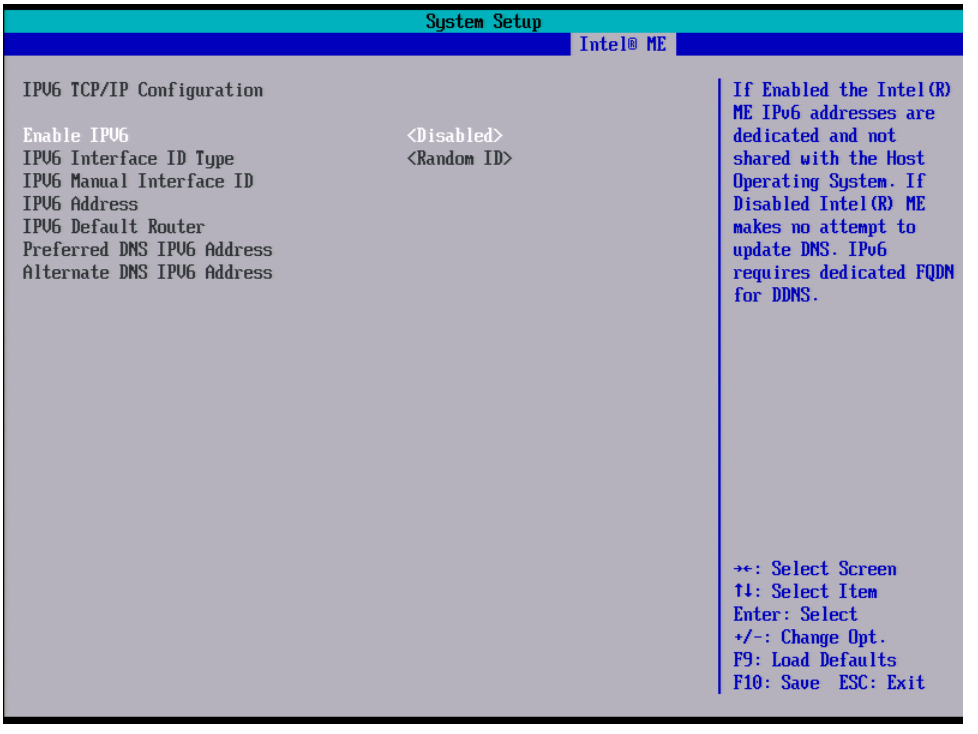


Figure 17. Intel AMT - Local Configuration, IPV6 Configuration Options

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 18; KVM Remote Control (Keyboard Video Mouse) Configuration in Figure 19; and PRTC (Protected Real Time Clock).

