INTEL VPRO PROCESSOR TECHNOLOGY SETUP AND CONFIGURATION FOR THE HP Z210 WORKSTATION

Table of Contents:

Introduction

The HP Z210 Workstation utilizes Intel vPro processor technology to simplify PC management and reduce IT related expenditures. Intel vPro processor technology utilizes Intel Active Management Technology (AMT), which allows for improved management of PC systems and better security.

AMT provides Out-of-Band (OOB) remote access to a system regardless of the system power state or operating system condition as long as the system is connected to a power source and a network. AMT is a hardware and firmware platform resident solution relying upon the Management Engine (ME) within the Intel C206 chipset.

Below is a brief history of AMT evolution on HP Workstations.

-
- AMT 6.0 Introduced with the Z200 Workstation..
- AMT 7.0 Introduced with the Z210 Workstation..

This whitepaper has been updated to include the new features of AMT 7.0. By default, the AMT shipping on the HP Z210 Workstation will be inactive. It must be setup and configured in the system before it can be used. The setup and configuration process is also known as provisioning.
There are two methods of AMT setup and configuration:

- Manual mode (similar to Small Medium Business (SMB) mode in AMT 5.0)
- Enterprise mode

This whitepaper details Manual mode and Enterprise mode setup and configuration for the client PC along with the usage of a Setup and Configuration Server (SCS) in Enterprise mode. Please consult with your Management Console ISV provider for details regarding installation procedures for a Setup and Configuration Server.

Basic knowledge of Intel AMT and networking are required.

Please refer to the Intel website: www.intel.com/technology/vpro/index.htm for other whitepapers and technical information regarding Intel vPro™ Technology.

AMT Setup and Configuration

AMT must be setup and configured in a system before it can be used. AMT Setup involves the necessary steps to enable AMT such as setting up the system for AMT mode and enabling network connectivity. It is generally performed only once for the lifetime of the system. When AMT is enabled, it can be discovered by management software over a network.

AMT Configuration is setting up all the other AMT options not covered in AMT Setup such as enabling the system for Serial-Over-LAN (SOL) or IDE-Redirect (IDE-R). Settings modified in the Configuration phase can be changed many times over the course of a system's lifespan. Changes can be made to the system locally or through a management console.

AMT System Phases

An AMT system can be in one of three phases in regards to its current stage of AMT Setup and Configuration.

Three Phases of AMT Setup and Configuration:

- Factory
- In-Setup
- Operational

The Factory phase is the initial stage. The system had been built from the factory. No AMT Setup and Configuration has been done. The only way to access AMT in Factory phase is through the MEBx. This phase will end for Manual mode systems once the default password has been changed. Enterprise mode systems also require the Provisioning ID (PID) and Provisioning Passphrase (PPS) to be set. More details on passwords, PIDs, and PPS in later sections.

The In-Setup phase is the next stage where most AMT options are set. This can be a manual procedure or an automated one with a Setup and Configuration Server.

The Operational phase is the final stage. AMT is fully Setup and Configured in the system and ready for normal use.

Manual Mode (SMB) AMT Setup and Configuration with MEBx

Manual mode is for customers who do not have Independent Software Vendors (ISV) management consoles, or the necessary network and security infrastructures to use encrypted Transport Layer Security (TLS). Manual mode AMT Setup and Configuration is a manual process done through the Intel ME BIOS Extension (MEBx).

Manual mode is the easiest to implement since it does not require much infrastructure, but it is the least secure since all network traffic is not encrypted. HP recommends that this be done in a closed network.

> **Note:**
>
> The MEBx is an option ROM module that is provided to HP by Intel to be included in the HP system BIOS. The MEBx is not HP-specific and contains options that are not used by HP. If an option is not used by HP, ignore it and do not modify it from the default state.

Password Guidelines

MEBx passwords must meet the minimum criteria to be accepted. These restrictions are enforced by the MEBx to reduce vulnerability of passwords to a dictionary attack.

Criteria:

- Password must be between 8 and 32 characters long.
- Password must contain both upper and lower case Latin characters (e.g. A, a, B, b).
- Password must have at least one digit character (e.g. 0, 1, 2, … 9).
- Password must have at least one 7-bit ASCII non-alphanumeric character with an ASCII value between 33d and 126d that is <u>not</u> one of the invalid characters list below:
    - Exclamation   !
    - At   @
    - Number   #
    - Dollar $
    - Percent   %
    - Caret   ^
    - Asterisk   *

The underscore (_) is considered alpha-numeric.

The following characters are not allowed:

- Quotation mark   "
- Apostrophe   '
- Comma   ,
- Greater than   >
- Less than   <
- Colon   :
- Ampersand   &
- Space

BIOS Prerequisite

This whitepaper is for the HP Z210 Workstation. The Z210 Workstation uses the J51 BIOS family.

For best performance and to take advantage of AMT 7.0 features, make sure the HP Z210 Workstations have a BIOS revision of at least version 1.00, a ME FW of at least version 7.1.10.1065, and a MEBx of at least version 7.0.0.0054.

The system BIOS and the ME FW must be updated individually. Refer to the BIOS Flash whitepaper at www.hp.com for more information on flashing the system BIOS and ME FW. AMT 7.0 allows ME FW to be downgraded to previous versions (only certain versions of ME FW can be downgraded).

Manual Mode (SMB Mode) – AMT Setup and Configuration Procedure

When going through the options in the MEBx for the first time (Factory phase), the default settings are in place. This whitepaper details HP recommended settings on options, some of which may be the same as the default selection. Even though the default setting is set and used for certain options, it is good practice to double check important options.

1. Press **Ctrl-P** during POST to enter Management Engine BIOS Extension (MEBx) Setup (Figure 1). This option is not shown during the HP splash screen but can be displayed during POST if set in F10-Setup.
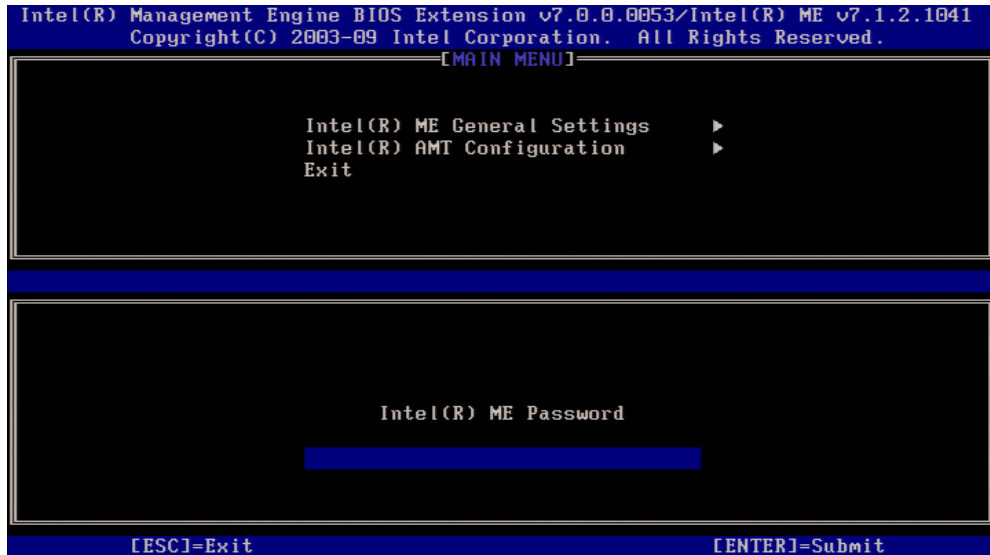

Figure 1. Intel MEBx Password Screen

2. Enter the default password of "admin" (passwords are case-sensitive). The user must change the default password before any changes can be made in the MEBx.

3. Change the password for the MEBx. The new password must meet the criteria defined in the Password Guideline Section, also known as a strong password. It must be entered twice for verification. Changing the password indicates that AMT ownership has been established. The system will go from Factory phase to In-Setup phase. The ME and AMT options within the MEBx are accessible and the system can be accessed via the AMT WebGUI.

4. Go to the Intel ME General Settings (Figure 2).

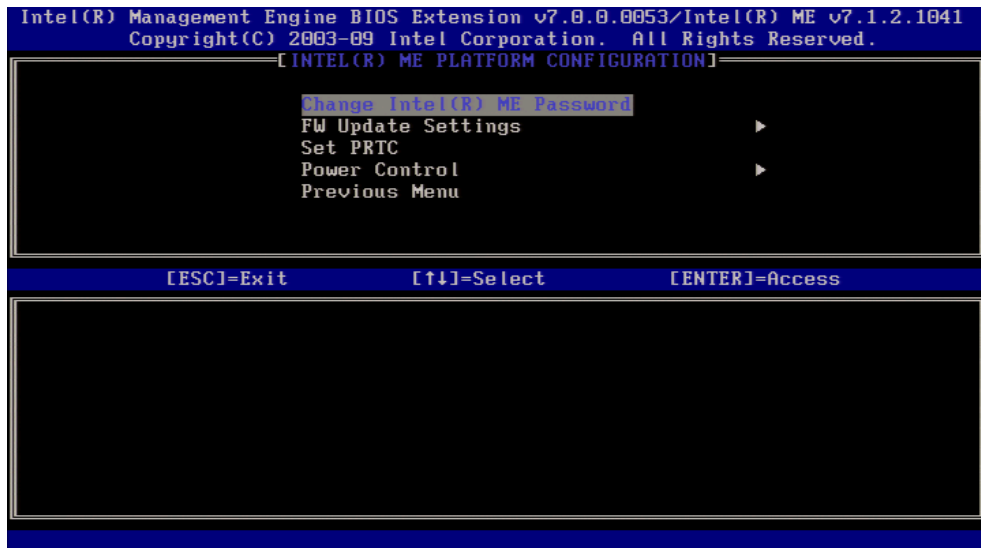**Figure 2. Intel ME General Settings Screen**

5. Select **FW Update Settings**.
   Local FW Update (Figure 3):
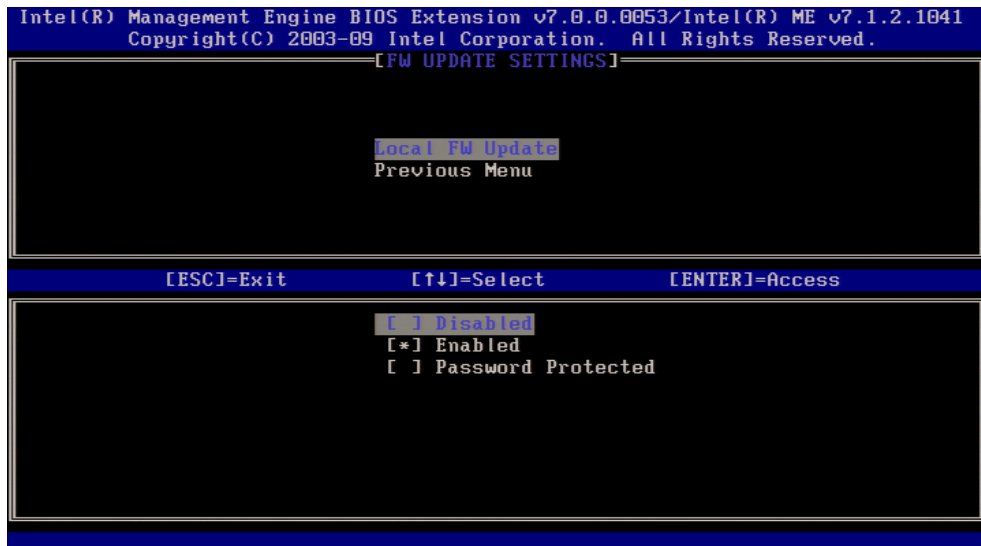   <u>Default (and recommended) setting</u>:   Enabled

Figure 3. Local FW Update Settings Screen

By default, the system BIOS allows for local ME FW updates without password protection. However, the administrator can modify the Local FW Update setting to be password protected.

