vPro Setup and Configuration for the 8000 Elite Business PC with Intel vPro Processor Technology

Introduction

The HP Compaq 8000 Elite Business PC uses Intel vPro processor technology to simplify PC management and reduce IT-related expenditures. Intel vPro processor technology is a combination of Active Management Technology (AMT) and Intel Virtualization Technology (VT), which allows for improved management of PC systems and enhanced security.

Intel vPro processor technology no longer supports Virtual Appliances. This is a change from previous generations of HP Compaq dx7 Business PCs with Intel vPro processor technology.

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 Q965, Q35, and Q45 Express chipsets.

The following is a brief history of AMT evolution:

- AMT 1.0 - Introduced with the Intel 945 chipset, but was not shipped with HP Business PCs.
- AMT 2.0 - Introduced with the Intel Q965 chipset and was shipped with HP Compaq dc7700p Business PCs.
- AMT 2.1 - Introduced in March 2007 and was shipped with HP Compaq dc7700p Business PCs.
- AMT 2.2 - Will be available as a Web download in the Fall of 2007 with HP Compaq dc7700p Business PCs.
- AMT 3.0 - Introduced with the Intel Q35 Express chipset and will be shipped with HP Compaq d7800p systems.
- AMT 3.2 - Introduced with the HP Compaq dc7800p April 2008 Refresh.
- AMT 5.0 - Introduced with the Intel Q45 Express chipset and shipped with HP Compaq dc7900 systems.
- AMT 5.2 – Shipped on the HP Compaq 8000 Elite Business PCs.

AMT 5.0 is an important update that provides new features over the existing AMT 3.x feature set. This white paper has been updated to include the new features of AMT 5.0.

By default, AMT shipping on the HP Compaq 8000 Elite Business PC will be inactive. It must be set up 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 set up and configuration:

- Small Business (SMB) mode
- Enterprise mode

This white paper details Small Business 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 **www.hp.com** for other white papers and technical information regarding new HP Compaq 8000 Elite Business PCs and new Intel vPro processor technology.

AMT Setup and Configuration

AMT must be set up 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. This setup is generally performed only once in the lifetime of a system. When AMT is enabled, it can be discovered by management software over a network.

AMT Configuration sets up all 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 life span. 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, as follows:

- Factory
- In-Setup
- Operational

The Factory phase is the initial stage in which the system has been built from the factory and 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 SMB mode systems after changing the default password. Enterprise mode systems also require that you set the Provisioning ID (PID) and Provisioning Passphrase (PPS). More details about passwords, PIDs, and PPS are provided in later sections of this paper.

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

The Operational phase is the final stage in which AMT is fully setup and configured in the system and ready for normal use.

SMB Mode - AMT Setup and Configuration with MEBx

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

SMB mode is the easiest to implement since it does not require much infrastructure, but is the least secure since all network traffic is not encrypted. HP recommends using this process only 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 from its default state.

Password Guidelines

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

Passwords must:

- Be between 8 and 32 characters long.
- Contain both upper and lower case Latin characters (e.g. A, a, B, b).
- Have at least one digit character (e.g. 0, 1, 2, … 9).
- Have at least one 7-bit ASCII non-alphanumeric character with an ASCII value between 33d and 126d that is not part of the invalid character list below.

  Examples of valid characters include:

  - 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 white paper is for use with HP Compaq 8000 Elite Business PCs. The HP Compaq 8000 Elite Business PC uses the 786G7 BIOS family.

For best performance and to take advantage of AMT 5.2 features, use the latest version of BIOS and ME firmware for HP Compaq 8000 Elite Business PC, which is available at **www.hp.com**.

The system BIOS and the ME firmware must be updated individually. Refer to the BIOS Flash white paper at **www.hp.com** for more information about flashing the system BIOS and ME firmware.

SMB Mode - AMT Setup and Configuration Steps

When going through the options in the MEBx for the first time (Factory phase), the default settings are in place. This white paper details HP-recommended settings for 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 Manageability Engine BIOS Extension (MEBx) Setup. You can display this option only during POST if set in F10-Setup.

