

# **Cannon Lake/Coffee Lake Platform Intel® Management Engine BIOS Extension (Intel® MEBX)**

**User Guide**

---

***For Systems Based on Cannon Lake/Coffee Lake Processor  
Line***

***February 2018***

***Revision 1.1***

**Intel Confidential**



You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at [Intel.com](http://Intel.com), or from the OEM or retailer.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at [intel.com](http://intel.com), or from the OEM or retailer.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visit [www.intel.com/design/literature.htm](http://www.intel.com/design/literature.htm).

By using this document, in addition to any agreements you have with Intel, you accept the terms set forth below.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

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

© 2018 Intel Corporation. All rights reserved.



# Contents

1	Introduction .....	6
1.1	Intel® Management Engine BIOS Extension (Intel® MEBX) Overview .....	6
1.2	Scope of Document .....	6
1.3	Target Audience .....	6
1.4	Acronyms .....	6
1.5	Related Documentation.....	8
2	Client System Requirements .....	9
3	Intel® ME Manageability Features .....	10
3.1	Access Intel® MEBX Configuration User Interface .....	10
3.2	Intel® MEBX Main Menu .....	11
3.3	Intel® ME Password .....	11
3.4	Intel® ME Platform Configuration Menu .....	13
3.4.1	Change Intel® ME Password .....	14
3.4.2	FW Update.....	15
3.5	Intel® AMT Configuration .....	15
3.5.1	Manageability Feature Selection .....	16
3.5.2	SOL/Storage Redirection/KVM .....	16
3.5.3	User Consent .....	18
3.5.4	Password Policy.....	20
3.5.5	Network Setup .....	20
3.5.6	Activate Network Access.....	29
3.5.7	Unconfigure Network Access .....	30
3.5.8	Remote Setup and Configuration .....	31
3.5.9	Power Control .....	45
3.6	Exit.....	48
3.7	Intel® Standard Manageability Configuration .....	49
3.8	Intel® MEBX CPU Replacement Flow .....	49
Appendix A	: Changes to Configuration Modes .....	53
Appendix B	: Global Reset from Intel® MEBX.....	54
Appendix C	: Intel® MEBX Options Being Reflected in Firmware.....	55



## Figures

Figure 3-1. Intel® MEBX Configuration User Interface Main Menu .....	11
Figure 3-2. Intel® ME Platform Configuration .....	13
Figure 3-3. Change Intel® ME Password .....	14
Figure 3-4. FW Update Settings .....	15
Figure 3-5. Intel® AMT Configuration .....	16
Figure 3-6. SOL/Storage Redirection/KVM .....	16
Figure 3-7. User Consent .....	19
Figure 3-8. Intel® ME Network Setup .....	21
Figure 3-9. Intel® ME Network Name Settings .....	22
Figure 3-10. Periodic Update Interval .....	24
Figure 3-11. TTL Screen .....	25
Figure 3-12. TCP/IP Settings .....	26
Figure 3-13. Wired LAN IPV4 Configuration .....	27
Figure 3-14. DHCP Mode Disabled .....	28
Figure 3-15. Activate Network Access .....	29
Figure 3-16. Unconfigure Network Access .....	31
Figure 3-17. Intel® Remote Setup and Configuration .....	32
Figure 3-18. Current Provisioning Mode .....	33
Figure 3-19. Provisioning Record .....	34
Figure 3-20. Intel® Remote Configuration .....	36
Figure 3-21. Activate RCFG .....	37
Figure 3-22. Intel® Remote Configuration .....	38
Figure 3-23. Manage Hashes .....	39
Figure 3-24. Adding New Hash Name .....	40
Figure 3-25. Add Hash - Certificate .....	41
Figure 3-26. Add Hash - Active .....	42
Figure 3-27. Deleting Hash .....	43
Figure 3-28. Change Active State of Hash .....	44
Figure 3-29. View Hash Details .....	45
Figure 3-30. Power Control .....	46
Figure 3-31. Idle Timeout .....	48
Figure 3-32. Exit Confirmation .....	49
Figure 3-33. Intel® MEBX CPU Replacement Popup Message .....	52

## Tables

Table 3-1. Intel® AMT Unprovisioning .....	30
Table 3-2. Supported Power Packages .....	47



## Revision History

---

Revision Number	Description	Revision Date
0.5	Draft version: Carry over from Kaby Lake MEBx user guide	February 2017
0.8	Update revision to align with document release milestone	May 2017
0.9	Update Screenshots.	August 2017
1.0	Update new "Intel ® AMT" option in main menu of MEBx. Remove Unsecure Redirection Authentication method from MEBx.	January 2018
1.1	Update Appendix B	February 2018

§



# 1 Introduction

---

## 1.1 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 feature independent of the installed OS:

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

Intel® ME configuration is included in the BIOS by the Intel® Management Engine BIOS Extension (Intel® MEBX). Intel® MEBX provides the ability to change and 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® 10-Series Chipset Family / Intel® PCH platforms with Intel® AMT. This document is applicable only for Intel® ME FW Corporate SKU.

**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. Refer 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



Acronym	Description
BIOS	Basic Input Output System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
FIT	Flash Image Tool, provided by Intel® FW kit
FPT	Flash programming Tool, provided by Intel® FW kit.
FW	Firmware
G3	Complete Power loss from chipset point of view, except RTC well.
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
PP1	Power Package 1, refer to Power control section
PP2	Power Package 2, refer to Power control section
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
TCP	Transmission Control Protocol
UTC	Coordinated Universal Time
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/vproexpert?view=documentsln>

§





## 2 Client System Requirements

---

The client system referred to in this document is based on the Intel® 10-Series Chipset Family / Intel® PCH platforms based on Mobile H/U/Y-Processor Line 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 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 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, some 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 changed settings are **NOT** saved. Refer Appendix D for detail of Intel® MEBX options being reflected in firmware.

### 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 Intel® MEBX UI in this scenario.

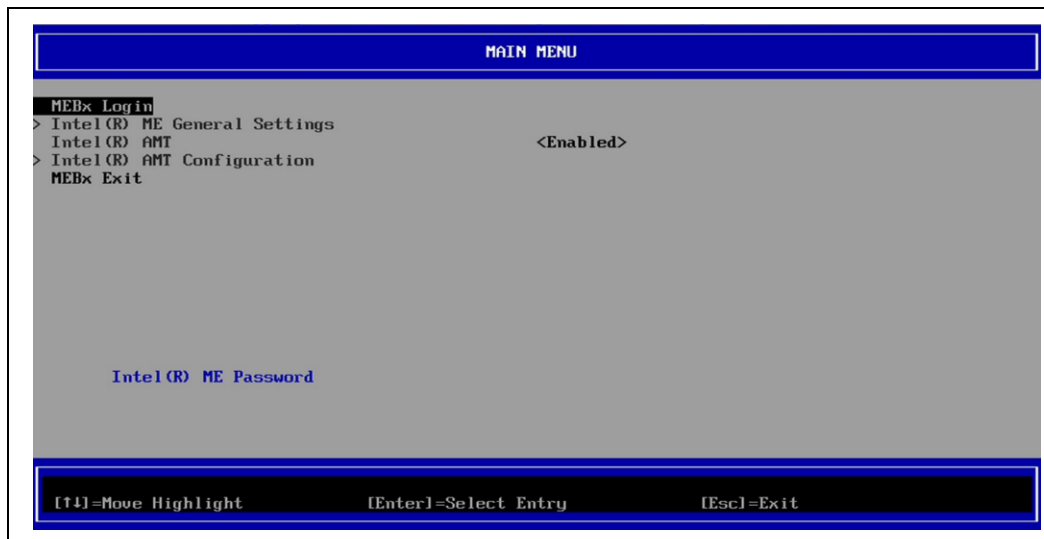
**Note:** If Intel® AMT has been configured, <CTRL-ALT-F1> will also be displayed along with <CTRL-P>. It is designed for end users to use Fast call for Help feature either inside or outside of corporate network environment when Intel® AMT systems are not discovered by management console.

2. Enter the Intel® Management Engine password under **'MEBX Password'** and press Enter. The default password is 'admin'. This default password must be altered by the user. 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 3-1. 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:

- Intel® MEBX Login
- Intel® ME General Settings
- Intel® AMT
- Intel® AMT Configuration
- Intel® 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.

**Note:** If Intel® AMT is set to disabled, Intel® MEBX will not display Intel® AMT Configuration.

## 3.3 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:** When entering more than 32 characters, every new character pressed after 32<sup>nd</sup> character in the Intel® MEBX UI, will get ignored and thus no error message will pop up.

**Note:** On systems where Intel® ME is configured to support un-configure on RTC clear (default), the password can be reset to the default setting by shutting down the system, removing AC and DC power and performing an RTC reset. The method for performing Intel® ME un-configure can vary by system design. Thus, it may be necessary to consult with the system manufacturer on the appropriate method to reset the password to the default setting.

**Note:** During manufacturing, OEM is able to configure default MEBx password different from "admin". When OEM closing manufacturing mode, the current MEBx password will become default MEBx password.



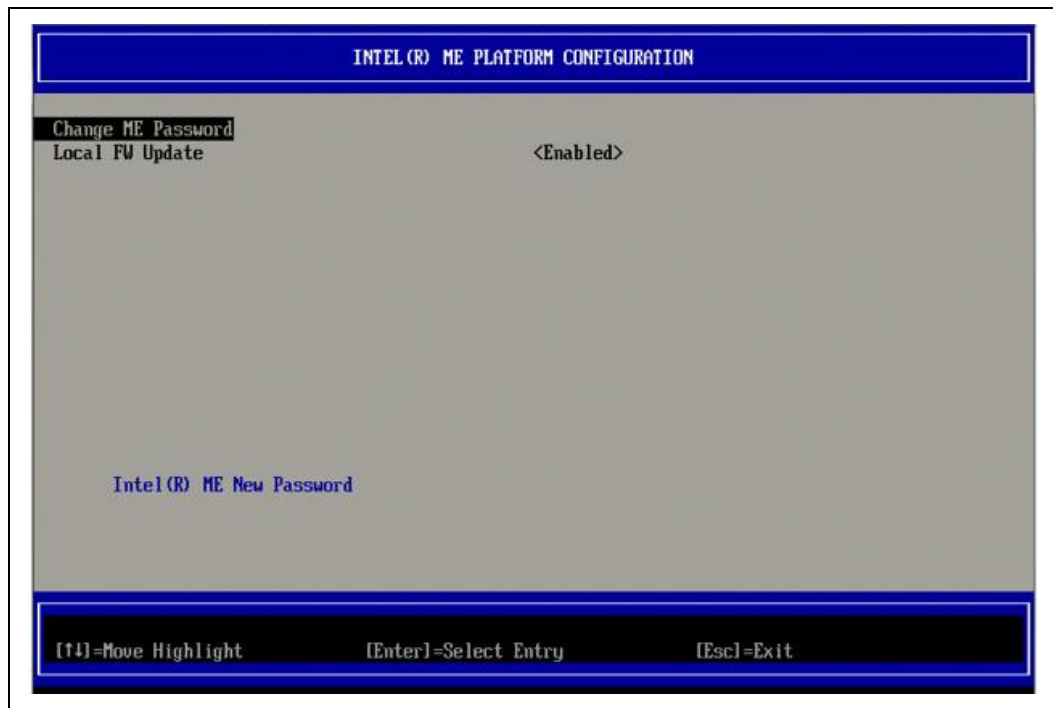
### 3.4 Intel® ME Platform Configuration Menu

Under the Intel® MEBX main menu:

1. Select 'Intel® ME General Settings'.
2. Press Enter to select.

The Intel® MEBX main menu changes to the Intel® ME Platform Configuration menu. This menu allows the IT administrator to configure the specific functionality of the Intel® ME, such as password and so on.