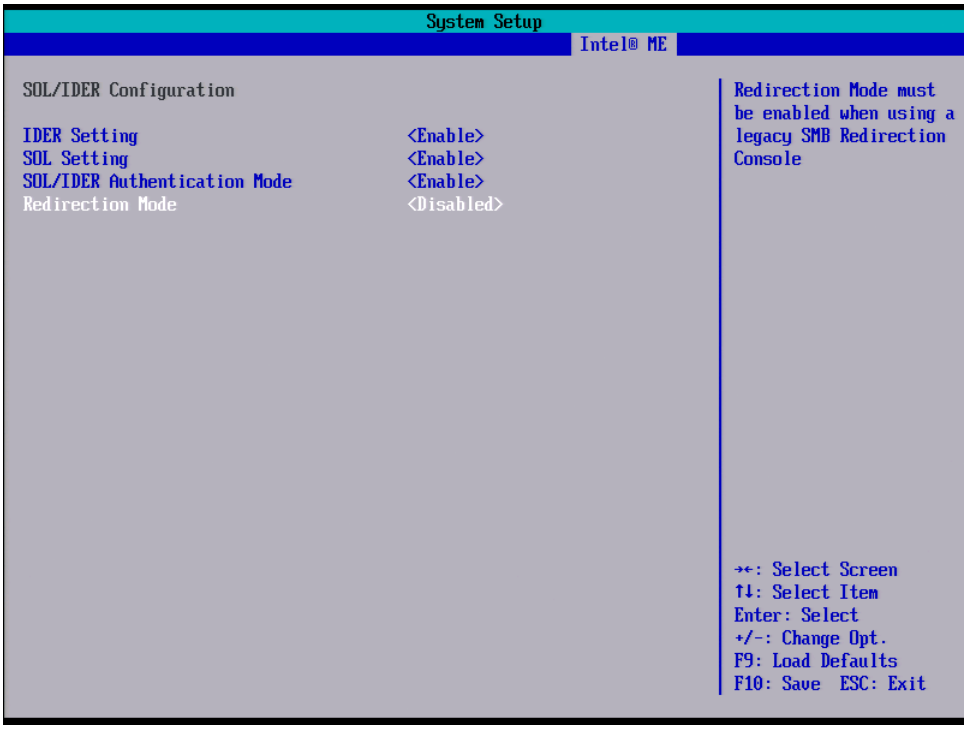


Figure 18. Intel AMT - SOL/IDE-R Configuration

The Redirection Mode setting under SOL/IDE-R, as highlighted in Figure 18, is to allow the use of remote consoles designed for legacy platforms (Intel AMT 5.0 and earlier). These require specific port initialization commands whenever performing redirection operations. Enabling this mode allows the use of Intel AMT 5.0 (and earlier) management consoles with this platform.

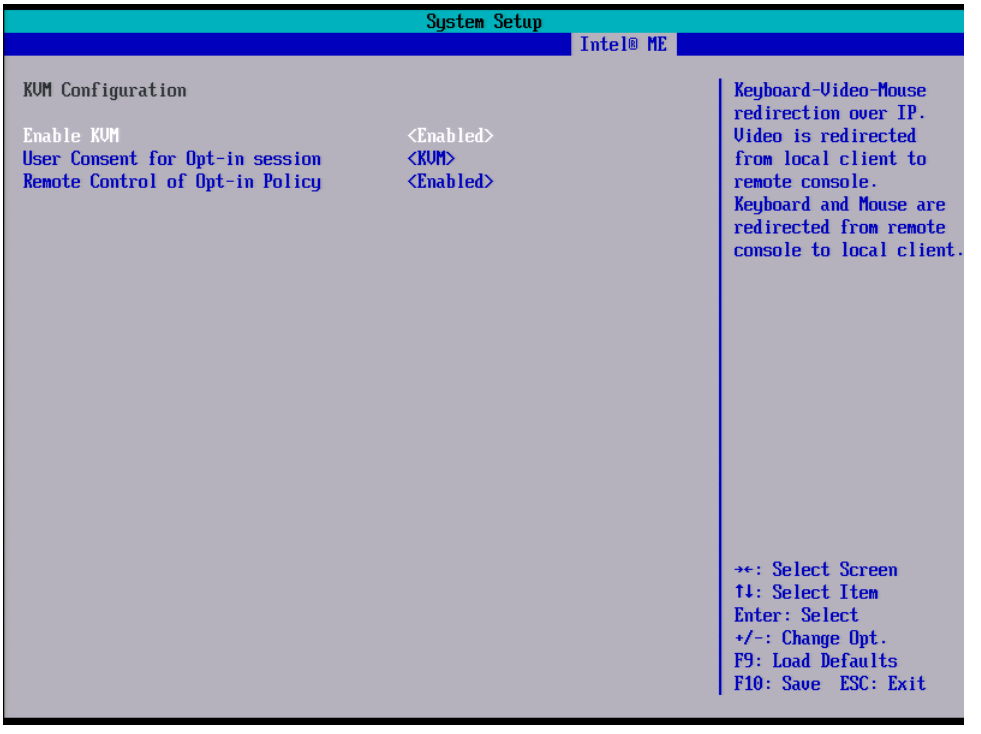


Figure 19. Intel AMT KVM Remote Control Configuration

As shown in Figure 19, the options for KVM Remote Control not only include enabling and disabling the KVM Remote Control feature, but also include the ability to set the level of user-controlled security. The user can choose to allow 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 – Quick Configuration: Local

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 Boards DQ67SW, DQ67EP and DQ67OW in Local Mode, the user needs to:

- Enter **Intel ME** in BIOS Setup.
- Under **Intel AMT Configuration**, set the **Setup and Configuration Mode** to <**Local**>.
- Under **Local Setup and Configuration**, enter a **Computer Name**, as shown in Figure 20. 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 synchronizes the firmware with the updated information.