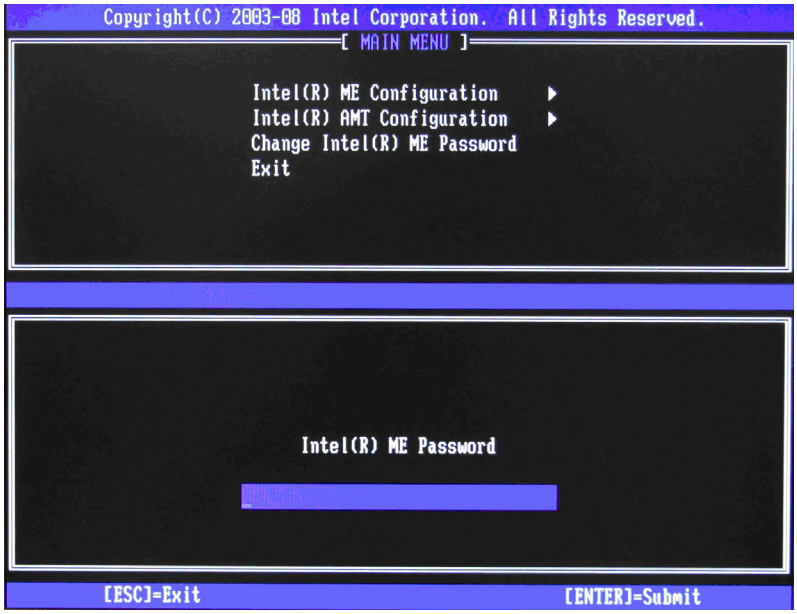


Figure 1 Intel MEBx Password Screen

2. Type the default password, which is **admin**. Passwords are case-sensitive.

   NOTE: You must change the default password before making changes to the MEBx options.

3. Change the MEBx password. The new password must meet the Strong Password criteria defined in the Password Guidelines Section. Type the password twice for verification.

   Change the password to establish AMT ownership. The system will go from Factory phase to In-Setup phase. The ME and AMT options within the MEBx are accessible and you can access the system using the AMT WebGUI.

4. Select the Intel ME Platform Configuration. A window displays indicating that the system resets after configuration.

5. Select **Y**. ME platform configuration allows IT personnel to configure ME features such as AMT/ASF selection, power options, firmware update capabilities, and so on.

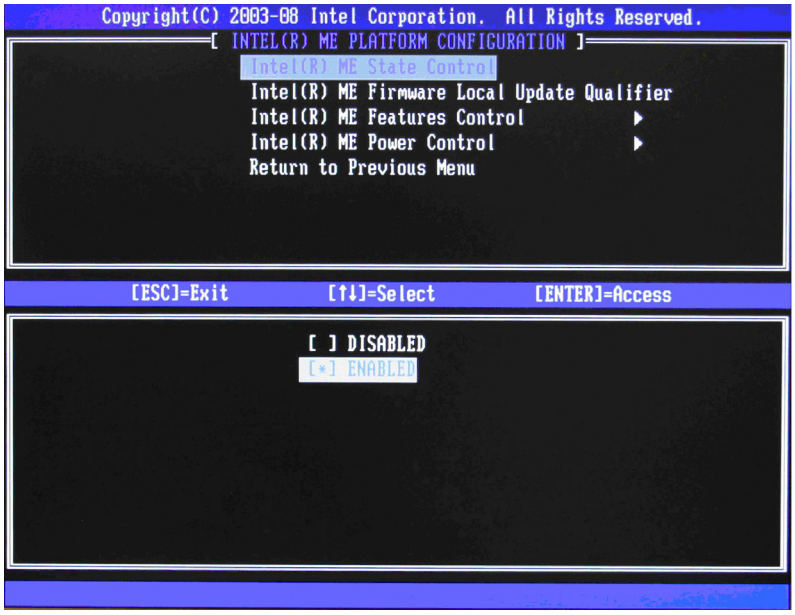


Figure 2 Intel ME Platform Configuration screen

6. Select **Intel ME State Control**, and then select **Enabled**.

   Default Setting = Enabled, Recommended Setting = Enabled

   This option enables or disables the ME and is used for diagnostic purposes. If set to **Disabled**, the ME is still initialized during POST, but is halted soon afterward so that it does not generate any traffic. If there is a problem that affects the ME, it can be removed from the system to eliminate it from the suspect list until root cause is found.

   Note that if the ME is disabled, then all AMT and ASF functions are also disabled. The system will not be remotely manageable.