**Figure 3-2. Intel® ME Platform Configuration**



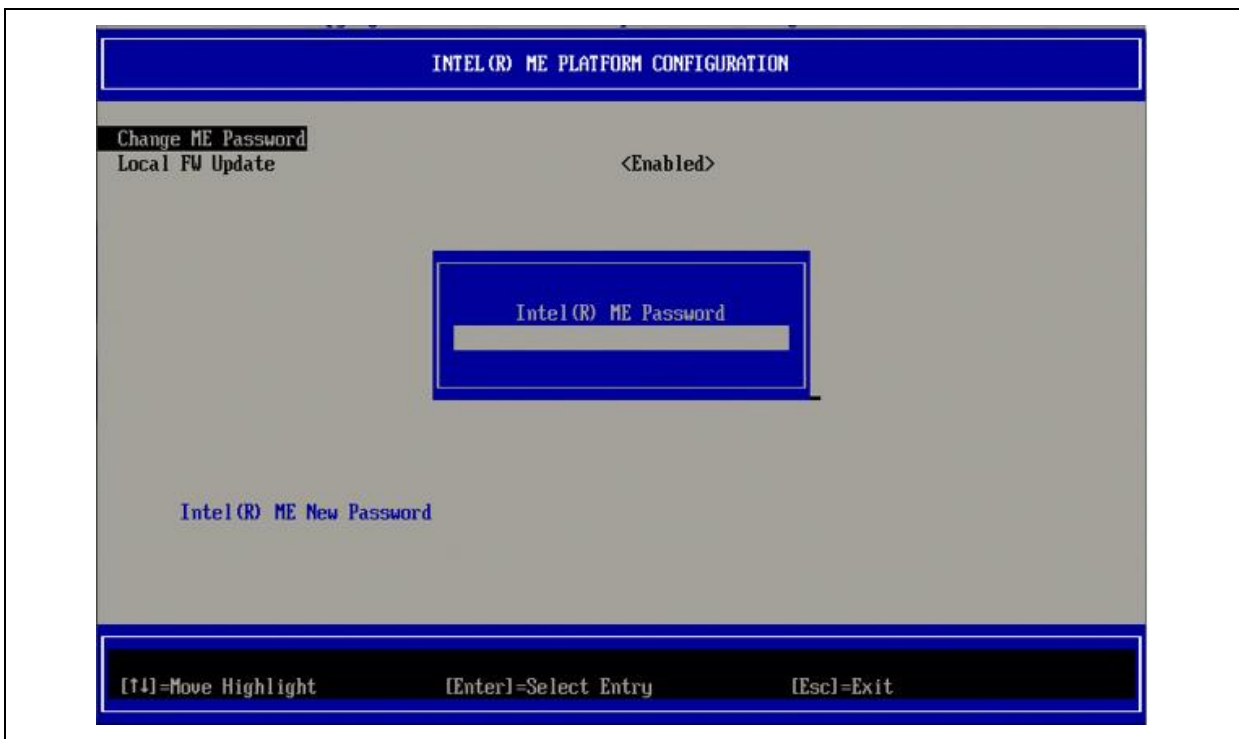


### 3.4.1 Change Intel® ME Password

Under the Intel® ME Platform Configuration menu:

1. Select 'Change Intel® ME Password'
2. Press Enter to change password.
3. The Intel® ME New Password prompt is displayed as in [Figure 3-3](#).
4. At the Intel® ME Password prompt, enter your old password.
5. At the Intel® ME New Password prompt, enter your new password. (Be aware of the password policies and restrictions mentioned in [section 3.3](#))
6. At the Verify Password prompt, re-enter your new password. Your password is now changed.

**Figure 3-3. Change Intel® ME Password**



**NOTE:** This password is also the password which Intel® Platform Enablement Test Suit (Intel® PETS) tool require by default.

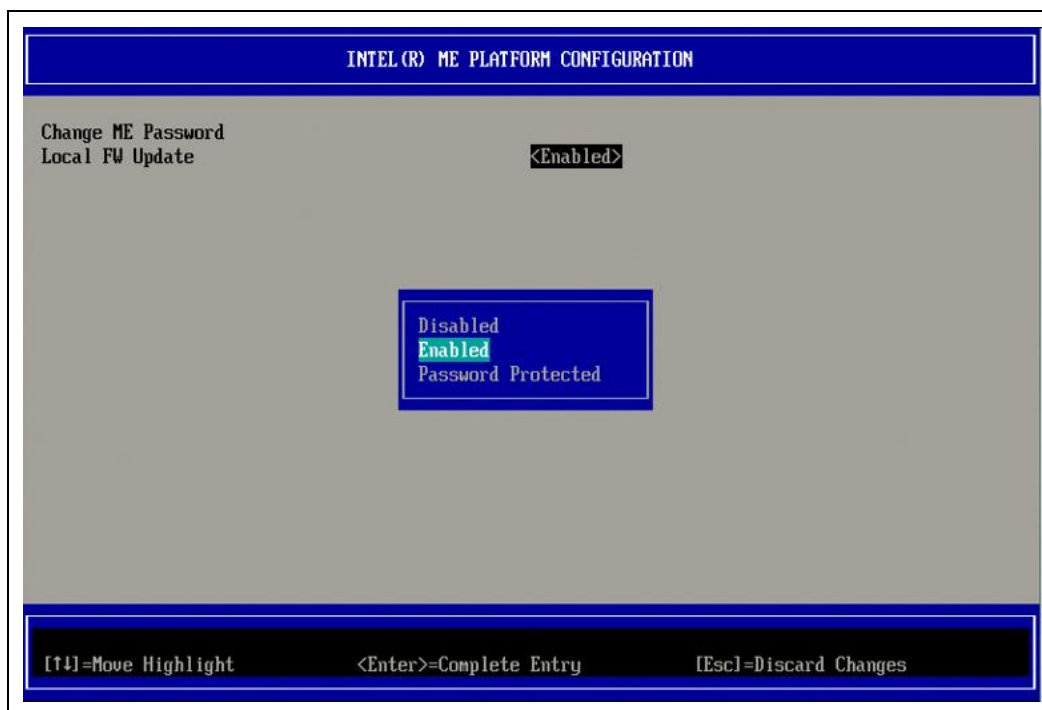


### 3.4.2 FW Update

Under Intel® ME Platform Configuration menu:

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

**Figure 3-4. FW Update Settings**



Intel® ME Firmware Update provides the capability to allow or prevent firmware update in the field. When the “Enabled” option is selected, the administrator is able to update the Intel® ME firmware locally via the local Intel® Management Engine interface.

The following options can be selected:

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

When **Hide FW Update Control** setting in FIT is set, Intel® MEBX will hide FW Update option.

## 3.5 Intel® AMT Configuration

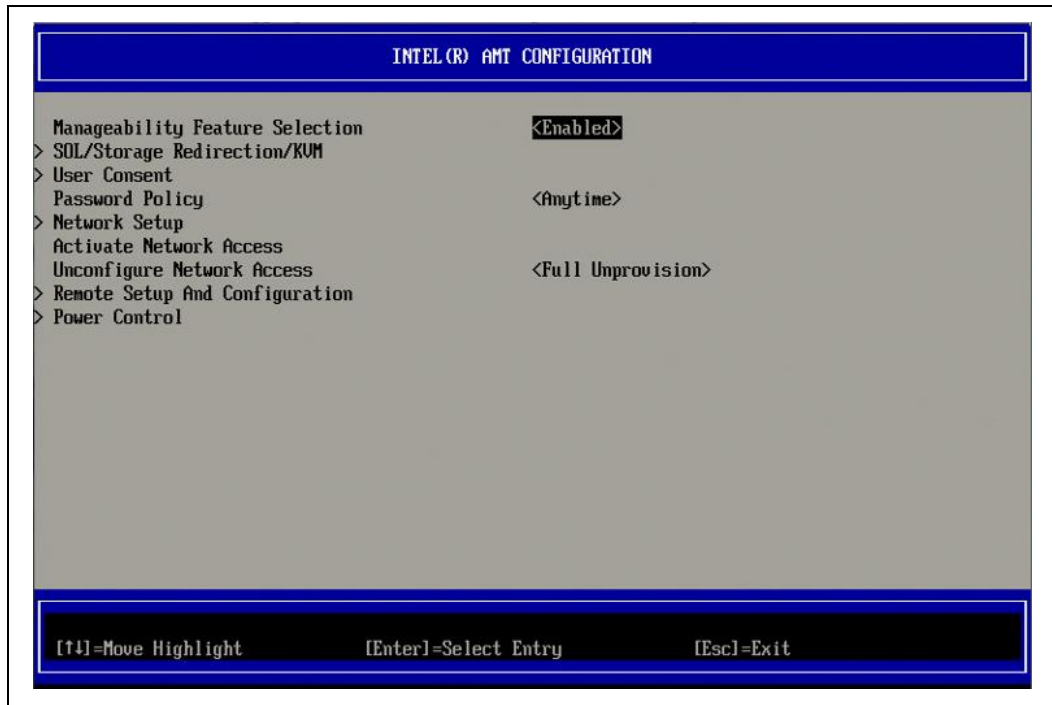
Under the Main Menu:

1. Select 'Intel® AMT Configuration'.
2. Press Enter to select.

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



Figure 3-5. Intel® AMT Configuration



### 3.5.1 Manageability Feature Selection

Under the Intel® AMT Configuration menu:

1. Select 'Manageability Feature Selection'.
2. Press Enter to select.

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.

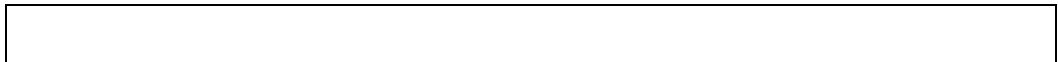
### 3.5.2 SOL/Storage Redirection/KVM

Under the Intel® AMT Configuration menu **(with Intel® AMT enabled)**:

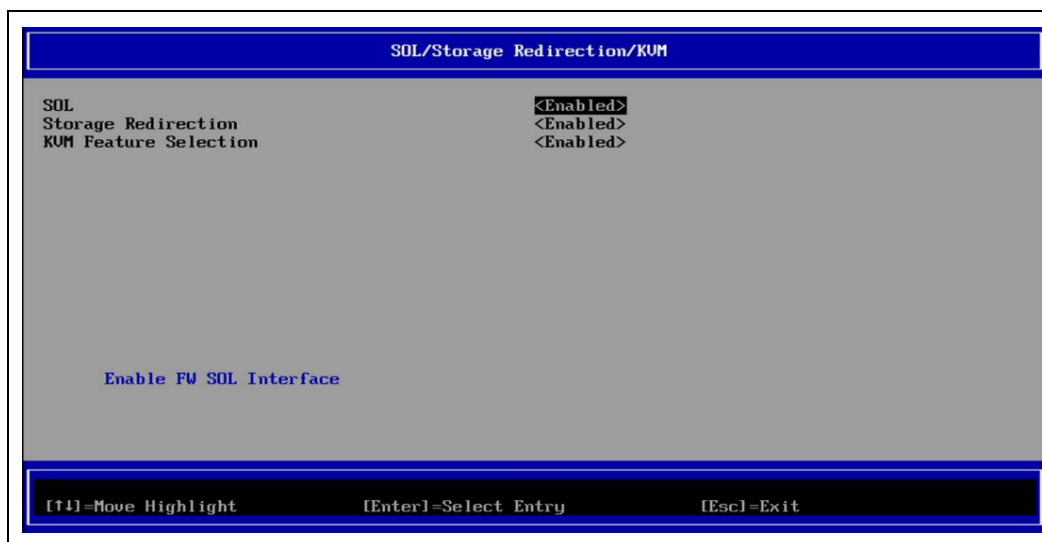
1. Select 'SOL/Storage Redirection/KVM'.
2. Press Enter to select.