6. Select **Set PRTC** (Figure 4). This option sets the Protected Real Time Clock (PRTC). Setting the PRTC value is used for virtually maintaining PRTC during the power-off (G3) state. PRTC has a valid date range of 1/1/2004 to 1/4/2021.
    <u>Default setting</u>:   (None)
    <u>Recommended setting</u>:   (Current Date and Time)
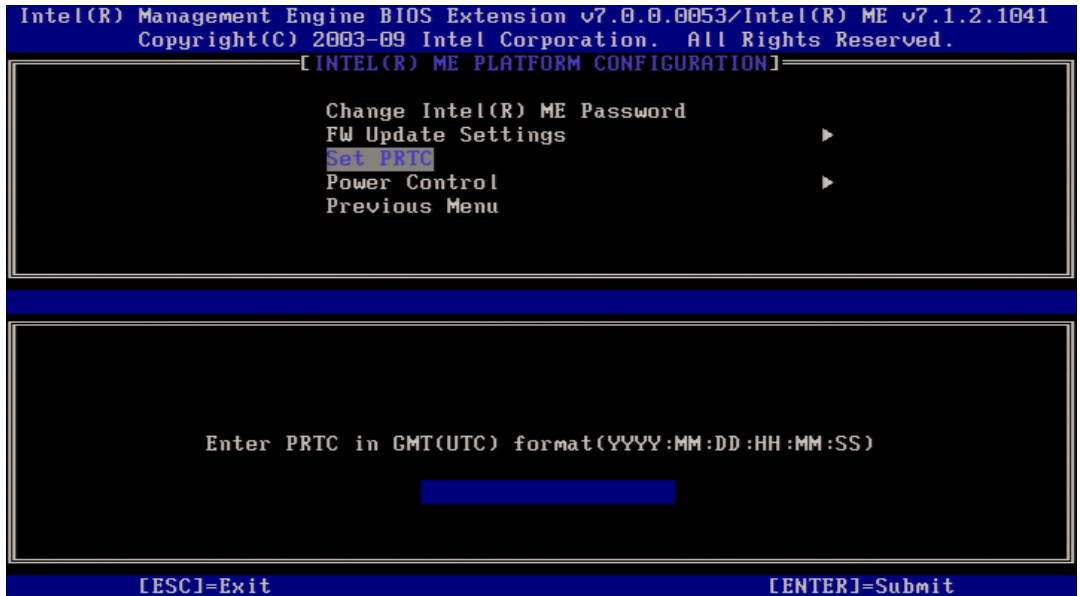
Figure 4. Intel ME FW Update Settings Screen

7. At the previous menu, select **Power Control** and then select **Intel ME ON in Host Sleep States** (Figure 5)
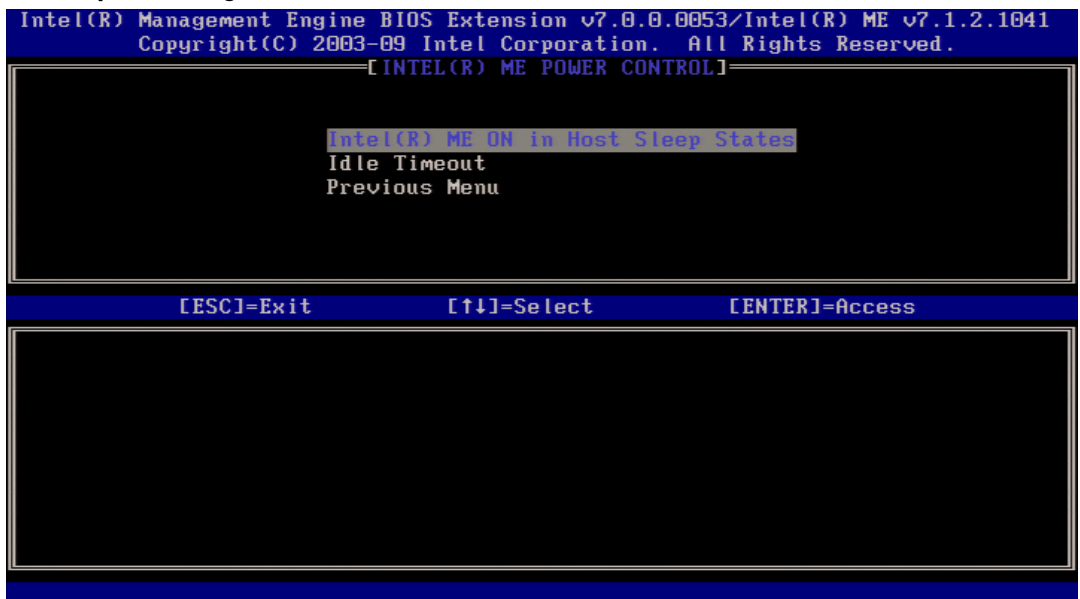
Figure 5. Intel ME Power Control Screen

a. Intel ME ON in Host Sleep States (Figure 6).
   Default setting: Desktop ON in S0
   Recommended setting: Desktop ON in S0, ME Wake in S3, S4-5.

> **Note:**
>
> The ME On in Host Sleep State mode will automatically set to Desktop: ON in S0, ME Wake in S3, S4-5 after Activating the Network Access (step 16).

Figure 6. Intel ME Host Sleep States Screen

b. Select **Idle Timeout** (Figure 7).
   Default (and recommended) setting: 65535

Figure 7. Intel ME Idle Timeout Screen

The Idle Timeout option sets the timeout value for Wake-On-ME. The default timeout value is 65535 from the factory and it is in units of a minute. HP recommends a setting of 65535 for most applications. Certain console vendor's product falsely detects an AMT system as disconnected if the software has to wait for the ME to wake and re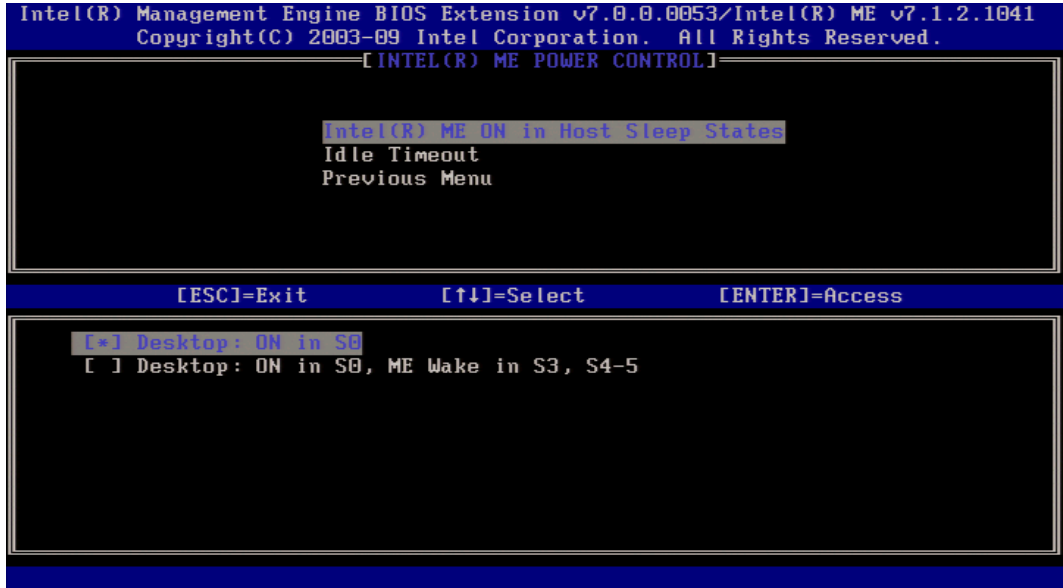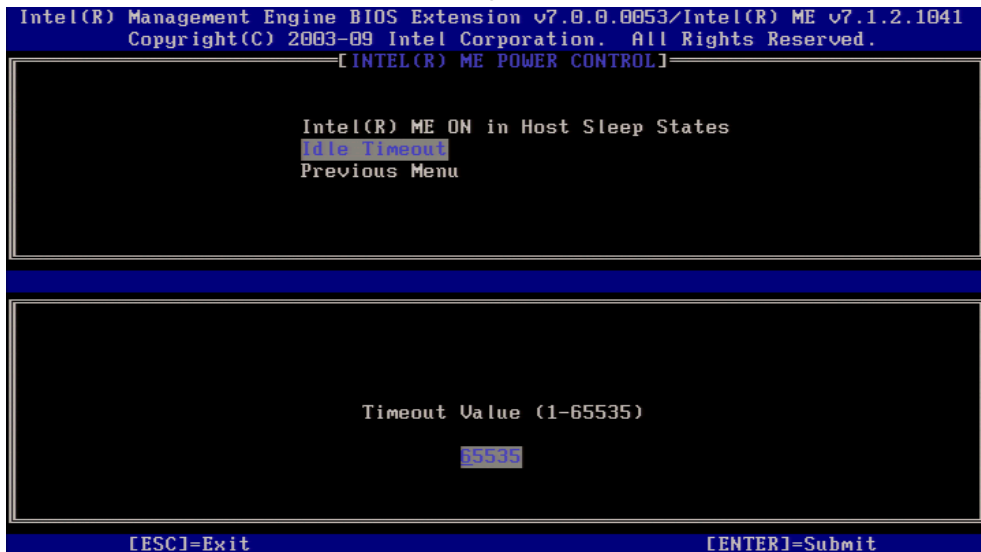spond. If the console software being used does not have this issue, HP recommends a setting of 1, which allows the ME to go to sleep after approximately 1 minute of inactivity. This allows for maximum power savings when the ME is enabled to be on in S3, S4, or S5.

The timeout value can be set in decimal and hexadecimal notation, and must be set to a non-zero value for the ME to take advantage of Wake-On-ME.
This value is not used when the system is in an active state – S0.
This value is used only if the ME ON in Host Sleep State setting is set to allow ME WoL.

See Appendix C for an explanation of Wake-On-ME / ME WoL.

