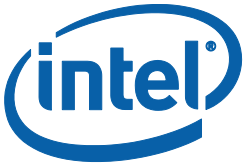


Intel® Management Engine BIOS Extension (Intel® MEBX) User's Guide

User's Guide

For systems based on Intel® 7 Series/C216 Chipset Family

December 2011

Revision 1.0

Contents

Figures

Revision History

Document Number	Revision Number	Description	Revision Date
	1.0	1. 3.5.3 Update user consent description. 2. 3.8 Update SBA new changes.	December 2011
	0.8	1. 3.4.3.2 Correct idle time out unit. 2. 3.5.8.6.1 Give valid string for PID and PPS example. 3. 3.5.8.7.4 Remove un-support process	August 2011
	0.7	Add 3.8 Small Business Manageability. 3.9 CPU replacement flow Modify 3.4.2 Local FW update	May 2011
	0.6	Technical review version	April 2011
	0.5	Draft version	March 2011

§

1 Introduction

1.1 Intel® Management Engine (Intel® ME) and Intel® Management Engine BIOS Extension (Intel® MEBX) Overview

The Intel® Management Engine (Intel® ME) is an isolated and protected computing resource. The Intel ME provides the following IT management features independent of the installed OS:

- Intel® Active Management Technology (Intel® AMT 8.0), allowing improved management of corporate assets.

Intel ME configuration is included in the BIOS by the Intel® Management Engine BIOS Extension (Intel® MEBX). The Intel MEBX provides the ability to change and/or collect the system hardware configuration, passes it to the management firmware and provides the Intel ME configuration user interface.

1.2 Scope of document

This document describes how to configure the Intel MEBX for Intel® 7 Series Chipset Family/Intel® PCH platforms with Intel AMT 8.0.

Note: The Intel ME configuration procedures described in this guide are part of the larger Intel® vPro™ technology activation and provisioning process. These configuration procedures can vary significantly (or be performed automatically) and depend on which third-party management console you are using. See the Related Documentation section of this guide (section 1.5) for a list of Intel-authored provisioning guides that are specific to several popular management consoles. These provisioning guides provide the end-to-end process for provisioning your Intel® vPro™ computers with the specified management console, and may or may not include references to the Intel ME manual configuration procedures in this guide (depending on which provisioning model is used).

1.3 Target Audience

This user guide is primarily intended for Information Technology (IT) administrators and system integrators with experience in implementing complex computer and network installations. It is not intended for general audiences.

Note: Readers should have a basic understanding of networking and computer technology terms, such as TCP/IP, DHCP, IDE, DNS, Subnet Mask, Default Gateway and Domain Name. Explanation of these terms is beyond the scope of this document.

1.4 Acronyms

Acronym	Description
ASF	Alert Standard Format
BIOS	Basic Input Output System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
EIT	Embedded Information Technology (see VA)
EPS	VA Private Store Intel's VA Specific Store in an ME-owned flash area separate from 3PDS. The size is one (1) physical page (4K bytes)
FW	Firmware
G3	Complete Power loss (AC power plug pulled)
GbE	Gigabit Ethernet
GMT	Greenwich Mean Time
HW	Hardware
HBP	Host Based Provisioning
Intel® AMT	Intel® Active Management Technology
Intel® ME	Intel® Management Engine
Intel® MEBX	Intel® Management Engine BIOS Extension
Intel® MEI	Intel® Management Engine Interface
IP	Internet Protocol
LAN	Local Area Network
MSP	Manageability Service Provider
OPK	OEM Pre-Installation Kit
OS	Operating system
PRTC	Protected Real Time Clock
RCFG	Remote Configuration
S3	Standby sleep state
S4	Hibernate sleep state
S5	Shutdown sleep state
SPI	Serial Peripheral Interface
SW	Software

Acronym	Description
TCP	Transmission Control Protocol
UTC	Coordinated Universal Time
VA	Virtual Appliance
VLAN	Virtual LAN
WOL	Wake on LAN

1.5 Related Documentation

Refer to the Intel® vPro™ Expert Center's user documentation page, available at the link below, for a collection of documents containing further information on the Intel® vPro™ provisioning process, including specific documents for implementing Intel® vPro™ technology with a number of popular management consoles:
http://communities.intel.com/community/openportit/vproexpert?view=documents
In addition, please refer to the Intel® vPro™ Expert Center at the link below for general information about Intel® vPro™ technology:
http://communities.intel.com/community/openportit/vproexpert

§

2 Client System Requirements

The client system referred to in this document is based on the Intel® 7 Series Chipset Family/Intel® PCH platform, and is managed by Intel Management Engine. The following firmware and software requirements are required to be installed and set up before the Intel Management Engine can be configured and run in the client system:

- SPI flash device programmed with Intel AMT 8.0 flash image integrating BIOS, Intel Management Engine and GbE component images
- BIOS set up with Intel AMT enabled
- To enable all of the Intel Management Engine features within Microsoft Operating System, device drivers (Intel® MEI/SOL/LMS) must be installed and configured on the client system for features to work/run correctly in the client system

§

3 Intel® ME Manageability Features

The Intel MEBX menu for digital office SKUs provides platform level configuration options for the IT-administrator to configure the behavior of the Intel ME platform. The behavior includes platform configuration such as individual feature enable/disable and power configurations.

The following section provides the details on each Intel MEBX configuration option and the constraints, if any, for a given option.

Note: When you change Intel® ME Platform Configuration settings, the changes are committed to the Intel ME's non-volatile memory when you exit from Intel MEBX (the changes are not cached). Therefore, if Intel MEBX crashes before you exit, the changes made until that point are **LOST** and the changed settings are **NOT** saved.

3.1 Access Intel® MEBX Configuration User Interface

The Intel MEBX configuration user interface can be accessed on a client system through the following steps:

1. On rebooting the system, after the initial boot screen, the following message will be displayed: **'Press <CTRL-P> to enter Intel® ME Setup'**

Note: To enter the Intel MEBX, press <Ctrl-P> as soon as possible, since this message is displayed for only a few seconds. Also note that the OEM may replace the control character <Ctrl-P> with another one or don't display it at all.

Note: <Ctrl-P> will be hidden when SoL or KVM session is established. Users are not able to access MEBx UI in this scenario.

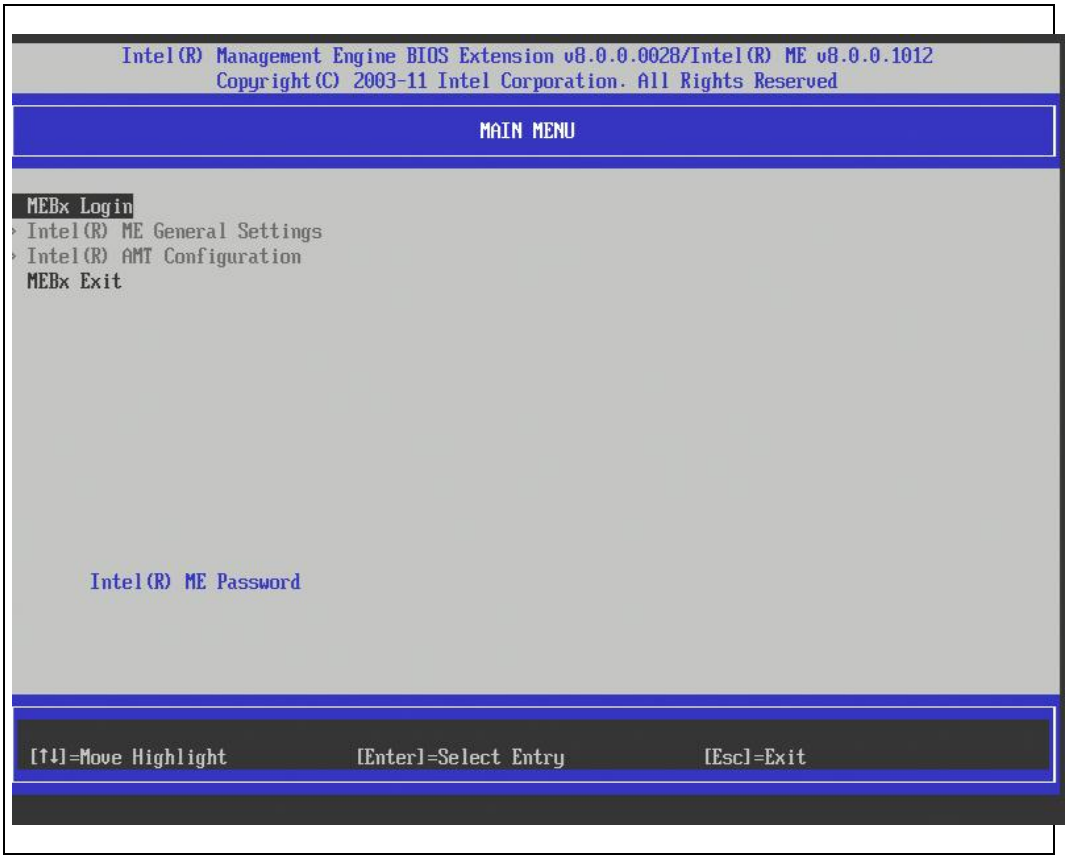
Note: If Intel® AMT has been configured, <CTLR-ALT-F1> will also be displayed along with <CTRL-P>. It is designed for end users to use Fast call for Help feature either inside or outside of corporate network environment when Intel® AMT systems are not discovered by management console.

2. Enter the Intel Management Engine password under **'MEBX Password'**. Press Enter. The default password is 'admin'. This default password can be altered by the user. Please refer to section 3.3 for Intel ME password details.
3. The Intel MEBX screen is displayed, as shown in section 3.2.

4. [Esc] means exit current setting page.

3.2 Intel® MEBX Main Menu

Figure 1: Intel® MEBX Configuration User Interface Main Menu



The options displayed in the main menu can vary depending on OEM implementation decisions. The main menu selections are:

- MEBx Login
- Intel ME General Settings
- Intel® AMT Configuration
- MEBx Exit

Note: Intel MEBX will display only detected options. If one or more of these options does not appear, verify that the system supports the relevant missing feature.

3.3 Change Intel® ME Password

The default password is “admin” and is configured identically on all newly deployed platforms. When an IT administrator first enters the Intel MEBX configuration menu with the default password, he or she must change the default password before any feature can be used.

The new Intel MEBX password must meet the following requirements for strong passwords:

1. **Password Length**: At least 8 characters, and no more than 32.
2. **Password Complexity**: Password must include the following:

At least one digit character (‘0’, ‘1’, … ‘9’)

At least one 7-bit ASCII non alpha-numeric character (e.g. '!', '$', ';'), but excluding ‘:’, ‘,’ and ‘”’ characters.

At least one lower-case letter ('a', ‘b’…’z’) and at least one upper case letter ('A', ‘B’…'Z').

Note: ‘_’ (underscore) and ‘ ‘ (whitespace) are valid password characters but do NOT contribute to the password’s complexity.

Note: There are certain limitations creating passwords with non-US layout keyboards. Remote system connectivity may occur if different keyboard layouts are used on the same hardware.

Note: When entering more than 32 characters the software changes the 32nd character on every new character pressed when in the last character position in the MEBx UI. So whatever the last character typed on the 32nd position, it will replace the existing character in that position.

Note: The password can be reset to the default setting (admin) by shutting down the system, removing AC and DC power and performing a RTC reset.

3.4 Intel® ME Platform Configuration Menu

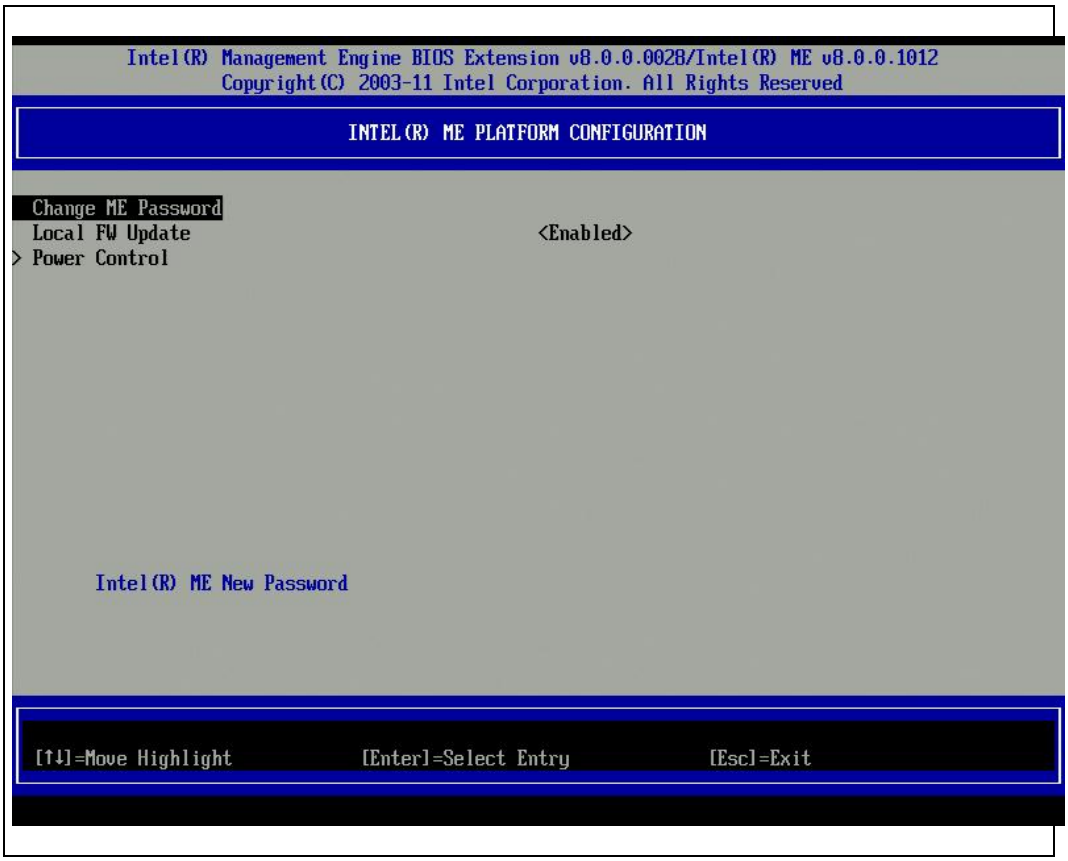
Under the Intel MEBX main menu,

1. Select ‘Intel ME General Settings’.
2. Press Enter.

The following message is displayed: ‘Acquiring General Settings configuration’.

The Intel® MEBX main menu changes to the Intel® ME Platform Configuration page. This page allows the IT administrator to configure the specific functionality of the
Intel® ME, such as password, power Control, etc.

Figure 2: Intel® ME Platform Configuration



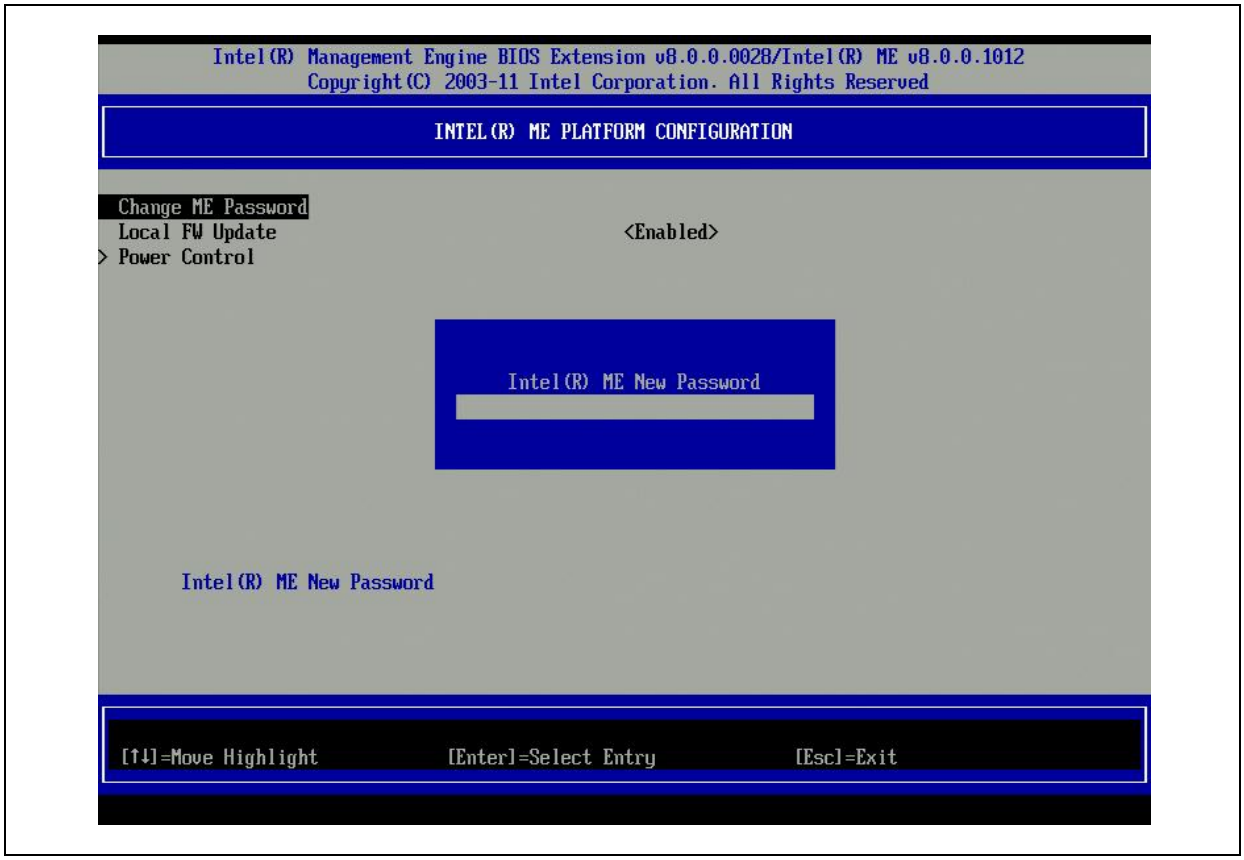
3.4.1 Change Intel® ME Password

Under the Intel® ME Platform Configuration menu,

1. Select ‘Change ME Password’.
2. Press Enter to change password.

The Intel ME New Password prompt is displayed as in Figure 3.

Figure 3: Change Intel® ME Password



1. At the Intel® ME New Password prompt, enter your new password. (Please be aware of the password policies and restrictions mentioned in section 3.3)
2. At the Verify Password prompt, re-enter your new password.

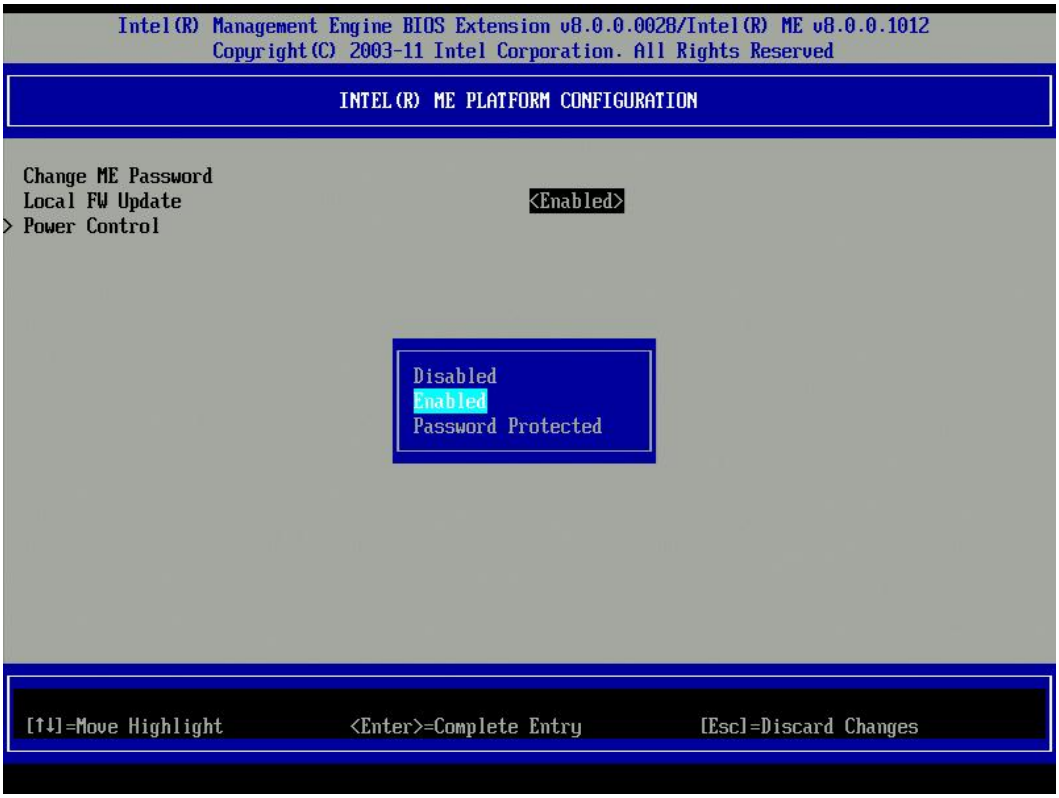
Your password is now changed.