The Intel® AMT Configuration changes to the SOL/Storage Redirection/KVM menu.

Figure 3-6. SOL/Storage Redirection/KVM







**NOTE:** SOL, Storage Redirection, and Intel® KVM here are just for enabling CAPABILITY. User still needs to use other tools like Intel® AMT SDK to execute features.

### 3.5.2.1 SOL

Under the SOL/Storage Redirection/KVM menu:

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 should not be set.

Disabling SOL does not remove this feature but just blocks it from being used.

### 3.5.2.2 Storage Redirection

Under the SOL/Storage Redirection/KVM menu:

1. Select 'Storage Redirection'.
2. Press Enter to select.

The following options can be selected:

- Disabled
- Enabled

Storage Redirection allows an Intel® AMT to mount a remote disk by a management console. If the client system does not support Storage Redirection, this value should not be set.

Disabling Storage Redirection does not remove this feature but just blocks it from being used.



### **3.5.2.3 Intel® KVM Feature Selection**

Under the SOL/ Storage Redirection /KVM menu:

1. Select 'Intel® KVM Feature Selection'.
2. Press Enter to select.

The following options can be selected:

- Disabled
- Enabled

Intel® KVM redirection capability provides IT to remotely control an end-user's platform using a remote keyboard, mouse and see the managed end-user machine's screen output at the remote screen on the IT management console.

Disabling Intel® KVM does not remove this feature but disables it. Intel® KVM will not work in this case.

### **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:

- Storage Redirection
- Intel® 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

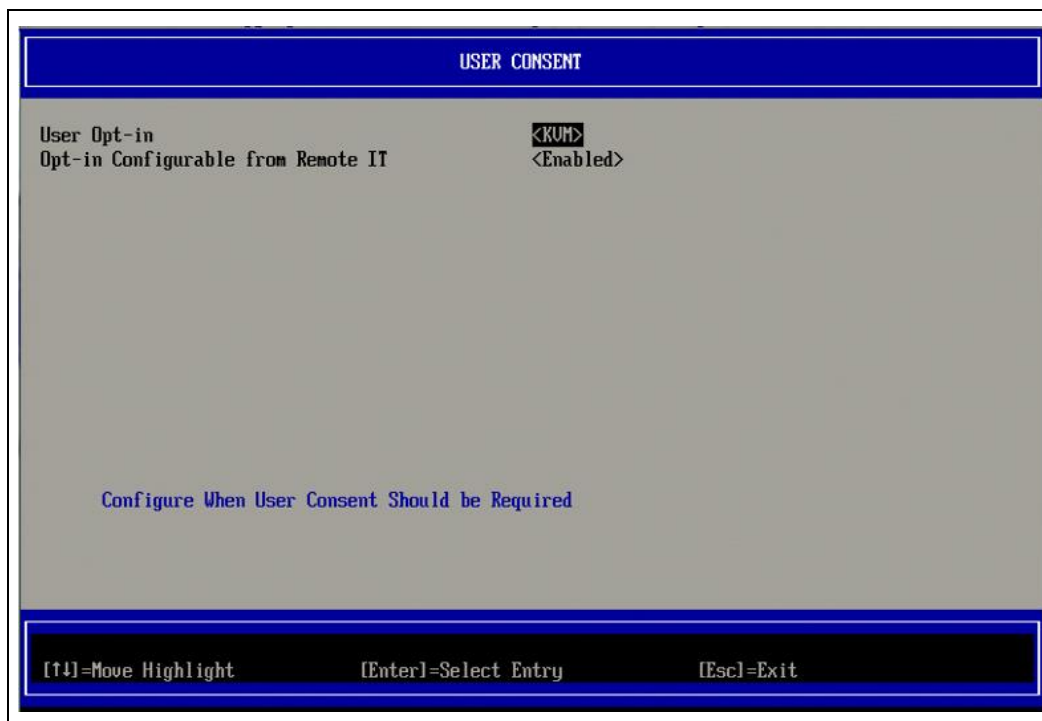
Under the Intel® AMT Configuration menu:

1. Select 'User Consent'.
2. Press Enter to select.

The Intel® AMT Configuration changes to the User Consent menu, refer [Figure 3-7](#).



Figure 3-7. User Consent



### 3.5.3.1 User Opt-in

Under the User Consent Configuration menu:

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 "Intel® AMT Release 11.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 menu:

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.

**Note:** "Privacy/Security Level" in FIT also affects redirection and user consent behavior as below:

- Default – Enable all ports with no user consent required for SOL/Storage Redirection/KVM.
- Enhanced – Requires user consent for SOL/Storage Redirection/KVM.
- Extreme – Disable SOL/Storage Redirection/KVM.

### 3.5.4 Password Policy

Under the Intel® AMT Configuration menu:

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 any of the passwords is changed. Once changed over the network or the Intel® MEBX user interface, the network password and the Intel® MEBX password will always be kept separate.

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

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

### 3.5.5 Network Setup

Under the Intel® AMT Configuration menu:

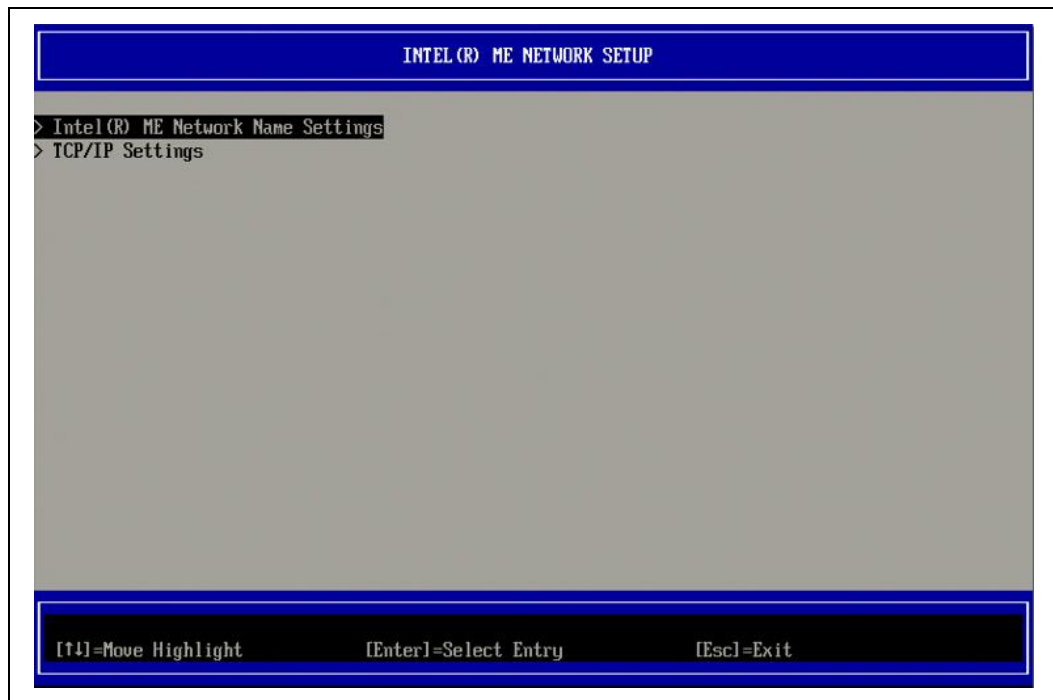
1. Select 'Network Setup'.



2. Press Enter to select.

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

**Figure 3-8. Intel® ME Network Setup**



### **3.5.5.1 Intel® ME Network Name Settings**

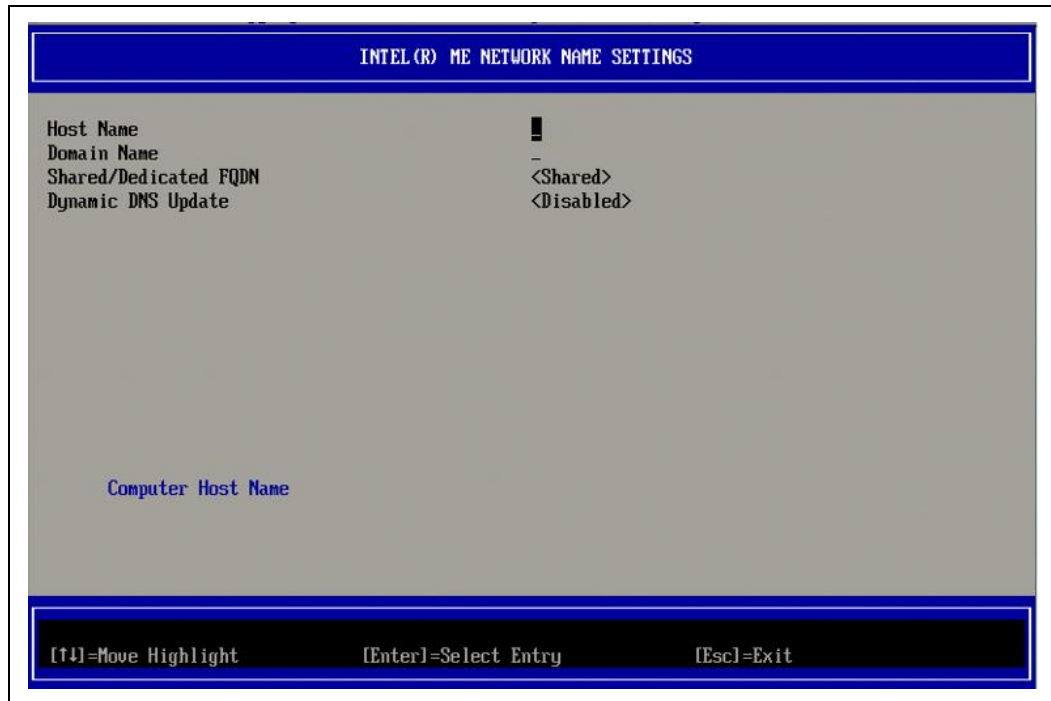
Under the Intel® ME Network Setup menu:

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

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



Figure 3-9. 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 is dedicated to Intel® ME.
- **Shared-** The FQDN 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.

- 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.
- Under Shared FQDN mode: Firmware uses DHCP option 81 for DNS registration but does not directly update DNS using the DDNS update protocol.

For selecting "Enabled" for Dynamic DNS Update it is required that the Host Name and Domain Name are set.