8.   Select **Previous menu** and press enter to go back to the MEBx Main menu.
9.   Go into the Intel AMT Configuration menu (Figure 8).
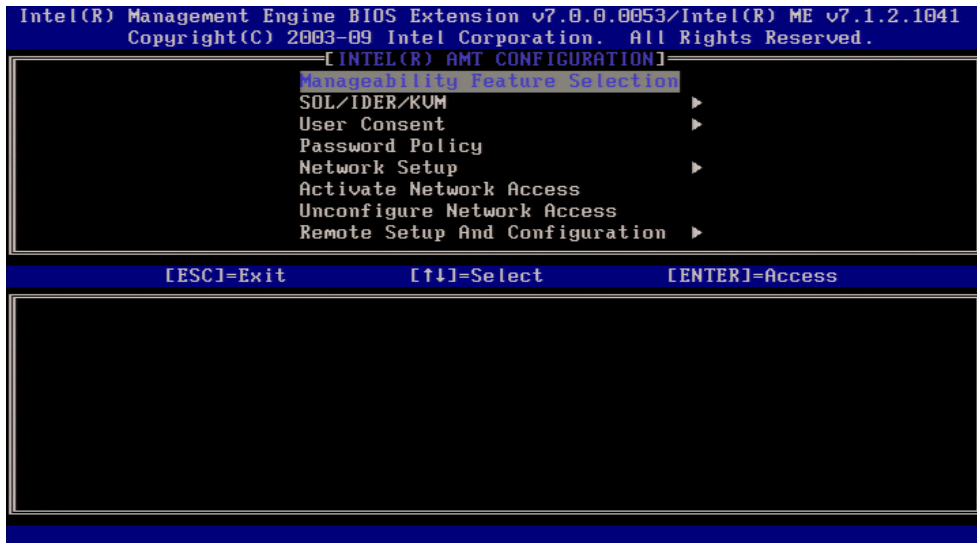
Figure 8. Intel AMT Configuration Screen

10. Select **Manageability Feature Selectio**n (Figure 9). This option allows Intel AMT to be enabled or disabled. By default, HP Z210 Workstations are set to enable Intel AMT. Note that selecting the **Disabled** option will disable all remote management capabilities and will also un-provision any AMT settings.
<u>Default (and recommended) setting:</u>   Enabled

Figure 9. Intel AMT Manageability Feature Selection Screen

11. At the previous menu select **SOL/IDER/KVM**. The SOL/IDER/KVM screen appears as shown in Figure 10'
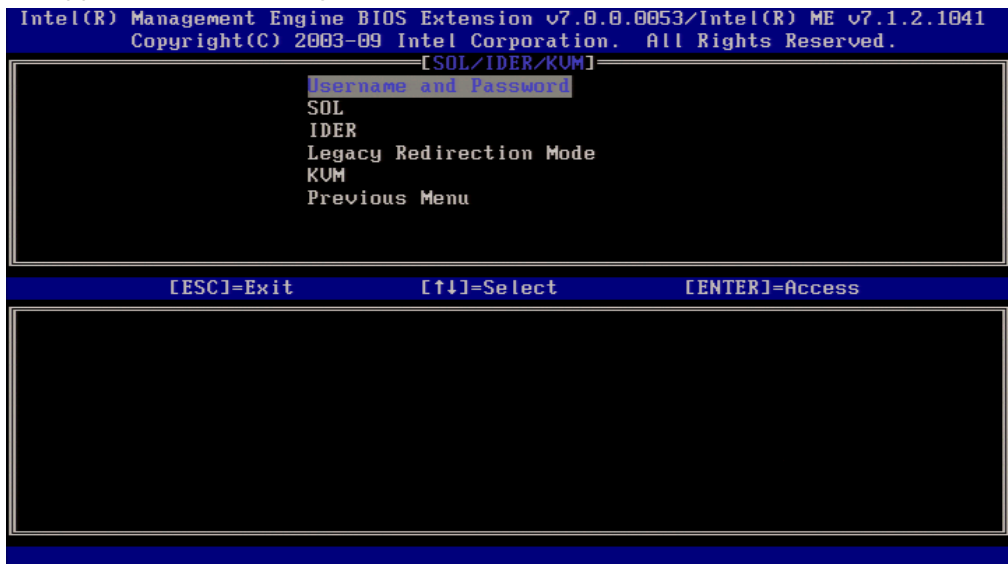
Figure 10. Intel AMT SOL/IDER/KVM Selection Screen

a. Username and password. This option allows users and passwords to be added from the WebGUI. If it is disabled, then only the administrator has MEBx remote access
   Default (and recommended) setting: Enabled.

b. SOL. This option enables/disables Serial Over LAN (SOL) functionality.
   Default (and recommended) setting: Enabled

c. IDE Redirection. This option enables / disables IDE Redirection (IDE-R) functionality.
   Default (and recommended) setting: Enabled

d. Legacy Redirection Mode. This option allows the Redirection feature to work with the pre-AMT 6.0 remote consoles.
   Default (and recommended) setting: Disabled

e. KVM Configuration.
   Default (and recommended setting: Enabled

12. User Consent menu (Figure 11).
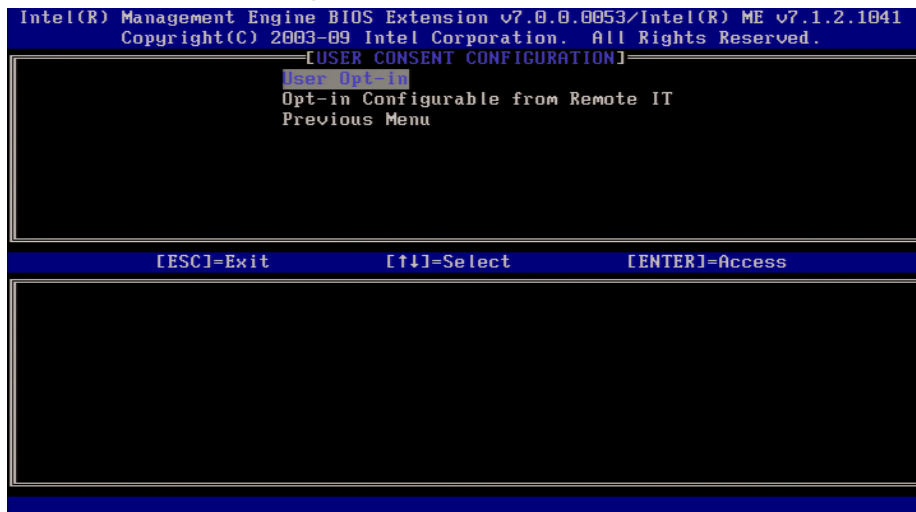
Figure 11. Intel AMT User Consent Configuration Screen

a. User Opt-in.
   Default setting: KVM
   Recommended setting: (User dependent)

b. Opt-in Configuration from Remote IT. This option disables/enables the Remote User's ability to select User OPT-IN Policy. If set to disabled, only the local user can control the opt-in policy.
   Default setting: Enabled Remote Control of KVM Opt-in Policy
   Recommended setting: (User dependent)

13. Password Policy. 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 through the Intel MEBX user interface. The options are:
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.
Default (and recommended) setting: Default Password Only
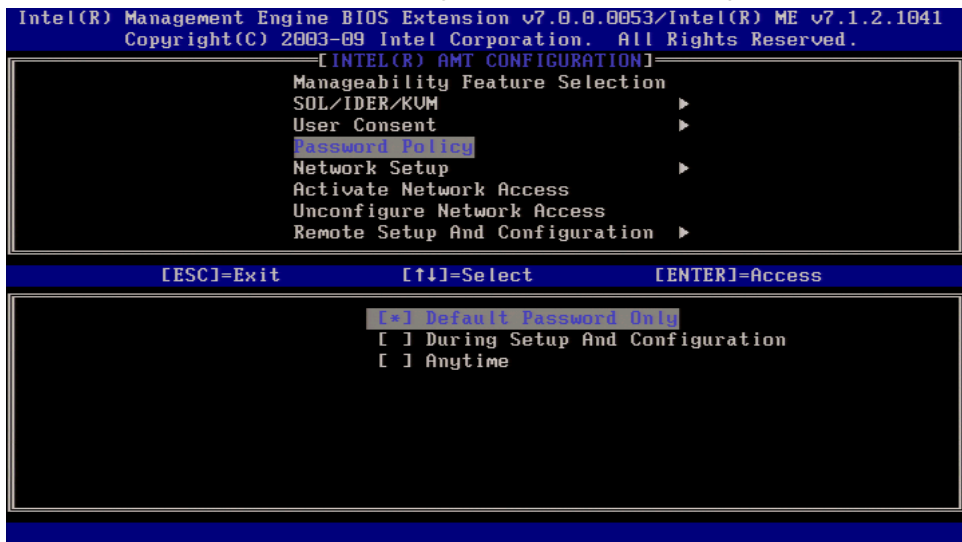

Figure 12. Intel AMT Password Policy Configuration Screen

14. At the previous menu (step 13) select Network Setup. The Network Setup menu appears as shown below in Figure 13.
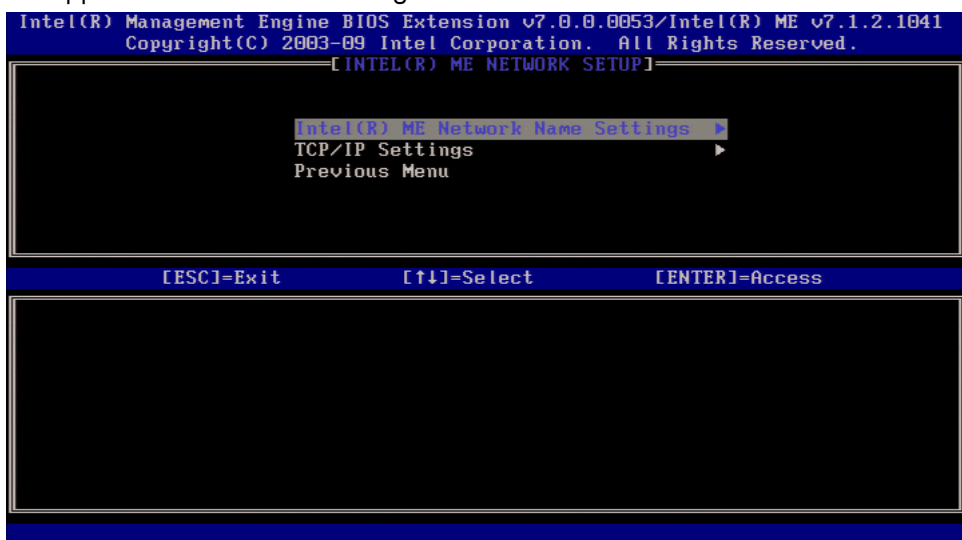

Figure 13. Intel AMT Network Setup Screen

a. Host Name. Hostnames can be used in place of the system's IP for any applications requiring the IP address.
    <u>Default setting</u>:   (None)
    <u>Recommended setting</u>:   (User dependent)

    Note that spaces are not accepted in the Host Name. Make sure there is not a duplicate host name on the network. Hostnames can be used in place of the system's IP for any applications requiring the IP address.

b. Domain Name. The domain name is blank by default. If it is not populated, then the default domain of "Provisionserver" will be used when connecting to a Setup and Configuration Server.

    If the name of the S&CS is not "Provisionserver" and the domain name is blank, then an alias must be set up in the DHCP server to redirect the connection for "Provisionserver" to the proper S&CS domain name.