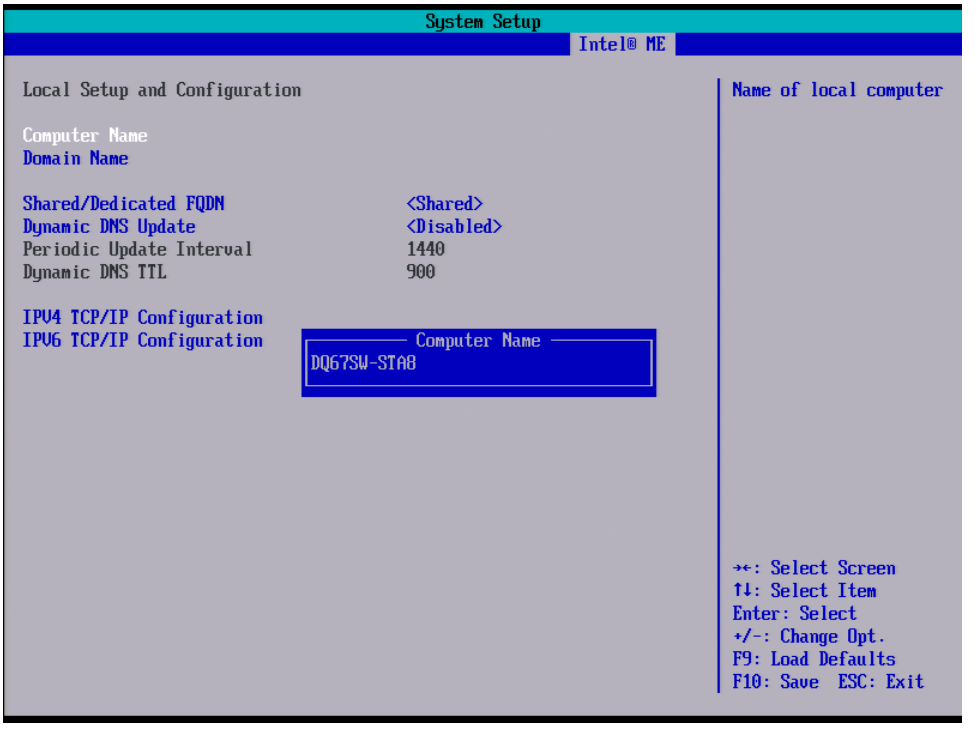


Figure 20. Intel AMT - Configuring Computer Name

Figure 21 and Figure 22 show the results of the MEINFO utility before and after Local Configuration.