#### **3.5.5.1.5 Periodic Update Interval**

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



Figure 3-10. Periodic Update Interval

INTEL(R) ME NETWORK NAME SETTINGS

Host Name	-
Domain Name	-
Shared/Dedicated FQDN	<Shared>
Dynamic DNS Update	<Enabled>
Periodic Update Interval	1440
TTL	900

Value=0 or >=20  
1440

<Enter>=Complete Entry      [Esc]=Discard Changes

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

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



**Figure 3-11. TTL Screen**

INTEL(R) ME NETWORK NAME SETTINGS	
Host Name	-
Domain Name	-
Shared/Dedicated FQDN	<Shared>
Dynamic DNS Update	<Enabled>
Periodic Update Interval	1440
TTL	900

Value in Seconds

900

<Enter>=Complete Entry      [Esc]=Discard Changes

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

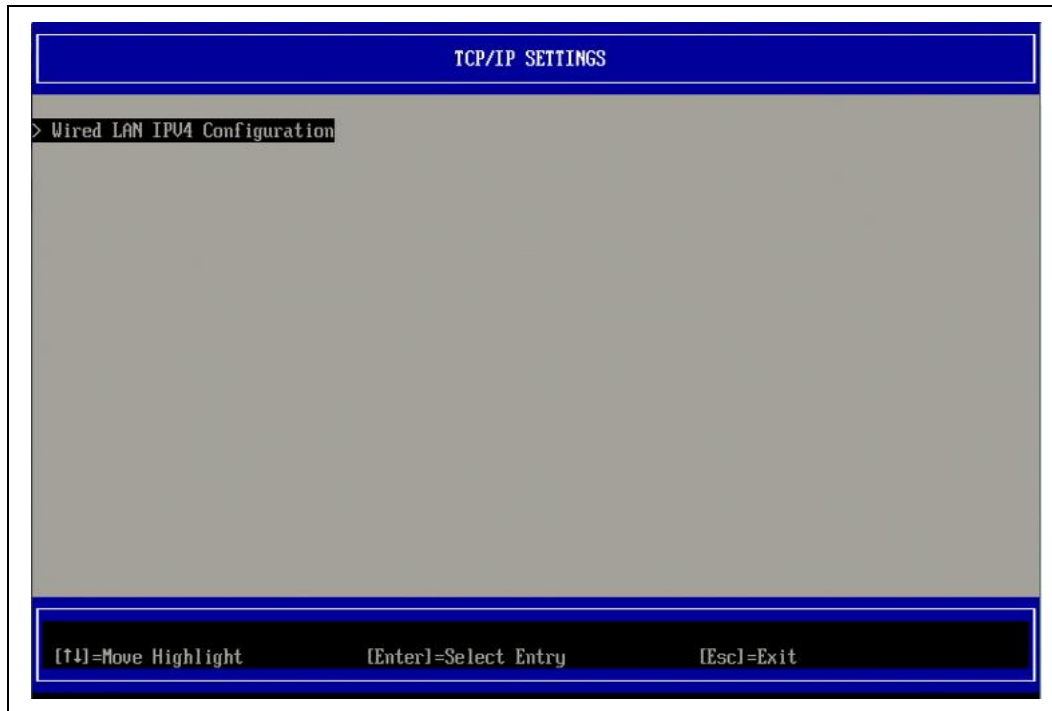
Under the Intel® ME Network Setup menu:

1. Select 'TCP/IP Settings'.
2. Press Enter to select.

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



Figure 3-12. TCP/IP Settings



### 3.5.5.2.1 Wired LAN IPV4 Configuration

Under the TCP/IP Settings menu:

1. Select 'Wired LAN IPV4 Configuration'.
2. Press Enter to select.

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



Figure 3-13. Wired LAN IPV4 Configuration



### 3.5.5.2.2 DHCP Mode

Under the Wired LAN IPV4 Configuration menu:

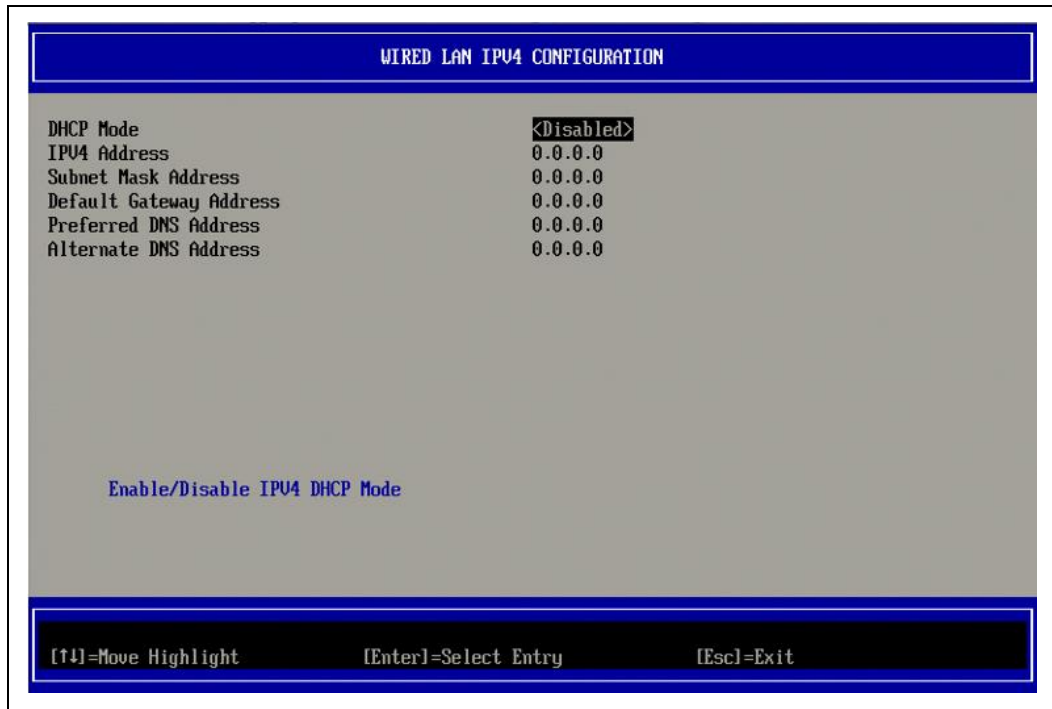
1. Select 'DHCP Mode'.
2. Press Enter to select.

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 Intel® MEBX User Guide scope). Check following sections [3.5.5.2.3](#) to [3.5.5.2.7](#).

Static IP and subnet mask are mandatory.

Figure 3-14. DHCP Mode Disabled



### 3.5.5.2.3 IPv4 Address

Under the Wired LAN IPV4 Configuration menu:

1. Select 'IPv4 Address'.
2. Press Enter to edit.

### 3.5.5.2.4 Subnet Mask Address

Under the Wired LAN IPV4 Configuration menu:

1. Select 'Subnet Mask Address'.
2. Press Enter to edit.

### 3.5.5.2.5 Default Gateway Address

Under the Wired LAN IPV4 Configuration menu:

1. Select 'Default Gateway Address'.
2. Press Enter to edit.



### 3.5.5.2.6 Preferred DNS Address

Under the Wired LAN IPV4 Configuration menu:

1. Select 'Preferred DNS Address'.
2. Press Enter to edit.

### 3.5.5.2.7 Alternate DNS Address

Under the Wired LAN IPV4 Configuration menu:

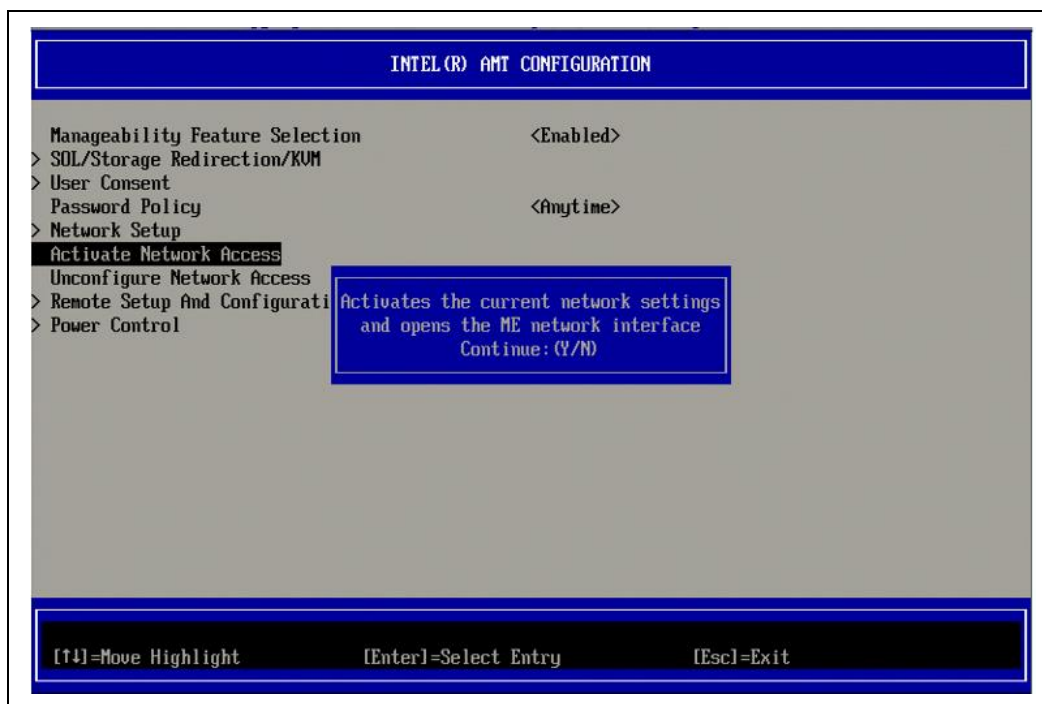
1. Select 'Alternate DNS Address'.
2. Press Enter to edit.

## 3.5.6 Activate Network Access

Under the Intel® AMT Configuration menu:

1. Select 'Activate Network Access'.
2. Press Enter to select.
3. Press **Y** to activate or press **N** to cancel.

**Figure 3-15. 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, Intel® ME will not be able to connect to the network.



### 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

**Table 3-1. Intel® AMT Unprovisioning**

<b>Intel® AMT Full Unprovisioning</b>	The following settings still Kept: Intel® MEBX password BIOS tables Privacy related settings: SOL/Storage Redirection/KVM local enable/disable Intel® KVM Opt-in settable through network enable/disable Storage Redirection boot log
<b>Intel® AMT Partial Unprovisioning</b>	Same as Intel® AMT Full Unprovisioning and more following settings Kept: All Remote Configuration settings (ZTC enable, OTP, customized hashes, configuration server FQDN, provisioning DNS suffix) ME Network Name Settings – Kept

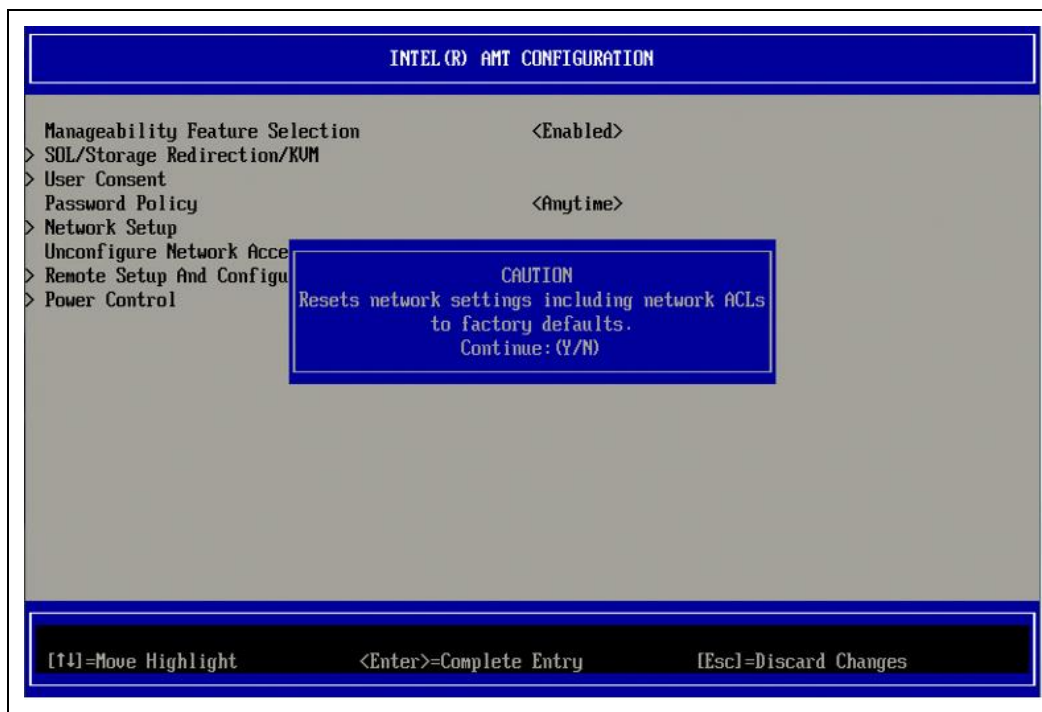
**NOTE:** Refer Appendix A Un-Provision Behavior Details in the document - Firmware Variable Structures for Intel® Management Engine Corporate/Consumer Technology for more details.