    If the domain name field is populated, then that will be the domain used. However, if there is no response after four DNS queries to the named domain, then that domain name will no longer be used and the default "Provisionserver" will be used.
    <u>Default setting</u>:   (None)
    <u>Recommended setting</u>:   (Network dependent)

c. Share/Dedicated FQDN. 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.
    <u>Default (and recommended) setting</u>:   Shared

d. Dynamic DNS Update.
    <u>Default (and recommended) setting</u>:   Disabled

    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 will make no attempt to update DNS using DHCP option 81 or Dynamic DNS update. If the DDNS Update state (Enabled or Disabled) is not configured by the user at all then the firmware will assume its old implementation where the firmware used DHCP option 81 for DNS registration but did 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 must be set.
    When DDNS Update option is enabled, the MEBx menu will display "Periodic Update Interval" and "TTL" options.
    — Periodic Update Interval: Enter a desired interval from
       20 to 1440 minutes
    — TTL: Enter desired time in seconds

15. At the previous menu (Figure 13), select **TCP/IP Settings** and view the AMT TCP/IP Settings screen (Figure 14). AMT 7.1 supports IPV4 and IPV6 interface. Follow steps 15a-15f to configure for IPV4 and 15g-15h for IPV6.
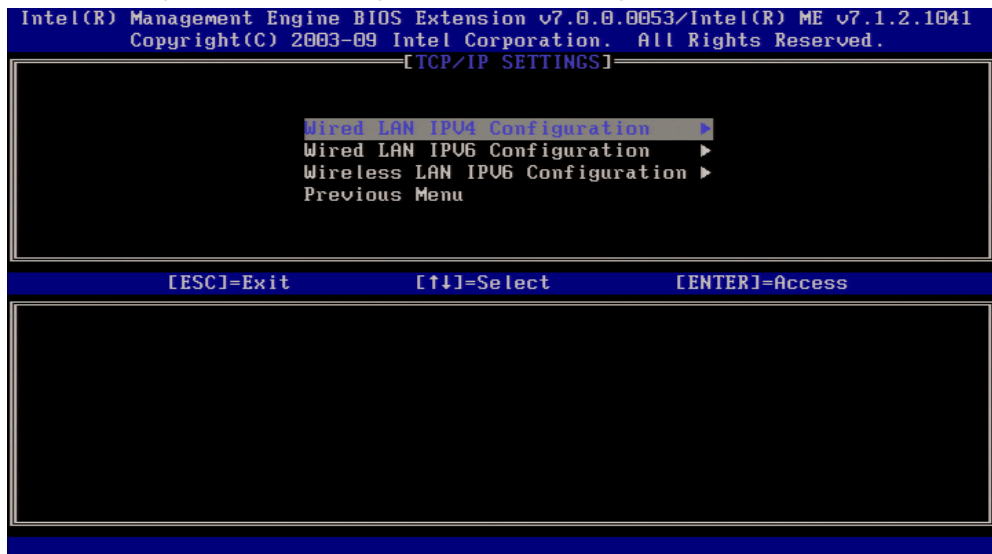

Figure 14. Intel AMT TCP/IP Settings Screen

 a. Wired LAN IPV4 Configuration:
   DHCP Mode
   <u>Default (and recommended) setting</u>: Enabled

   If DHCP is disabled, then steps 15b through 15f are required to configure the IPv4 static IP address for Intel AMT.
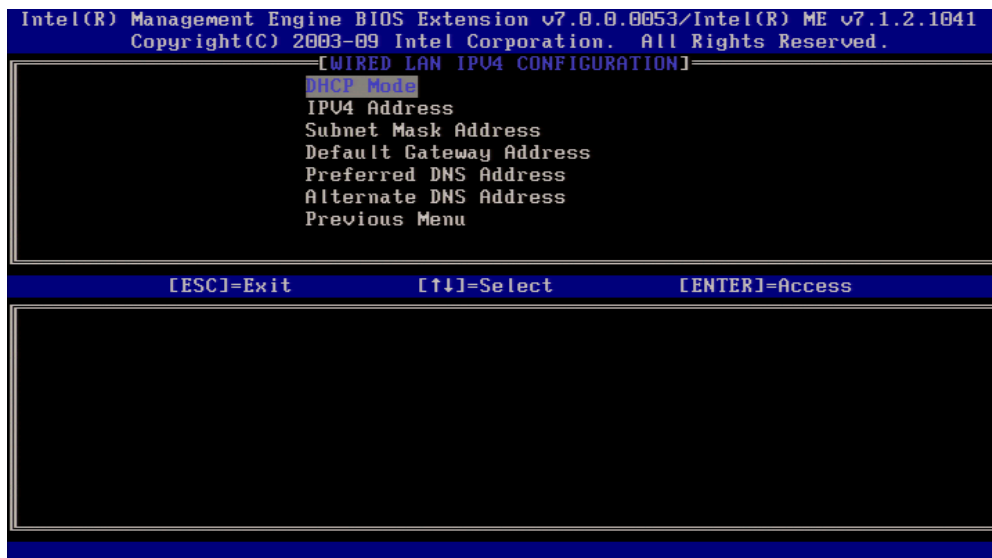
Figure 15. Intel AMT Wired LAN IPV4 DHCP Disabled Configuration Screen

b. IPV4 Address. Enter a specific address, making sure all AMT systems have a unique static IP address. Multiple systems sharing the same IP address can lead to network collisions, which will cause the systems to not respond correctly
Default setting: 0.0.0.0
Recommended setting: (Network dependent)
Example: 192.168.0.1

c. Subnet Mask. Enter the subnet mask.
Default setting: 255.255.255.0
Recommended setting: (Network dependent)

d. Default Gateway Address. If this option is not needed then press **Enter** to use the default value.
Default setting: 0.0.0.0
Recommended setting: (Network dependent)

e. Preferred DNS Address. If this option is not needed then press **Enter** to use the default value.
Default setting: 0.0.0.0
Recommended setting: (Network dependent)

f. Alternate DNS value. If this option is not needed then press **Enter** to use the default value.
Default setting: 0.0.0.0
Recommended setting: (Network dependent)

g. Wired IPV6 Configuration (Figure 16) .
Select Enabled option for IPv6 Feature Selection.
Default value: Disabled
Recommended setting: (Network dependent)
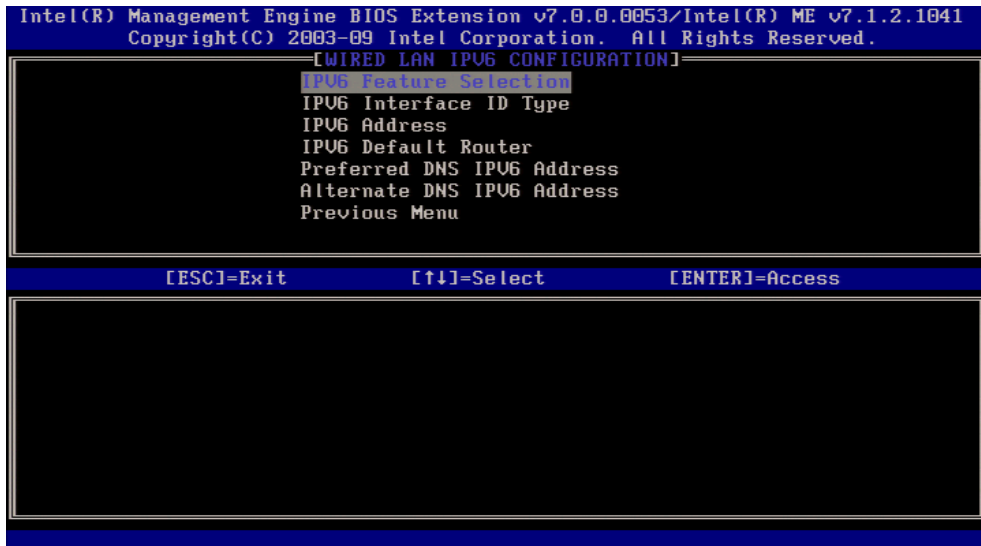
Figure 16. Intel AMT Wired LAN IPV6 Configuration Settings Screen

i. IPv6 Interface ID Type:
RANDOM ID (default) - The IPv6 Interface ID is automatically generated using a random number as described in RFC 3041.
Intel ID - The IPv6 Interface ID is automatically generated using the MAC address.
Manual ID - The IPv6 Interface ID is configured manually. Selecting this type requires that the Manual Interface ID is set with a valid value.

ii. IPv6 Address. Enter a static IP address.
Default setting: (None)
Recommended setting: (Network depended)
Example: 2001:db8::1428:57ab

iii. IPv6 default Router. Enter the preferred DNS IPv6 address
Default setting: (None)
Recommended setting: (Network dependent)
Example: 2001:db8::1428:57ab

iv. Preferred DNS IPv6 Address. Enter the preferred DNS IPv6 address.
Default setting: (None)
Recommended setting: (Network dependent)

v. Alternate DNS IPv6 Address. Enter the alternate DNS IPv6 address.
Default setting: (None)
Recommended setting: (Network dependent)
Example: 2001:db8::1428:57ab

16. Activate Network Access. From the Intel ME Platform Configuration menu Figure 22), select **Activate Network Access**. This function causes the Intel ME to transition to the POST provisioning state if all required settings are configured. The Un-configure Network Access option will cause the Intel ME to transition to PRE provisioning state.

Figure 22. Intel AMT Activate Network Access Screen

When MEBx displays "Update Network settings" in the General Settings menu press **Enter**.

At the MEBx CAUTION prompt (Figure 23), press **Y**.

```
        [ESC]=Exit              [↑↓]=Select              [ENTER]=Access



                            ═[CAUTION]═
                   Activates the current network settings
                  and opens the Intel(R) ME network interface
                              Continue:(Y/N)

```
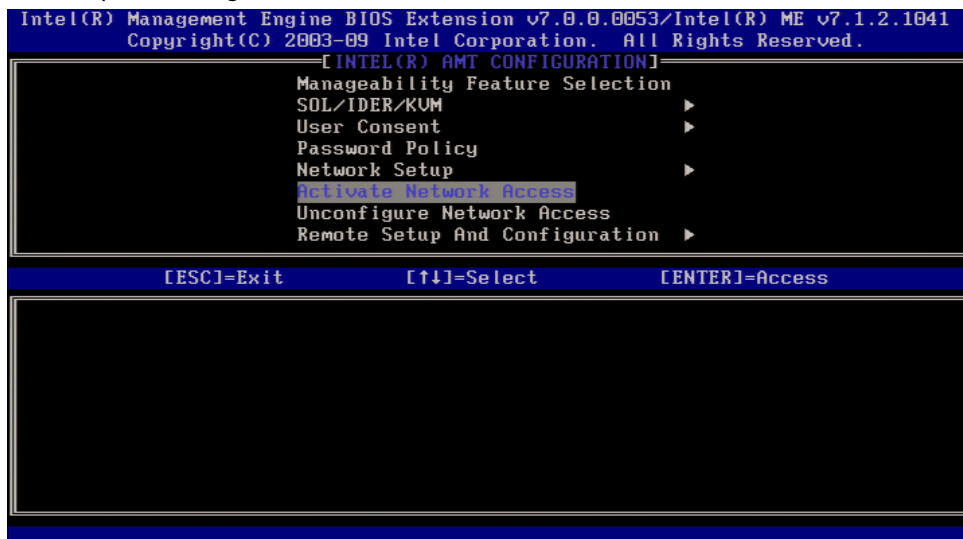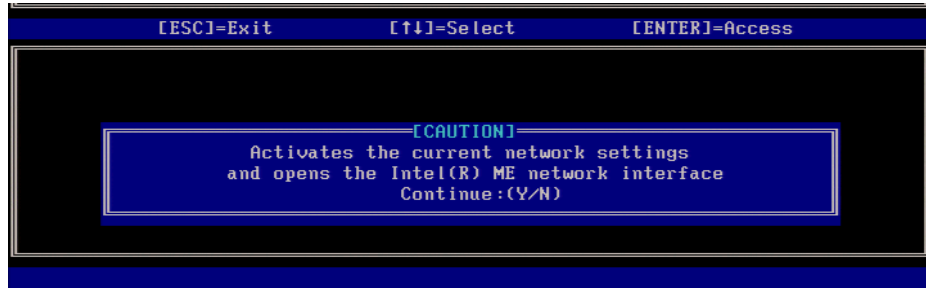
Figure 23. Intel AMT MEBx Cauton prompt screen.