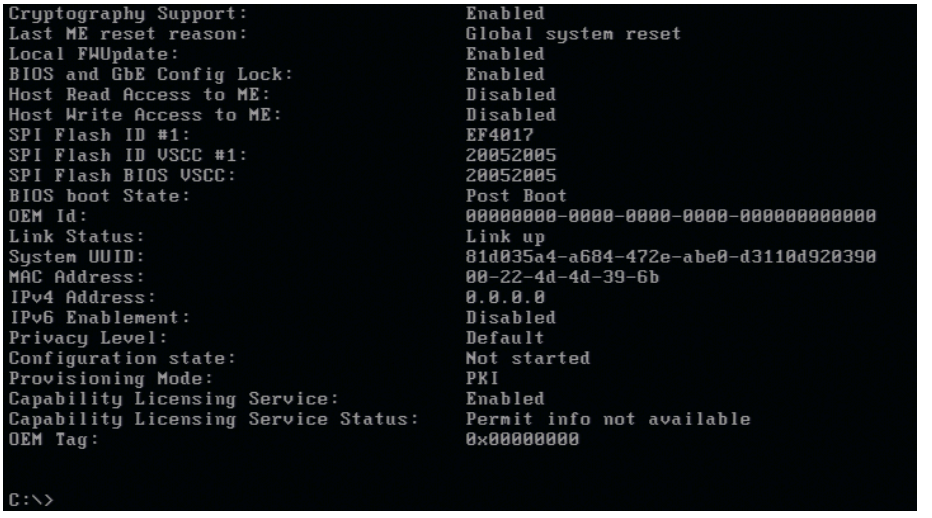


Figure 21. MEINFO Output - Intel AMT Defaults

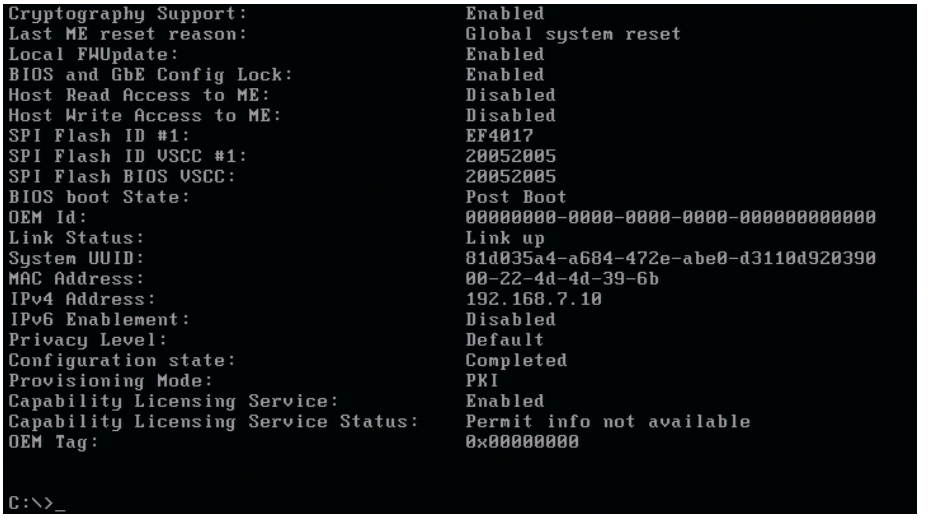


Figure 22. MEINFO Output - Local Configuration

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 13 and Figure 14, 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 Boards DQ67SW, DQ67EP or DQ67OW encountering a USB flash drive with a valid SETUP.BIN at startup is shown in Figure 23. At this point the user presses "Y" and the platform will complete TLS with PSK One Touch configuration.

Figure 23. 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 15 pre-installed permanent certificates. This method of configuration is shown in Section 1.1.5.2.1.1 and Figure 11 and Figure 12.

> **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 AMT Configuration – Host Based Configuration

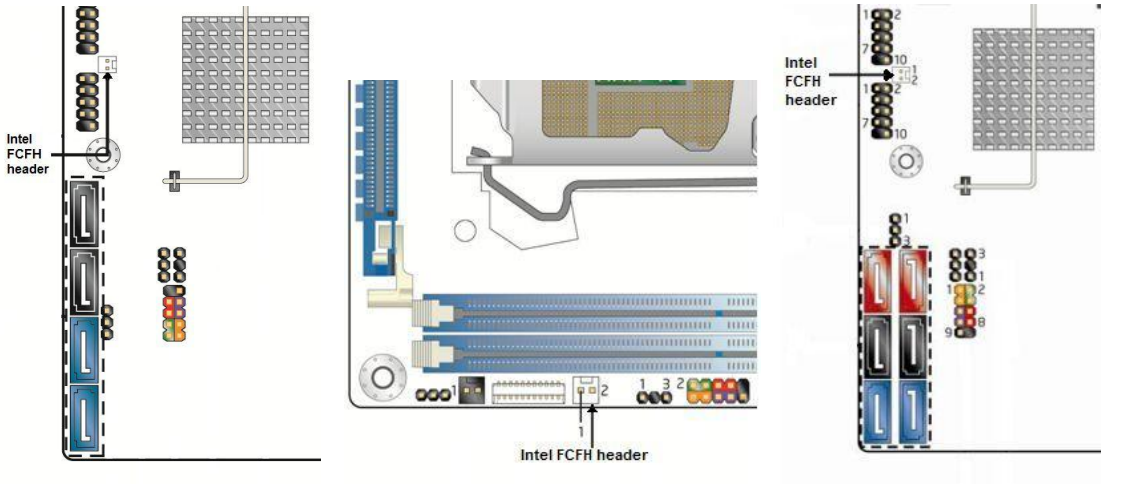
Host Based Setup and Configuration needs no BIOS or Intel MEBX configuration. Instead, an agent is pushed or downloaded to the client, requiring the configuration process to be done from within the operating system, while the client is up (In Band). This also requires a management console application that is capable of initiating Host Based Configuration. Once configured, the client is considered to be in Client Control Mode which restricts certain Intel AMT features, such as disabling the System Defense filters and forcing User Consent for redirection activities like KVM Remote Control and IDE-r.

1.6 Fast Call for Help (FCFH)

Fast Call for Help, or FCFH, requires no configuration out of the box. The user has two methods to activate FCFH: 1) F9 key and 2) FCFH header.

During the initial POST screen, Fast Call for Help can be initiated by repeatedly pressing the F9 key while the "Remote Assistance: F9" message is displayed (if enabled) on the screen (see Figure 1). The user may also choose to connect a momentary switch to the FCFH header located on the board's edge near the PCI slot, as illustrated in

Figure 24. When depressed, an alert will be sent to the system administrator's console. Additional configuration of the system administrator's console may be required in order to receive the alerts. Please refer to the setup and configuration manual for the console you are using for details.



DQ67SW DQ67EP DQ670W

Figure 24. FCFH Header Locations

Figure 25. Fast Call for Help Alert Screen

1.7 KVM Remote Control

KVM Remote Control is available on Intel vPro Q67 Express Chipset-based desktop boards that contain 2011 Intel Core i5 and Core i7 vPro and Intel Xeon processors with integrated Intel HD Graphics.