7. Select **Intel ME Firmware Local Update Qualifier.**

   Default Setting = Always Open, Recommended Setting = Always Open

   This option allows the BIOS to override the ME Firmware Locale Update option and to permit local ME firmware updates.

   Always Open is the default and allows for as many local updates as the system BIOS allows, which is unlimited.

   Choosing **Never Open** or **Restricted** adds the Intel ME Firmware Local Update option, which can be set to Enable or Disable. By default it is Disabled. This option, along with the Qualifier, dictates whether ME firmware local updates are allowed. "Never Open" ignores what is set in the system BIOS and follows the Intel ME Firmware Local Update option.

"Restricted" ignores what is set in the system BIOS and allows local ME firmware updates until the ME is configured.

	Never Open	Restricted
ME Firmware Local Update Enabled	Local ME firmware updates allowed.	Local ME firmware updates allowed.
ME Firmware Local Update Disabled	Local ME firmware updates NOT allowed.	Local ME firmware updates allowed only until the ME is configured.

8. Select **Intel ME Features Control**.

a. Select **Manageability Feature Selection**.

Default Setting = Intel AMT, Recommended Setting = Intel AMT

This option sets the platform management mode: None, Intel AMT, or ASF.

By default, HP Compaq 8000 Elite Business PCs are set to **Intel AMT**, and ASF is an available option.

Note that setting the **None** option will disable all remote management capabilities. Setting None will also unprovision any AMT settings.

i. Select **Intel AMT**.

ii. Select **Return to previous menu**.

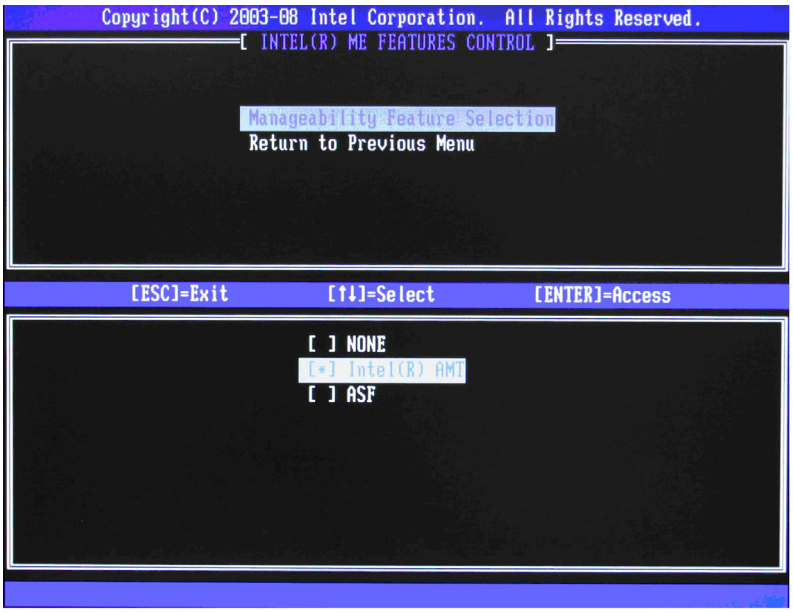


Figure 3 Intel ME Features Control Screen with AMT selected

iii. Select **Return to the previous menu**.