17. Select **Previous Menu** to get back MEBx Main Menu and select **Exit** to exit MEBx Setup and save settings. The system will reboot.

Once the system reboots, it will go from In-Setup phase to Operational phase. AMT is fully operational. Once in the Operational phase, the system can be remotely managed through the Intel AMT WebGUI or ISV remote console and can be provided to the end-user for regular use.

Intel AMT WebGUI

The Intel AMT WebGUI is a web browser based interface for limited remote system management.

The WebGUI is often used as a test to determine if AMT Setup and Configuration was performed properly on a system. A successful remote connection between a remote system and the host system running the WebGUI indicates proper AMT Setup and Configuration on the remote system.

The AMT WebGUI is accessible from the following web browsers:

- Microsoft Internet Explorer 6 SP1 or newer
- Netscape Navigator 7.1 or newer
- Mozilla Firefox 1.0 or newer
- Mozilla 1.7 or newer

Limited remote system management includes:

- Hardware inventory
- Event logging
- Remote system reset
- Changing of network settings
- Addition of new users and passwords
- Updating ME firmware

WebGUI support is enabled by default for SMB Setup and Configured systems. WebGUI support for Enterprise Setup and Configured systems is determined by the Setup and Configuration Server.

Connecting with the Intel AMT WebGUI - SMB Example

1. Power on an AMT system that has completed AMT Setup and Configuration.

2. Execute a web browser from a separate system, such as a Management PC that is also on the same subnet as the AMT PC.

3. Connect to the IP address specified in the MEBx and port of the AMT system.
   -- By default the port is 16992
   -- If DHCP was used, then use the Fully Qualified Domain Name (FQDN) for the ME. The FQDN is the combination of the hostname and domain.
   Example A: http://192.168.0.1:16992 (IPv4 address)
   Example B: http://hpsystem.hp.com:16992 (from Step 14)
   Example C: http://[2001:ABC::ABC]:16992 (IPv6 address)

4. The Management PC makes a TCP connection to the AMT system and accesses the top level AMT embedded webpage within the Management Engine of the AMT system.

5. Enter username and password. The default username is "admin" and the password is the one set during AMT Setup in the MEBx. After login, the System Status screen appears (Figure 24).
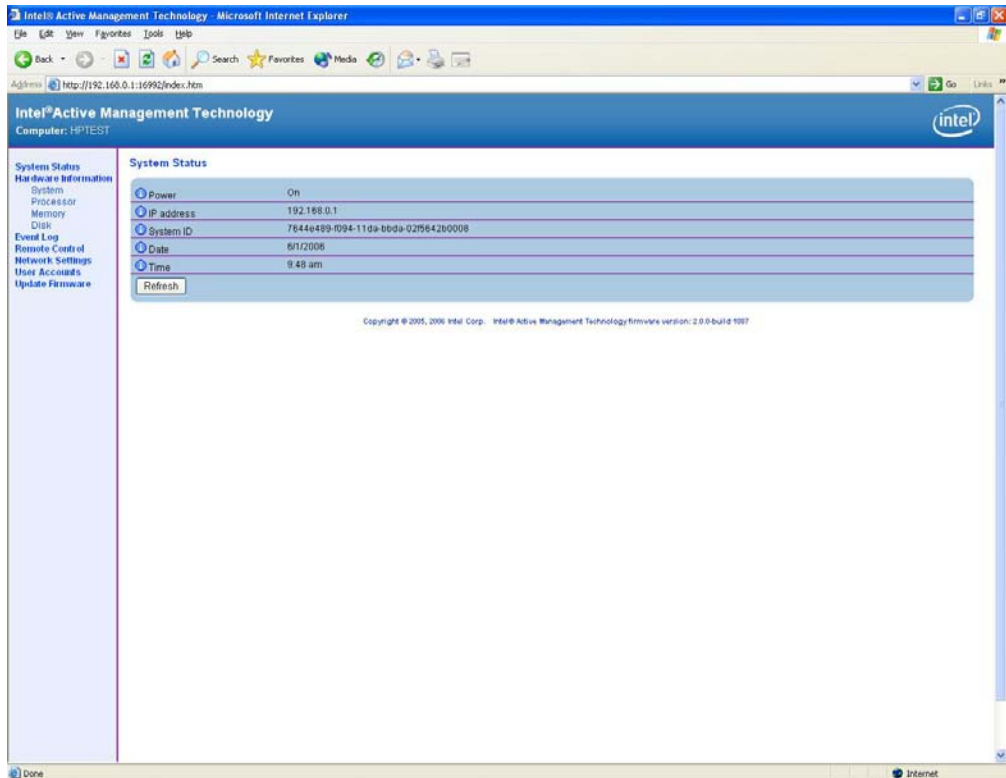
Figure 24. Intel AMT WEB GUI Screen

6. Review system information and make any necessary changes.

> **Note:**
> The MEBx password can be changed for the remote system in the WebGUI.
> Changing the password in the WebGUI or a remote console will result in two passwords. The new password, known as the "remote" MEBx password, will **only** work remotely with the WebGUI or remote console. *The local MEBx password used to access the MEBx locally will not be changed!* The user will have to keep track of both local and remote MEBx passwords to be able to access the system MEBx locally and remotely. When the MEBx password is initially set in AMT Setup, it serves as both the local and remote password. They are in sync. If the remote password is changed, then the passwords are out of sync. The remote MEBx password must also follow the criteria defined in the Password Guideline section for a strong password.

7. Exit.

Enterprise Mode AMT Setup and Configuration

Enterprise mode is for large corporate customers. A Setup and Configuration Server (SCS) is required for Enterprise Mode Setup and Configuration. The SCS is also known as a Provisioning Server as seen in the MEBx.

Setup and Configuration Server

A Setup and Configuration Server (SCS) is simply an application that executes over a network performing AMT Setup and Configuration. It is required for Enterprise mode setup and configuration.

In a PSK Setup and Configuration, both the AMT client system and the SCS must share a set of Provisioning ID (PID) and Provisioning Passphrase (PPS). This pair forms a Pre-Shared Key (PSK).

PIDs are 8 characters long and PPS are 32 characters. There are dashes between every set of four characters so counting dashes PIDs are 9 characters and PPS are 40 characters. Once these PIDs and PPS are generated, they are added to the Setup and Configuration server's secure PSK database. This database can be transferred to another Setup and Configuration server's database.

The initial communication between an AMT client system and an SCS consists of the following basic steps:

1. The AMT system sends out a "hello" message which includes the PSK over the network.
2. The SCS receives the "hello" message and verifies the PSK.
3. If the verification passes, then the SCS begins setup and configuration.
4. Once setup and configuration completes, the original PSK is deleted from the AMT client system and a new PSK is given.

The initial "hello" message is unencrypted. However, afterwards all communication between the AMT client and the SCS can be encrypted with Transport Layer Security (TLS).

There are several independent software vendors (ISV) offering Setup and Configuration Servers on the market. SCSs currently available include:

- HP Client Configuration Manager
- Altiris
- LANDesk
- Microsoft SMS

Enterprise Mode AMT Setup and Configuration

The AMT Setup portion for Enterprise mode is the same as SMB mode. Repeat Steps 1 through 15 to perform AMT Setup. This will take the system from Factory mode to In Setup Mode.

Refer to Manual Mode AMT Setup and Configuration for screen shots of MEBx menus and full text.

The following are quick steps for AMT Setup.

1. Get into the MEBx by pressing **Ctrl-P** during POST.
2. Enter the default password "admin."
3. Change the MEBx password using strong password guidelines.
4. In the Intel ME General Settings menu enter the default password "admin."
5. FW Update Settings. By default BIOS allows to update the ME firmware without password protected, the administrator can select the Password Protected (the user must provide the password in order to upgrade the ME firmware.
   Default (and recommended) setting: Enabled
6. Skip Set PRTC.
7. Power Control.
   a. Intel ME ON in Host Sleep States
      Default (and recommended) setting: 65535
   b. Idle Timeout. This option sets the timeout value for Wake-On-Me.
      Default (and recommended) setting: 65535

   The default timeout value of 65535 is in units of a minute. HP recommends a setting of 65535 for most applications. Certain console vendor's product falsely detects an AMT system as disconnected if the software has to wait for the ME to wake and respond. If the console software being used does not have this issue, HP recommends a setting of 1 which allows the ME to go to sleep after approximately 1 minute of inactivity. This allows for maximum power savings when the ME is enabled to be on in S3, S4, or S5.

   The timeout value can be set in decimal and hexadecimal notation. It must be set to a non-zero value for the ME to take advantage of Wake-On-ME.

   This value is not used when the system is in an active state – S0.

   This value is used only if the ME ON in Host Sleep State setting is set to allow ME WoL.

   See Appendix C for an explanation of Wake-On-ME / ME WoL.

8. Go into Intel AMT Configuration (Figure 25).
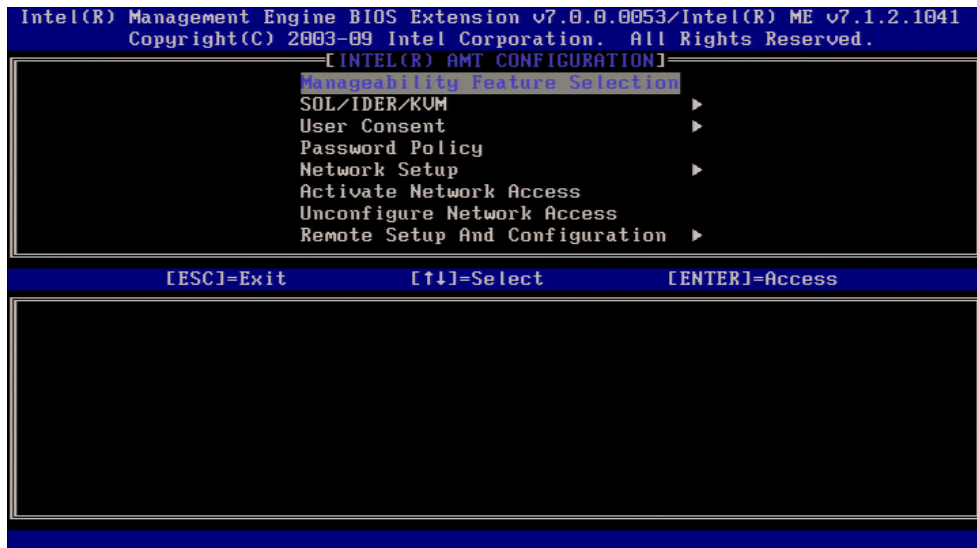
Figure 25. Intel AMT Configuration screen.