Note: 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 26. For Authentication, use the Intel AMT administrator password. On the client system, a six-digit access code will appear (Figure 27). This is used in the VNC Viewer+ console to gain access (Figure 28). Figure 29 shows the view of the Intel AMT client as seen from the VNC Viewer+ console.

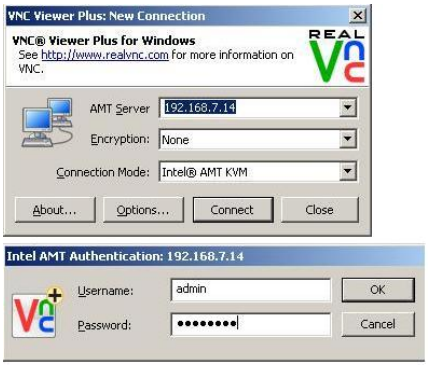


Figure 26. VNC Viewer+ Console Remote Login

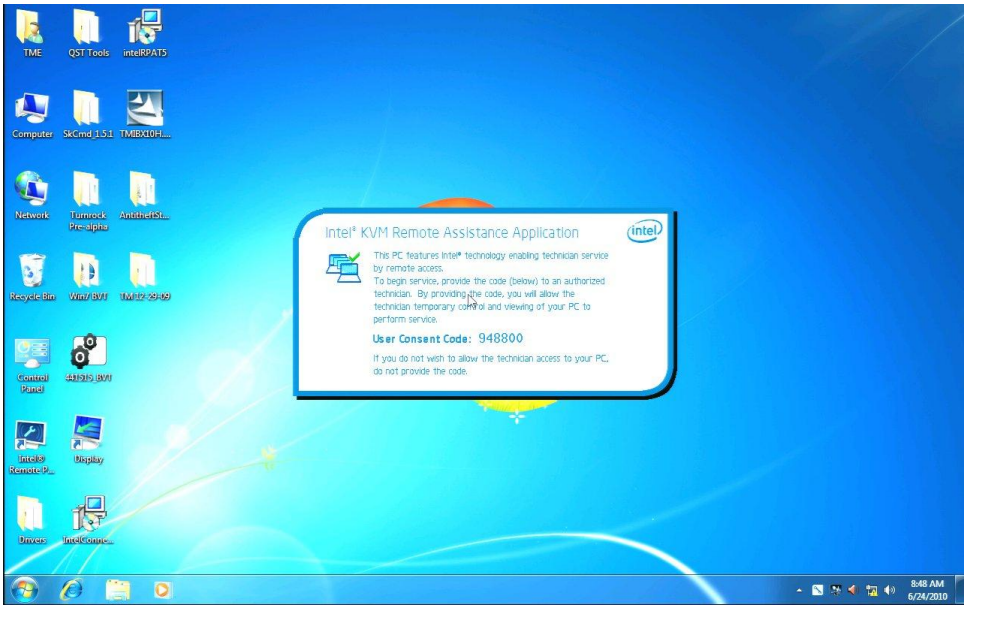


Figure 27. Intel AMT Client Screen Showing KVM Remote Control Access Code

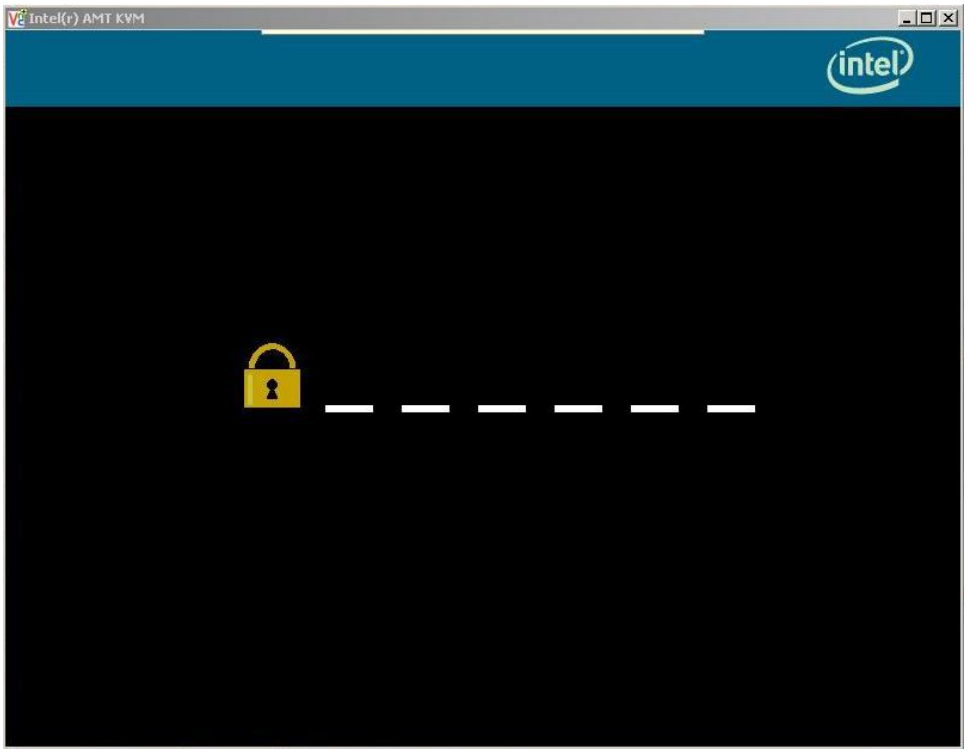


Figure 28. VNC Viewer+ Management Console Access Code Screen

Figure 29. VNC Viewer+ Management Console View

1.8 Intel® Identity Protection Technology (Intel® IPT)

Although not part of Intel vPro technology, Intel® Identity Protection Technology (Intel® IPT) is an integral element in Intel's comprehensive security model. Intel IPT is available on most Intel Desktop Boards with 6 Series Express chipsets. Additional requirements are a 2nd Generation Intel Core or Intel Core vPro processor; a system BIOS containing Intel ME firmware version 7.1 and above; the Intel IPT software stack; and a 3rd-party security agent, such as VASCO* DIGIPASS* for Web or Symantec* VIP Access*, running on the client system.