9. Select **Intel ME Power Control**.

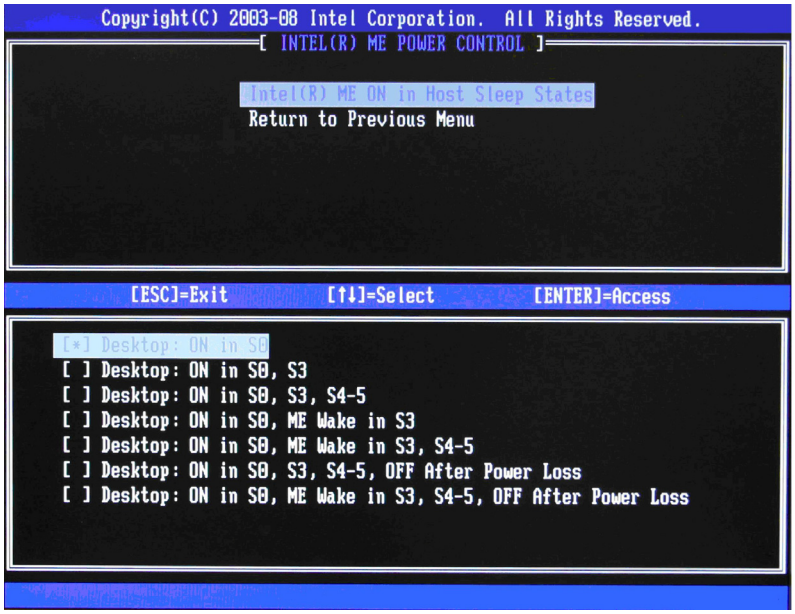


Figure 4 Intel ME Power Control Screen

a. Select **Intel ME ON in Host Sleep States**, and then select **Desktop:ON in S0, S3, ME WoL in S3, S4-5, OFF After Power Loss.**

Default Setting = Desktop: ON in S0, Recommended Setting = Desktop: ON is S0, S3, ME WoL in S3, S4-5, OFF After Power Loss

This option sets the ME power policy when the system is in a sleep state (Sx) and when returning from a G3 power loss.

Table 2: ME Power State During Host Sleep State

ME ON in Host Sleep State	ME Behavior
Option 1	ME is ON only when the system is in S0.
Option 2	ME is ON only when the system is in S0 or S3.
Option 3	ME is ON at all times S0, S3, S4, and S5.
Option 4	ME is ON only when the system is in S0. It will be asleep in S3 unless it is called upon. Timer for ME sleep is set by the Idle Timeout option.
Option 5	ME is ON only when the system is in S0. It will be asleep in S3 - S5 unless it is called upon. Timer for ME sleep is set by the Idle Timeout option.
Option 6	ME is ON at all times S0, S3, S4, and S5. ME will not automatically initialize after recovering from a G3 power loss.
Option 7	ME is ON only when the system is in S0. It will be asleep in S3 - S5 unless it is called upon. Timer for ME sleep is set by the Idle Timeout option. ME will not automatically initialize after recovering from a G3 power loss.

See **"Appendix B: Power / Sleep / Global States Explained" on page 34** for an explanation of sleep/ power states.

See **"Appendix C: Wake-On-ME Explained" on page 35** for an explanation of Wake-On-ME/ ME WoL.

b. Select **Return to the previous menu**.

10. Return to previous menu to exit the MEBx Setup and save ME configuration. The system will display an Intel ME Configuration Complete message and reboot. After the ME Configuration is complete, you can configure the AMT on the next boot.
11. Press **Ctrl-P** during POST to enter MEBx Setup again.
12. Type the MEBx password.
13. Select **Intel AMT Configuration**.

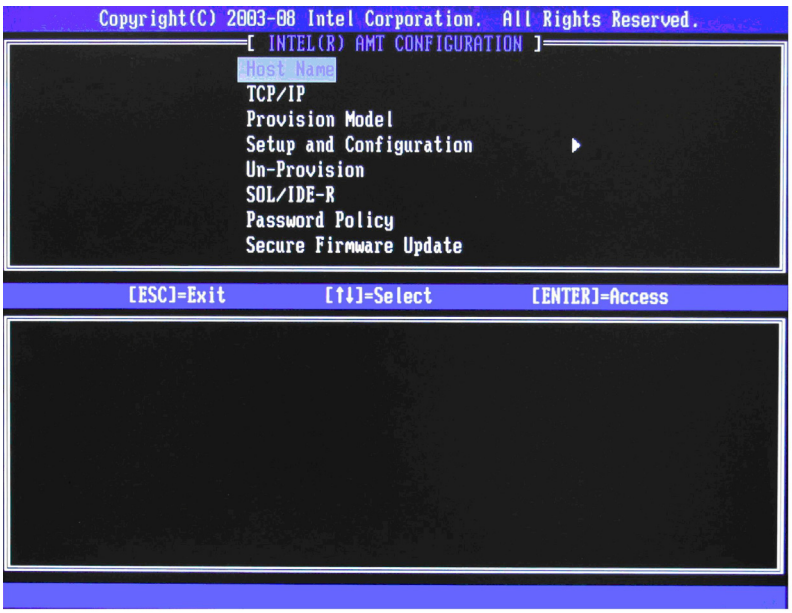


Figure 5 Intel AMT Configuration screen

14. Select **Host Name**, and then type a host name.

Default Setting = HPSystem, Recommended Setting = User Dependent

NOTES: Spaces are not accepted in the host name. Make sure there is not a duplicate host name on the network. You can use host names in place of the system's IP for any applications requiring the IP address.