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



The following screen appears:

**Figure 3-16. Unconfigure Network Access**



### 3.5.8 Remote Setup and Configuration

Under Intel® AMT Configuration:

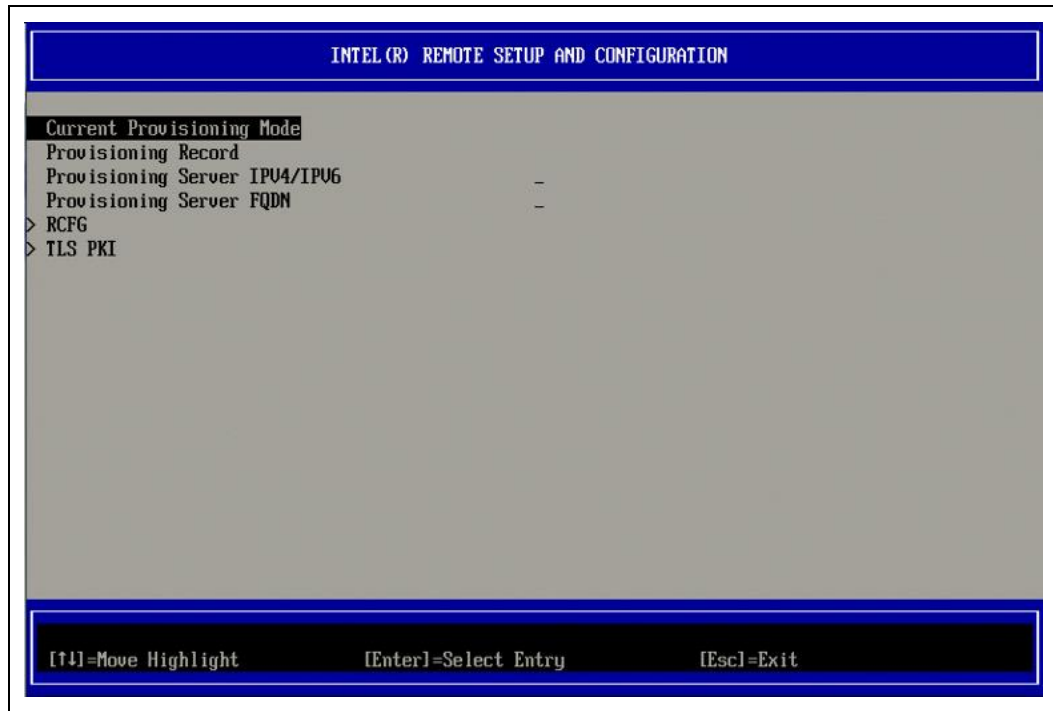
1. Select 'Remote Setup and Configuration'.
2. Press Enter to select.

Intel® AMT Configuration menu changes to the Intel Remote Setup and Configuration menu.

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



Figure 3-17. Intel® Remote Setup and Configuration

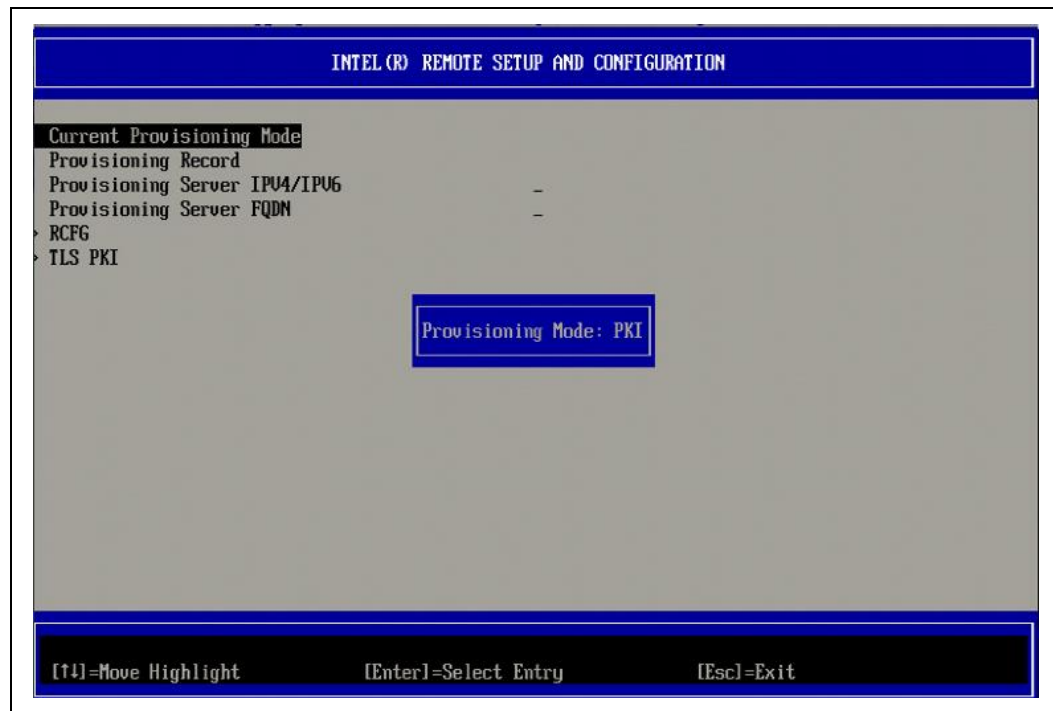


### 3.5.8.1 Current Provisioning Mode

Under Intel Remote Setup and Configuration menu:

1. Select 'Current Provisioning Mode'.
2. Press Enter to select.



**Figure 3-18. Current Provisioning Mode**

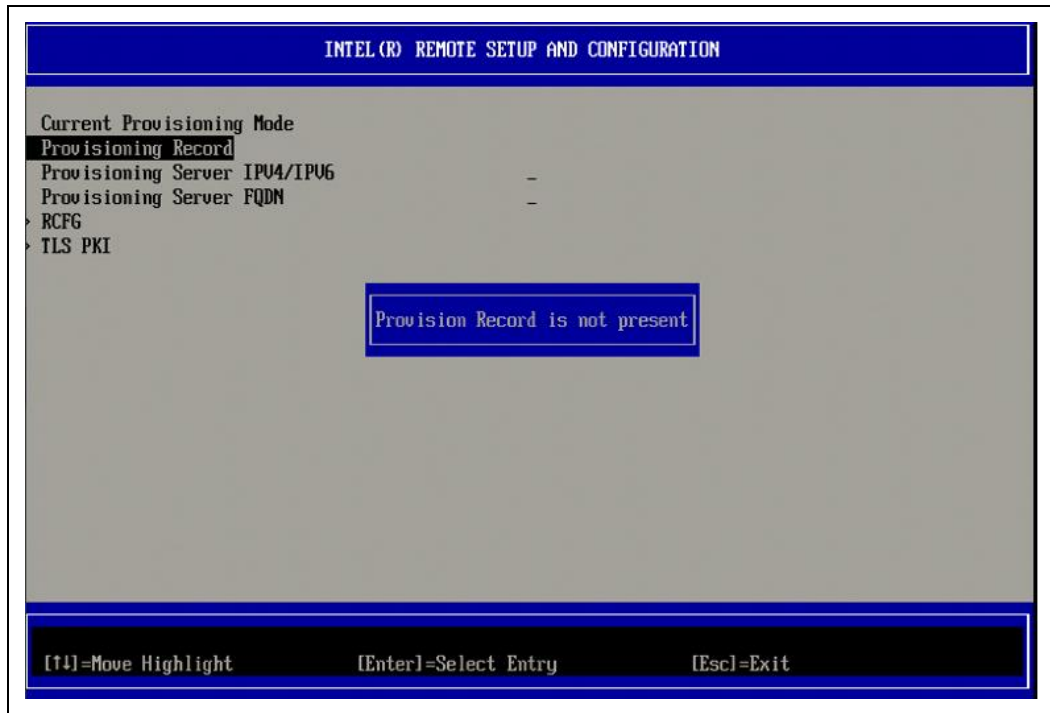
**Current Provisioning Mode** – Displays the current provisioning TLS Mode: None, PKI.

### 3.5.8.2 Provisioning Record

Under Intel Remote Setup and Configuration menu:

1. Select 'Provisioning Record'.
2. Press Enter to select.

Figure 3-19. Provisioning Record



**Provisioning Record** – Displays the system’s provision PKI record data. If the data has not been entered, the Intel® MEBX displays a message stating “Provision Record is 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 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 Remote Setup and Configuration menu:

1. Select 'Provisioning Server IPV4/IPV6'.
2. Press Enter to edit the IP address of the Intel® AMT provisioning server.
3. Edit 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 Remote Setup and Configuration menu:

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 Intel® AMT sends hello packets to PKI

### **3.5.8.5 RCFG**

Under Intel Remote Setup and Configuration menu:

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

The Intel Remote Setup and Configuration menu changes to the Intel Remote Configuration menu.