For Intel Desktop Board DQ67SW, DQ67EP and DQ67OW, BIOS versions 0052 and later contain the proper ME firmware. The Intel IPT software stack and the latest system BIOS can be obtained from the Intel Download Center. The security agent can be found at the respective 3rd-party websites. See Section 2 for links to more information on Intel IPT, as well as links to Intel Download Center and suggested sites for 3rd-party security agents. Figure 30 represents a Symantec VIP Access security credential; Figure 31 shows a security credential for VASCO DIGIPASS for Web Powered by Intel IPT.

Figure 30. Symantec VIP Access Security Credential

Figure 31. VASCO DIGIPASS for Web Security Credential

1.9 BIOS Maintenance Mode

A quick way to reset Intel AMT to default settings (including the Intel ME administrator 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 35 for location). From the BIOS Maintenance screen, select "Reset Intel® AMT to default factory settings" as displayed in Figure 32 and press "Y".

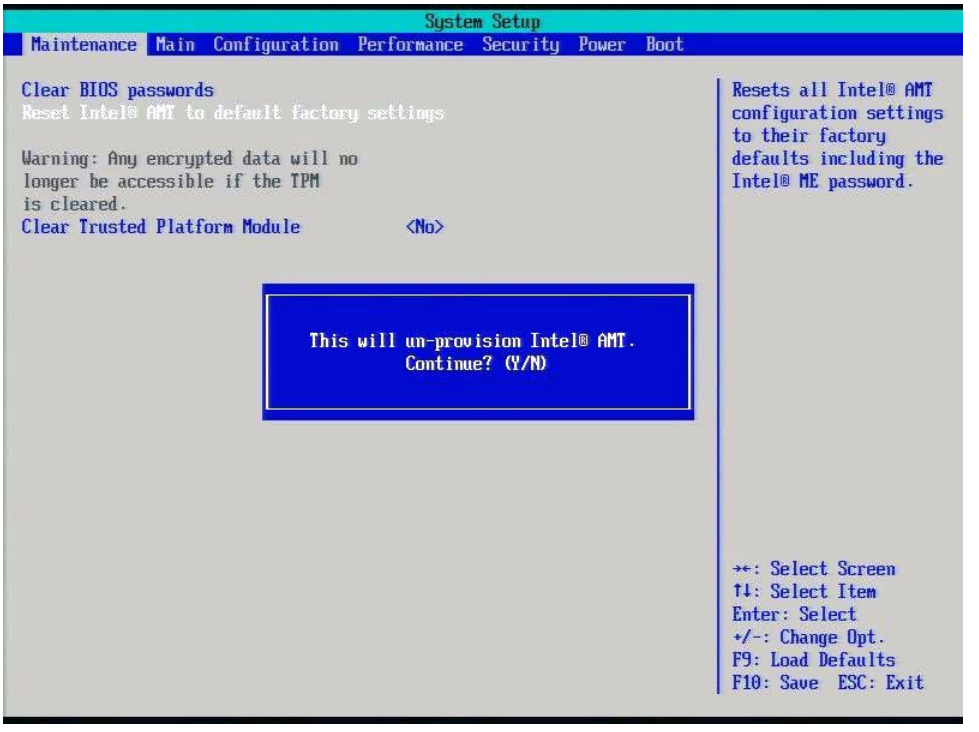


Figure 32. BIOS Maintenance Intel AMT Reset to Defaults

During reset, the screen of Figure 33 is shown. Once finished, the user will receive the notification shown in Figure 34. 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.