15. Select **TCP/IP**.

a. Select **Disable Network Interface**, and then select **N**.

Default Setting = Network Interface Enabled, Recommended Setting = Network Interface Enabled

If the network is disabled, then all remote AMT capabilities are disabled and TCP/IP settings are not necessary.

This option is a toggle, and the next time you access it you are prompted with the opposite setting.

b. Select **DHCP Disable**, and then select **Y**.

Default Setting = DHCP Enabled, Recommended Setting = User Dependent

You can use DHCP if it is available. If you use DHCP, then steps 15c through 15g are not necessary. Otherwise, the system administrator will have to configure TCP/IP settings.

For the purpose of this white paper, DHCP is disabled so steps 15c through 15g can be illustrated. Step h will appear for both DHCP and Static configurations.

c. Select **IP Address**, and then type a static address.

Default Setting = 10.0.0.2, Recommended Setting = Network Dependent

Example: 192.168.0.1

Make 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.

d. Select **Subnet Mask**, and then type a subnet mask.

Default Setting = 255.255.255.0, Recommended Setting = Network Dependent

Example: 255.255.255.0

e. Select **Default Gateway Address**, and then accept the default and press **Enter**.

Default Setting = 0.0.0.0, Recommended Setting = Network Dependent,

Leave as 0.0.0.0 if this option is not needed.

f. Select **Preferred DNS Address**, and then accept the default value and press **Enter**.

Default Setting = 0.0.0.0, Recommended Setting = Network Dependent

Leave as 0.0.0.0 if this option is not needed.

g. Select **Alternate DNS Address**, and then accept the default value and press **Enter**.

Default Setting = 0.0.0.0, Recommended Setting = Network Dependent

Leave as 0.0.0.0 if this option is not needed.

h.Select **Domain Name**, and then type a domain name

Default Setting = none, Recommended Setting = Network Dependent

The domain name is blank by default. If not populated, then the default domain of “Provisionserver” is 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, that is the domain used. However, if there is no response after four DNS queries to the named domain, then that domain name is no longer used and the default “Provisionserver” is used.

16. Select **Provision Model**.

    a. Change to **Small Business**, and the select **Y**.

    Default Setting = Enterprise, Recommended Setting = Small Business

    This option is a toggle, and the next time you access it you are prompted with the opposite setting.

    Notice that the Setup and Configuration option is no longer available once the system is in Small Business mode. This option is only used in Enterprise Mode.

    b. Select **Return to previous menu**.

17. Skip **Un-Provision**. This option returns the system to factory defaults.

18. Skip **VLAN**.

    Default Setting = Disabled, Recommended Setting = User Dependent

    This option enables or disables VLAN support. If VLAN is enabled, then you must provide the VLAN tag (label) (1-4094).

    VLAN support is not necessary for AMT or Virtual Appliances. If enabled, it allows the grouping of systems from different networks into one virtual network.

19. Select **SOL/IDE-R**.

    a. Select **Y** in the message window.

    b. Select **Username and Password**, and then select **Enabled**.

    Default Setting = Enabled, Recommended Setting = Enabled

    This option allows users and passwords to be added from the WebGUI. If the option is disabled, then only the administrator has MEBx remote access.

    c. Select **Serial Over LAN**, and then select **Enabled**.

    Default Setting = Enabled, Recommended Setting = Enabled

    This option enables/disables Serial Over LAN (SOL) functionality.

    d. Select **IDE Redirection**, and then select **Enabled**.

    Default Setting = Enabled, Recommended Setting = Enabled

    This option enables/disables IDE Redirection (IDE-R) functionality.

20. Select **Password Policy**.

    Default Setting = Default Password Only, Recommended Setting = Default Password Only

    This option determines if the local MEBx password can be modified from a remote console.

Option	Effect
Default Password Only	This option will allow the MEBx password to be remotely modified only if it is the default "admin" password.

Option	Effect
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.

21. Select **Secure Firmware Update,** and then select **Enabled**.

    Default Setting = Enabled, Recommended Setting = Enabled

    This option enables/disables the ability to remotely update the ME firmware.