3.4.2 Local FW Update

Under Intel® ME Platform Configuration,

1. Select 'Local FW Update'.
2. Press Enter to select.

Figure 4: Local FW Update Settings



Intel® ME Firmware Local Update provides the capability to allow or prevent firmware local update in the field. When the "Enabled" option is selected, the IT-admin is able to update the Intel® ME firmware locally via the local Intel Management Engine interface or via the local secure interface.

The following options can be selected:

- **Disabled –** Do NOT allow Local Intel ME FW Update
- **Enabled –** Allow Local Intel ME FW Update
- **Password Protected** – Local FW update is protected by MEBx password

Note: When **Hide FW Update Control** setting in FITC is set, MEBx will hide Local FW Update option.

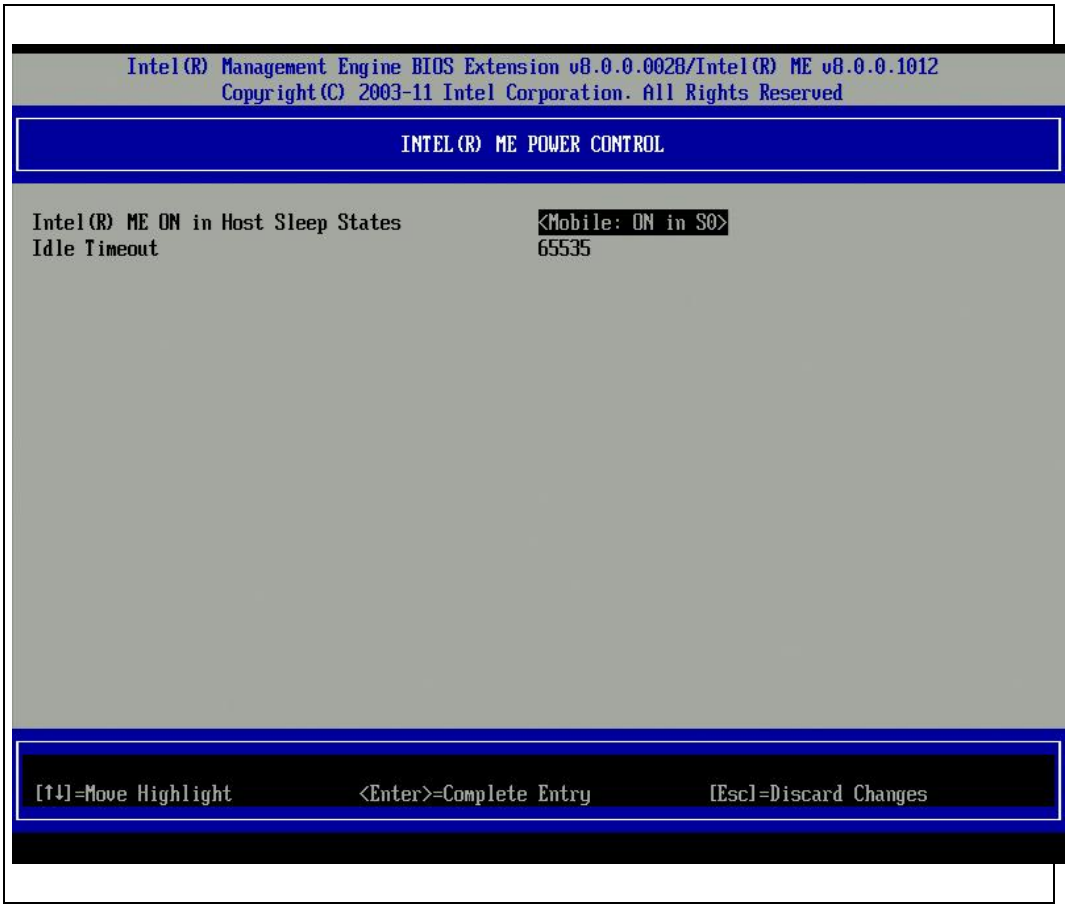
3.4.3 Power Control

Under Intel® ME Platform Configuration,

1. Select ‘Power Control’.
2. Press Enter.

The Intel® ME Platform Configuration screen changes to the Intel® ME Power Control screen.

Figure 5: Power Control



To comply with ENERGY STAR* and EUP LOT6 requirements, the Intel ME can be turned off in various sleep states. The Intel ME Power Control menu configures the Intel ME platform power related policies.

3.4.3.1 Intel® ME ON in Host Sleep States

Under Intel ME Power Control,

1. Select 'Intel ME ON in Host Sleep States'.
2. Press Enter to select.

The following options can be selected:

- **Mobile: On in S0 –** Power Package 1
- **Mobile: On in So, ME Wake in S3, S4-5 –**Power Package 2

Table 1: Supported Power Packages

Power Package	1	2
S0	ON	ON
S3	OFF	ON /ME WoL
S4/S5	OFF	ON/ ME WoL

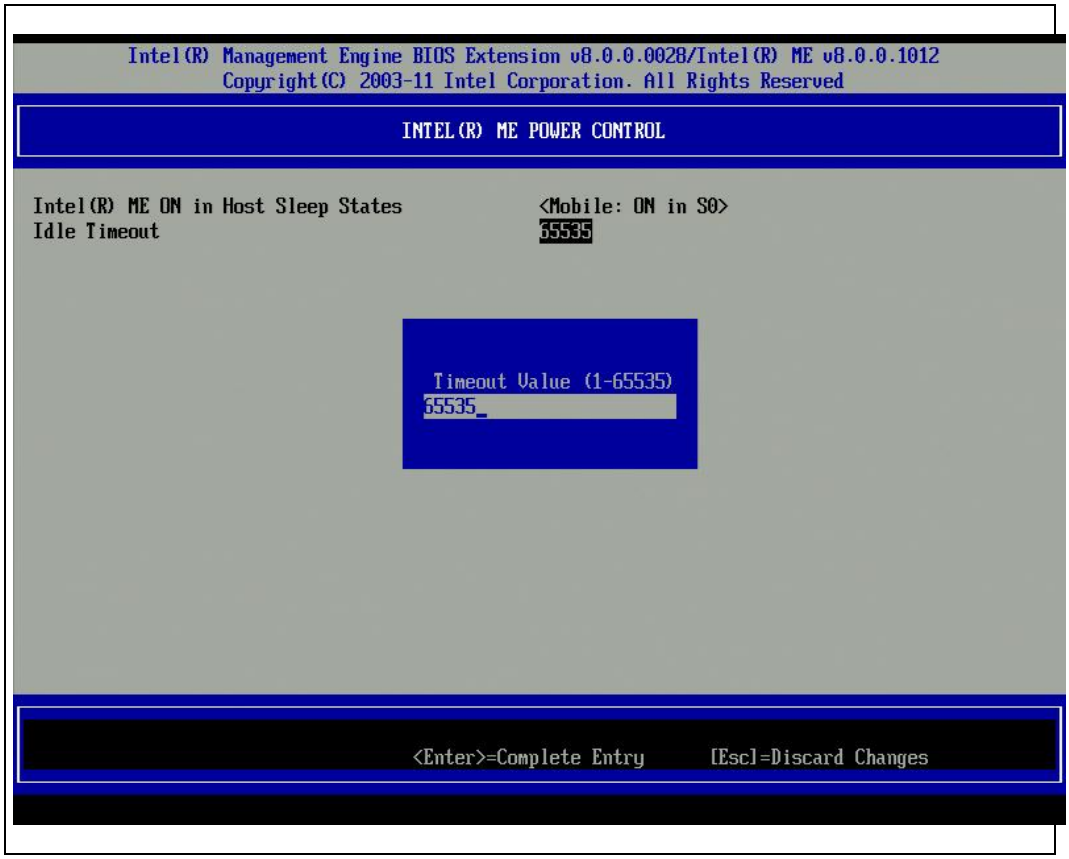
The selected power package determines when the Intel ME is turned ON. The default power package can be modified by using FITC or by FPT.
The end user administrator can choose which power package to use depending on the systems usage.
The table Above illustrates the details of the power packages.
With Intel® ME WoL, after the time-out timer expires, the Intel® ME remains in the M-off state until a command is sent to the ME. After this command has been sent, the Intel® ME will transition to an M0 or M3 state and will respond to the next command that is sent. A ping to the Intel® ME will also cause the Intel® ME to go into an M0 or M3 state.
The Intel ME takes a short time to transition from the M-off state to the M0 or M3 state. During this time, Intel® AMT will not respond to any Intel® ME commands. When the Intel® ME has reached the M0 or M3 state, the system will respond to Intel® ME commands.

3.4.3.2 Idle Time Out

Under Intel® ME Power Control,

1. Select 'Idle Time Out'.
2. Press Enter to type timeout value <in minutes>.

Figure 6: Idle Timeout



This setting is used to enable the Intel ME Wake on and to define the Intel ME idle timeout in M3 state. The value should be entered in minutes. The value indicates the amount of time that the Intel ME is allowed remain idle in M3 before transitioning to the M-off state. **Note:** If the Intel ME is in M0, it will NOT transition to M-off.

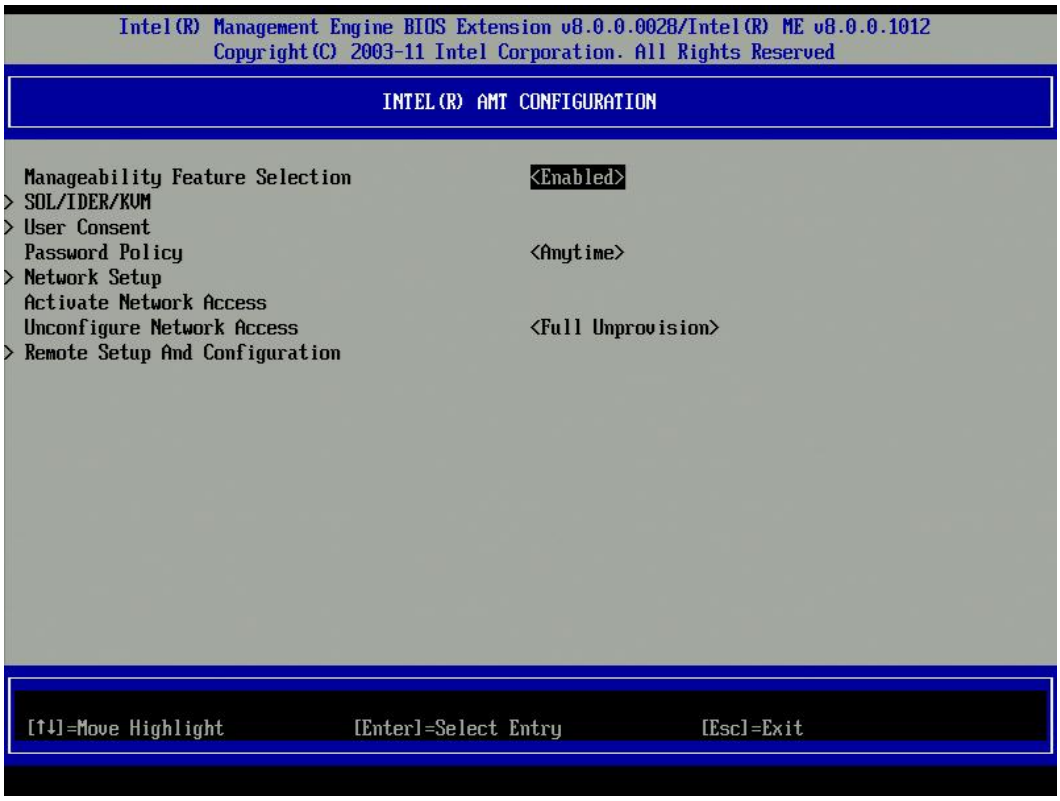
3.5 Intel® AMT Configuration

Under the Main Menu,

1. Select ‘Intel® AMT Configuration’.
2. Press Enter.

The Main Menu changes to the Intel® AMT Configuration screen.

Figure 7: Intel® AMT Configuration



3.5.1 Manageability Feature Selection

Under the Intel® AMT Configuration screen,

1. Select ‘Manageability Feature Selection’.
2. Press Enter to select.
3. A message is displayed: **[Caution] Disabling reset network settings including network ACLs to factory default. System resets on MEBx exit. Continue: (Y/N)**. Press Y to change setting or N to cancel.

The following options can be selected:

- **Disabled**
- **Enabled**

When the Manageability Feature Selection is enabled, the Intel ME manageability feature menu will be shown. Leaving it disabled means that manageability will not be enabled.

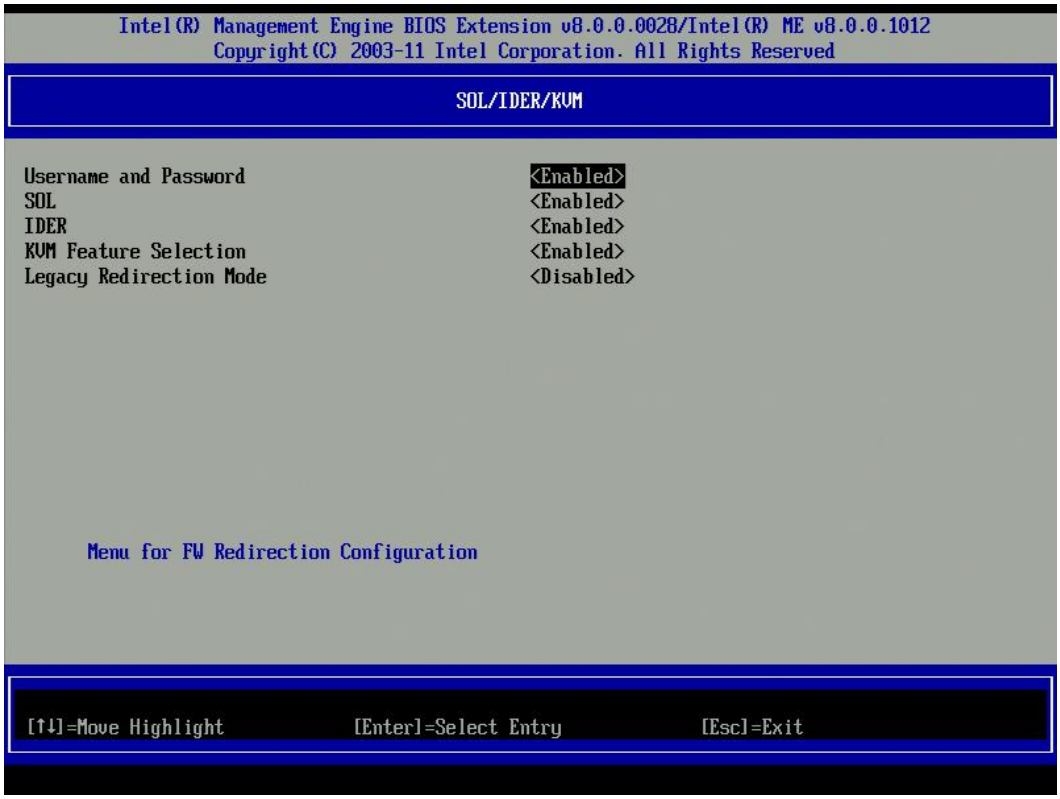
3.5.2 SOL/IDER/KVM

Under the Intel® AMT Configuration **(with Intel AMT enabled)**,

1. Select 'SOL/IDER/KVM'.
2. Press Enter.

The Intel® AMT Configuration changes to the SOL/IDER/KVM screen.

Figure 8: SOL/IDER/KVM



Note: SOL, IDER, KVM here are just for enabling CAPABILITY. User still needs to use other tools like AMT SDK to execute features.

3.5.2.1 Username and Password

Under the SOL/IDER/KVM screen,

1. Select 'Username and Password'.
2. Press Enter to select.

The following options can be selected:

- **Disabled**
- **Enabled**

This option provides the user authentication for SOL/IDER session. If Kerberos* is used, this option should be set to DISABLED. The user authentication is handled through Kerberos. If Kerberos is not used, the IT administrator has the choice to enable or disable user authentication on SOL/IDER session.

3.5.2.2 SOL

Under the SOL/IDER/KVM screen,

1. Select 'SOL'.
2. Press Enter to select.

The following options can be selected:

- **Disabled**
- **Enabled**

SOL allows the console input/output of an Intel AMT managed client to be redirected to a management server console (if the client system supports SOL). If the system does not support SOL, this value cannot enable it.

Note: disabling SOL does not remove this feature but just blocks it from being used.

3.5.2.3 IDER

Under the SOL/IDER/KVM screen,

1. Select ‘IDER’.
2. Press Enter to select.

The following options can be selected:

- **Disabled**
- **Enabled**

IDE-R allows an Intel AMT managed client to be booted by a management console from a remote disk image. If the client system does not support IDE-R, this value cannot enable it.

Note: disabling IDER does not remove this feature but just blocks it from being used.

3.5.2.4 KVM Feature Selection

Under the SOL/IDER/KVM screen,

1. Select ‘KVM Feature Selection’.
2. Press Enter to select.

The following options can be selected:

- **Disabled**
- **Enabled**

Note: disabling KVM does not remove this feature but disables it. KVM will not work in this case.

3.5.2.5 Legacy Redirection Mode

Under the SOL/IDER/KVM screen,

1. Select 'Legacy Redirection Mode'.
2. Press Enter to select.

The following options can be selected:

- **Disabled**- legacy redirection Mode is disabled. (default)
- **Enabled**- the port is left open at all times when redirection is enabled in the Intel MEBX. It is the same as what used to be SMB mode in previous projects. Old (before Intel AMT 6.0) SMB consoles will need this mode in order to succeed opening redirection sessions.

Legacy Redirection Mode controls how the redirection works. If set to disabled, the console needs to open the redirection ports before running sessions. This is meant for enterprise consoles and new SMB consoles that support opening the redirection ports. The old SMB consoles (before Intel AMT 6.0) which don't support opening the redirection ports function need to manually turn on the redirection port through this Intel MEBX option.

3.5.3 User Consent

The user consent feature requires the IT-administrator to supply a code, generated by the Intel AMT platform and displayed to the user. This enhances security when sensitive operations are performed. It also allows the local user to grant permission before certain remote actions take place. The following features may require user consent depending on the User Opt-in setting below:

- IDE-Redirection (IDE-R)
- KVM
- Remotely setting BIOS boot options
- Changing boot sources for remote boot (e.g. causing a boot from PXE).

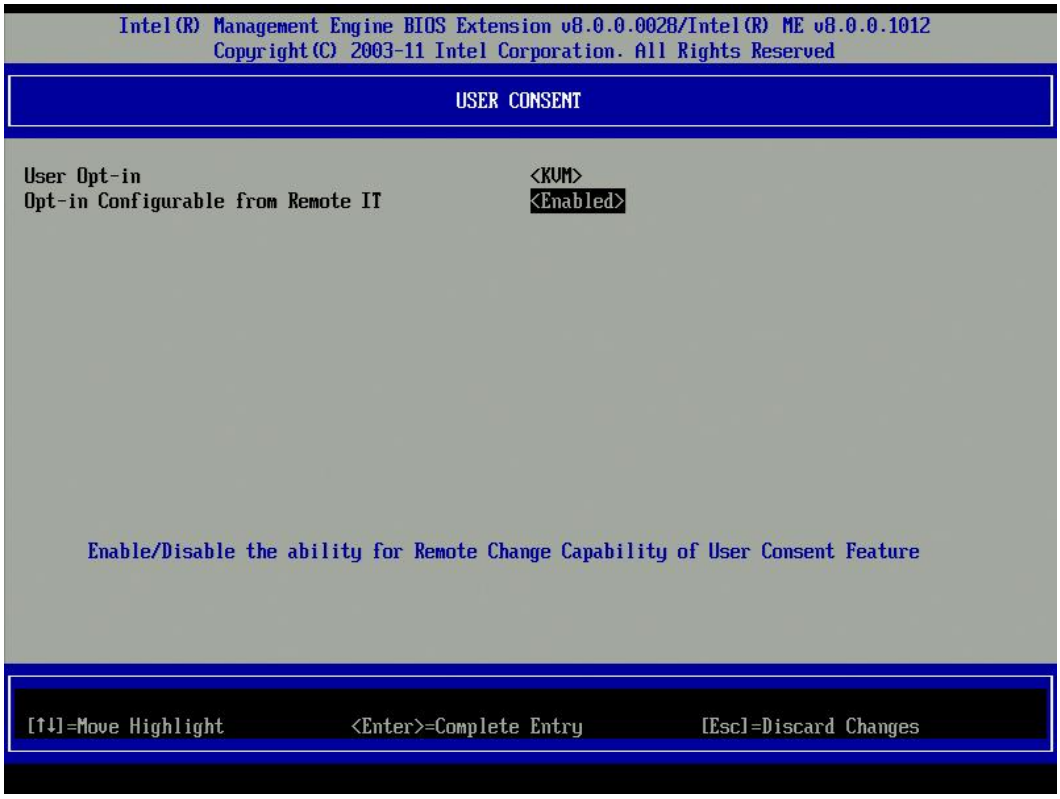
- Using Serial Over LAN specifically to redirect BIOS screens and OS Boot text screens

Under the Intel® AMT Configuration,

1. Select ‘User Consent’.
2. Press Enter.

The Intel® AMT Configuration changes to the User Consent Configuration screen.