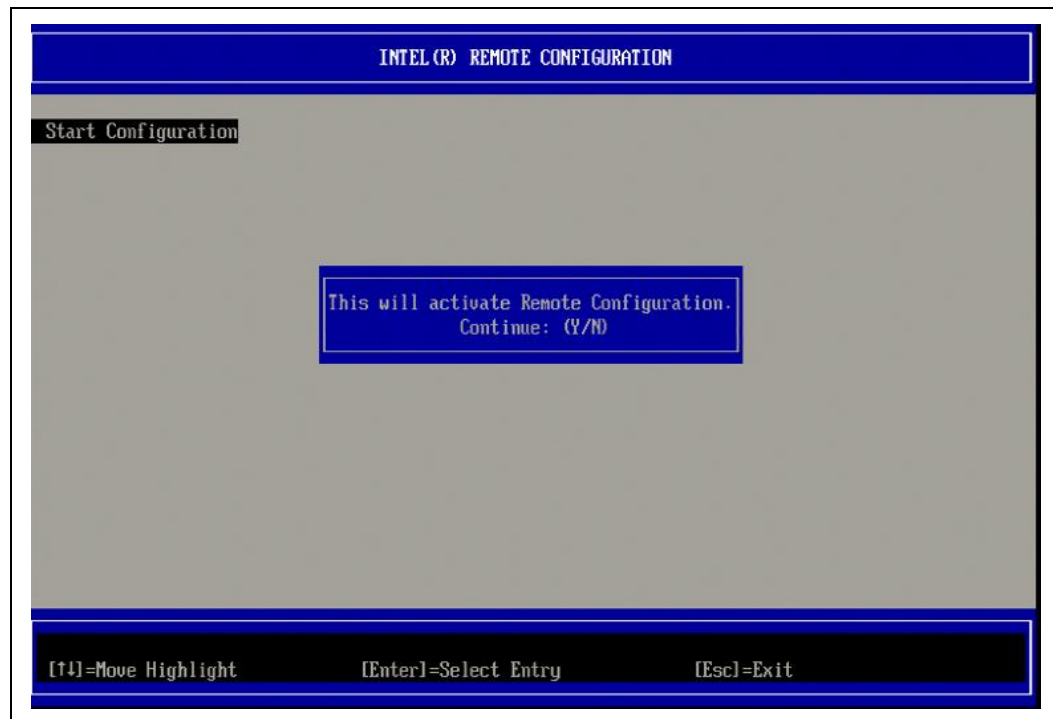
Figure 3-20. Intel® Remote Configuration



#### 3.5.8.5.1 Start Configuration

Under the Intel Remote Configuration menu:

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

**Figure 3-21. Activate RCFG**

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

### 3.5.8.6 TLS PKI

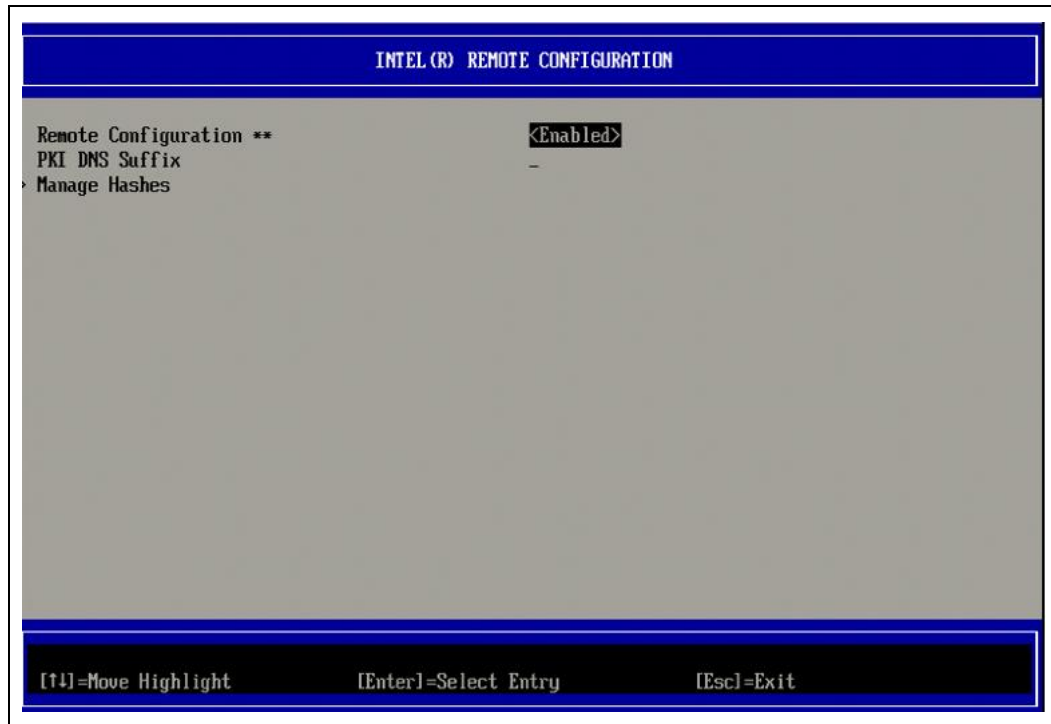
Under Intel Remote Setup and Configuration menu:

1. Select 'TLS PKI'.
2. Press Enter to select.

The Intel Remote Setup and Configuration menu changes to the Intel Remote Configuration menu.



Figure 3-22. Intel® Remote Configuration



#### 3.5.8.6.1 Remote Configuration

Under the Intel Remote Configuration menu:

1. Select 'Remote Configuration'.
2. Press Enter to select.

The following options can be selected:

- **Disabled-** remote configuration is disabled. Only 'Remote Configuration' item is 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".

#### 3.5.8.6.2 PKI DNS Suffix

Under the Intel Remote Configuration menu:

1. Select 'PKI DNS Suffix'.
2. Press Enter to edit.

#### 3.5.8.6.3 Manage Hashes

Under the Intel Remote Configuration menu:

1. Select 'Manage Hashes'.
2. Press Enter to select.



Figure 3-23. Manage Hashes

INTEL(R) REMOTE CONFIGURATION			
Hash Name	Active	Default	Algorithm
VeriSign Class 3	Active : [*]	Default : [*]	SHA256
VeriSign Class 3	Active : [*]	Default : [*]	SHA256
Go Daddy Class 2	Active : [*]	Default : [*]	SHA256
Comodo AAA CA	Active : [*]	Default : [*]	SHA256
Starfield Class 2	Active : [*]	Default : [*]	SHA256
VeriSign Class 3	Active : [*]	Default : [*]	SHA256
VeriSign Class 3	Active : [*]	Default : [*]	SHA256
VeriSign Class 3	Active : [*]	Default : [*]	SHA256
GTE CyberTrust G1	Active : [*]	Default : [*]	SHA256
Baltimore CyberTr	Active : [*]	Default : [*]	SHA256
Cybertrust Global	Active : [*]	Default : [*]	SHA256
Verizon Global Ro	Active : [*]	Default : [*]	SHA256
Entrust.net CA (2	Active : [*]	Default : [*]	SHA256
Entrust Root CA	Active : [*]	Default : [*]	SHA256
VeriSign Universa	Active : [*]	Default : [*]	SHA256
Go Daddy Root CA	Active : [*]	Default : [*]	SHA256
Entrust Root CA -	Active : [*]	Default : [*]	SHA256
Starfield Root CA	Active : [*]	Default : [*]	SHA256

[Ins]=Add New Hash	[Delete]=Delete Hash	[*]=Activate Hash
[↑↓]=Move Highlight	[Enter]=View Hash	[Esc]=Exit

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

- **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.

#### 3.5.8.6.4 Adding Customized Hash

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



Figure 3-24. Adding New Hash Name

The screenshot displays the 'INTEL(R) REMOTE CONFIGURATION' utility. It features a table with four columns: 'Hash Name', 'Active', 'Default', and 'Algorithm'. The table lists various certificates, including VeriSign Class 3, Go Daddy Class 2, Comodo AAA CA, Starfield Class 2, VeriSign Class 3, VeriSign Class 3, VeriSign Class 3, GTE CyberTrust G1, Baltimore CyberTr, Cybertrust Global, Verizon Global Ro, Entrust.net CA (2), Entrust Root CA, VeriSign Universa, Go Daddy Root CA, Entrust Root CA -, and Starfield Root CA. A dialog box is overlaid on the table, prompting the user to 'Enter Custom Hash Certificate Name' with a text input field. At the bottom of the screen, a legend defines the keyboard shortcuts: [Ins]=Add New Hash, [Delete]=Delete Hash, [\*]=Activate Hash, [↑↓]=Move Highlight, [Enter]=View Hash, and [Esc]=Exit.

Hash Name	Active	Default	Algorithm
VeriSign Class 3	Active : [*]	Default : [*]	SHA256
VeriSign Class 3	Active : [*]	Default : [*]	SHA256
Go Daddy Class 2	Active : [*]	Default : [*]	SHA256
Comodo AAA CA	Active : [*]	Default : [*]	SHA256
Starfield Class 2	Active :		
VeriSign Class 3	Active :		
VeriSign Class 3	Active :		
VeriSign Class 3	Active :		
GTE CyberTrust G1	Active :		
Baltimore CyberTr	Active :		
Cybertrust Global	Active : [*]	Default : [*]	SHA256
Verizon Global Ro	Active : [*]	Default : [*]	SHA256
Entrust.net CA (2	Active : [*]	Default : [*]	SHA256
Entrust Root CA	Active : [*]	Default : [*]	SHA256
VeriSign Universa	Active : [*]	Default : [*]	SHA256
Go Daddy Root CA	Active : [*]	Default : [*]	SHA256
Entrust Root CA -	Active : [*]	Default : [*]	SHA256
Starfield Root CA	Active : [*]	Default : [*]	SHA256

Enter Custom Hash Certificate Name

[Ins]=Add New Hash      [Delete]=Delete Hash      [\*]=Activate Hash  
[↑↓]=Move Highlight      [Enter]=View Hash      [Esc]=Exit

**To add 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.

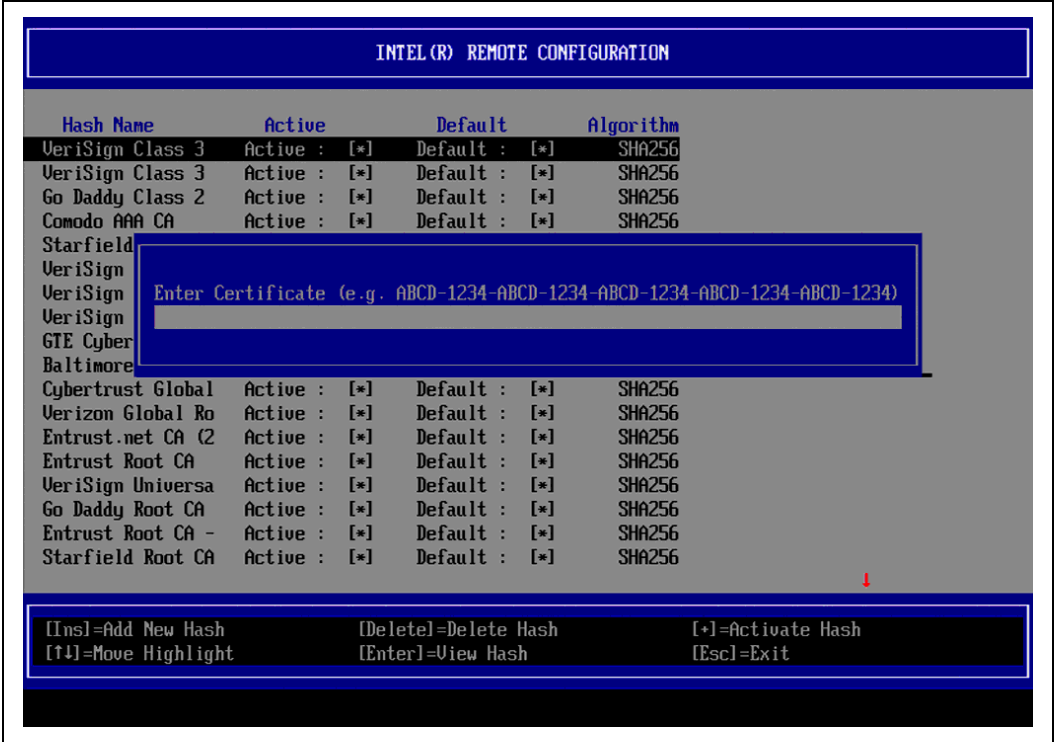
The supported hash algorithms are SHA1 **ONLY**.