22. Skip Set PRTC.

    Default Setting = None, Recommended Setting = Current Date and Time

    This option sets the PRTC (Protected Real Time Clock). It is used with TLS mutual authentication which checks for the client certificate for expiration based on its PRTC.

    PRTC has a valid date range of 1/1/2004 to 1/4/2021.

23. Select **Idle Timeout**.

    Default Setting = 1, Recommended Setting = 1

    This option sets the timeout value for Wake-On-ME.

    The default timeout value is 1 from the factory and it is in units of a minute. A value of 0 means the Wake-On-ME feature is disabled and the ME will not go to sleep when not being used in a non-active system. HP recommends a setting of 1, which allows the ME to go to sleep after 1 minute of inactivity.

    The timeout value can only be set in both decimal and hexadecimal notation, which is a minor change from the dc7700p that allowed both 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: Wake-On-ME Explained" on page 35** for an explanation of Wake-On-ME/ME WoL.

24. Select **Return to previous menu**.

25. Select **Exit**, and then select **Y** to exit the MEBx Setup and save settings.

    The system displays an Intel ME Configuration Complete message, and then the system reboots.

    After the system reboots, it changes from In-Setup phase to Operational phase, and AMT is fully operational. Once in Operational phase, you can remotely manage the system through the Intel AMT WebGUI or ISV remote console and you can provide the system 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 - a Management computer on the same subnet as the AMT computer.
3. Connect to the IP address specified in the MEBx and port of the AMT system.

   a. By default, the port is 16992.

   b. 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

   Example B: http://hpsystem.hp.com:16992 (from steps 14 and 15h)

   The Management computer makes a TCP connection to the AMT system and accesses the top level AMT-embedded Web page within the Management Engine of the AMT system.

4. Type the user name and password. The default username is **admin** and the password is what you set during AMT Setup in the MEBx.

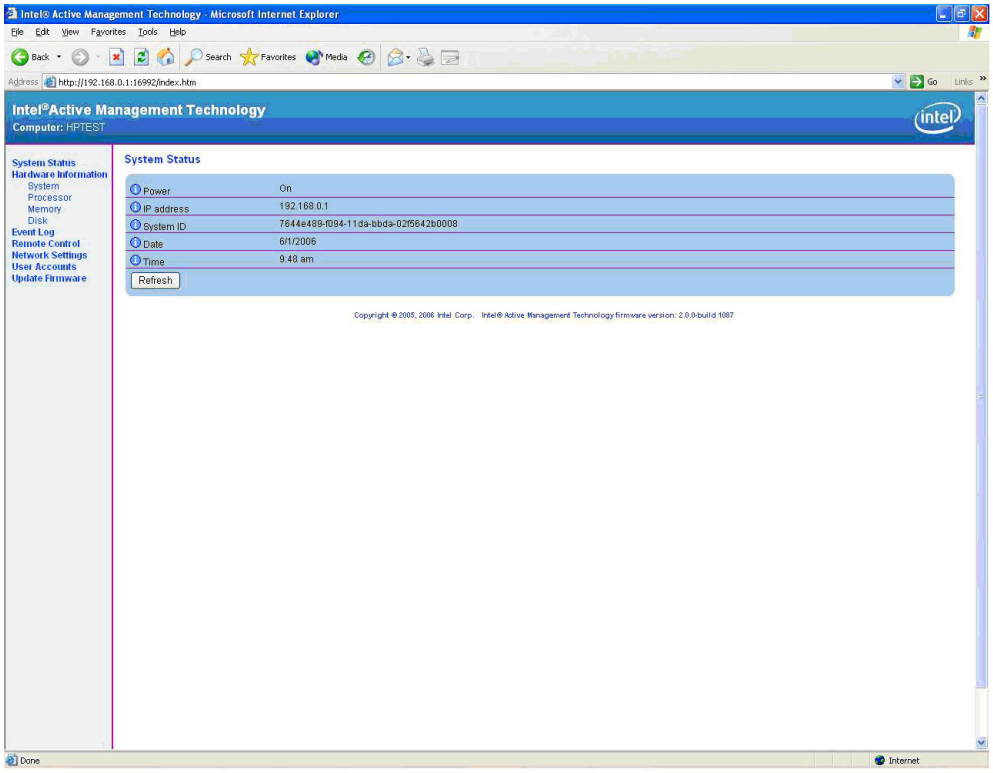


Figure 6 Intel AMT WebGUI Screen

5. Review system information and/or make any necessary changes.

NOTE: You can change the MEBx password for the remote system in the WebGUI.