9. Select **Manageability Feature Selection**.
   Default (and recommended) setting: Enabled

10. Select SOL/IDE-R/KVM.

   a. Username and password. This option allows users and passwords to be added from the WebGUI. If it is disabled, then only the administrator has MEBx remote access.
      Default (and recommended) setting: Enabled

   b. Serial Over LAN (SOL).
      Default (and recommended) setting: Enabled

   c. IDE Redirection.
      Default (and recommended) setting: Enabled

   d. Legacy Redirection Mode. This option allows the Redirection feature to work with the pre-AMT 7.0 remote consoles (need to set to Enabled).
      Default (and recommended) setting: Disabled

   e. KVM.
      Default (and recommended) setting: Enabled

11. Select **User Consent**

   a. User opt-in.
      Default setting: User Consent is required for KVM session
      Recommended setting: User dependent

   b. Opt-in Configuration from remote IT.
      Disable Remote Control of KVM Opt-in Policy – This option disables the Remote User's ability to select User OPT-IN Policy. In this case only the local user can control the opt-in policy. Enable Remote Control of KVM Opt-in Policy - Enables Remote User's ability to select User OPT-IN Policy.
      Default setting: Enabled Remote Control of KVM Opt-in Policy
      Recommended setting: (User dependent)

12. Select **Password policy**. This option will determine if the local MEBx password can be modified from a remote console.
<u>Default (and recommended) setting</u>:   Default Password Only

<u>Option</u>	<u>Effect</u>
Default Password Only	This option will allow the MEBx password to be remotely modified only if it is the default "admin" password.
During Setup and Configuration	This option will allow the MEBx password to be remotely modified only during Setup and Configuration of the AMT platform.
Anytime	This option will allow the MEBx password to be remotely modified at any time.

13. Select **Network Setup**. Enter a Host Name (spaces are not accepted).
<u>Default setting</u>:   (None)
<u>Recommended setting</u>:   (User dependent)

14. In the Network Setup menu, select **TCP/IP**.

   a. Wired LAN IPv4 Configuration.
       DHCP Mode
       <u>Default setting</u>:   DHCP Enabled
       <u>Recommended setting</u>:   (User dependent. For the purposes of this paper, DHCP is enabled.)

   b. Wired LAN IPv6 Configuration.
       <u>Default setting</u>:   Disabled
       <u>Recommended setting</u>:   (User dependent. For the purposes of this paper, DHCP is enabled.)

       i. IPv6 interface ID Type.
           RANDOM ID (default) - The IPv6 Interface ID is automatically generated using a random number as described in RFC 3041.

           Intel ID - The IPv6 Interface ID is automatically generated using the MAC address.

           Manual ID - The IPv6 Interface ID is configured manually. Selecting this type requires that the Manual Interface ID is set with a valid value.

       ii. IPv6 Address. Enter a static IPv6 address.
           <u>Default setting</u>:   (None)
           <u>Recommended setting</u>:   (Network dependent)
           <u>Example</u>:   2001:db8::1428:57ab

       iii. IPv6 Default Router. Enter the IPv6 default router address.
           <u>Default setting</u>:   (None)
           <u>Recommended setting</u>:   (Network dependent)
           <u>Example</u>:   2001:db8::1428:57ab

iv. Preferred DNS IPv6 Address. Enter the preferred DNS IPv6 address.
Default setting: (None)
Recommended setting: (Network dependent)
Example: (2001:db8::1428:57ab)

v. Alternate DNS IPv6 Address. Enter the alternate DNS IPv6 address.
Default setting: (None)
Recommended setting: (Network dependent)
Example: 2001:db8::1428:57ab

15. Skip Activate Network Access.

16. Skip Un-Configure Network Access

17. Select **Remote Setup and Configuration**. The Intel Automated Setup and Configuration Screen (Figure 26) is where the Enterprise mode provisioning data is entered. The submenu selections are described in the following steps.
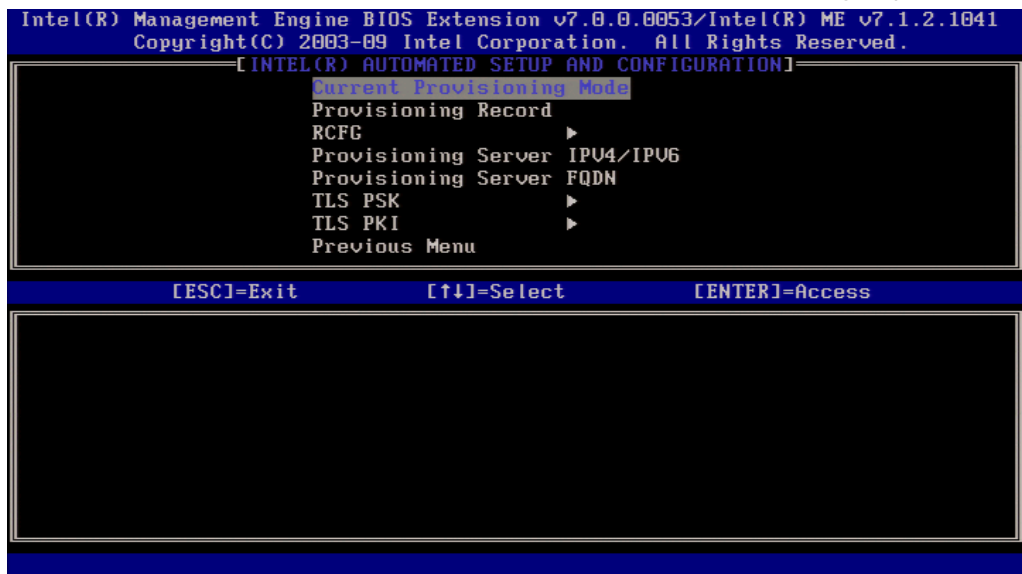

Figure 26. Intel Automated Setup and Configuration Screen

a. Current Provisioning Mode. This menu displays the current provisioning TLS mode. The three mode types are: None, PKI (default), and PSK. No changes can be made at this menu.

b. Provisioning Record. This menu displays provision record data of the system. No changes can be made at this menu.
Default setting: Not present

The record for a system with PSK provisioning will include the following information:
-- TLS Provisioning Mode
-- Provisioning IP
-- Date of Provisioning

The provisioning record for a system with PKI provisioning will include the following information:
-- TLS Provisioning Mode
-- DNS
-- Host Initiated
-- Hash Data
-- Serial Algorithm
-- ISDefault Bit
-- Time Validity Pass
-- FQDN
-- Provisioning IP
-- Date of Provisioning

c. RCFG. This option is for Remote Configuration (RCFG) also known as Zero Touch Configuration (ZTC) or Host Based provisioning. Refer to the RCFG section for more information.

d. Provisioning Server IPV4/IPV6. Enter the address for the Provisioning server.
Default setting: 0.0.0.0
Recommended setting: (Network dependent)

This option is used in Enterprise mode when an Intel AMT Setup and Configuration (Provisioning) Server is available. It points to the IP address of the SCS. If the IP is left as the default, the ME will look for "ProvisionServer" on DNS. The default port for many SCSs is at 9971. Some ISV's may require additional settings, such as the SCS port number and SCS IP address. Contact your Management Console ISV for more details.

e. Provisioning Server FQDN. Enter the address for the FQDN server.
Default setting: (None)
Recommended setting: (Network dependent)

This option is used in Enterprise mode when an Intel AMT Setup and Configuration (Provisioning) Server is available. It points to the Fully Qualified Domain Name (FQDN) of the SCS.

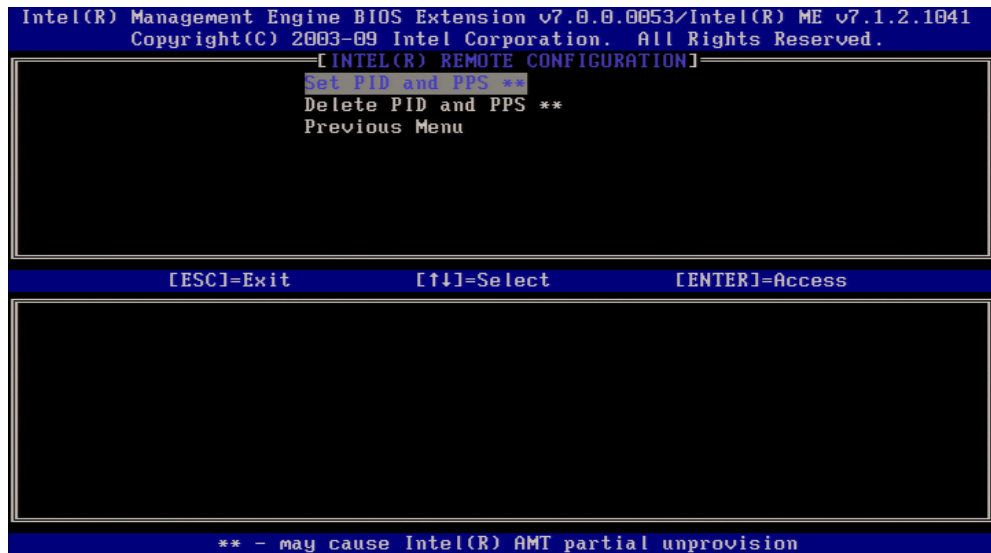f. Select **TLS PSK**. The Intel TLS PSK Configuration Screen appears (Figure 27).

Figure 27. Intel TLS PSK Configuration Screen

    i. Select **Set PID and PPS**.

        Default setting: (None)
        Recommended setting: (System dependent)

        This option is for Provisioning ID (PID) and Provisioning Passphrase (PPS) entry. PIDs are 8 characters and PPS are 32 characters. There are dashes between every set of four characters so counting dashes PIDs are 9 characters and PPS are 40 characters. They must be generated by an SCS.

        The Admin Password, PID, and PPS can be pre-populated by HP during manufacturing. Refer to the OEM TLS-PSK section for more information.

    ii. Skip Delete PID and PPS. This function deletes the current PID and PPS entries in the system.

    iii. Select **Previous Menu**.

g. Skip TLS PKI.

h. Select **Previous Menu**.

18. Select **Previous Menu** to return to the MEBx Main Menu.

19. Select **Exit** to exit the MEBx Setup and save settings).

20. The system will display an Intel ME Configuration Complete message (only once).

21. System will reboot.

22. Turn off system and remove power. At this point the system is out of Factory Mode and is in In-Setup mode. It is ready to be deployed in a corporation.

23. User plugs system into a power source and connects to the network. Only the integrated Intel NIC should be used. Intel AMT does not work with any other NIC solution.

24. When power is reapplied to the system, it will immediately look for a Setup and Configuration Server. If one is found, the AMT system will send a "Hello" message to the server.

    DHCP and DNS must be available for the Setup and Configuration Server search to automatically succeed. If DHCP and DNS are not available, then the Setup and Configuration Server's IP address must be manually entered into the AMT system's MEBx.