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





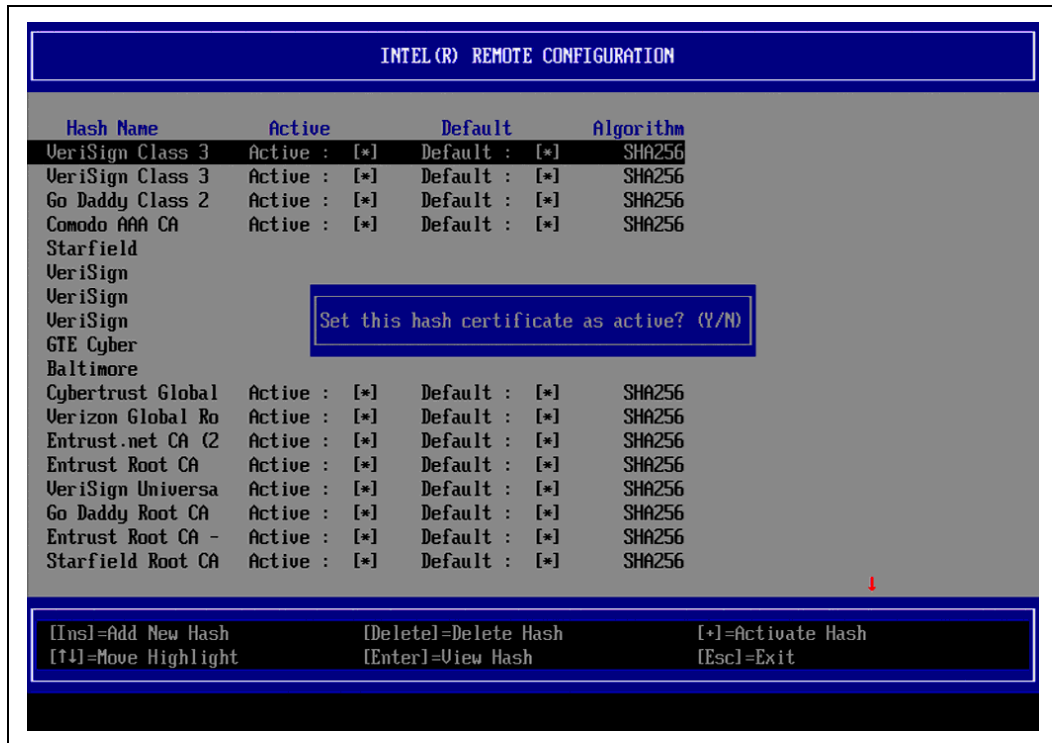
Figure 3-25. Add Hash - Certificate



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 3-26. 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 but will not be active

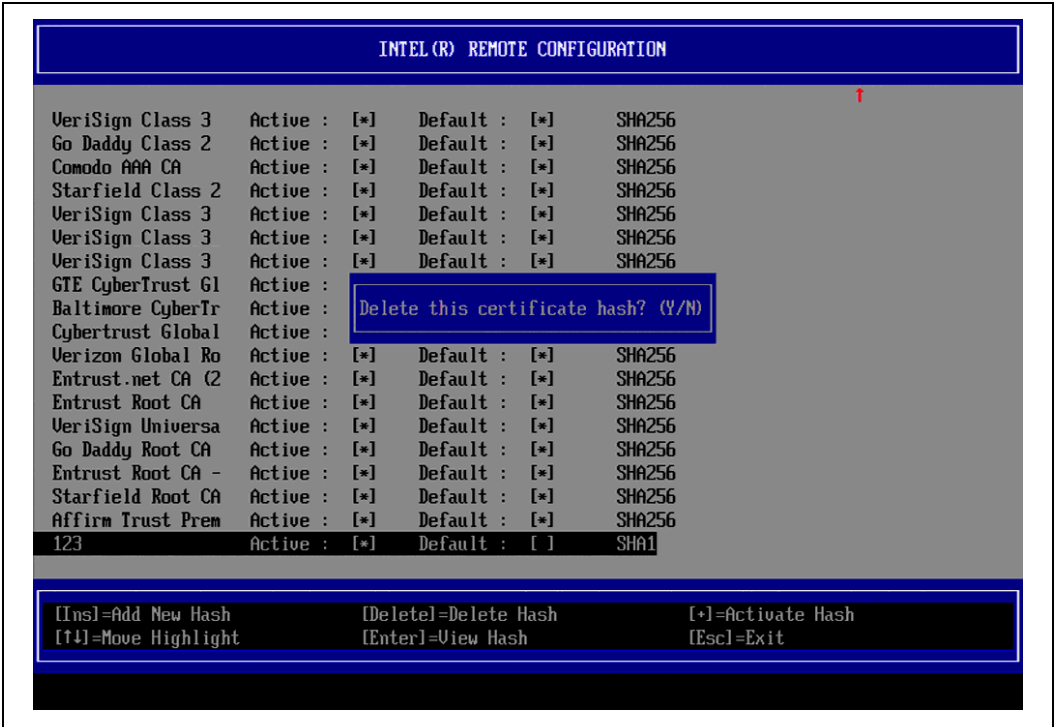
### 3.5.8.6.5 Deleting Hash

A certificate hash cannot be deleted if it is set to Default.

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



Figure 3-27. Deleting 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 Manage Certificate Hash list.

### 3.5.8.6.6 Changing Active State

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



Figure 3-28. Change Active State of Hash

INTEL(R) REMOTE CONFIGURATION			
Hash Name	Active	Default	Algorithm
VeriSign Class 3	Active : [*]	Default : [*]	SHA1
VeriSign Class 3	Active : [*]	Default : [*]	SHA1
Go Daddy Class 2	Active : [*]	Default : [*]	SHA1
Comodo AAA CA	Active : [*]	Default : [*]	SHA1
Starfield Class 2	Active : [*]	Default : [*]	SHA1
VeriSign Class 3	Active : [*]	Default : [*]	SHA1
VeriSign Class 3	Active		
VeriSign Class 3	Active		
GTE CyberTrust G1	Active		
Baltimore CyberTr	Active : [*]	Default : [*]	SHA1
Cybertrust Global	Active : [*]	Default : [*]	SHA1
Verizon Global Ro	Active : [*]	Default : [*]	SHA1
Entrust.net CA (2	Active : [*]	Default : [*]	SHA1
Entrust Root CA	Active : [*]	Default : [*]	SHA1
VeriSign Universa	Active : [*]	Default : [*]	SHA1
test	Active : [*]	Default : [ ]	SHA1

Set this hash certificate as deactive? (Y/N)

[Ins]=Add New Hash	[Delete]=Delete Hash	[*]=Activate Hash
[↑↓]=Move Highlight	[Enter]=View Hash	[Esc]=Exit

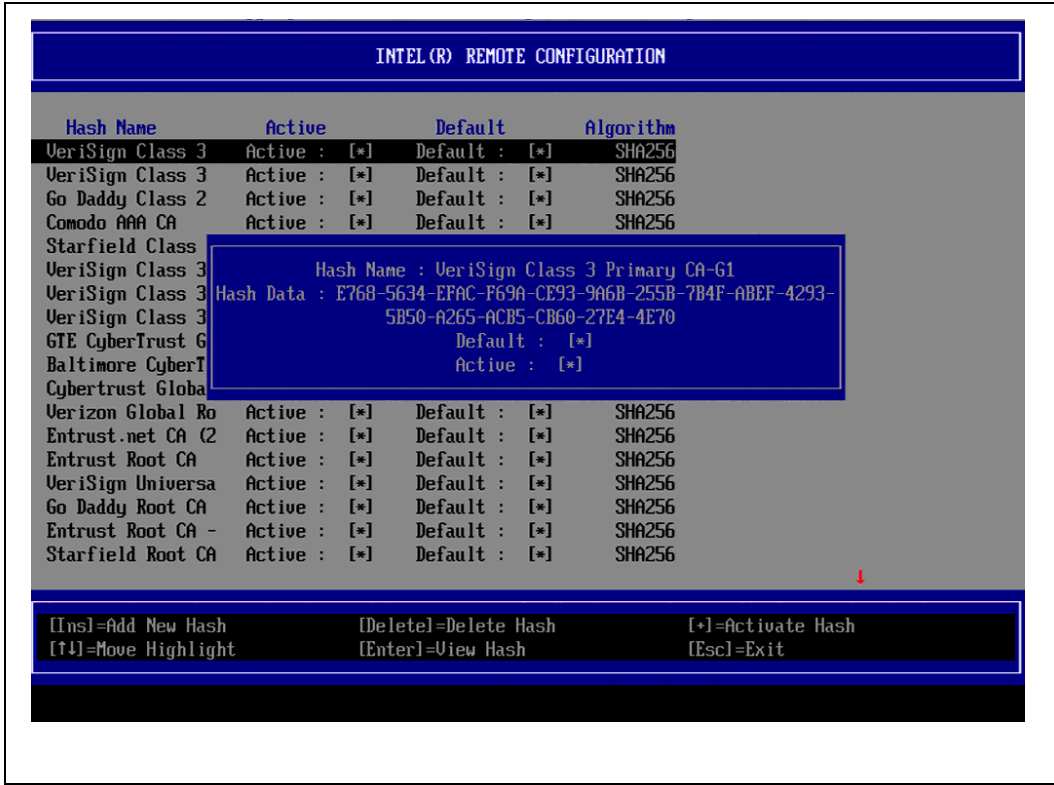
Answering **Y** toggles the active state of the currently selected certificate hash. Setting a hash as active indicates that the hash is available for use during PKI provisioning.

#### 3.5.8.6.7 View Certificate Hash

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



Figure 3-29. View Hash Details



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

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

### 3.5.9 Power Control

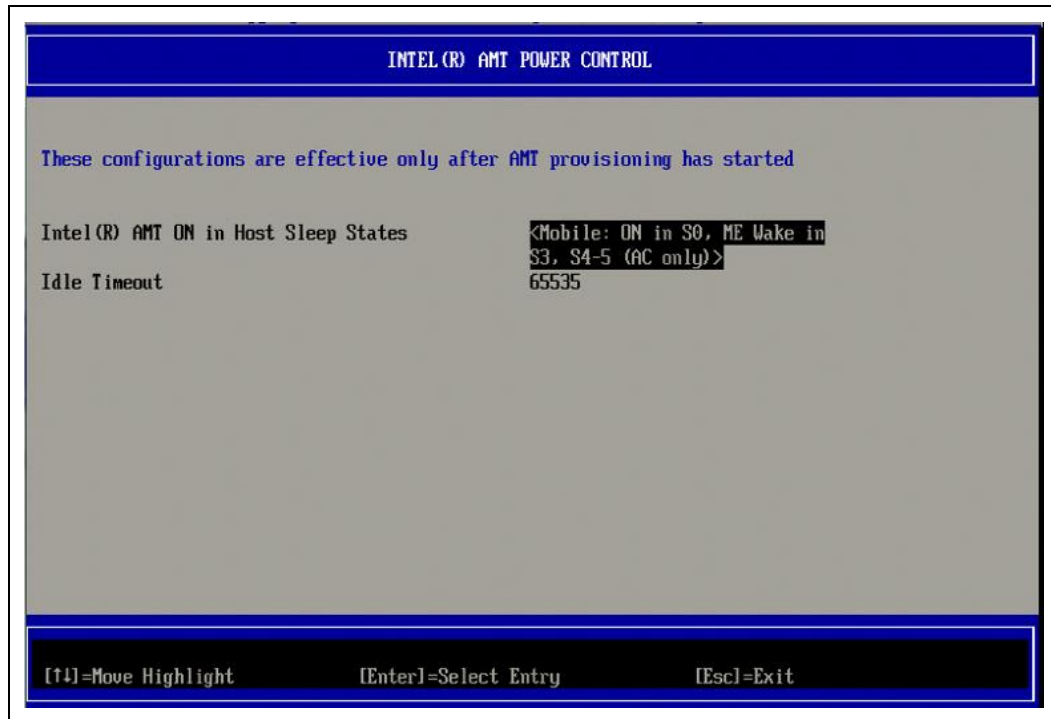
Under Intel® ME Platform Configuration menu:

1. Select 'Power Control'.
2. Press Enter to select.

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



Figure 3-30. Power Control



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

Since Intel® ME 9.0, Power Control has moved to Intel® AMT configuration, the way Intel® MEBX presenting value of Power Package and Idle timeout also changed. These settings are effective only after Intel® AMT provisioning. In other words, users don't need to care about these settings if Intel® AMT remains un-provisioned.