Figure 9: User Consent



3.5.3.1 User Opt-in

Under the User Consent Configuration screen,

1. Select ‘User Opt-in’.

2. Press Enter to select.

The following options can be selected:

- **None** - User consent is not required.
- **KVM** - Local User Consent is required for a remote computer to establish KVM Remote Control session.
- **All** - Local User Consent is required for all features listed above.

NOTE: When using Host Based Configuration, Client Control Mode will override this setting and behave as if the “ALL” option has been selected. More details regarding Host Based Configuration and Client Control Mode can be found in the Activator++ User guide and "Intel AMT Release 7.x Start Here" HTML document in the SDK kit

3.5.3.2 Opt-in Configurable from remote IT

If Intel AMT was setup locally and is in Client Control mode, this setting is not working. If Intel AMT was setup in Admin Control mode, this setting allows IT people to change user Opt- in policy remotely.

Under the User Consent Configuration screen,

1. Select ‘Opt-in Configurable from remote IT’.
2. Press Enter to select.

The following options can be selected:

- **Disabled** – This option disables the remote user’s ability to change User OPT-IN Policy. In this case only the local user can control the opt-in policy.
- **Enabled** – Enables remote user’s ability to change User OPT-IN Policy. Allows remote user to choose whether or not to request local user consent.

3.5.4 Password Policy

Under the Intel® AMT Configuration screen,

1. Select 'Password Policy'.
2. Press Enter to select.

The following options can be selected:

- **Default Password Only** – The Intel MEBX password can be changed through the network interface if the default password has not been changed yet.
- **During Setup and Configuration –** The Intel MEBX password can be changed through the network interface during the setup and configuration process but at no other time. Once the setup and configuration process is complete, the Intel MEBX password cannot be changed via the network interface.
- **Anytime –** The Intel MEBX password can be changed through the network interface at any time.

Note: The network interface mentioned above is NOT talking about WebUI. There are two passwords for the firmware. The Intel MEBX password is the password that is entered when a user is physically at the system. The network password is the password that is entered when accessing an Intel ME enabled system through the network. By default they are both the same until the network password is changed via the network. Once changed over the network, the network password will always be kept separate from the local Intel MEBX password.

This option determines when the user is allowed to change the Intel MEBX password through the network.

Note: The Intel MEBX password can always be changed via the Intel MEBX user interface.

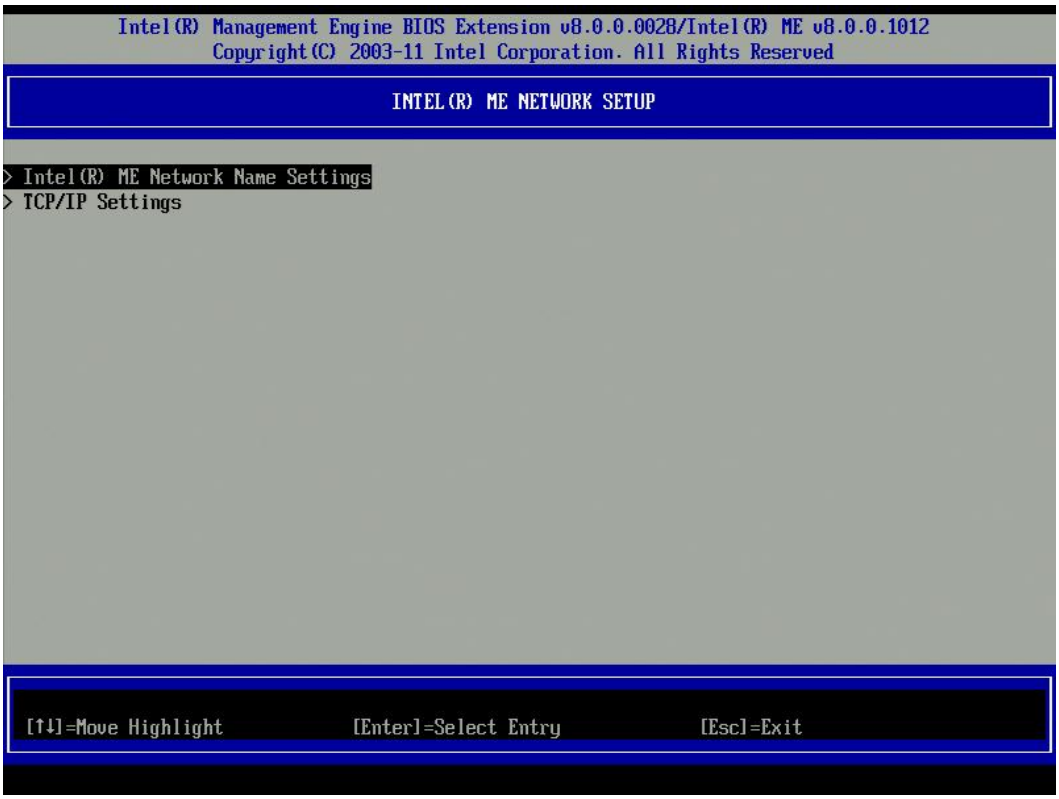
3.5.5 Network Setup

Under the Intel® AMT Configuration screen,

1. Select 'Network Setup'.
2. Press Enter.

The Intel® AMT Configuration screen changes to the Intel® ME Network Setup page.

Figure 10: Intel® ME Network Setup



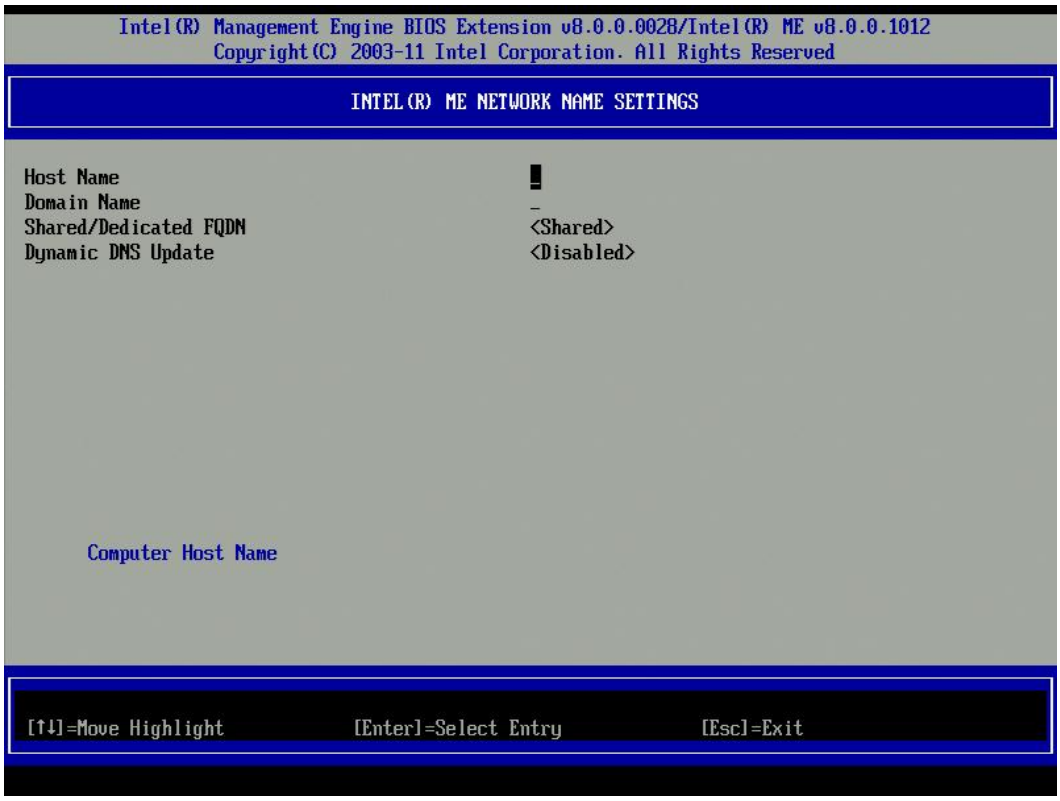
3.5.5.1 Intel® ME Network Name Settings

Under the Intel® ME Network Setup menu,

1. Select 'Intel® ME Network Name Settings'.
2. Press Enter.

The Intel® ME Network Setup menu changes to the Intel® ME Network Name Settings page.

Figure 11: Intel® ME Network Name Settings



3.5.5.1.1 Host Name

Under the Intel® ME Network Name Settings menu,

1. Select 'Host Name'.
2. Press Enter to edit.

A host name can be assigned to the Intel AMT machine. This will be the hostname of the Intel AMT enabled system.

3.5.5.1.2 Domain Name

Under the Intel® ME Network Name Settings menu,

1. Select 'Domain Name'.
2. Press Enter to edit.

A domain name can be assigned to the Intel AMT machine.

3.5.5.1.3 Shared/Dedicated FQDN

Under the Intel® ME Network Name Settings menu,

1. Select ‘Shared/Dedicated FQDN’.
2. Press Enter to select.

The following options can be selected:

- **Dedicated-** The FQDN domain name is dedicated to ME.
- **Shared-** The FQDN domain name is shared with the Host.

This setting determines whether the Intel ME Fully Qualified Domain Name (FQDN) (i.e. the "HostName.DomainName") is shared with the host and identical to the operating system machine name or dedicated to the Intel ME.

3.5.5.1.4 Dynamic DNS Update

Under the Intel® ME Network Name Settings menu,

1. Select ‘Dynamic DNS Update’.
2. Press Enter to select.

The following options can be selected:

- **Disabled**
- **Enabled**

If Dynamic DNS Update is enabled then the firmware will actively try to register its IP addresses and FQDN in DNS using the Dynamic DNS Update protocol. If DDNS Update is disabled then the firmware acts depending on FQDN setting.

a.) Under Dedicated FQDN mode: Firmware makes no attempt to update DNS using DHCP option 81 or Dynamic DNS update. DNS server will not be updated.

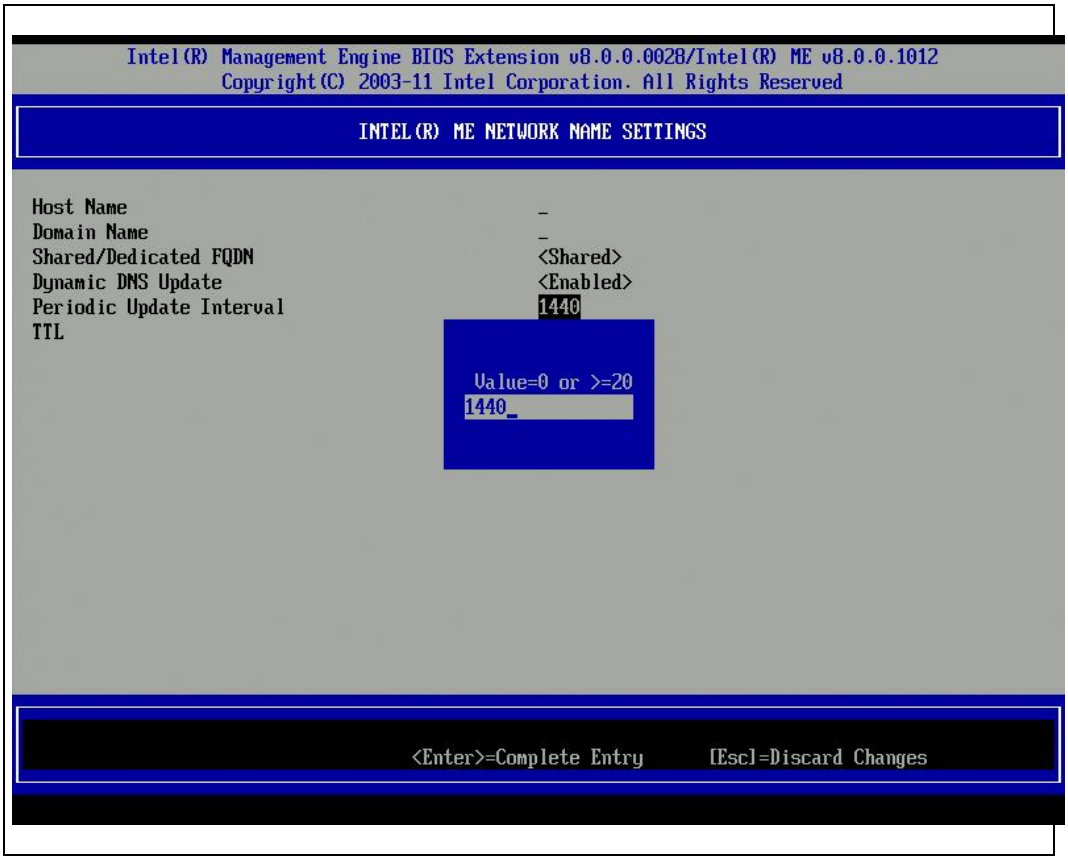
b.) Under Shared FQDN mode: Firmware used DHCP option 81 for DNS registration but did not directly update DNS using the DDNS update protocol.

Note: For selecting “Enabled” for Dynamic DNS Update it is required that the Host Name and Domain Name be set.

3.5.5.1.5 Periodic Update Interval

Note: This option is only available when Dynamic DNS Update is enabled.

Figure 12: Periodic Update Interval



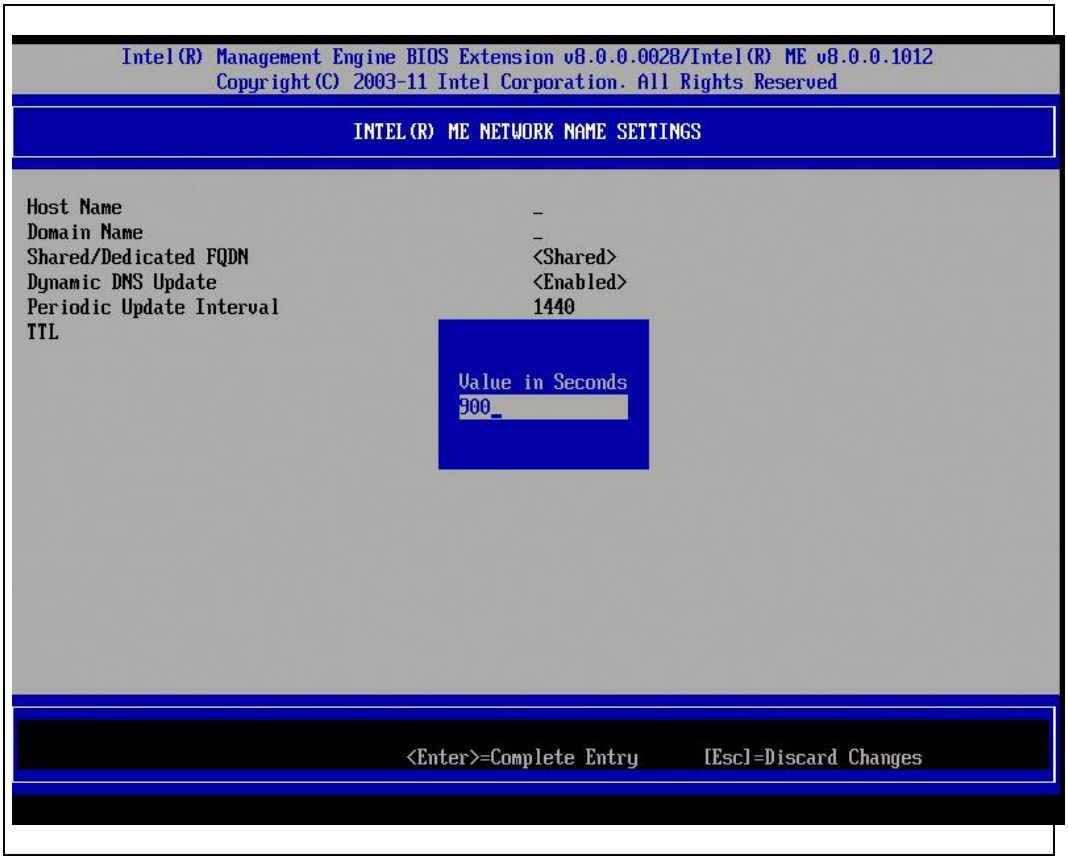
Defines the interval at which the firmware DDNS Update client will send periodic updates. It should be set according to corporate DNS scavenging policy. Units are minutes. A value of 0 disables periodic update. The value set should be equal or greater than 20 minutes. The default value for this property is 24 hours - 1440 minutes.

1. Select ‘Periodic Update interval’.
2. Press Enter to edit <in minutes>.

3.5.5.1.6 TTL

Note: This option is only available when Dynamic DNS Update is enabled.

Figure 13: TTL



TTL (Time-to-live) here is a period of time that determines how long the record should not be scavenged in DNS server when dynamic DNS update is enabled. This setting allows configuring the TTL time in seconds and should be greater than zero. The default value is 15 min.

1. Select ‘TTL’.
2. Press Enter to edit <in seconds>.

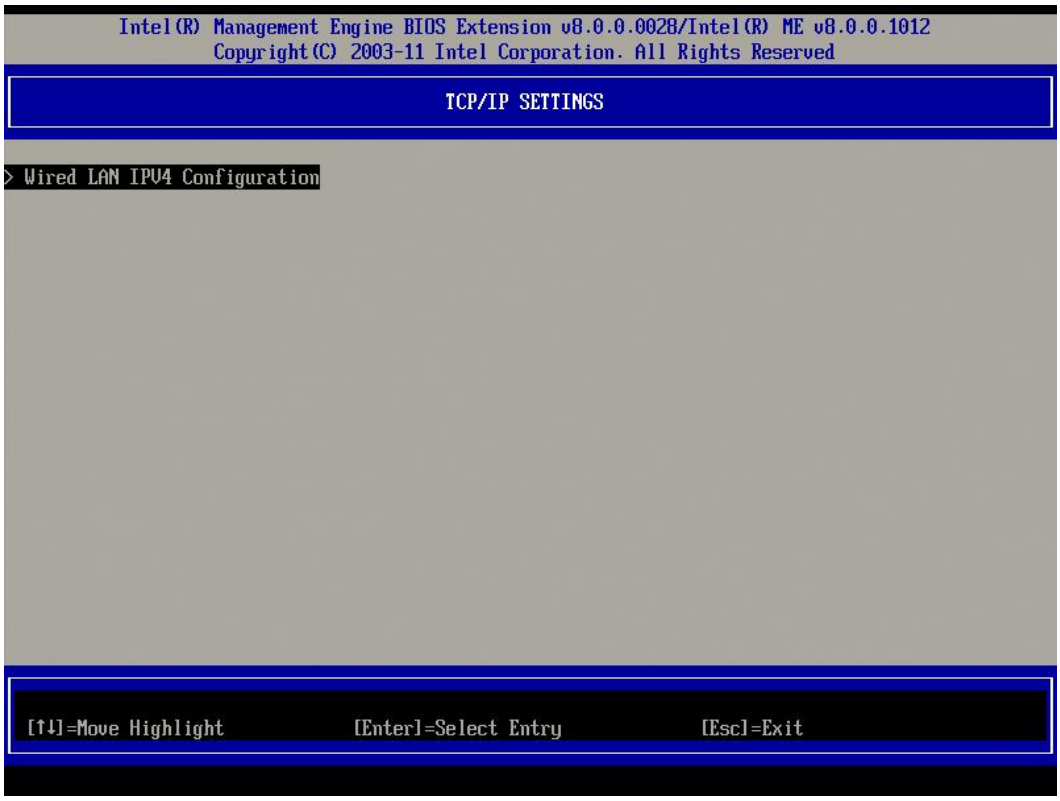
3.5.5.2 TCP/IP Settings

Under the Intel® ME Network Setup menu,

1. Select ‘TCP/IP Settings’.
2. Press Enter.

The Intel Network Setup menu changes to the TCP/IP Settings page.