    The "Hello" message will contain the following information;
    -- PID
    -- UUID (Universally Unique Identifier)
    -- IP address
    -- ROM and FW version numbers

    The "Hello" message is transparent to the end-user. There is no feedback mechanism to tell the user the "Hello" message is being broadcast.

25. The Setup and Configuration Server will use the information in the "Hello" message to initiates a Transport Layer Security (TLS) connection to the AMT system using TLS Pre-Shared-Key (PSK) cipher suite if TLS is supported.

26. The Setup and Configuration server uses the PID to lookup PPS in provisioning server database and uses the PPS and PID to generate TLS Pre-Master Secret.

    TLS is optional. For secure and encrypted transactions, TLS should be used if the infrastructure is available.

    If TLS is not used, then HTTP Digest will be used for mutual authentication. It is not as secure as TLS.

27. Setup and Configuration Server logs into AMT system with the username and password, and provisions all required data items, including:
    -- New PPS and PID (for future Setup and Configuration)
    -- TLS certificates
    -- Private keys
    -- Current date and time
    -- HTTP Digest credentials
    -- HTTP Negotiate credentials

    Other options can be set depending on S&CS implementation.

28. The system goes from In-Setup phase to Operational phase. AMT is fully operational. Once in the Operational phase, the system can be remotely managed and can be provided to the end-user for regular use.

There are three methods of provisioning a system with Enterprise mode:

- Legacy
- IT TLS-PSK
- OEM TLS-PSK

Legacy

Legacy method of AMT Setup and Configuration should be executed on an isolated network separate from the corporate network if TLS is desired. An S&CS server would have to have a secondary network connection to Certification Authority for TLS configuration.

Legacy AMT Setup and Configuration is done by the customer. The customer initially receives systems in the Factory phase with AMT disabled. These systems will need to go through AMT Setup to go from Factory to In-Setup phase.

Once the system is in In-Setup phase, the system can continue to be configured manually or be connected to a network where it will connect with an S&CS and begin Enterprise Mode – AMT Configuration.

The Legacy method places all of the work of AMT Setup and Configuration on the customer. It is no touch for the OEM.

IT TLS-PSK

IT TLS-PSK AMT Setup and Configuration is usually done in the IT department of a corporation.

The following is needed:

- Setup and Configuration Server
- Network and security infrastructure

AMT systems in the Factory phase will be given to the IT department of a company. The IT department is responsible for AMT Setup and Configuration. The IT department is free to use any method to enter in AMT Setup information. Once this is done, the systems will be in Enterprise mode and in the In-Setup phase. An S&CS will need to generate PID and PPS sets.

AMT Configuration has to occur over a network. The network can be encrypted via Transport Layer Security Pre-Shared Key (TLS-PSK) protocol. Once the systems connect to an S&CS, Enterprise mode Configuration will occur.

The IT TLS-PSK method places the work of AMT Setup and Configuration on the IT departments of major corporations. They must have the personnel and infrastructure in place for system configuration and deployment. It is no touch for the OEM

OEM TLS-PSK

OEM TLS-PSK AMT Setup and Configuration is done in two stages. The first stage is performed during OEM manufacturing and the second stage at the customer location.

In the first stage, customers purchase systems from HP. HP will setup those systems during manufacturing bringing them to the In-Setup phase. The new Admin Password, PID, and PSS generated during HP manufacturing are transferred to the customer in a separate and secured fashion. That information along with the new admin password is provided to the customer. After manufacturing, the systems are shipped to the customer in the In-Setup state.

Alternatively, the customer can provide HP with their own set of Admin Password, PID, and PPS to use for the order. HP will use the customer generated Admin PW, PID and PPS to bring the systems into the In-Setup phase.

In the second stage, the customer receives the In-Setup systems and the PID, PPS, and password information. The PID, PPS, and password information is integrated into the customer S&CS. The In-Setup systems are then connected to the network and powered on. Enterprise Mode – AMT Configuration occurs. Some ISV's may require additional settings, such as the SC&S port number and SC&S IP address. Contact your Management Console ISV for more details.

During the second stage AMT Configuration, the S&CS will generate a new PID and PPS combination for each of the systems and delete OEM PID/PPS from and Configuration Server database.

The OEM TLS-PSK method places the work of AMT Setup on the OEM. All the customer needs to do is plug in the systems and finish the configuration. Once this is done, the system will be in the Operational phase and ready to use.

HP provides a fee-based customized service that will perform AMT Setup of systems in the factory and securely provide pre-shared keys to the customer. HP offers a secured service that will eliminate manual AMT Setup of each unit at the customer site. Please contact HP for more information about this valuable service.

USB Drive Key Setup and Configuration

Password, PID, and PPS information can be setup and configured locally with a USB Drive Key. This allows an IT technician to setup and configure systems manually without the problems of typing in entries.

The following is a typical USB Drive Key Setup and Configuration procedure:

1. An IT technician inserts a USB Drive Key into a system with a management console.
2. The IT technician requests local Setup and Configuration records from an SCS through the console.
3. The SCS will:
   a. Generate the appropriate amount of passwords, PID and PPS sets and store them in its database.
   b. Return the information to the management console.

4. The management console writes the password, PID and PPS sets to a Setup.bin file in the USB Drive Key.

5. The IT technician takes the USB Drive Key to the staging area where new AMT platforms are located and performs the following:

   a. Unpack and connect platforms if necessary.

   b. Insert USB Drive Key into a platform.

   c. Turn on that platform.

6. The system BIOS will check for the presence of a USB Drive Key.
   -- If a USB drive key is detected, the BIOS will look for a Setup.bin file at the beginning of the Drive Key and continue with Step 7.
   -- If no USB Drive Key is detected or Setup.bin file is found, then the system will boot normally and the remaining actions in steps 7 thru 11 will not be performed.

7. The system BIOS will display a message that automatic Setup and Configuration will occur and take the following actions:

   a. The first available record in the Setup.bin will be read into memory and:
      - Validate the file header record
      - Locate the next available record
      - Invalidate the current record so it cannot be used again

   b. The memory address is placed into the MEBx parameter block.

   c. MEBx is called.

8. MEBx processes the record.

9. MEBx writes completion message to display.

10. IT technician powers down the system. At the time, the system is in In-Setup phase at this time and is ready to be distributed to the user in an Enterprise mode environment.

11. Return to Step 5 for additional systems.

Refer to your management console supplier for more information on USB Drive Key Setup and Configuration.

The USB Drive Key must meet the following requirements for it to be usable in USB Drive Key Setup and Configuration:

- It must be greater than 16MB in size.

- The sector size must be 1KB.

- The USB Drive Key is not formatted to boot.

- The Setup.bin file must be the first file landed on the USB Drive Key.

Remote Configuration (RCFG)

Remote Configuration (RCFG) is the ability to use a single OEM image to provision systems securely without the need to manually modify AMT options. RCFG uses a Public Key Infrastructure with Certificate Hashes (PKI-CH) protocol to maintain security. A DHCP environment is required.

RCFG relies on several new AMT features:

- Embedded Hash Root Certificates
- Self Signed Certificate
- One-Time Password
- Delayed network access

One or more hash root certificates are embedded into the AMT FW. These certificates are integrated into the Hello messages sent by the AMT system to the SCS. The SCS must have compatible certificates to authenticate the AMT system.

A self signed certificate can be generated to create a secure connection between the AMT system and the SCS. This certificate is used for encryption, not authentication. The SCS will use the public key from the self signed certificate to encrypt the session key it generates and sends it to the AMT system. The AMT system can decrypt SCS session key with its private key.

The One-Time Password (OTP) is created during provisioning. This password is used with the remote console to initiate RCFG and it is sent to both the AMT system and the SCS. This password is used to improve security.

The network interface used to send out Hello messages is functional for a limited amount of time once remote configuration has been activated which is known as delayed remote provisioning.

Delayed as the name implies is remote configuration at a later time when an OS has been installed on the AMT system. In this implementation, Setup and Configuration is started when a remote console application initiates the process by communicating with the ME through the HECI driver. This requires a functional OS and agent to be installed on the AMT system. OTP authentication can be used, it is optional. The remote console provides the OTP to the AMT system and to the SCS.

Consult your ISV management console provider for details on OS agents for Delayed remote configuration support.

Remote Configuration Timeouts in HP Systems

The HP Compaq dc8200 Business PCs are shipped out of the factory with the Remote Configuration Timer set to 0 (no Hello message broadcasting). In order to enable ME to broadcast Hello messages, an Intel Activator local agent must be used.

The Activator local agent will typically set ME to broadcast Hello messages for 6 hours when the ME is active and the system is connected to a network. Consult your ISV management console provider for exact details concerning delay remote configuration timeouts.

If no SCS responds to the Hello messages within the timeout period, then the network interface that sends out the Hello messages will be disabled.

The network interface can be re-enabled to send out Hello messages again by the following methods:

- Restarted by a local agent.
- Partial Unprovisioning through the MEBx.

Once the network interface has been re-enabled it will send out Hello messages for the next 6 hours as long as the ME is active and the system is connected to a network.

Remote Configuration (RCFG) Prerequisites

RCFG requires certain prerequisites before it can be used.

1. Both the AMT system and the SCS must be on a DHCP server. The SCS must have the name of "Provisionserver" or if not, it must have an alias in DNS, and be on the same domain as the AMT system.
2. The AMT system must have at least one pre-programmed active root certificate hash.
3. The SCS must have a server certificate with the proper OID or OU values.
   a. OID value in the Extended Key Usage field = 2.16.840.1.113741.1.2.3
   b. This is the unique Intel AMT OID.
   c. OU value in Subject field = "Intel(R) Client Setup Certificate"
   d. This OU value is case sensitive and must be entered exactly as shown.
4. In the case of a Delayed Setup and Configuration, an OS and local agent must be installed on the AMT system.

MEBx and Hashes

AMT 7.1 has the feature in the MEBx to allow IT administrators to manually activate a hash and to add up to three additional certificate hashes.