Under Intel® AMT Power Control menu:

1. Select 'Intel® AMT 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 3-2. Supported Power Packages**

Host ME \	PP1	PP2
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.

Note: Since Intel® ME 9.x, the default power package cannot be modified by using FIT or by FPT anymore.

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 idle timeout timer expires, the Intel® ME remains in the CM-off state until a command is sent to the ME. After this command has been sent, the Intel® ME will transit to CM3 state and will respond to the next command that is sent. A ping to the Intel® ME will cause the Intel® ME to go into CM3 state.

Since Intel® ME 9.0, a ping to the Intel® ME will transit from CM-off to CM3 state without resetting the idle timer. As a result, the Intel® ME will re-enter CM-off state in less than 20 seconds. The Intel® ME takes a short time to transit from the CM-off state to the CM0 or CM3 state. During this time, Intel® AMT will not respond to any Intel® ME commands. When the Intel® ME has reached the CM0 or CM3 state, the system will respond to Intel® ME commands.

### 3.5.9.1 Idle Time Out

Under Intel® ME Power Control menu:

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



Figure 3-31. Idle Timeout



This setting is used to enable the Intel® ME wake on and to define the Intel® ME idle timeout in CM3 state. The value should be entered in minutes. The value indicates the amount of time that the Intel® ME is allowed remain idle in CM3 state before transitioning to the CM-off state.

**Note:** If the platform is in DC only state, Intel® ME will not transit to CM3 state.

**Note:** If the platform is in S0 state, Intel® ME will not transit to CM-off state.

## 3.6 Exit

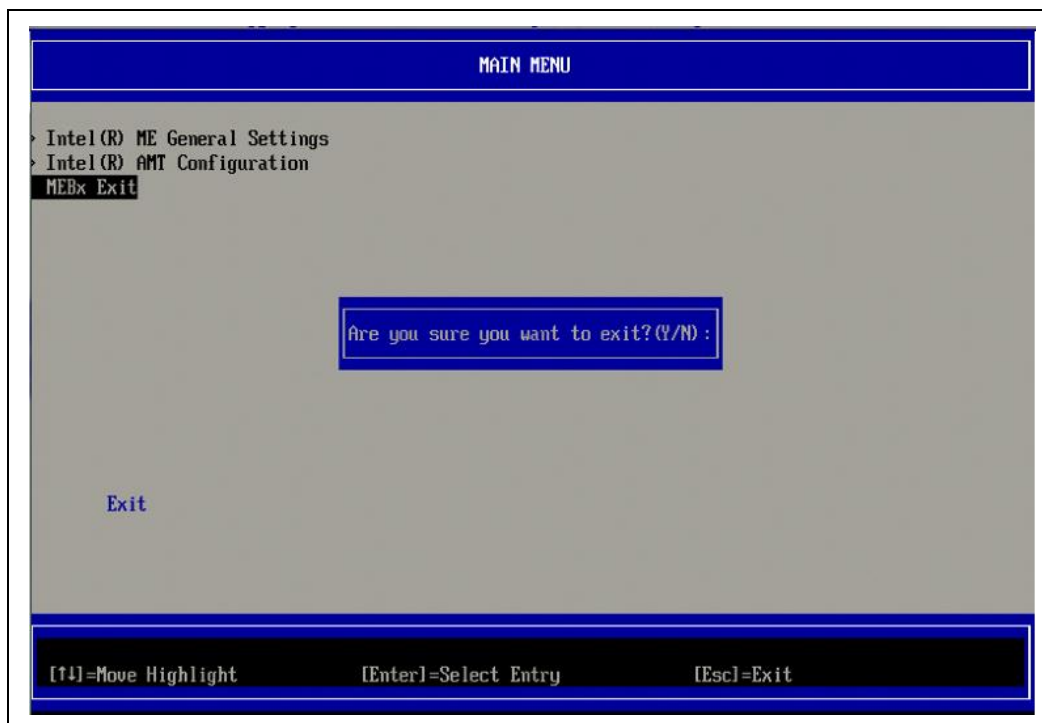
Under the Main Menu:

1. Select 'Exit'.
2. Press Enter to exit.





Figure 3-32. Exit Confirmation



To exit Intel® MEBX, select **Y**, else select **N**.

## 3.7 Intel® Standard Manageability Configuration

For platforms supporting Intel® Standard Manageability, instead of Intel® AMT Configuration, the option of Intel® Standard Manageability Configuration will be displayed in Intel® MEBX setup menu. The menu under Intel® Standard Manageability Configuration is the same as that displayed in Intel® AMT Configuration.

Intel® KVM feature is not supported by Intel® Standard Manageability. The Intel® KVM-related options are removed in the menus of SOL/Storage Redirection/KVM and "User Consent".

## 3.8 Intel® MEBX CPU Replacement Flow

The Intel® ME FW is responsible for identifying CPU replacement, whenever CPU Type changes between Intel® Core™ vPro™ processor (Intel® vPro™ technology eligible), Intel® Core™ processor (Not Intel® vPro™ technology eligible), Pentium® processor and Celeron® processor. Intel® MEBX is responsible for inquiring Intel® ME FW whether End User approval is required for given processor change. Only when indicated by Intel® ME FW that End User approval is needed, Intel® 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 Intel® Core™ vPro™ processor (Intel® vPro™ technology eligible) to Pentium® processor or from Intel® Core™ processor (Non-Intel® vPro™ technology eligible) to Celeron® processor.

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 losing 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.

When the following exceptions are captured, Intel® ME FW will not request CPU Replacement confirmation from End User (and the CPU Replacement message will not be shown):

- a. When system is in Manufacturing Mode, Intel® ME FW does not expect any messaging from user –in other words it's assumed to be informed CPU change.
  - b. First boot after flashing in ME Region – Intel® ME FW does not expect any CPU replacement related flows that require user assistance.
  - c. Clearing CMOS will cause Intel® 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 does not expect any CPU replacement related flows that require user assistance. The examples of such an upgrade are:
    - a. Celeron® processor changed to Pentium® processor
    - b. Celeron® processor changed to Intel® Core™ processor (Non-Intel® vPro™ technology eligible)
    - c. Celeron® processor changed to Intel® Core™ vPro™ processor (Intel® vPro™ technology eligible)
    - d. Pentium® processor changed to Intel® Core™ processor (Non-Intel® vPro™ technology eligible)
    - e. Pentium® processor changed to Intel® Core™ vPro™ processor (Intel® vPro™ technology eligible)
    - f. Intel® Core™ processor (Non-Intel® vPro™ technology eligible) changed to Intel® Core™ vPro™ processor (Intel® vPro™ technology eligible)

**Figure 3-33** represents the 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® processor to another Pentium® processor). **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. Intel® Core™ vPro™ processor (Intel® vPro™ technology eligible) changed to Intel® Core™ processor (Non-Intel® vPro™ technology eligible).



2. Intel® Core™ vPro™ processor (Intel® vPro™ technology eligible) changed to Pentium® processor.
3. Intel® Core™ vPro™ processor (Intel® vPro™ technology eligible) changed to Celeron® processor.
4. Intel® Core™ processor (Non-Intel® vPro™ technology eligible) changed to Pentium® processor.
5. Intel® Core™ processor (Non-Intel® vPro™ technology eligible) changed to Celeron® processor.
6. Pentium® processor changed to Celeron® processor.

The following actions are expected to be done by End User when the message from [Figure 3-33](#) 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 performed 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 Intel® ME infrastructure (kernel and all applications) based on modified CPU type.

\*\* Two resets may be observed. The 2nd reset will occur if some Intel® AMT features (SOL/ Storage Redirection/KVM) get disabled when a Intel® vPro™ technology eligible CPU is replaced with a non-Intel® vPro™ technology eligible CPU and this information has synced with BIOS. Refer Appendix B for different causes to global reset.



**Figure 3-33. 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”.

**Table A-1. Configuration Modes**

Setting	Intel® AMT 6.0 and above Default
TLS mode	Disabled, can be enabled at a later time
Web UI	Enabled
IDER*/SOL/KVM** Redirection network interface enabled	Enabled, can be disabled at a later time

\* IDER technology is replaced by Storage Redirection in Intel® AMT 11.

\*\* Intel® KVM technology was first introduced in Intel® AMT 6.

Manual configuration can be performed using the following six steps:

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.

**Note:** You must have a DHCP server in your environment.



## Appendix B : Global Reset from Intel® MEBX

Several Intel® MEBX configuration options require a global reset after they have been edited by the user. The reset is flagged while in the Intel® MEBX UI and passed back to BIOS to perform the reset request. The Intel® MEBX UI has to keep track of which configuration options require a global reset after exiting Intel® MEBX. Multiple techniques are used to ensure the global reset flow is entered correctly. The Intel® 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 Intel® MEBX. The 'Exit' flag is used to force the user out of the Intel® MEBX UI.

**Reboot** – Intel® 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** – Intel® MEBX must completely exit the UI immediately after editing the option.

**Table B-1. Intel® 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 Storage Redirection Username/Password	N	Y
KVM State	Y	N
SOL state	Y	N
Intel® AMT (EN->DIS)	Y	N
Intel® AMT (DIS->EN)	Y	N

Other Intel® MEBX global reset scenarios include:

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

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



## Appendix C : Intel® MEBX Options Being Reflected in Firmware

Below is the list of Intel® 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.

**Table C-1. Intel® MEBX Options**

Option	Reflected in Firmware
Intel® MEBX Login	Instantly
Change ME Password	Instantly
FW Update	Upon Exiting Intel® MEBX
Intel® ME ON in Host Sleep States	Upon Exiting Intel® MEBX
Idle Timeout	Upon Exiting Intel® MEBX
Manageability Feature Selection (EN->DIS)	Instantly
Password Policy	Upon Exiting Intel® MEBX
Activate Network Access	Instantly
Unconfigure Network Access	Instantly
Username and Password	Instantly
SOL	Instantly
Storage Redirection	Instantly
Intel® 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
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



<b>Option</b>	<b>Reflected in Firmware</b>
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
Remote Configuration	Instantly
Manage Hashes	Instantly
PKI DNS Suffix	Upon Exiting Intel® MEBX

§