Figure 14: TCP/IP Settings



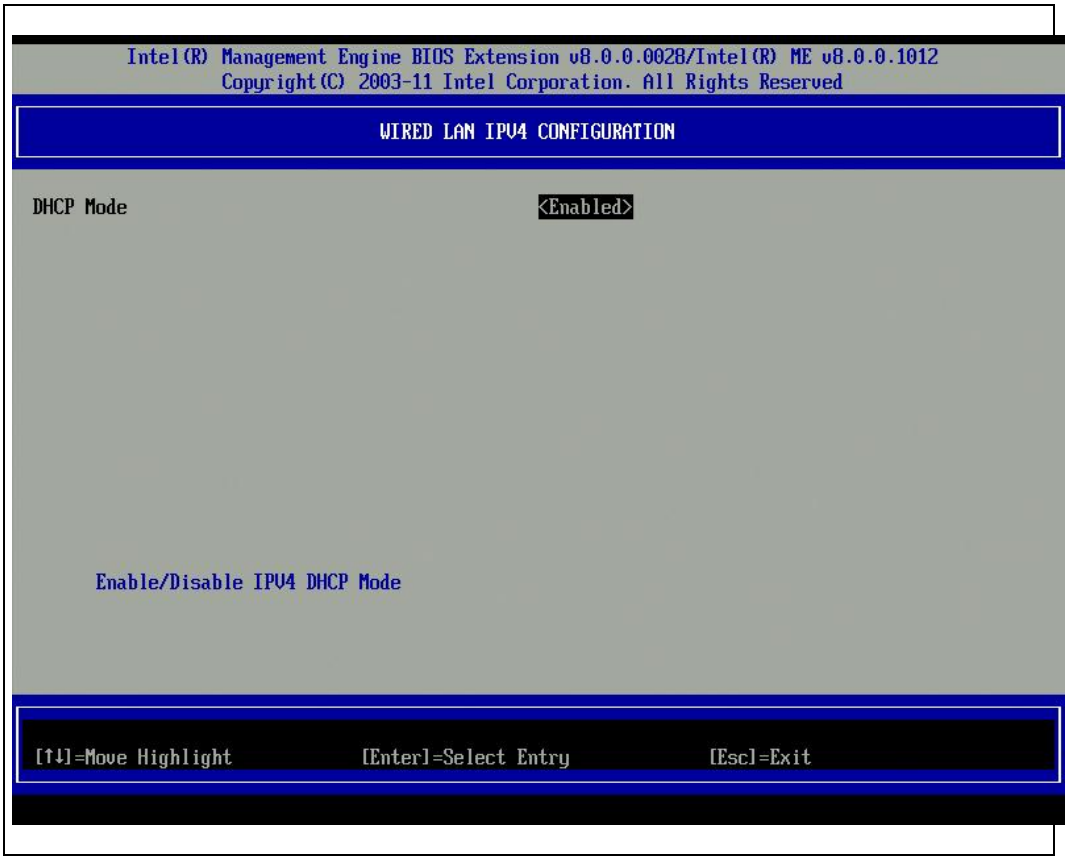
Wired LAN IPV4 Configuration

Under the TCP/IP Settings,

1. Select ‘Wired LAN IPV4 Configuration’.
2. Press Enter.

The TCP/IP Settings menu changes to the Wired LAN IPV4 Configuration page.

Figure 15: Wired LAN IPV4 Configuration



3.5.5.2.1 DHCP Mode

Under the Wired LAN IPV4 Configuration,

1. Select 'DHCP Mode'.
2. Press Enter to select.

The following options can be selected:

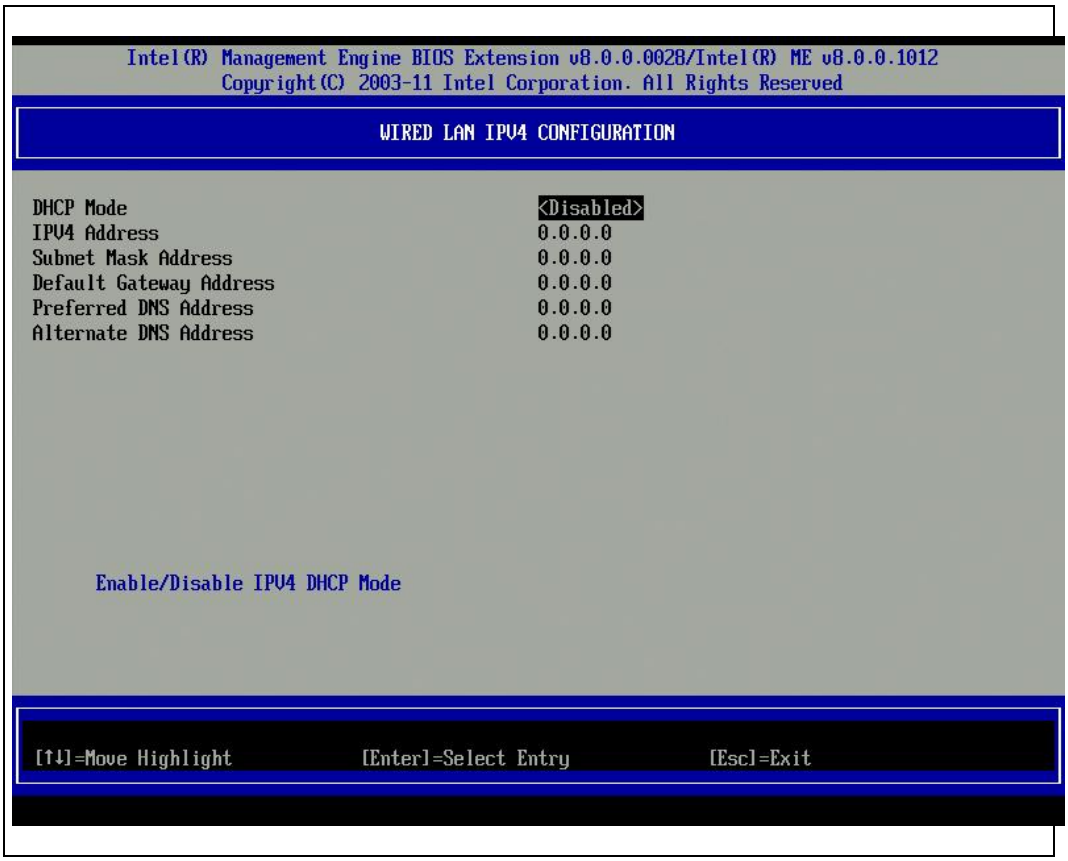
ENABLED - If DHCP Mode is enabled, TCP/IP settings will be configured by a DHCP server. No additional steps are required.

DISABLED - If DHCP mode is disabled, the following static TCP/IP settings are required for Intel AMT. If a system is in static mode the system should require a second IP address. This IP address, often called the Intel ME IP address has to be

different than host IP address (unless in shared static IP mode, which is out of MEBx User Guide scope). Please check following sessions 3.5.5.2.3 ~ 3.5.5.2.7.

Note: Static IP and subnet mask are mandatory.

Figure 16: DHCP Mode Disabled



3.5.5.2.2 IPv4 Address

Under the Wired LAN IPV4 Configuration,

1. Select ‘IPv4 Address’.
2. Press Enter to edit.

3.5.5.2.3 Subnet Mask Address

Under the Wired LAN IPV4 Configuration,

1. Select ‘Subnet Mask Address’.
2. Press Enter to edit.

3.5.5.2.4 Default Gateway Address

Under the Wired LAN IPV4 Configuration,

1. Select ‘Default Gateway Address’.
2. Press Enter to edit.

3.5.5.2.5 Preferred DNS Address

Under the Wired LAN IPV4 Configuration,

1. Select ‘Preferred DNS Address’.
2. Press Enter to edit.

3.5.5.2.6 Alternate DNS Address

Under the Wired LAN IPV4 Configuration,

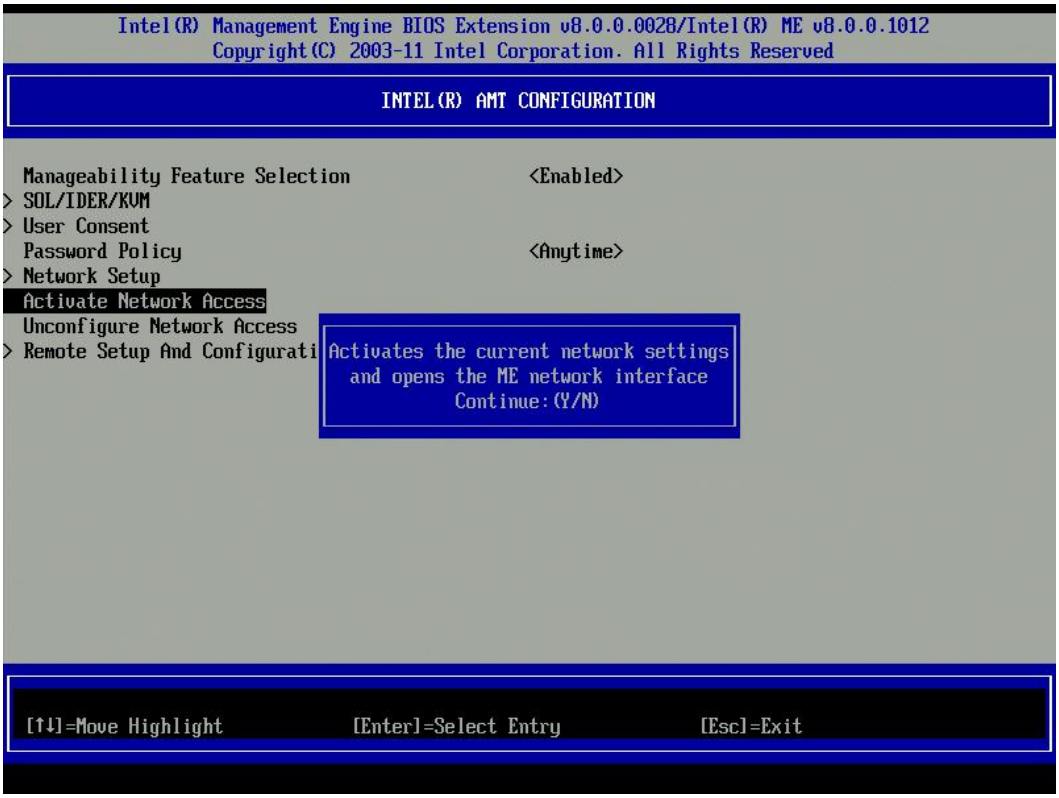
1. Select ‘Alternate DNS Address’.
2. Press Enter to edit.

3.5.6 Activate Network Access

Under the Intel® AMT Configuration menu,

1. Select ‘Activate Network Access’.
2. Press Enter.
3. Press ‘Y’ to activate or press ‘N’ to cancel

Figure 17: Activate Network Access



Activate Network Access causes the Intel ME to transition to the POST provisioning state if all required settings are configured. Without Activating Network Access, ME will not be able to connect to the network.

Note: Power policy will change to PP2 after activating if the default power policy is set to PP1.

3.5.7 Unconfigure Network Access

Under the Intel® AMT Configuration menu,

1. Select 'Unconfigure Network Access'.
2. Press Enter to select.

The following options can be selected:

- **Full Unprovision**

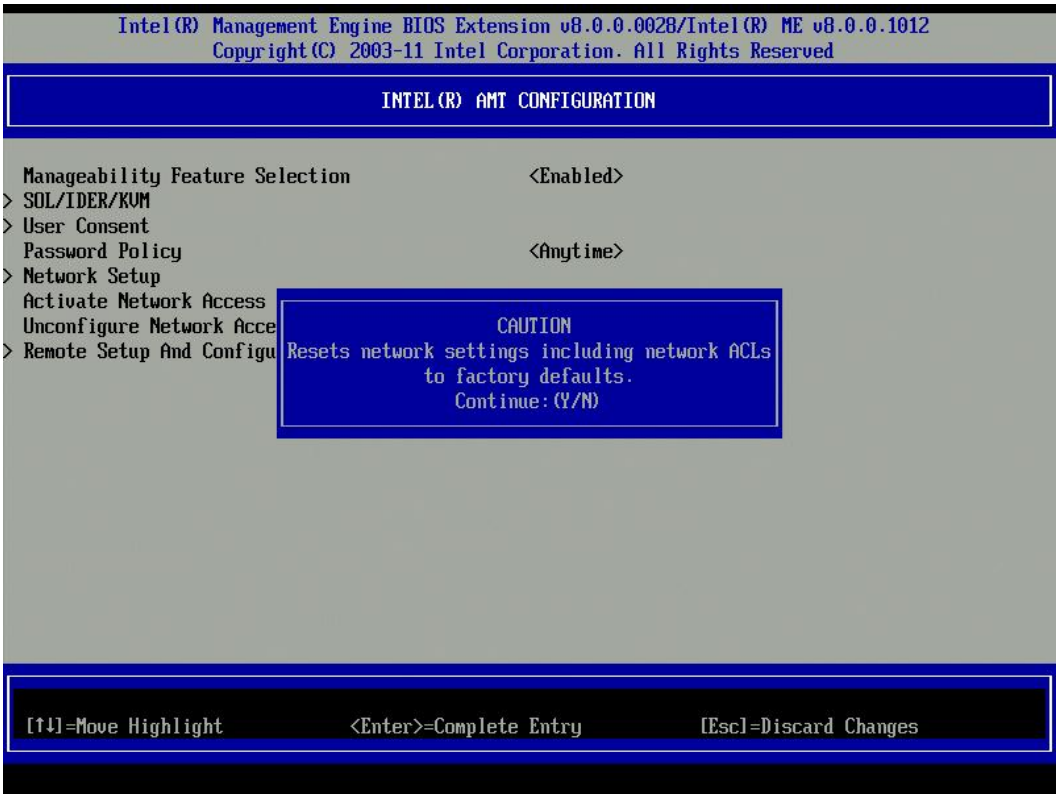
- **Partial Unprovision -**

AMT Full Unprovisioning	**Same as ME Un-configure with the following settings Kept:** **MEBx password** **BIOS tables are kept (except PLDM tables)** **Privacy related settings are kept:** • **SOL/IDER/KVM local enable/disable** • **KVM Opt-in settable through network enable/disable** • **IDER boot log**
AMT Partial Unprovisioning	Same as AMT Full Unprovision with the following settings **Kept**: • PSK settings (PID/PPS) • All Remote Configuration settings (ZTC enable, OTP, customized hashes, configuration server FQDN, provisioning DNS suffix) • Network settings - Kept

3. Select Y to unconfigure or N to exit without change.

The following screen appears:

Figure 18: Unconfigure Network Access



3.5.8 Remote Setup and Configuration

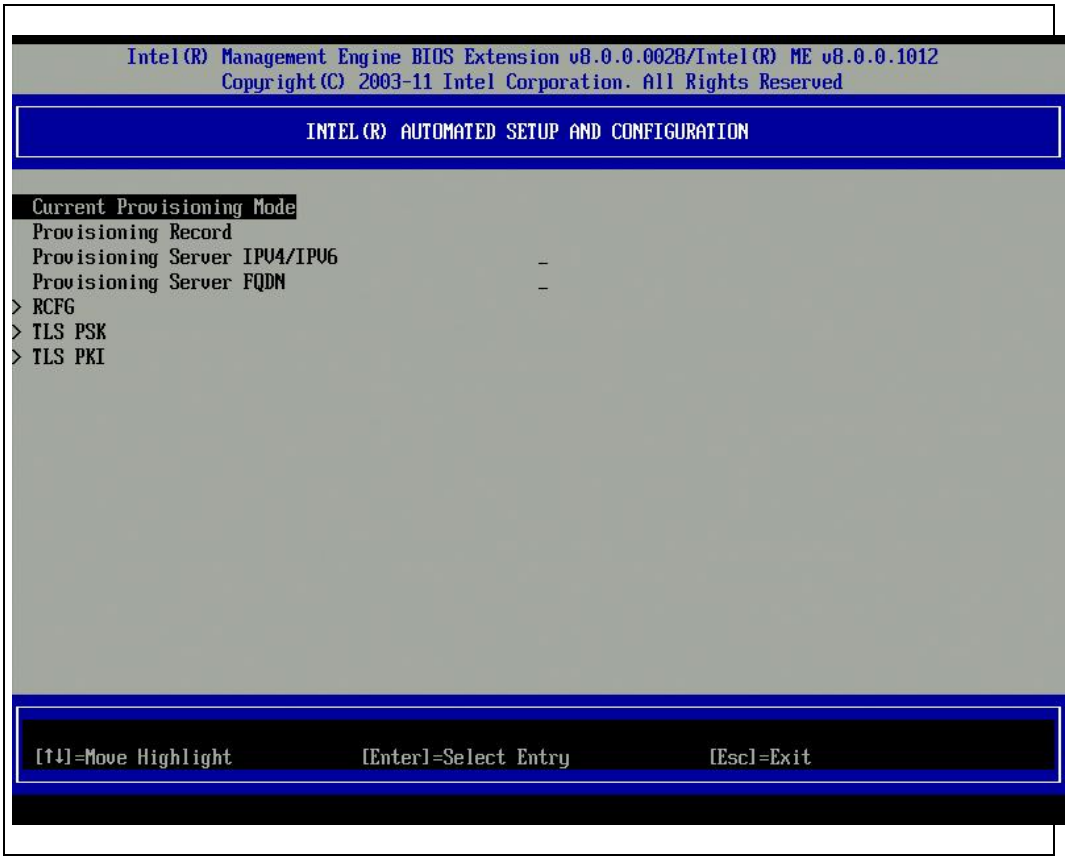
Under Intel® AMT Configuration,

1. Select 'Remote Setup and Configuration'.
2. Press Enter.

The Intel® AMT Configuration screen changes to the Intel® Automated Setup and Configuration screen.

Note: The following list is displayed when Intel® AMT is in pre-provision mode.

Figure 19: Intel® Automated Setup and Configuration

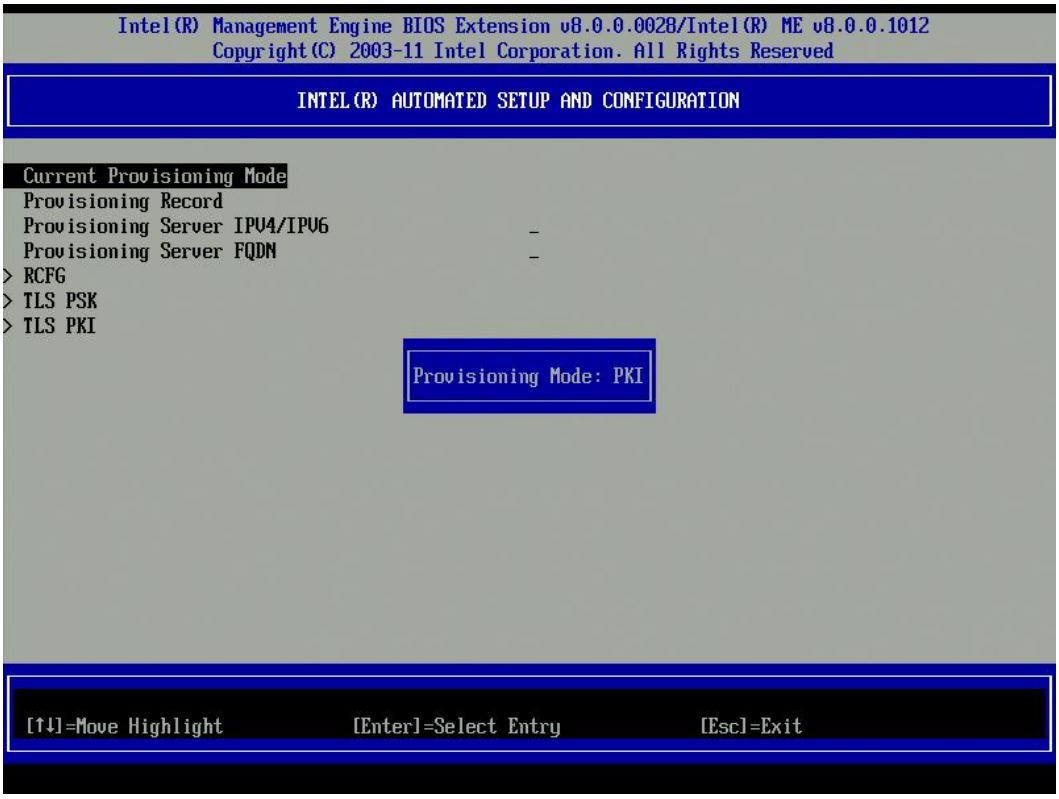


3.5.8.1 Current Provisioning Mode

Under Intel Automated Setup and Configuration,

1. Select ‘Current Provisioning Mode’.
2. Press Enter.

Figure 20: Current Provisioning Mode



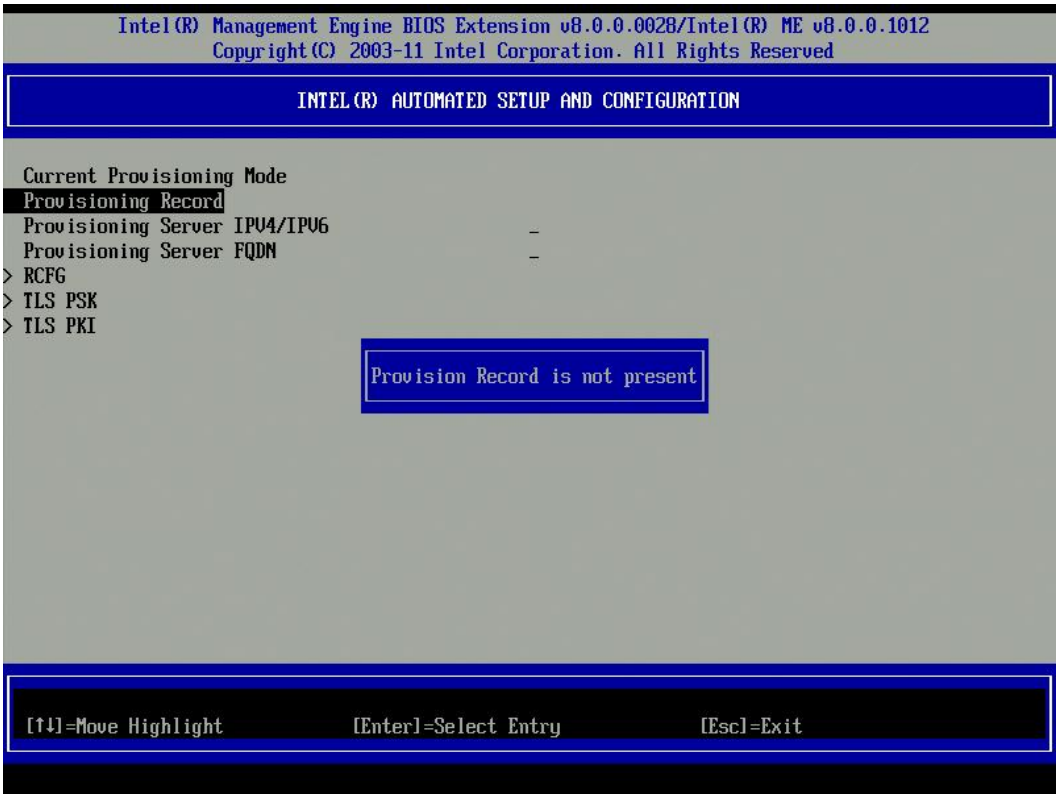
Current Provisioning Mode – Displays the current provisioning TLS Mode: None, PKI, or PSK.