To enter the Remote Configuration screen in the MEBx:

1. Press **CTRL-P** for the MEBx and enter the MEBx password.
2. Select the **Intel® AMT Configuration** option.
3. Select the **Setup and Configuration** option.
4. Select the **TLS PKI** option. The Remote Configuration screen appears as shown in Figure 28.
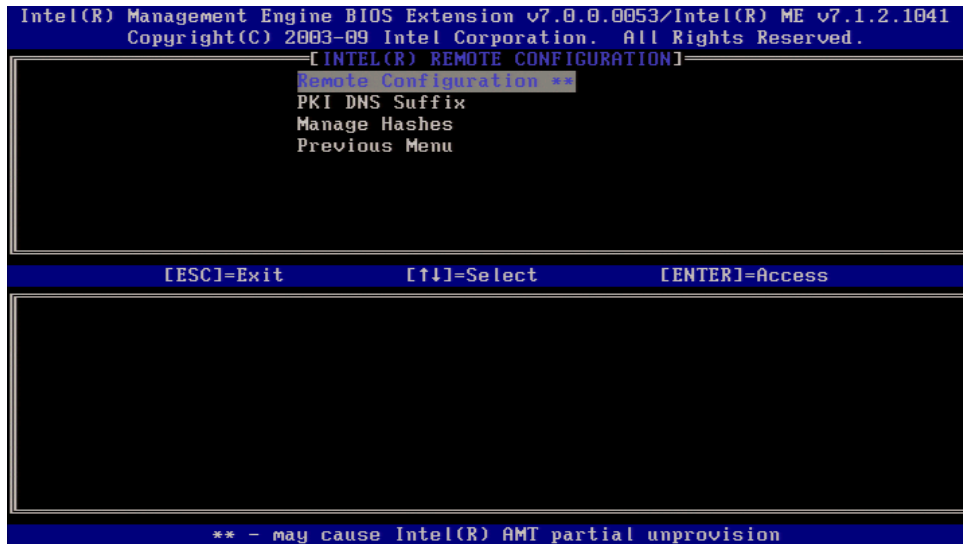
```
Intel(R) Management Engine BIOS Extension v7.0.0.0053/Intel(R) ME v7.1.2.1041
         Copyright(C) 2003-09 Intel Corporation.  All Rights Reserved.
                        ==[INTEL(R) REMOTE CONFIGURATION]==
                        Remote Configuration **
                        PKI DNS Suffix
                        Manage Hashes
                        Previous Menu



            [ESC]=Exit          [↑↓]=Select          [ENTER]=Access




                   ** - may cause Intel(R) AMT partial unprovision
```

Figure 28. Intel Remote Configuration screen

5. Remote Configuration. This option enables or disables Remote Configuration. Default (and recommended) setting: Enabled

6. PKI DNS Suffix. This option allows the PKI DNS Suffix of the SCS to be entered.

7. Manage Hashes. This option shows the hashes in the system including the name of the hash and whether it is active or not. If no hashes are in the system, then an option to add one is available. If hashes are available, then an option to delete one or more is available.

    To add a hash:
    a. Press the Insert key.
    b. Enter a name for the hash.
    c. Enter the fingerprint of the hash.
    d. Choose to set this hash active or not. Hashes can be made active, not active, default or not default at this menu.

8. Select **Previous Menu**.

Host-Based Configuration (Client control configuration mode)

Host-Based configuration uses the Intel Activator local agent to enable vPro functionality while disabling the more security-sensitive features.

Host-based configuration mode has the following requirements and characteristics:

- The host OS must be present on the AMT client.
- The System defense feature will be disabled.
- User consent will be required for all redirection operations.
- Auditor consent to un-configuration is not supported.
- Programmatically changing the MEBX password is not supported.
- The ability to be transitioned to Enterprise mode (admin control configuration mode) is supported.

By default, HP Z210 Workstations are shipped ready for the Host-based configuration.

The Intel vPro Activator Wizard can be downloaded here:

http://communities.intel.com/docs/DOC-1171/

List of Supported CA Certificates

The following are a list of supported Certificate Authorities and certificates. Not all of the certificates might be populated in certain configurations[*].

- VeriSign Class 3 Primary CA-G1
- VeriSign Class 3 Primary CA-G3
- Go Daddy Class 2 CA
- Comodo AAA CA
- Starfield Class 2 CA
- VeriSign Class 3 Primary CA-G2
- VeriSign Class 3 Primary CA-G1.5
- VeriSign Class 3 Primary CA-G5
- GTE CyberTrust Global Root
- Baltimore Global Trust Root
- Cybertrust Global Root
- Verizon Global Root
- Entrust .net CA (2048)
- Entrust Root CA
- VeriSign Universal Root CA

Return to Default

Return to Default is also known as Unprovisioning. An AMT Setup and Configured system can be unprovisioned through the ME Platform Configuration Screen and the "Un-Configure Network Access" option (Figure 29).
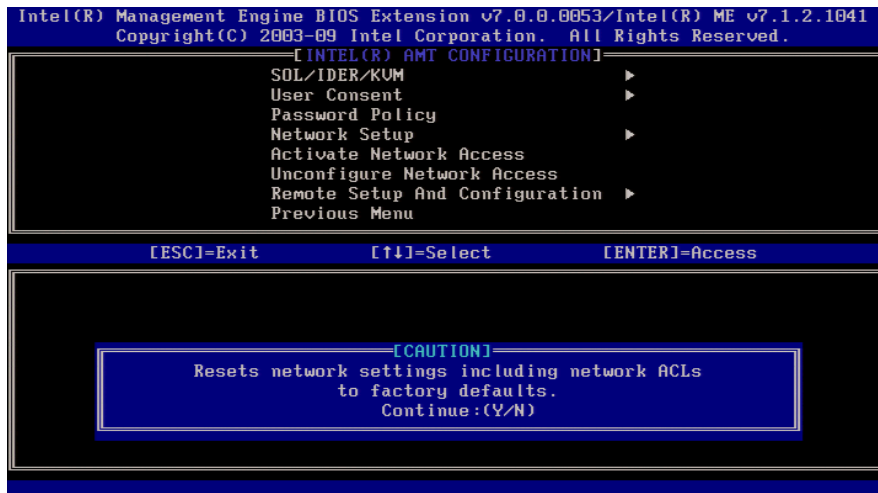

Figure 29. Intel AMT Un-configure Network Screen

Depending on how the system was previously provisioned, one or both unprovisioning options may appear.

1. Select **Unconfigure Network Access**.

   a. Select the needed Unprovision mode.
      Full unprovisioning is available for Manual and Enterprise mode provisioned systems. It will return all AMT Configuration settings to factory defaults. All certificate hashes will be deleted and the default hash will be made active. It does not reset all ME Configuration settings or passwords.

      Partial unprovisioning is available for Enterprise mode provisioned systems. Partial unprovisioning will return all AMT Configuration setting to factory defaults with the exception of the PID, PPS, and PKI-CH. It does not reset ME Configuration settings or passwords.

   b. After about a minute, an Un-provisioning message will appear.

   c. After unprovisioning is done, control is passed back to the AMT Configuration screen.

   Notice that the Setup and Configuration option is available again since the system is set to the default Enterprise mode.

2. Return to the previous menu.

3. Exit. Select **Y**.

4. System will reboot.

A partial unprovisioning will re-open the network interface for 6 hours of Hello message broadcasts. The F-10 BIOS setup also has an option to fully unprovision the ME to factory defaults. The "Unconfigure AMT/ME" option is located under the Advanced\AMT Configuration menu.

Full Return to Factory Defaults

All MEBx settings can be returned to the factory default by clearing CMOS. This includes resetting the password to the "admin" default. The system will need to be Setup and Configured again before remote management is possible. Any non-default certificate hashes will have to be re-applied.

Appendix A: Frequently Asked Questions

Q: How can the MEBx be locally accessed?
A: The MEBx can be locally accessed by pressing CTRL-P during POST.

Q: Why is the CTRL-P prompt not displayed during POST?
A: By default the CTRL-P prompt is hidden during POST, but it can be display if set in F10 Setup.

Q: What is the default username and password for the MEBx?
A: The default username and password are both "admin".

Q: Why does the MEBx not accept my new password?
A: All MEBx passwords, other than the default password, must comply with the strong password guidelines. See the Password Guidelines section for more details.

Q: If the password is not known, how can the system be recovered?
A: Clearing CMOS will reset all MEBx options including the password. The password will revert back to the default password of "admin".

Q: How can all MEBx options be restored to the factory defaults?
A: See Full Return to Factory Defaults section.

Q: What happens if the wrong password is entered incorrectly multiple times?
A: Once the password is entered incorrectly three times, the system will reboot. The user can go back into the MEBx after the reboot and attempt to enter the password again.

Q: Can the WebGUI be used locally to access the MEBx on the system it is running from?
A: No. This is because WebGUI access has to come from an outside network to a specific IP and port. Local access does not originate from an outside network.

Q: Why does a new password set with the WebGUI cannot be used locally in the MEBx?
A: A password set with the WebGUI is a remote password and will only work when accessing the MEBx remotely. It does not work with the MEBx locally. The local password must be used to locally access the MEBx.

Q: Is TLS required?
A: No. TLS is optional.

Q: If TLS is not used, then what is used?
A: HTTP Digest will be used for mutual authentication if TLS is not used.

Q: Who provides Setup and Configuration Servers?
A: HP Client Configuration Manager and ISVs such as Altiris provide Setup and Configuration Servers. Check with your management console supplier to see if they offer this service.

Q: Can AMT be set for static address and the OS set for DHCP or vice versa?
A: No. Although it can be done, this is not a supported setting by Intel and may cause unexpected system behavior.

Q: What is the default port used by the Intel WebGUI?
A: The Intel WebGUI listens to port 16992.

Q: What is the difference between the ME and AMT?
A: The ME is the controller that manages AMT along with PAVP. Notice, clearing AMT settings does not affect ME settings since the ME is a separate entity.

Q: Why does Wake-On-ME not work after the Idle Timeout is set?
A: The Wake-On-ME feature only works if the ME ON in Host Sleep State setting is set to allow ME WoL and the system is fully provisioned.

Appendix B: Power / Sleep / Global States Explained

Under Advanced Configuration and Power Interface (ACPI) specification a PC can be in one of several Power states. These power states are also known as Sleep (Sx) states or Global (Gx) states.

S0 is the ON state. The PC is fully functioning. All system devices and operating system, if available, are running. S0 is also known as **G0**.

S3 is the Standby (Microsoft terminology) or Suspend-to-RAM state. The memory subsystem and V_{aux} power rail remains powered, while the rest of the system including the processor are not powered. When the system resumes from S3, the system context remains intact because the system memory was preserved and powered at all times.

S4 is the Hibernate (Microsoft terminology) or Suspend-to-Disk state. The system context (memory) is saved to the hard drive as a hibernation file. When the system resumes from S4, the system context is restored from the hibernation file. V_{aux} remains powered, but all other subsystems including system memory and the processor are not powered.

S5 is the Soft Off state. It is identical to S4 with the exception that the system context is not saved. When the system resumes from S5, it will power up and going through POST. S5 is also known as **G2**.

G3 is the Mechanical Off state. All subsystems are not powered in this state. The easiest way to achieve this state is by removing A/C power from the system via unplugging the power cord.

The ME has its own power states (Mx) similar to the Sx states.

M0 is the ON state for the ME when the system is in S0 state. The ME is fully powered and running.

M3 is the ON state for the ME when the system is in a non-S0 state. The ME is fully powered and running.

Moff is the OFF state for the ME. The system is in a non-S0 state.

The ME can be set to stay powered and active in all Sx states. If the system (host) is in S0, then the ME will be in the corresponding M0 state. However, if the system is in S3, S4, or S5, then the ME will still remain active, but it will be in M3 state.

Appendix C: Wake-On-ME Explained

Wake-On-ME, also known as ME WoL, is a feature that allows the ME to go into a low power state when it is not used.

There are three conditions that must be met for Wake-On-ME to function.

- The system is in a sleep state: S3, S4, or S5
- ME On in Host Sleep State setting is set to allow ME WoL.
- If the system is running (S5), then the ME is also running.

The ME On in Host Sleep State setting must be set to ME WoL so the ME can be put to sleep and awaken if needed when the system is in a sleep state. The ME counts down from the amount of time set in Idle Timeout before it will go to sleep.