Changing the password in the WebGUI or a remote console results in two passwords. The new password, known as the "remote" MEBx password, only works remotely with the WebGUI or remote console. The local MEBx password used to locally access the MEBx is not changed. The user has to remember both local and remote MEBx passwords to access the system MEBx locally and remotely.

When the MEBx password is initially set in AMT Setup, the password serves as both the local and remote password. If the remote password is changed, then the passwords are out of sync.

The remote MEBx password must follow the criteria defined in the Password Guideline section for a strong password.

6. Select **Exit**.

Setup and Configuration Server

A Setup and Configuration Server (SCS) is 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 and PPS are 32 characters. There are dashes between every set of four characters, so including dashes, PIDs are 9 characters and PPS are 40 characters. Once 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 following provides a brief outline of the initial communication between an AMT client system and an SCS:

1. The AMT system sends out a "hello" message that 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, afterward all communication between the AMT client and the SCS can be encrypted with Transport Layer Security (TLS).

Setup and Configuration Server Availability

There are several independent software vendors (ISV) that offer Setup and Configuration Servers, including:

- HP Out of Band Manager
- Altiris
- LANDesk
- Microsoft SMS

Enterprise Mode Setup and Configuration

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

Enterprise Mode - AMT Setup and Configuration Steps

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 **"SMB Mode - AMT Setup and Configuration with MEBx" on page 3** for examples of MEBx menus and full text. The following are quick steps for AMT Setup:

1. Access the MEBx by pressing **Ctrl-P** during POST.
2. Type the default password, which is **admin**.
3. Change the MEBx password, following strong password guidelines.
4. Select **Intel ME Platform Configuration**.
5. In **Intel ME State Control,** select **Enabled**.
6. In **Intel ME Firmware Local Update Qualifier,** select **Always Open**.
7. Select **Intel ME Features Control**.

   a. Select **Check Manageability Features**.

   b. Select **Intel AMT**.
8. Select **Intel ME Power Control**.

   a. Select **ME ON in Host Sleep States**.

   b. Select Option **7**.
9. Select **Exit and save**. The system displays the Intel ME Configuration Complete message, and then reboots.

   After the system reboots, starting with Step 10 you will set some of the options differently than SMB mode.
10. Press **Ctrl+P** during POST to enter MEBx Setup again.
11. Type the MEBx password.

12. Select **Intel AMT Configuration**. The Intel AMT Configuration screen includes numerous options, which are available by scrolling down the menu.