3.5.8.2 Provisioning Record

Under Intel Automated Setup and Configuration,

1. Select ‘Provisioning Record’.
2. Press Enter.

Figure 21: Provisioning record



Provisioning Record – Displays the system's provision PSK/PKI record data. If the data has not been entered, the Intel MEBX displays a message stating "Provision Record not present".

If the data is entered, the Provision record will display the following:

- TLS provisioning mode – Displays the current configuration mode of the system: None, PSK or PKI.
- Provisioning IP – The IP address of the setup and configuration server.
- Date of Provision – Displays the date and time of the provisioning in the format MM/DD/YYYY at HH:MM.
- DNS – indicates whether the "PKI DNS Suffix" was configured in Intel MEBX before remote configuration took place or not. A value of 0 indicates that the DNS Suffix was not configured and the firmware will rely on DHCP

option 15 and compare this suffix to the FQDN in the Configuration Server's client certificate. A value of 1 indicates that the DNS Suffix was configured and the firmware matched it against the DNS Suffix in the Configuration Server's client certificate. Host Initiated – Indicates whether the setup and configuration process was initiated by the host: 'No' indicates that the setup and configuration process was NOT host-initiated, 'Yes' indicates the setup and configuration process was host-initiated (PKI only).

- Hash Data – Displays the 40-character certificate hash data (PKI only).
- Hash Algorithm – Describes the hash type(PKI only).
- IsDefault – Displays 'Yes' if the Hash algorithm is the default algorithm selected. Displays 'No' if the hash algorithm is NOT the default algorithm used (PKI only).
- FQDN – FQDN of the provisioning server mentioned in the certificate (PKI only).
- Serial Number – The 32-character string that indicates the Certificate Authority serial numbers.
- Time Validity Pass – Indicates whether the certificate passed the time validity check.

3.5.8.3 Provisioning Server IPV4/IPV6

Under the Intel® Automated Setup and Configuration screen,

1. Select 'Provisioning Server IPV4/IPV6'.
2. Press Enter to edit the IP address of the Intel® AMT provisioning server.
3. Editor the port number of the Intel® AMT provisioning server. The default port number is 9971.

3.5.8.4 Provisioning Server FQDN

Under the Intel® Automated Setup and Configuration screen,

1. Select 'Provisioning Server FQDN'.

2. Press Enter to edit.

FQDN of the provisioning server mentioned in the certificate (PKI only).
This is also the FQDN of the server that AMT sends hello packets to both PSK and PKI

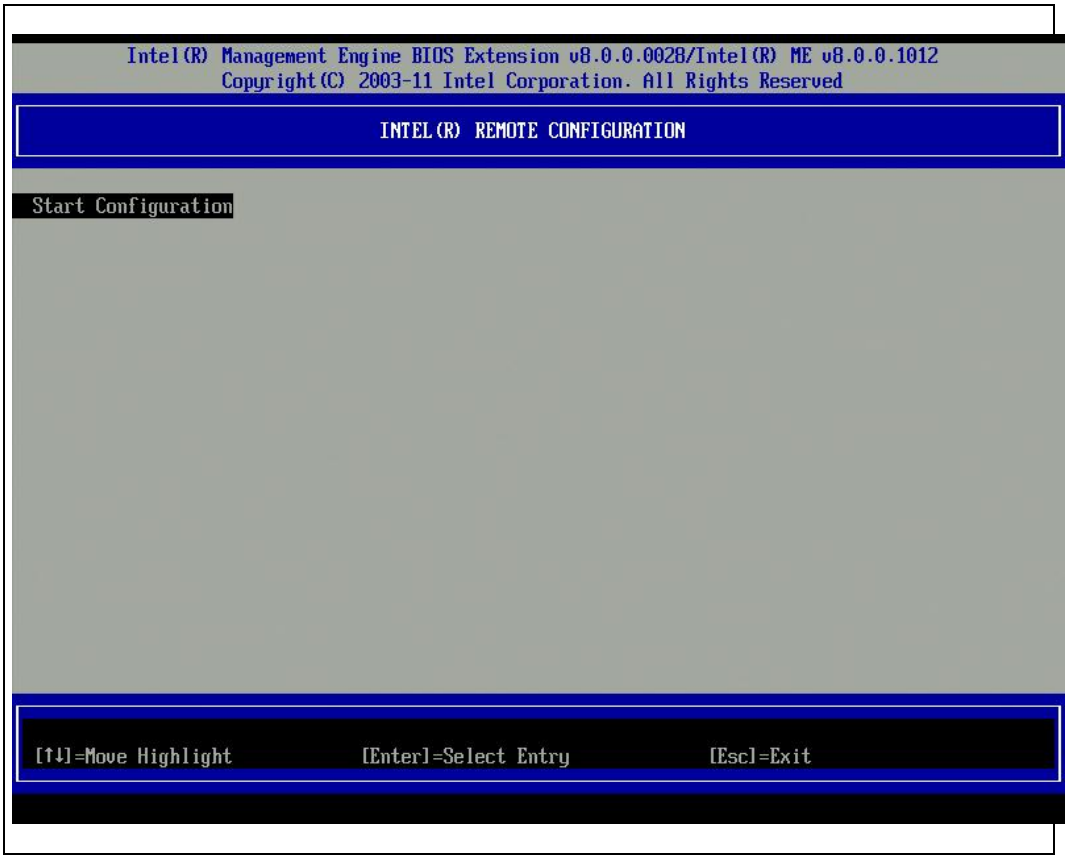
3.5.8.5 RCFG

Under Intel® Automated Setup and Configuration,

1. Select 'RCFG'.
2. Press Enter.

The Intel® Automated Setup and Configuration screen changes to the Intel® Remote Configuration screen.

Figure 22: Intel Remote Configuration

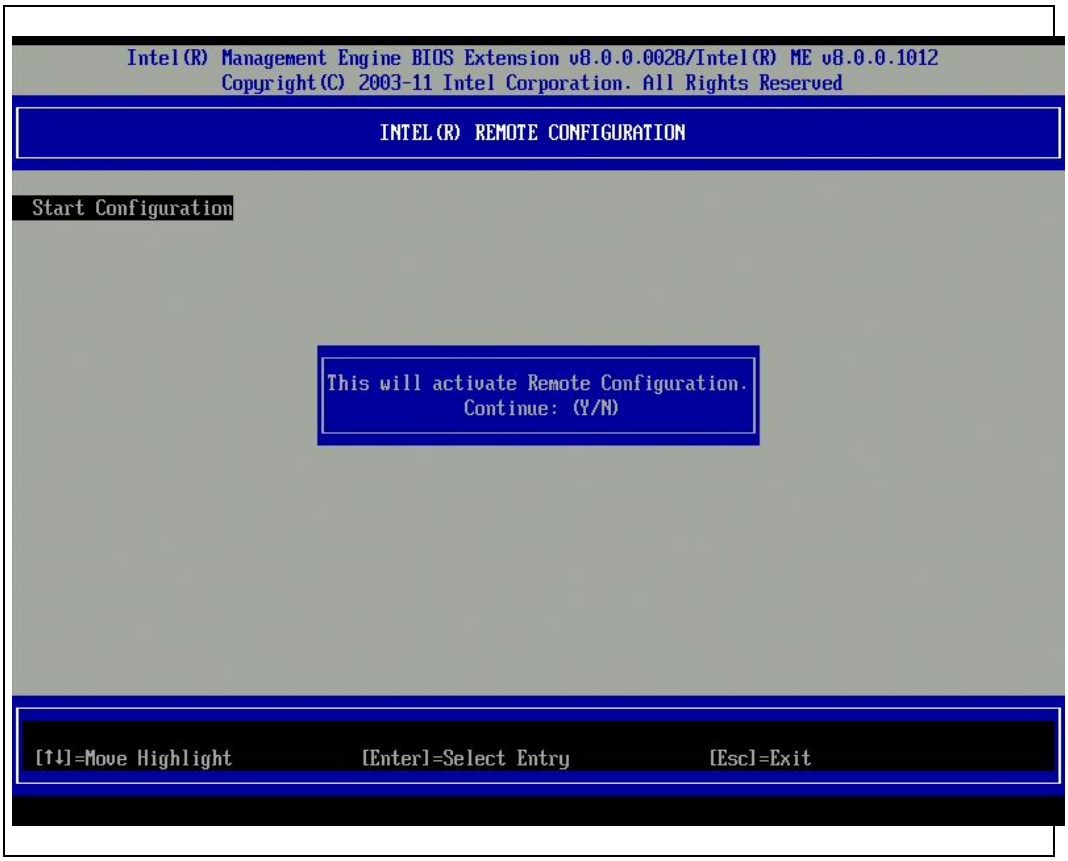


3.5.8.5.1 Start Configuration

Under the Intel® Remote Configuration screen,

1. Select ‘Start Configuration’.
2. Select Y to activate remote configuration or N to exit without change.

Figure 23: Activate RCFG



If Remote Configuration is not activated, Remote configuration cannot occur.

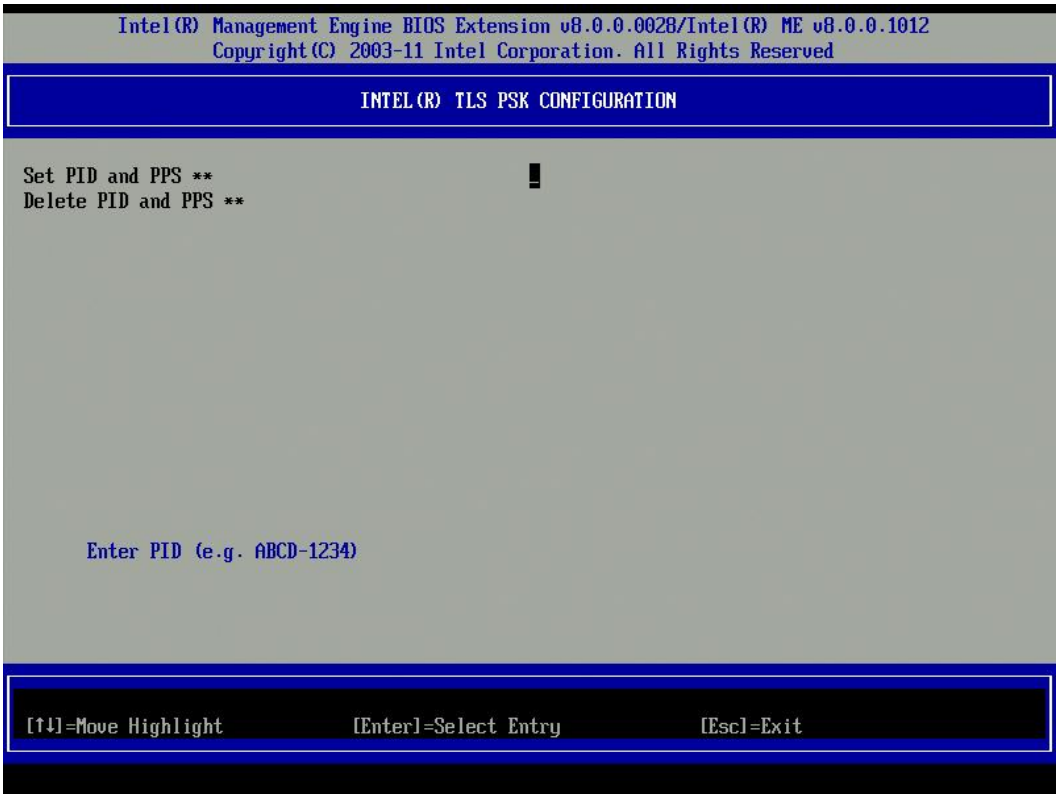
3.5.8.6 TLS PSK

Under Intel® Automated Setup and Configuration,

1. Select ‘TLS PSK’.
2. Press Enter.

The Intel® Automated Setup and Configuration screen changes to the Intel® TLS PSK Configuration screen.

Figure 24: Intel TLS PSK Configuration screen



This submenu contains the settings for TLS PSK configuration settings.

3.5.8.6.1 Set PID and PPS

Under the Intel® Remote Configuration screen,

1. Select 'Set PID and PPS'.
2. Press Enter to edit PID.
3. Edit PPS.

Setting the PID/PPS will cause a partial unprovision if the setup and configuration is "In-process". The PID and PPS should be entered in the dash format. (Ex. PID: AAAA-AAAN; PPS:AAAF-AAAF- AAAF-AAAF-AAAF-AAAF- AAAF-AAAF).

Note- A PPS value of '0000-0000-0000-0000-0000-0000-0000-0000' will not change the setup configuration state. If this value is used, the setup and configuration state will remain 'Not-started'.

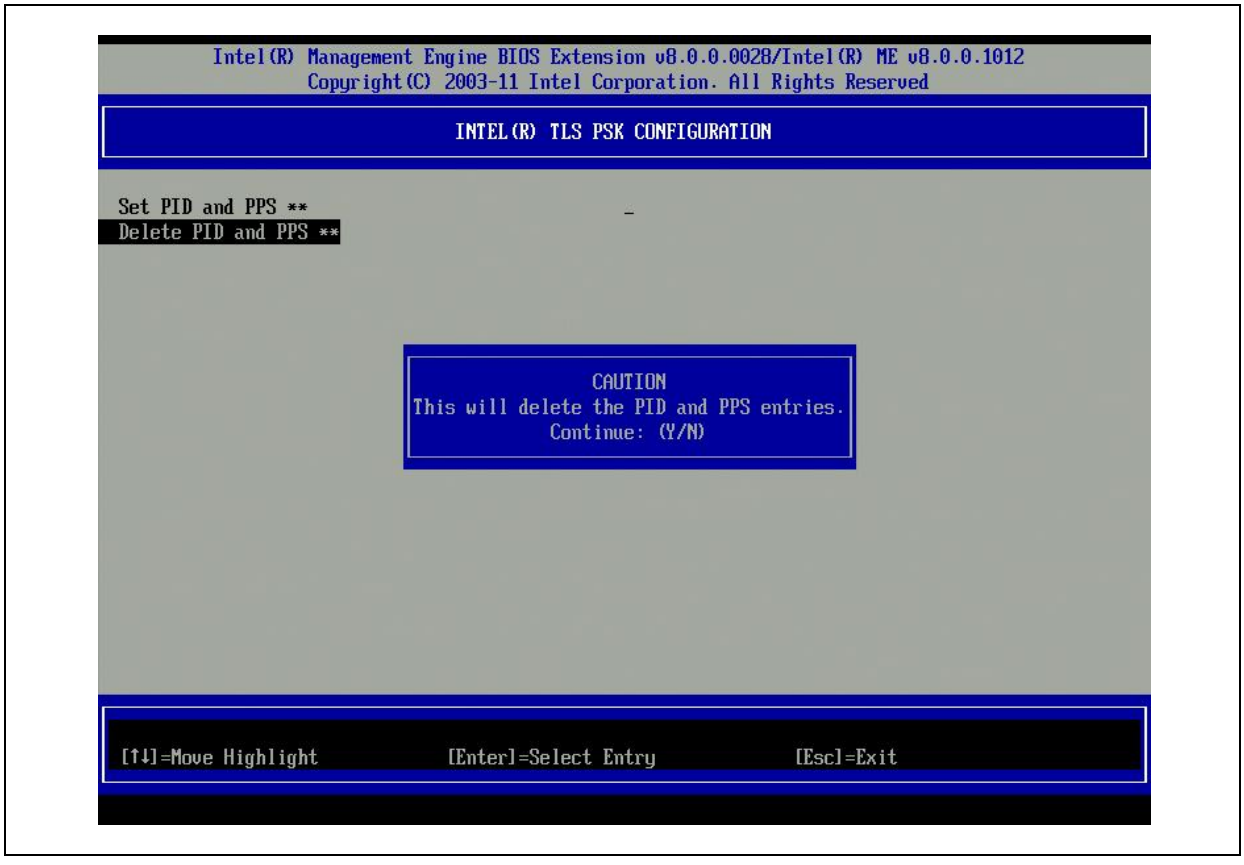
If an invalid entry is attempted, an error message will be displayed.

3.5.8.6.2 Delete PID and PPS

Under the Intel® Remote Configuration screen,

1. Select 'Delete PID and PPS'.
2. Press Enter.
3. Press Y to delete or N to exit without change.

Figure 25: Delete PID and PPS



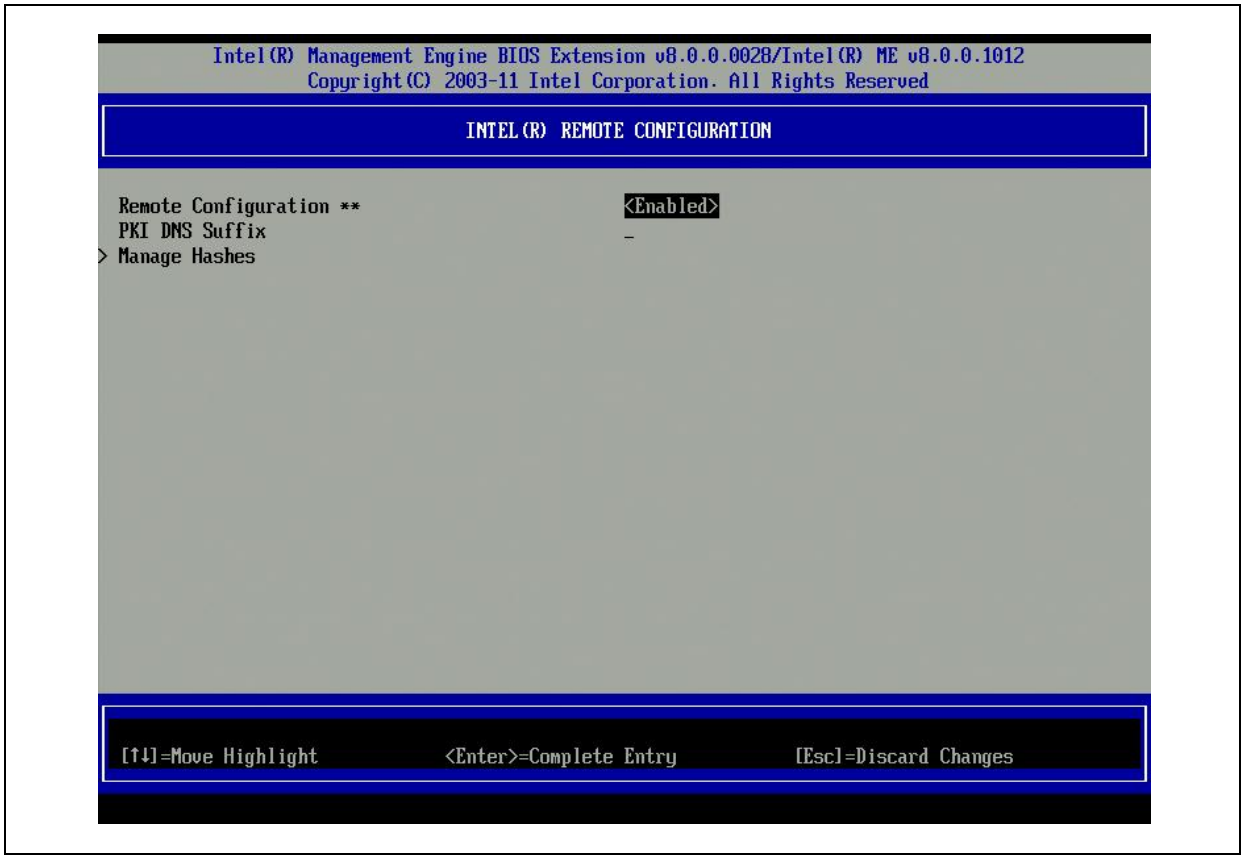
3.5.8.7 TLS PKI

Under Intel® Automated Setup and Configuration,

1. Select ‘TLS PKI’.
2. Press Enter.

The Intel® Automated Setup and Configuration screen changes to the Intel® Remote Configuration screen.