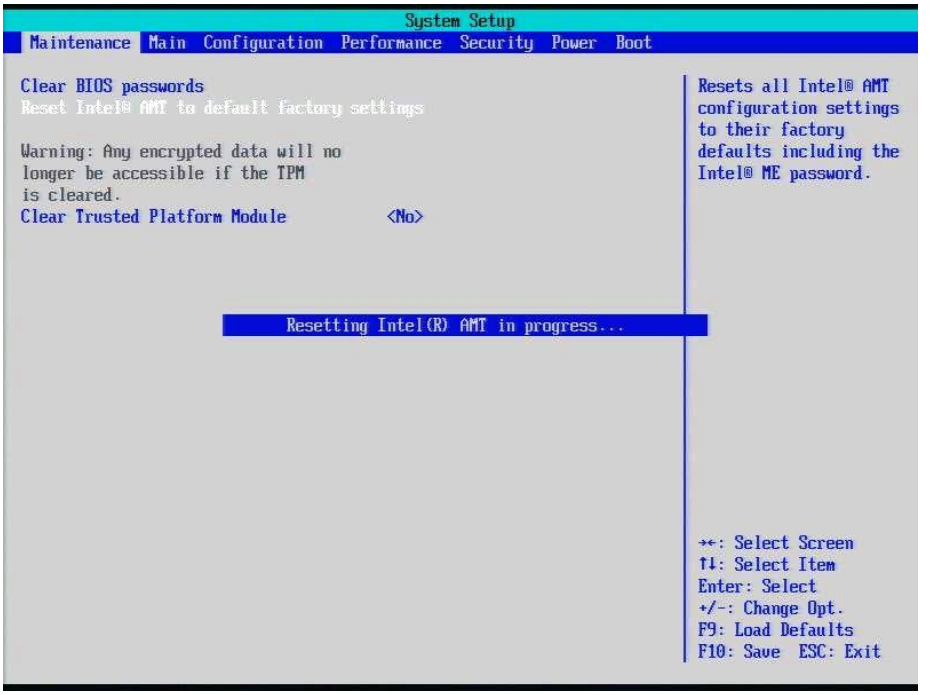


Figure 33. Intel AMT Reset in Progress

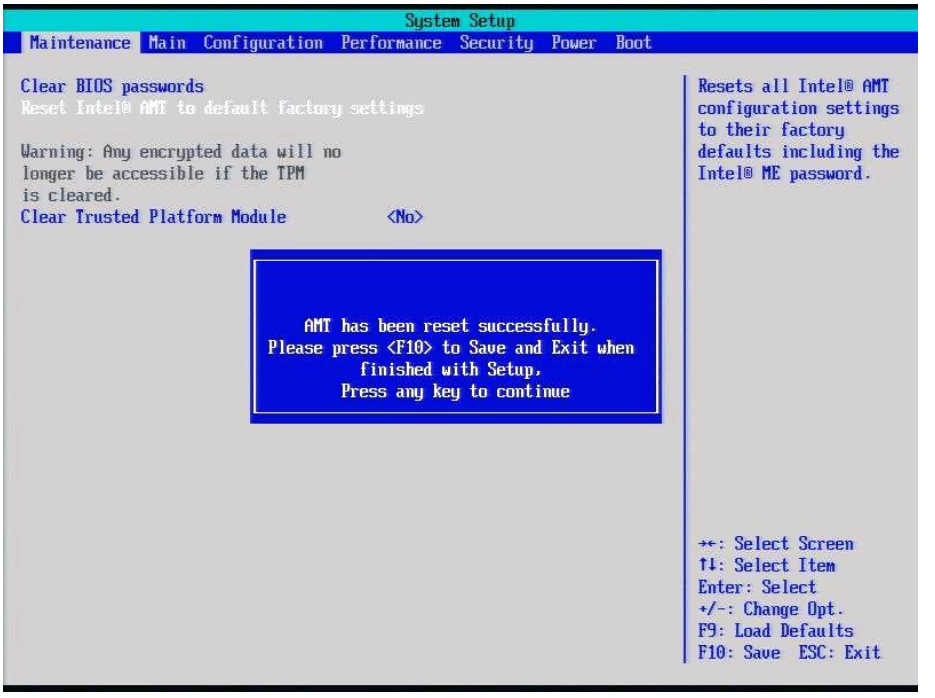
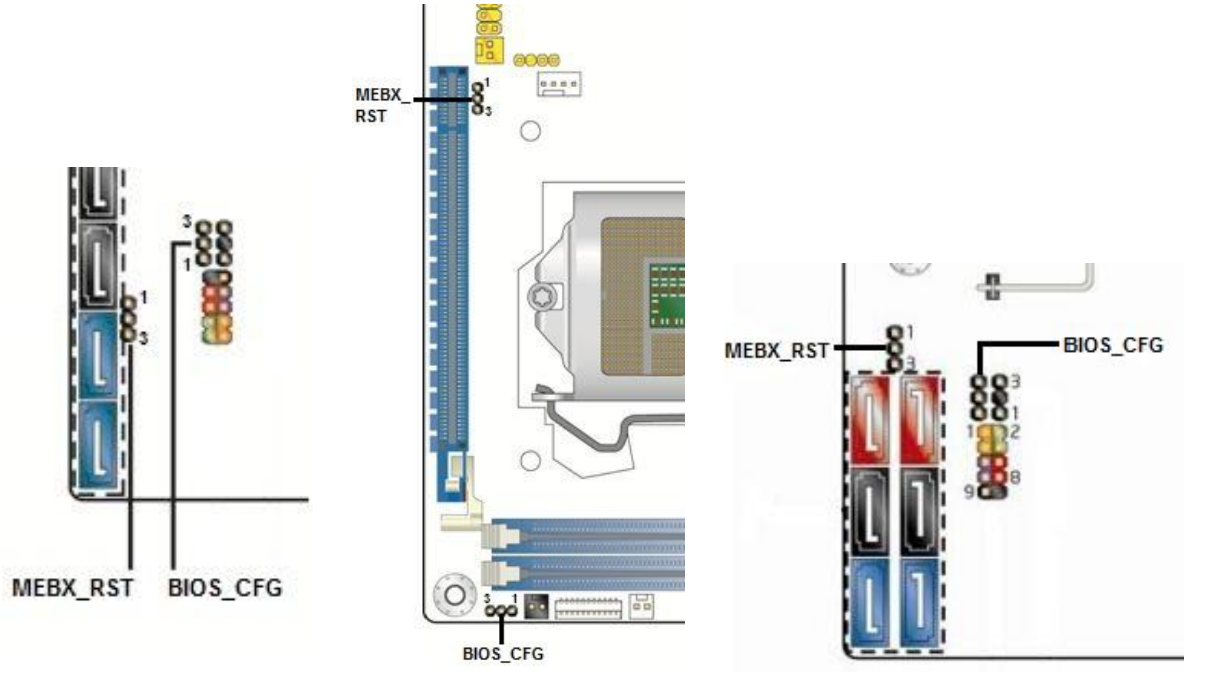


Figure 34. Intel AMT Reset Complete

One other way to reset Intel AMT back to defaults is to use the MEBX_RST 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 MEBX_RST 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 MEBX_RST header. Doing so may cause damage to the board and/or its firmware.

The BIOS_CFG and MEBX_RST headers are shown in Figure 35.



DQ67SW DQ67EP DQ670W

Figure 35. BIOS_CFG and MEBX_RST Header Locations

2. References

http://www.intel.com/support/vpro/sb/CS-030703.htm for a complete list of 1st- and 2nd-generation Intel Core i5 and Core i7 vPro processors.

http://www.intel.com/content/www/us/en/processors/vpro/vpro-technology-reference-guide.html for a high-level overview of Intel vPro technology and use cases.

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://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/xdbit/index.htm?iid=tech_vpro_body_edb for more information on the Execute Disable Bit.

http://software.intel.com/en-us/articles/fast-call-for-help-overview/?wapkw=(fast+call+for+help) for more information on Fast Call for Help.

http://downloadcenter.intel.com to download the latest drivers, BIOS and applications for your Intel Desktop Board.

http://ipt.intel.com to learn more about Intel Identity Protection Technology.

https://idprotect.verisign.com/desktop/home.v to download the Symantec VIP authentication agent and token generator.

http://asp.demo.vasco.com/dps/dp4web/index.jsp for registration and demo of VASCO DIGIPASS for Web Powered by Intel IPT.