Figure 26: Intel Remote Configuration



3.5.8.7.1 Remote Configuration

Under the Intel® Remote Configuration screen,

1. Select ‘Remote Configuration’.
2. Press Enter to select.

The following options can be selected:

- **Disabled**- remote configuration is disabled. Only ‘Remote Configuration’ item are visible.
- **Enabled**- remote configuration is enabled, this will show additional fields.

Enabling/Disabling Remote configuration will cause a partial un-provision if the setup and configuration server is “In-process”.

3.5.8.7.2 PKI DNS Suffix

Under the Intel® Remote Configuration screen,

1. Select ‘PKI DNS Suffix ’.
2. Press Enter to edit.

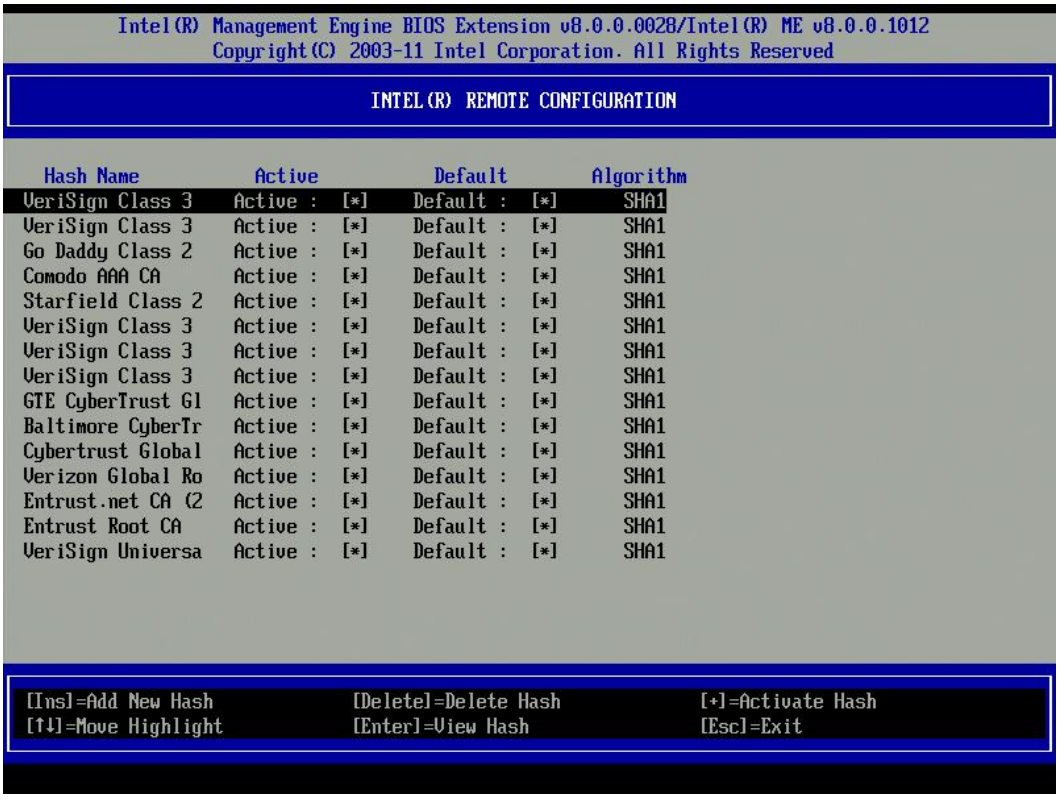
Key Value will be maintained in the EPS.

3.5.8.7.3 Manage Hashes

Under the Intel Remote Configuration screen,

1. Select ‘Manage Hashes ’.
2. Press Enter.

Figure 27: Manage Hashes



Selecting this option will enumerate the hashes in the system and display the Hash Name and the active and default state.

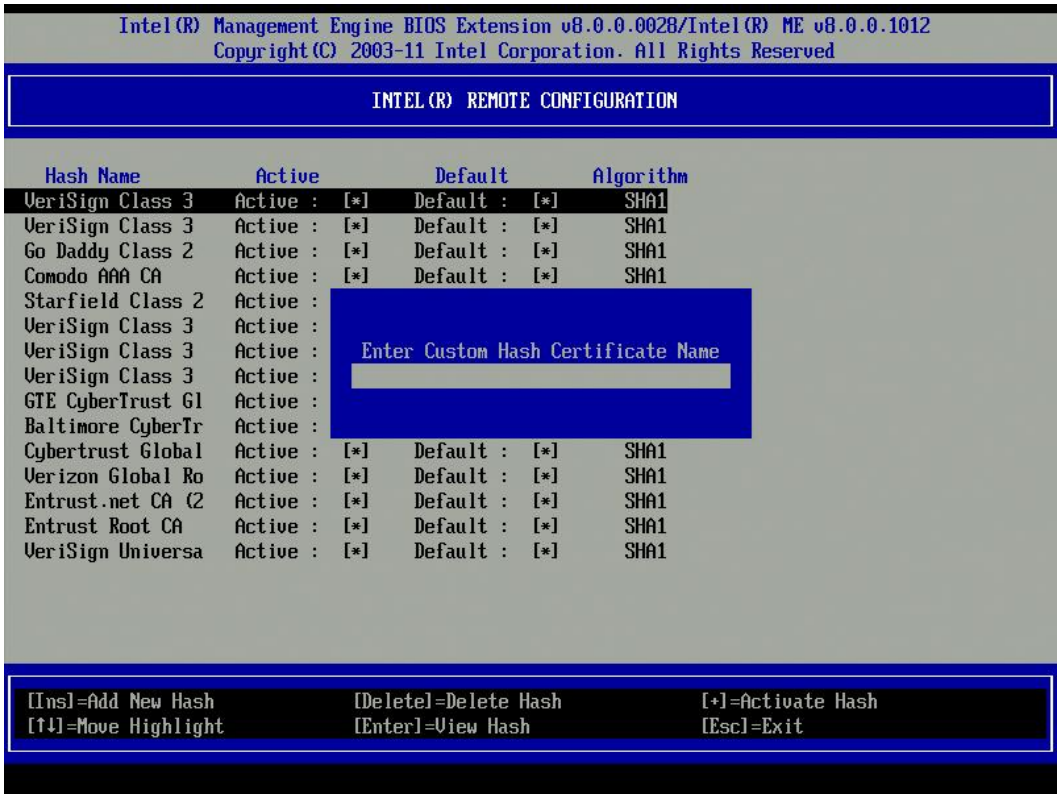
The Manage Certificate Hash screen provides keyboard controls for managing the hashes on the system. The following keys are valid when in the Manage Certificate Hash menu:

- **Escape** key – exits from the menu
- **Insert** key – adds a customized certificate hash to the system.
- **Delete** key –deletes the currently selected certificate hash from the system.
- '+' key – Changes the active state of the currently selected certificate hash.
- **Enter** key – Displays the details of the currently selected certificate hash.

3.5.8.7.4 Adding a Customized Hash

When the Insert key is pressed in the Manage Certificate Hash screen, the following screen is displayed.

Figure 28: Adding a new hash name



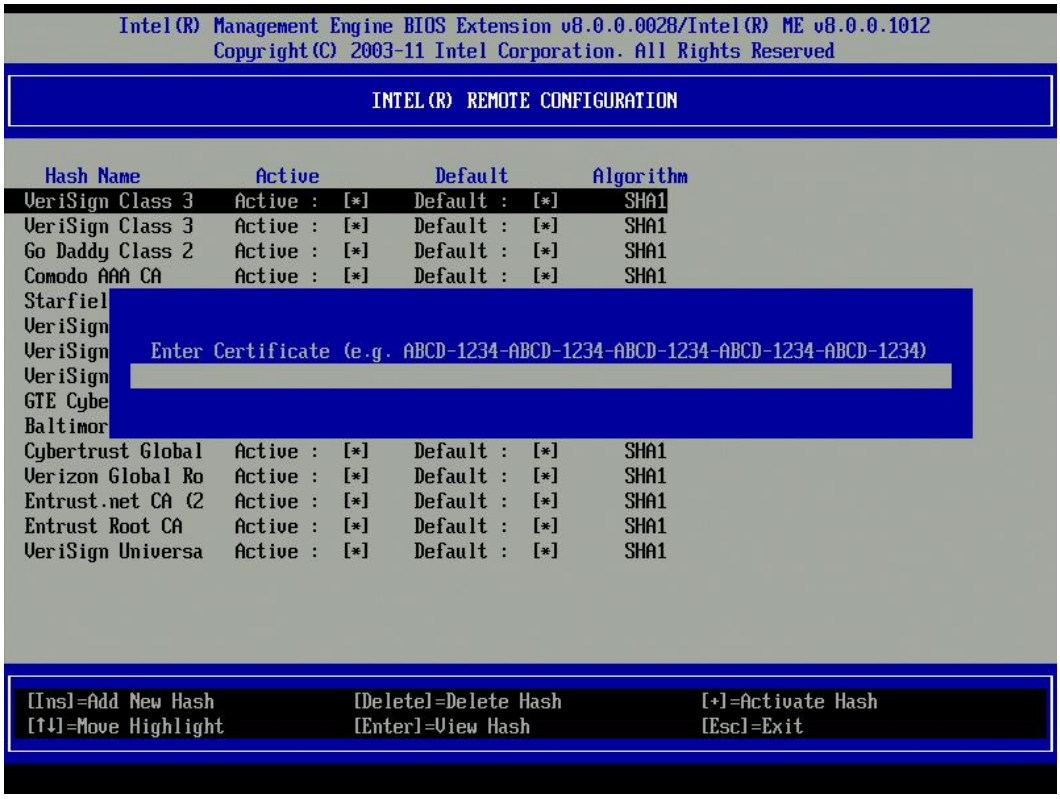
To add a customized certificate hash:

Enter the hash name (up to 32 characters). When you press 'Enter', you are prompted to select the algorithm of hash being used for PKI provisioning.

The supported hash algorithms are SHA1 **ONLY**.

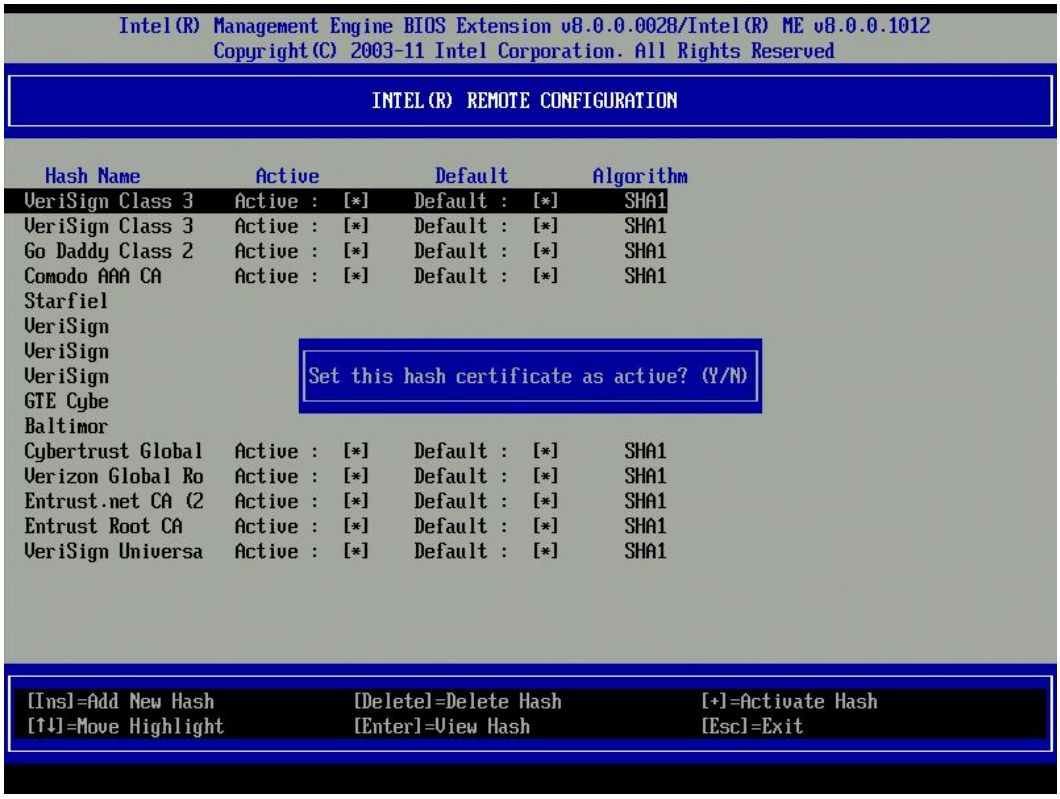
After selecting desired Hash Algorithm, you are prompted to enter the certificate hash value.

Figure 29: Add Hash - certificate



The Certificate hash value is a hexadecimal number (for SHA-1 it is 20 bytes). If the value is not entered in the correct format, the message “Invalid Hash Certificate Entered - Try Again” is displayed. When you press ‘Enter’, you are prompted to set the active state of the hash.

Figure 30: Add Hash - active



Your response sets the active state of the customized hash as follows:

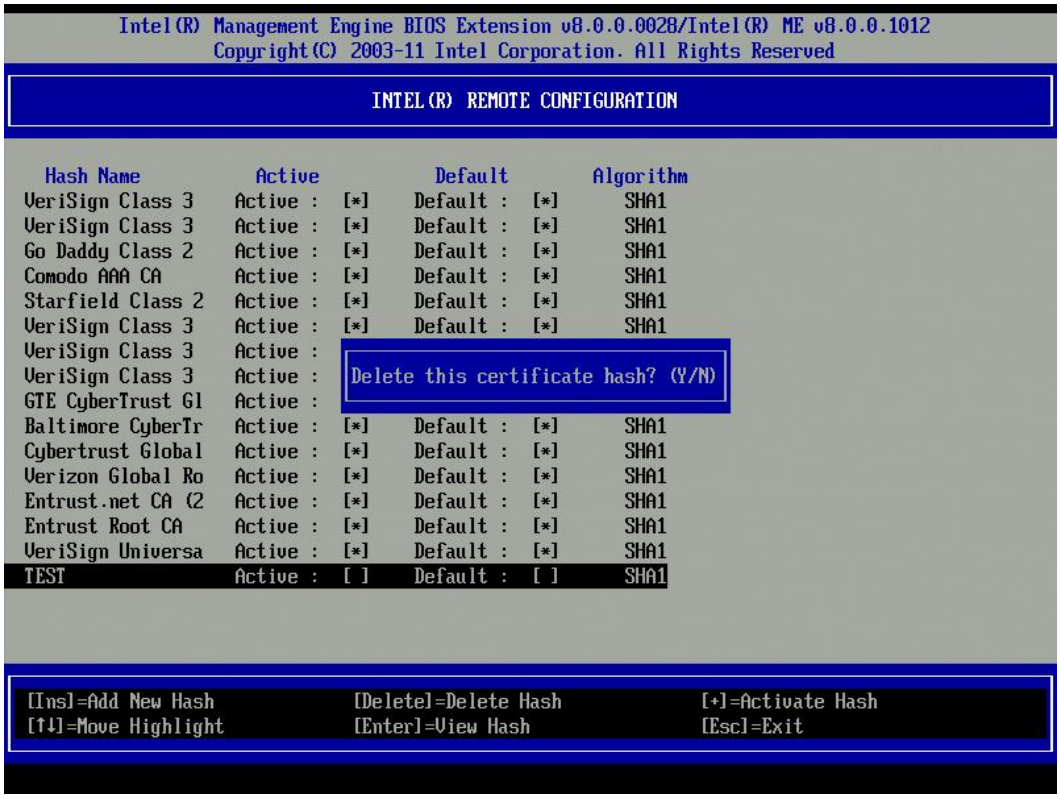
- **Yes** – The customized hash will be marked as active.
- **No (Default)** – The customized hash will added to the EPS but will not be active

3.5.8.7.5 Deleting a hash

Note: A certificate hash that is set to Default cannot be deleted.

When the Delete key is pressed in the Manage Certificate Hash screen, the following screen is displayed.

Figure 31: Deleting a hash



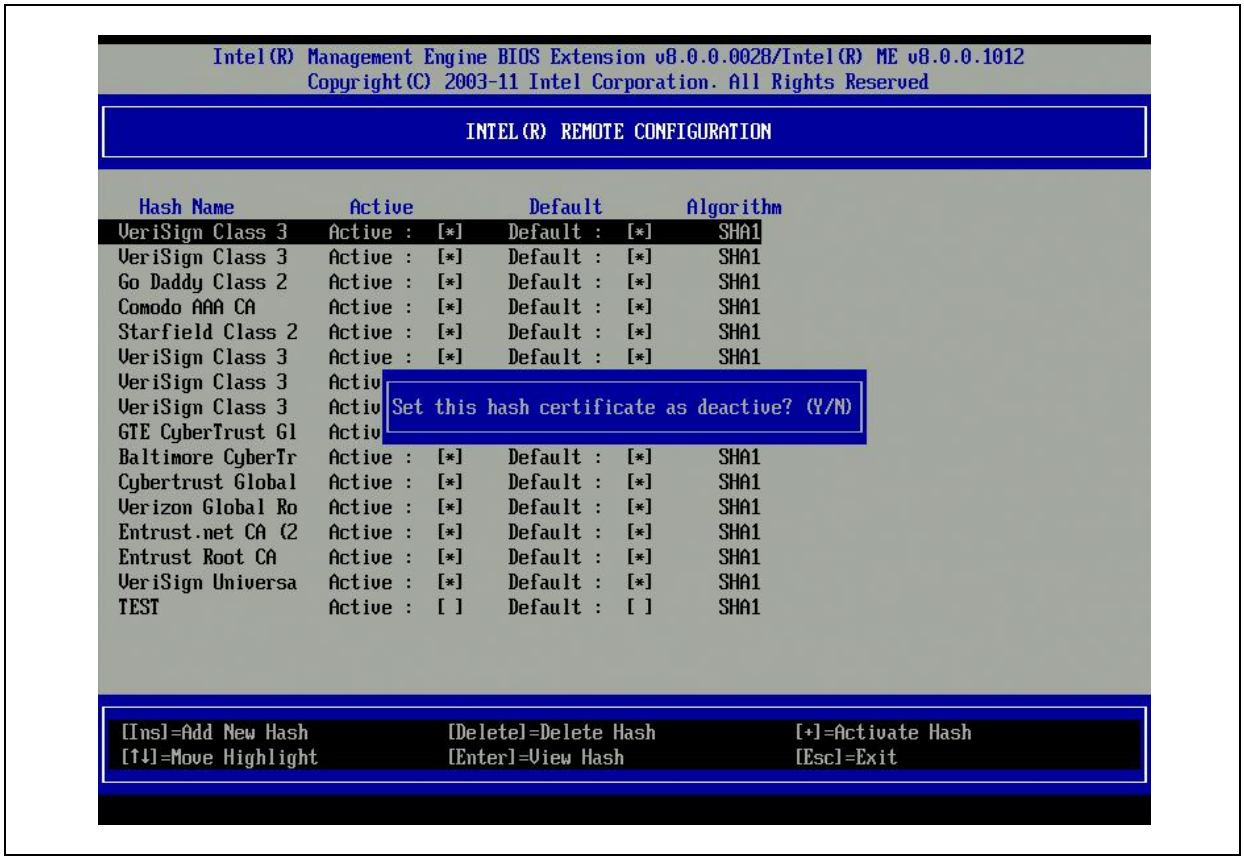
This option allows deleting of the selected certificate hash.

- **Yes** – Intel MEBX sends the firmware a message to delete the selected hash.
- **No** – Intel MEBX does not delete the selected hash, and returns to Remote Configuration.

3.5.8.7.6 Changing the Active State

When the '+' key is pressed in the Manage Certificate Hashes screen, the following screen is displayed as seen in the following screen.

Figure 32: Change Active State of Hash

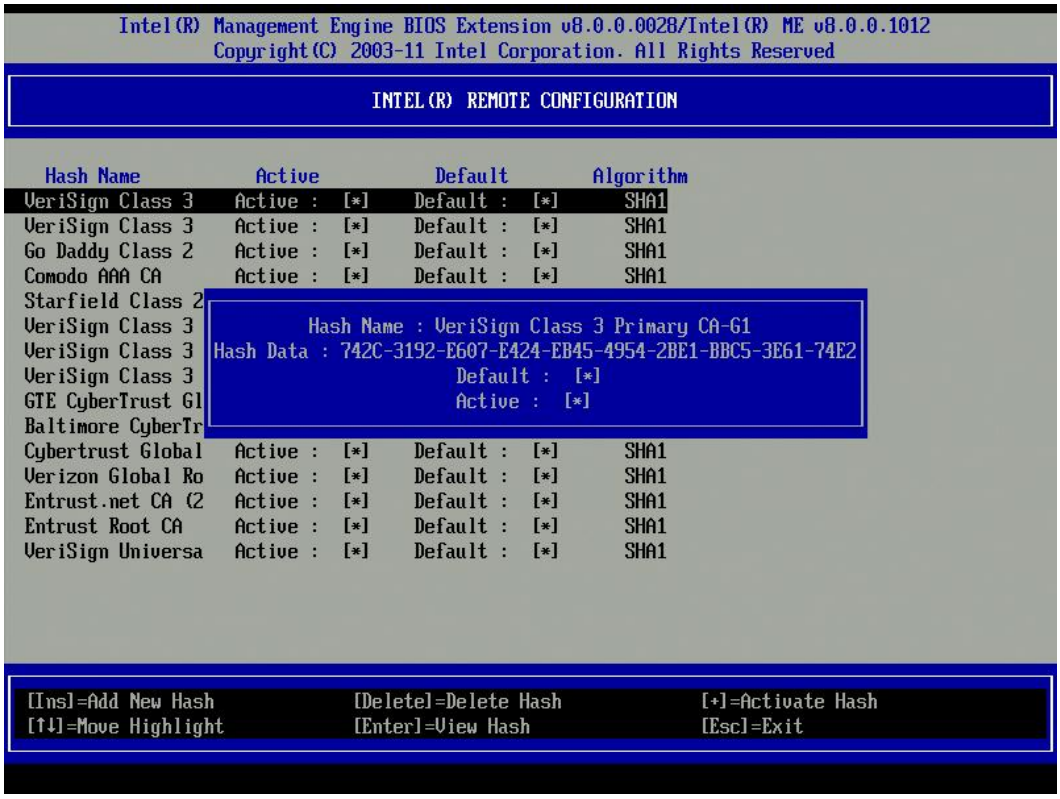


Answering **Y** toggles the active state of the currently selected certificate hash. Setting a hash as active indicates that the hash is available for use during PKI provisioning.

3.5.8.7.7 Viewing a Certificate Hash

When the Enter key is pressed in the Manage Certificate Hash screen, the following screen is displayed.

Figure 33: View Hash details



The details of the selected certificate hash are displayed to the user and include the following:

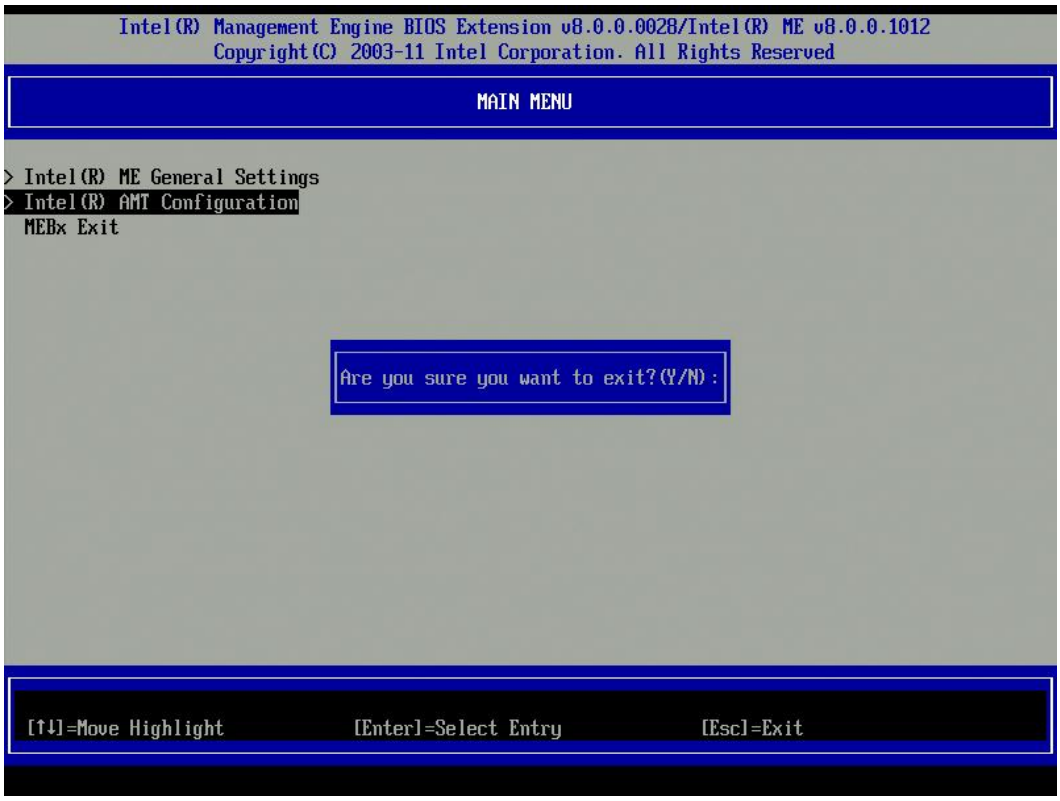
- hash name
- certificate hash data
- active and default states

3.6 Exit

Under the Main Menu,

1. Select ‘Exit’.
2. Press Enter.

Figure 34: Exit confirmation

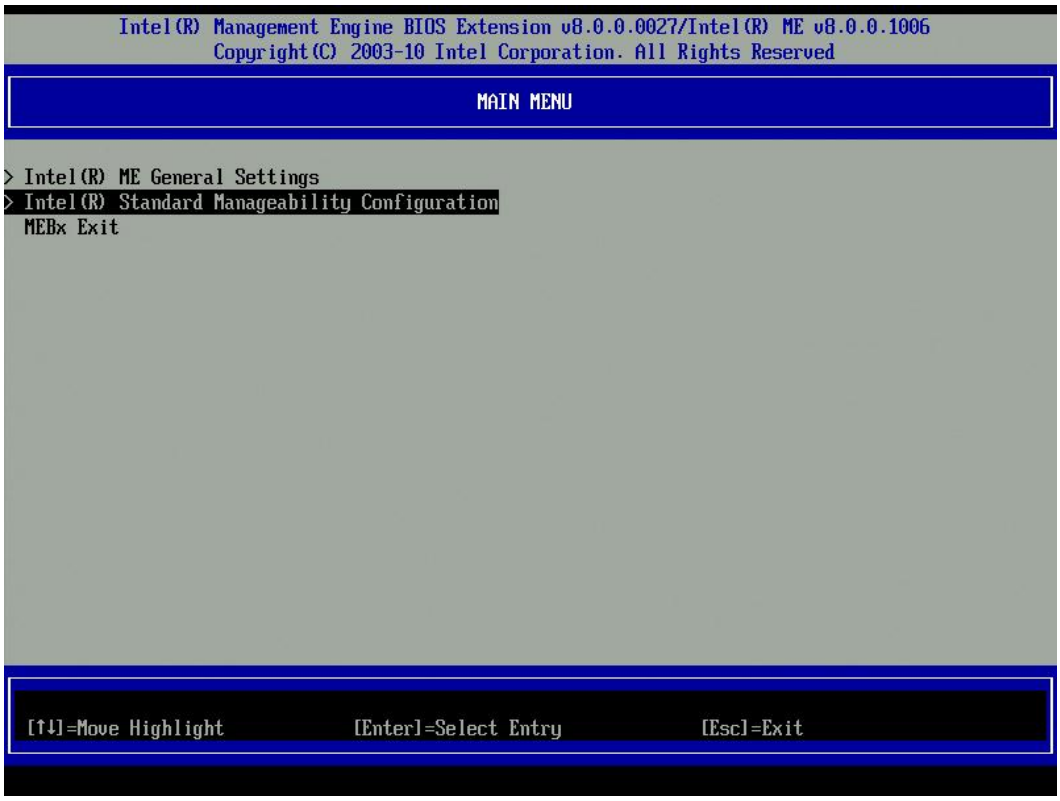


To exit MEBx, select “Y”, else select “N”

3.7 Intel® Standard Manageability Configuration

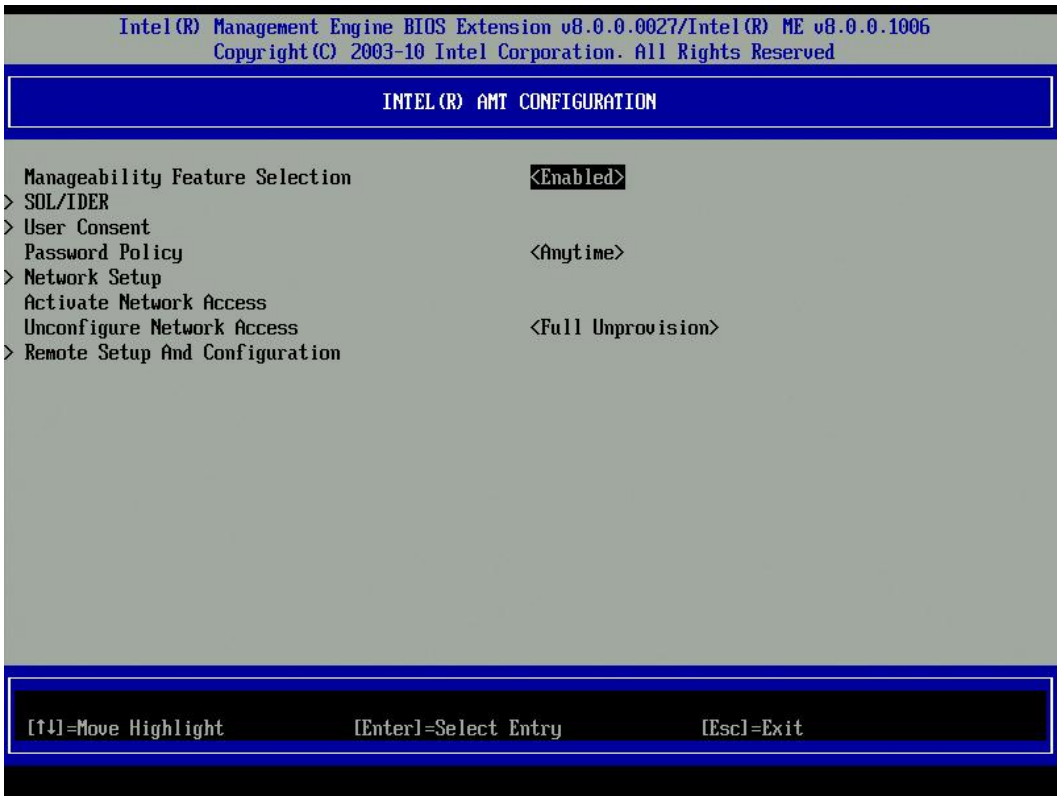
For platforms supporting Intel® Standard Manageability (e.g Q77 with non-vPro configuration and Q75), instead of Intel® AMT Configuration, the option of Intel® Standard Manageability Configuration will be displayed in MEBx setup menu.

Figure 35: Intel® Standard Manageability Configuration



The menu under Intel® Standard Manageability Configuration is the same as that displayed in Intel® AMT Configuration.

Figure 36: Intel® Standard Manageability Configuration menu



In the menus of SOL/IDER/KVM and “User Consent”, the KVM-related options are removed as KVM feature is not supported by Intel® Standard Manageability.

Figure 37: SOL/IDER/KVM Menu under Intel® Standard Manageability Configuration

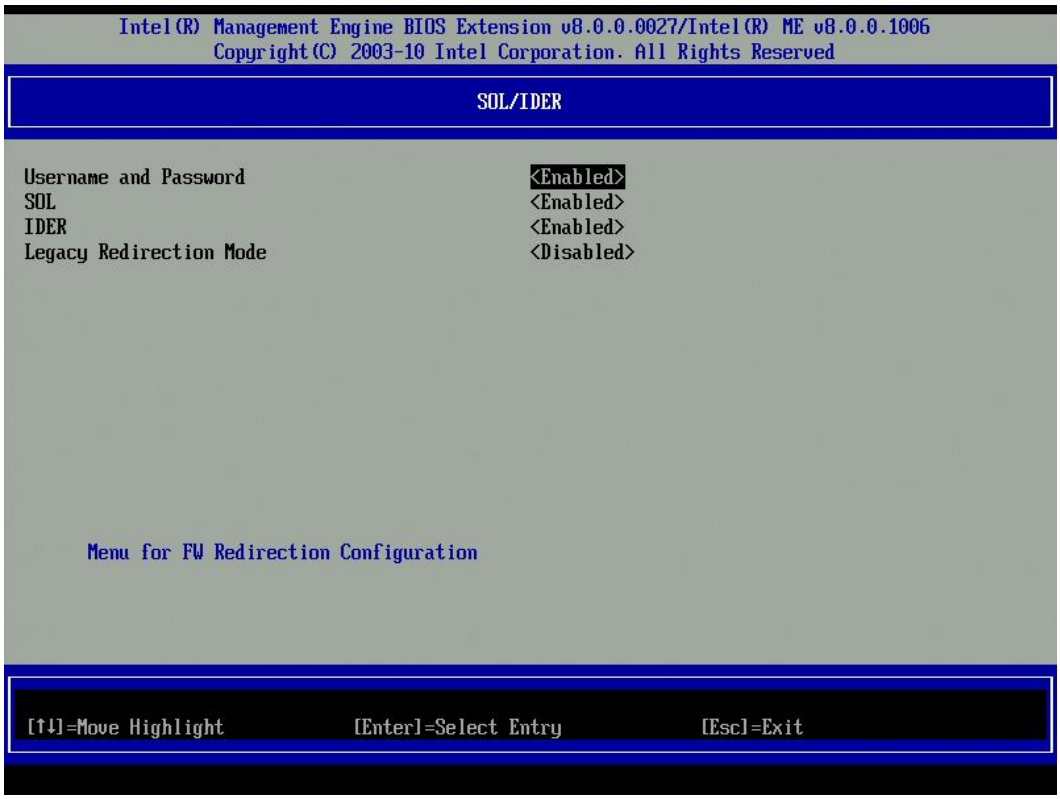
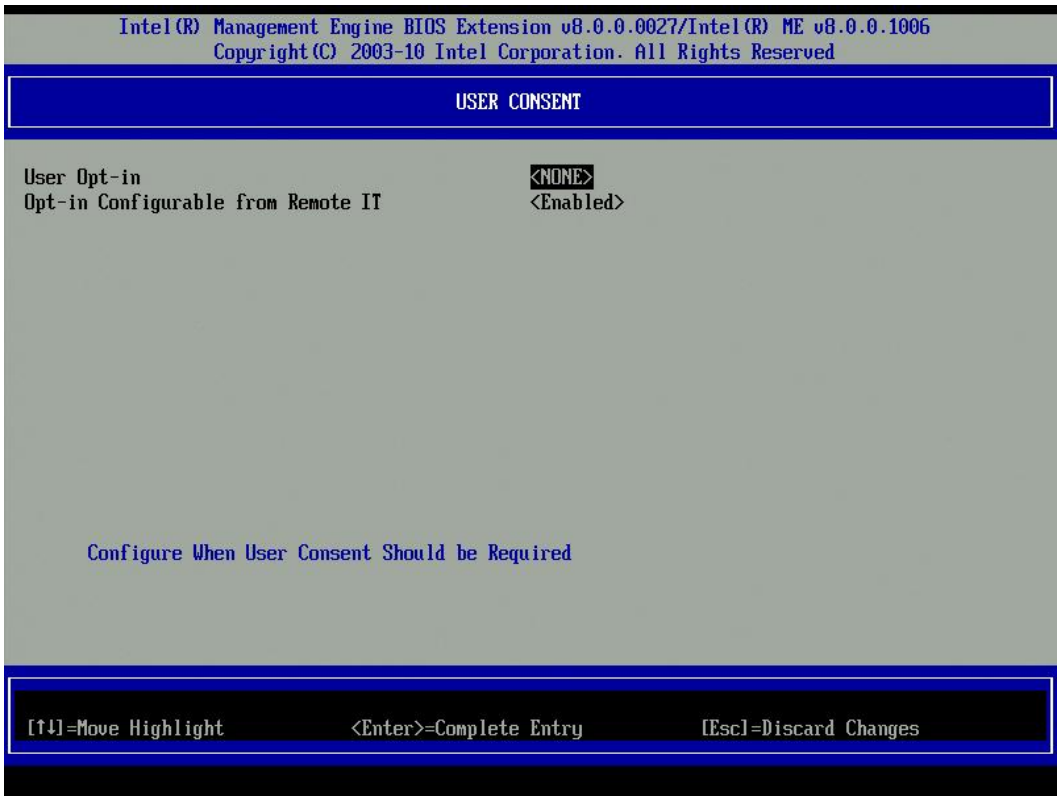


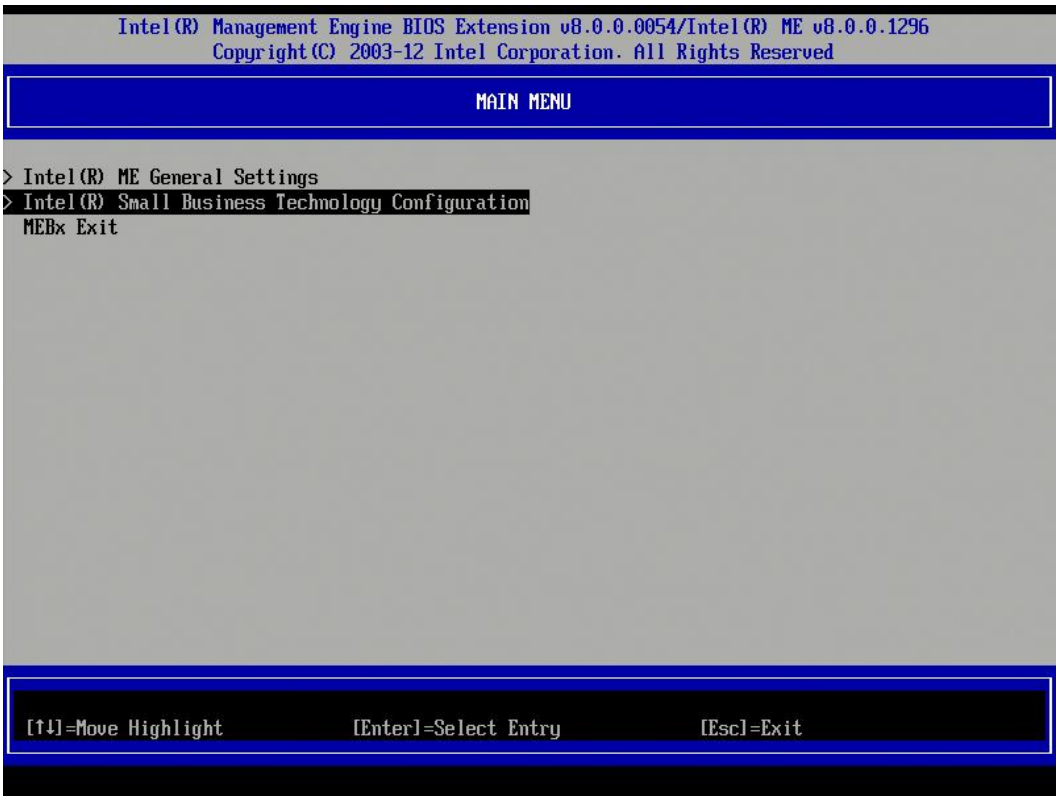
Figure 38: User Opt-in options under Intel® Standard Manageability Configuration



3.8 Intel® Small Business Technology Configuration

The "Intel® Small Business Advantage" has been defined beginning with ME8 platforms. Its features and capabilities shall be contained in the 5MB FW Image and its software. The Intel® Small Business Advantage disables out-of-band network access and provides key in-band features targeted for small business usages.

Figure 39: Main page of Intel® Small Business Technology



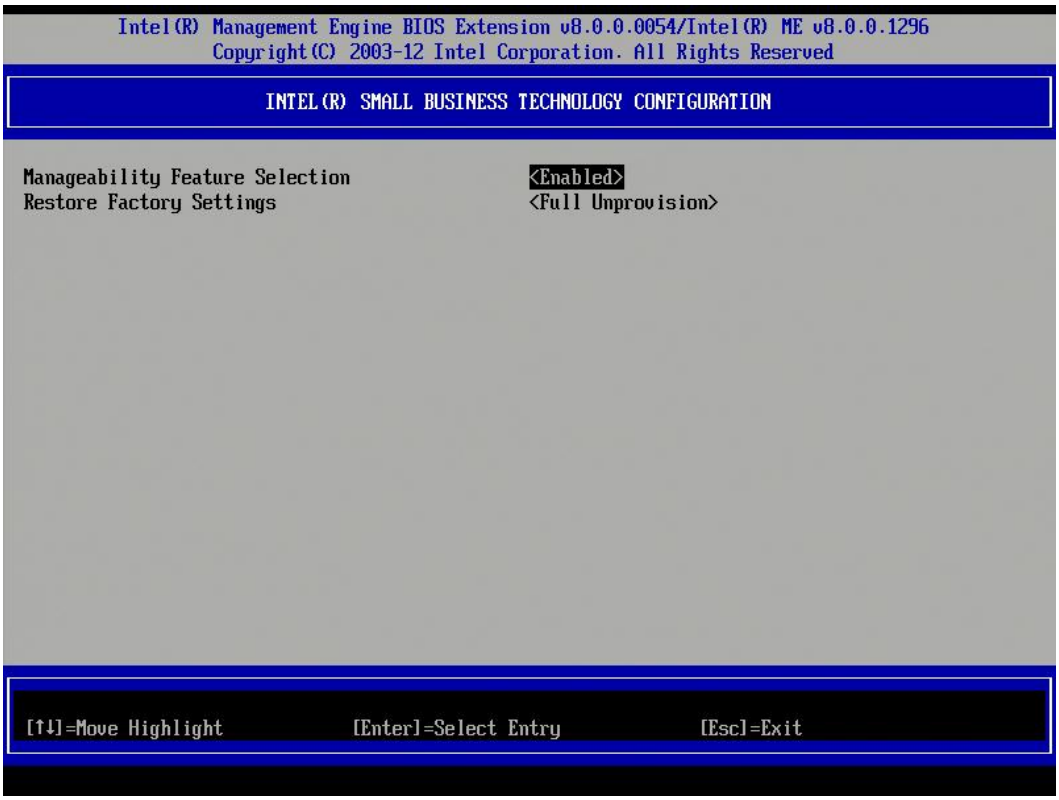
Under the Intel MEBX main menu,

1. Select 'Intel® Small Business Technology Configuration'.
2. Press Enter.

The following message is displayed: 'Acquiring Small Business Technology Configuration…'.

The Intel® MEBX main menu changes to the Intel® Small Business Technology Configuration page. This page allows the IT administrator to configure the specific functionality of the Intel® Small Business Technology, such as Manageability Feature Selection and Restore Factory Settings.

Figure 40: Intel® Small Business Technology Configuration



3.8.1 Manageability Feature Selection

Under the Intel® Small Business Technology Configuration screen,

1. Select 'Manageability Feature Selection'.
2. Press Enter to select.
3. A message is displayed: [Caution] Disabling reset network settings including network ACLs to factory default. System resets on MEBx exit. Continue: (Y/N). Press Y to change setting or N to cancel.

The following options can be selected:

- **Disabled**
- **Enabled**

3.8.2 Restore Factory Settings

Under the Intel® Small Business Technology Configuration menu,

4. Select 'Restore Factory Settings'.
5. Press Enter to select.

The following options can be selected:

- **Full Unprovision**

Note: When installing Intel® Small Business Advantage Software onto a vPro capable system, the MEBx menus will not display the Intel® Small Business Technology menu.

Intel ® Small Business Technology Configuration menu shows up on MEBx:

Chipset / Processor	Desktop		Mobile		ULV	
	Q77	**B75**	**QM77**	**HM77**	**UM77**	**QS77**
i7 vPro	**No**	Yes	**No**	Yes	Yes	**No**
i5 vPro	**No**	Yes	**No**	Yes	Yes	**No**
i7 (non vPro)		Yes	Yes	Yes	Yes	Yes
i5 (non vPro)		Yes	Yes	Yes	Yes	Yes
i3		Yes	Yes	Yes	Yes	Yes

3.9 Intel® MEBX CPU Replacement Flow

The Intel® ME FW is responsible for identifying CPU replacement, whenever CPU Type changes between CORE (vPro eligible) CPU, Core (Non-vPro eligible) CPU, PENTIUM CPU and CELERON CPU. MEBX is responsible for inquiring Intel ME FW whether End User approval is required for given CPU change. Only when indicated by ME FW that End User approval is needed, MEBx will show a message to End User demanding CPU Replacement approval.

The scenarios that result in Intel® MEBX displaying CPU Replacement related message to End User are:

1) **When CPU Type was Downgraded, e.g. from CORE (vPro eligible) CPU to PENTIUM CPU or from Core (Non-vPro eligible) CPU to CELERON CPU.**
   In this scenario Intel® ME FW will request End User Approval since Intel® ME FW feature set strongly relies on plugged in CPU TYPE. The message is displayed to guard End User before unintentional CPU downgrades which would automatically result in loosing Intel® ME FW feature set, for example un-configuration of AMT Feature Set. Instead, End User has option of either accepting CPU change or rejecting it before Intel® ME FW triggers System Features reconfiguration. If End User decides to reject the CPU change, it is required to shut down the platform and replace original CPU. If no End User interaction is provided then after 10 seconds wait time, Intel® MEBX will follow up assuming End User accepted CPU change.

The following exceptions capture when Intel® ME FW will not request CPU Replacement confirmation from End User (and the CPU Replacement message will not be shown):

1. When system is in Manufacturing Mode Intel® ME FW doesn't expect any messaging from user – in other words it's assumed to be informed change in CPU.
2. First boot after flashing in ME Region – Intel® ME FW doesn't expect any CPU replacement related flows that require user assistance
3. Clearing CMOS will cause ME un-configuration, any CPU change after clearing CMOS will not be considered as upgraded or downgraded from user perspective.

2) **When CPU Type was upgraded and new system features are enabled Intel® ME FW doesn't expect any CPU replacement related flows that require user assistance.** The examples of such an upgrade are:
   a. CELERON CPU changed to PENTIUM CPU
   b. CELERON CPU changed to Core (Non-vPro eligible) CPU
   c. CELERON CPU changed to CORE (vPro eligible) CPU

d. PENTIUM CPU changed to Core (Non-vPro eligible) CPU
e. PENTIUM CPU changed to CORE (vPro eligible) CPU
f. Core (Non-vPro eligible) CPU changed to CORE (vPro eligible) CPU

Figure 41 represents message that will be exposed to End User whenever CPU Replacement took place downgrading CPU capabilities. **This message will not be shown if replaced CPU has the same capabilities as the old one** (e.g. changing PENTIUM capable CPU to another PENTIUM capable CPU). **The message will be shown for 10 seconds and if End User did NEITHER pressed "y" or "Y" key NOR shut down the platform Intel® MEBX will proceed with assumption that End User approved CPU change.**
The valid changes that will result in the following message are:

1) CORE (vPro eligible) CPU changed to Core (Non-vPro eligible) CPU
2) CORE (vPro eligible) CPU changed to PENTIUM CPU
3) CORE (vPro eligible) CPU changed to CELERON CPU
4) Core (Non-vPro eligible) CPU changed to PENTIUM CPU
5) Core (Non-vPro eligible) CPU changed to CELERON CPU
6) PENTIUM CPU changed to CELERON CPU.

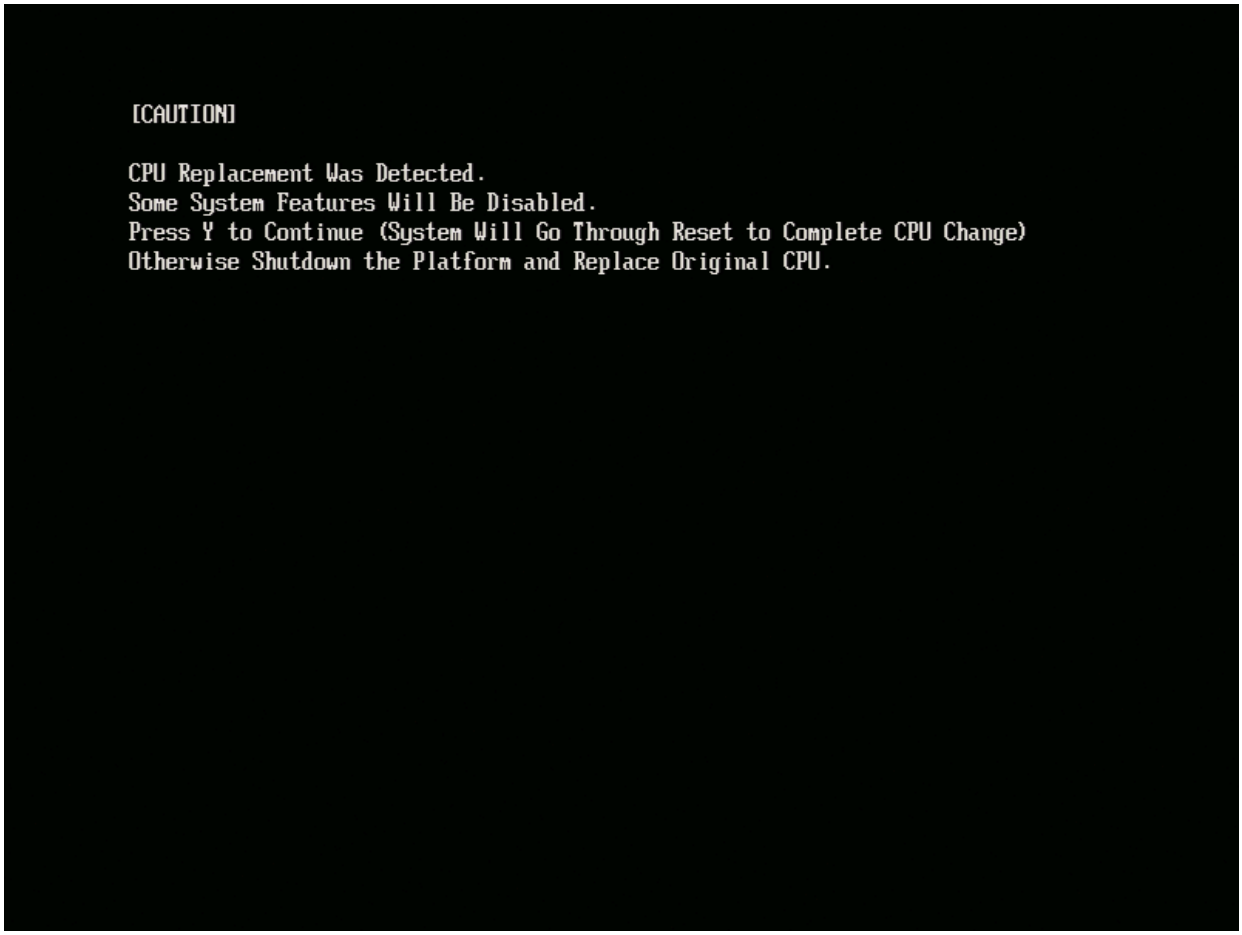
The following actions are expected to be done by End User when the message from Figure 41 is shown:

1) Press "y" or "Y" if End User approves CPU change that was performed on purpose. Platform global reset* will follow in which Intel® ME will populate new feature set to whole ME infrastructure (kernel and all applications) based on modified CPU type.
2) Press "n" or any other key if End User disapproves CPU replacement change and CPU was replaced unintentionally. The system will halt permanently displaying the message. End User is expected to shut down the platform and replace original CPU.
3) If no action is perfromed by End User for 10 seconds Intel® MEBX will follow up assuming End User accepted CPU change. Platform global reset* will follow in which Intel® ME will populate new feature set to

whole ME infrastructure (kernel and all applications) based on modified CPU type.

Note*: Two resets may be observed. The 2nd reset will occur if some AMT features (SOL/IDER/KVM) get disabled when a vPro CPU is replaced with a non-vPro CPU and this information has to synced with BIOS. Please refer to Appendix C for different causes to global reset.

Figure 41: Intel® MEBX CPU Replacement popup message



Appendix A: Changes to Configuration Modes

In Intel AMT 5.0 and under, there were two operational modes – SMB and Enterprise. In Intel AMT 6.0 and above, their functionality has been integrated to provide the same functionality previously available in Enterprise mode. The new configuration options are “Manual Setup and Configuration” available for SMB customers and “Automatic Setup and Configuration.

Figure 42: Configuration Modes

Setting	Intel® AMT 5.0 and under Default		Intel® AMT 6.0and above Default
	Enterprise Mode	SMB Mode	
TLS mode	Enabled	Disabled	Disabled, can be enabled at a later time
Web UI	Disabled	Enabled	Enabled
IDER/SOL/KVM Redirection network interface enabled	Disabled	Enabled if feature enabled in Intel® MEBX	Enabled, can be disabled at a later time
Legacy Redirection Mode (Controls FW listening for incoming redirection connections)	Disabled	Enabled if feature enabled in Intel® MEBX	Disabled (Need to set to “Enabled” in order to work with Legacy SMB consoles)

Manual configuration can be performed using the following six steps:

Note: you must have a DHCP server in your environment.

1. Burn the firmware.
2. Enter the Intel MEBX and change the password.
3. Enter Intel ME General Settings menu.
4. Select Activate Network Access.

5. Choose “y” in the confirmation message.
6. Exit the Intel MEBX.

Appendix B: Changes to Redirection Protocols

Before Intel AMT 6, firmware had the small/medium business (SMB) and the enterprise (ENT) provisioning modes. ENT was inherently more secure than SMB, which was meant to be more open and easy, but less secure. This change had an effect on the redirection protocols.

Before Intel AMT 6:

SMB: redirection ports were left open and Intel ME was listening constantly to the ports. ISV's writing consoles that dealt with redirection would then just open a connection to the ME machine. No extra steps were needed. The following flow was used:

1. Open a connection
2. Perform redirection actions (SOL/IDER)
3. Close the connection.

ENT: Redirection ports were closed meaning Intel ME was not listening for redirection connections. An SMB console wishing to open a connection to an ENT machine would fail since the ports were closed. For the connection to succeed (and how ENT consoles are implemented in the market) the following flow was used:

1. Send "open port" command to the Intel ME machine
2. Open a connection
3. Perform redirection actions (SOL/IDER)
4. Close the connection
5. Send "close port" command to the Intel ME machine

In Intel AMT 6 and above:

Since both provisioning modes are combined, the more secure option was chosen, but to ensure backwards compatibility for older SMB consoles (that need the ports left open to succeed in creating SOL/IDER connections since they do not send the open/close commands) we needed another setting, the "legacy redirection mode".

If "legacy redirection mode" is set to enabled, the ports are left open, and SMB consoles will be able to connect (open and close the port is not needed)

If “legacy redirection mode” is set to disabled, the ports are closed and the console needs the extra command to open/close the ports in order to connect. The user can go into Intel MEBx, or use a USB key to set this setting. If the USB key is a legacy one prepared by an SMB console, Intel MEBx automatically sets the legacy redirection mode to Enabled. Since SMB configuration required manual touch anyway, this poses no customer issue.

Appendix C: Global Reset from MEBx

Several MEBx configuration options require a global reset after they have been edited by the user. The reset is flagged while in the MEBx UI and passed back to BIOS to perform the reset request. The MEBx UI has to keep track of which configuration options require a global reset after exiting MEBx. Multiple techniques are used to ensure the global reset flow is entered correctly. The MEBx uses 2 flags for its logic related to signaling global resets: Reboot and Exit. The 'Reboot' flag indicates that the current option will require a reboot after exiting MEBx. The 'Exit' flag is used to force the user out of the MEBx UI.

Reboot – MEBx must set this flag when an option that requires a global reset has been edited from its original state. A list of global reset options is itemized in the table below.

Exit – MEBx must completely exit the UI immediately after editing the option.

Table of MEBx UI Global Reset Options:

Option	Reboot	Exit
Max Logins exceeded	Y	Y
CPU String Emulation	Y	N
Manageability Feature Selection (EN->DIS)	Y	N
Manageability Feature Selection (DIS->EN)	N	N
SOL IDER Username/Password	Y	N
KVM State	Y	N
SOL state	Y	N
IDER state	Y	N

Other MEBx global reset scenarios include

1. CPU replacement
2. ME Unconfiguration without MEBx password through system BIOS setting (BPF)
3. ME Unconfiguration by clearing CMOS

These global resets happen when BIOS execute MEBx binary during post. In these cases MEBx will pass the global reset flag to BIOS to perform global reset without going through MEBx User Interface.

Appendix D: PID-PPS Checksum

The PID and PPS are made up of ASCII codes of some combination of characters – capital alphabet characters (A–Z), and numbers (0–9).

- The PID is an eight character entry of the form: XXXX-XXXC (where "C" is the CRC (Cyclic Redundancy Check) of the preceding characters) and is sent in the open.
- The PPS is a thirty-two character quantity of the form:

  XXXC-XXXC-XXXC-XXXC-XXXC-XXXC-XXXC-XXXC (where "C" is the CRC of the preceding characters) and is a secret shared between the Intel AMT device and the Setup and Configuration Server.

When the PID and PPS are entered via the MEBx sub menu/USB key, the firmware checks for checksum characters embedded in the values. The last character of the PID is expected to be a checksum of the previous seven characters, and the fourth character in each group of four characters in the PPS is expected to be a checksum of the previous three characters. This check is made to reduce the possibility of operator error when entering these values.

Appendix E: Intel® MEBX Options Being Reflected in the Firmware

Below is the list of MEBx options which will be reflected in FW when saved.

Note: Those settings are located in data region of the FW, and, when saved, FW will look at the saved settings and run the corresponding execution when necessary.

Option	Reflected in the firmware
MEBx Login	Instantly
Change ME Password	Instantly
Local FW Update	Upon Exiting Intel MEBX
Intel(R) ME ON in Host Sleep States	Upon Exiting Intel MEBX
Idle Timeout	Upon Exiting Intel MEBX
Manageability Feature Selection	Upon Exiting Intel MEBX
Password Policy	Upon Exiting Intel MEBX
Activate Network Access	Instantly
Unconfigure Network Access	Instantly
Username and Password	Instantly
SOL	Instantly
IDER	Instantly
Legacy Redirection Mode	Instantly
KVM Feature Selection	Instantly
User Opt-in	Upon Exiting Intel MEBX
Opt-in Configurable from Remote IT	Upon Exiting Intel MEBX
Host Name	Upon Exiting Intel MEBX
Domain Name	Upon Exiting Intel MEBX
Shared/Dedicated FQDN	Upon Exiting Intel MEBX
Dynamic DNS Update	Upon Exiting Intel MEBX
Periodic Update Interval	Upon Exiting Intel MEBX
TTL	Upon Exiting Intel MEBX
DHCP Mode	Upon Exiting Intel MEBX
IPV4 Address	Upon Exiting Intel MEBX

Option	Reflected in the firmware
Subnet Mask Address	Upon Exiting Intel MEBX
Default Gateway Address	Upon Exiting Intel MEBX
Preferred DNS Address	Upon Exiting Intel MEBX
Alternate DNS Address	Upon Exiting Intel MEBX
Current Provisioning Mode	Upon Exiting Intel MEBX
Provisioning Record	None
Provisioning Server IPV4/IPV6	Upon Exiting Intel MEBX
Provisioning Server IPV4/IPV6	Upon Exiting Intel MEBX
Provisioning Server FQDN	Upon Exiting Intel MEBX
Start Configuration	Instantly
Halt Configuration	Instantly
Set PID and PPS **	Instantly
Delete PID and PPS **	Instantly
Remote Configuration **	Instantly
Manage Hashes	Instantly
PKI DNS Suffix	Upon Exiting Intel MEBX