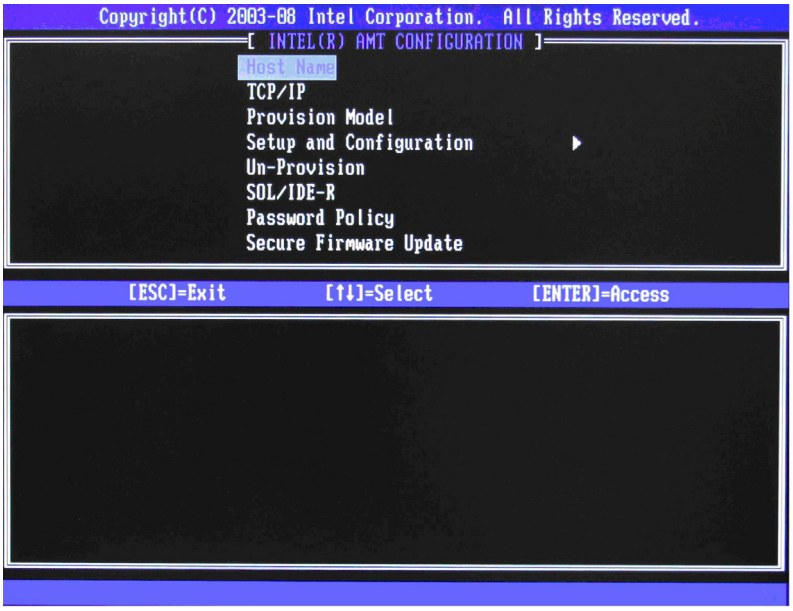


Figure 7 Intel AMT Configuration Screen

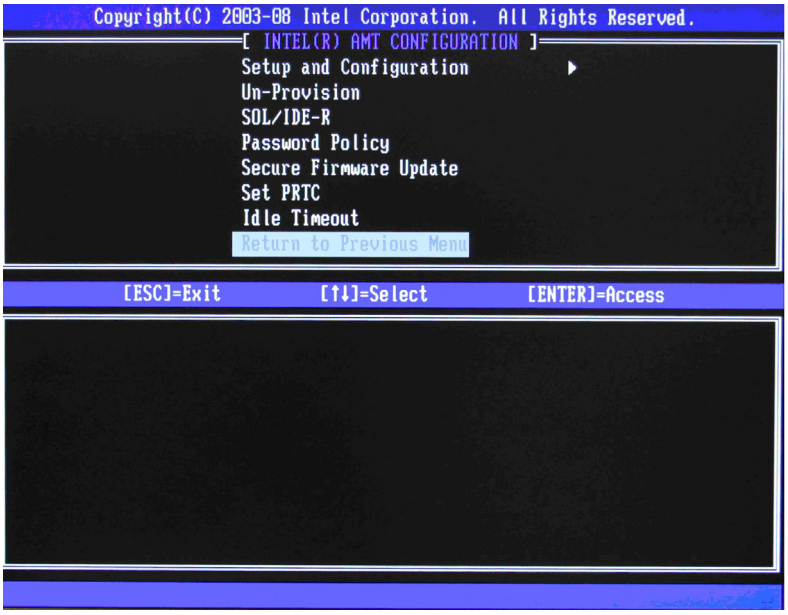


Figure 8 Intel AMT Configuration Screen Continued

13. Select **Host Name,** and then type a host name

    Default Setting = HPSystem, Recommended Setting = User Dependent

    Spaces are not accepted in the host name.

14. Select **TCP/IP**.

    a. Select **Disabling Network Interface**, and then select **N**.

       Default Setting = Network Interface Enabled, Recommended Setting = Network Interface Enabled

       If network is disabled, then all remote AMT capabilities are disabled and TCP/IP settings will not be necessary. This option is a toggle, and the next time you access it you are prompted with the opposite setting.

    b. Select **DHCP Disable**, and then select **N**.

       Default Setting = DHCP Enabled, Recommended Setting = User Dependent

       For the purpose of this white paper, DHCP is enabled.

15. Select **Provision Model**.

    a. Change to **Small Business,** and then select **N**.

       Default Setting = Enterprise, Recommended Setting = Enterprise

    b. Select **Return to previous menu**.

16. Select **Setup and Configuration**.

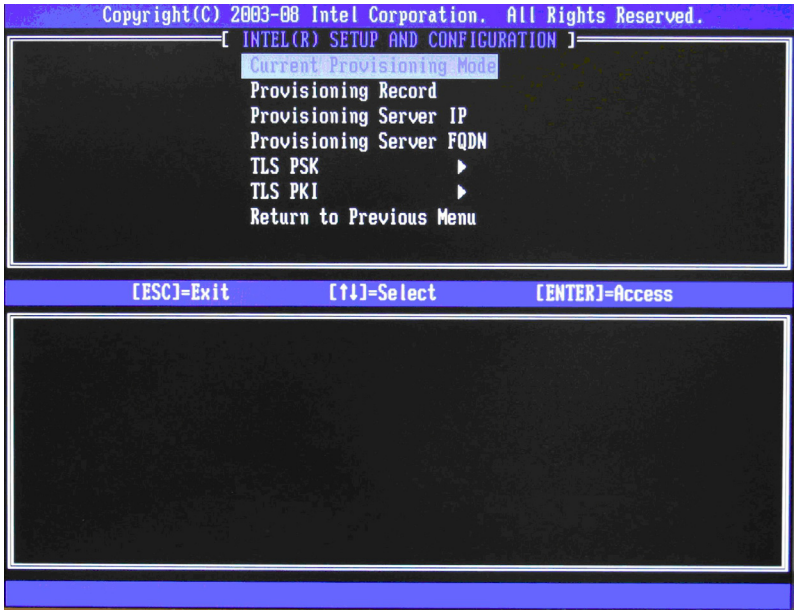


Figure 9 Intel Setup and Configuration Screen

This is the menu where the Enterprise mode provisioning data is entered.

a. Select **Current Provisioning Mode**.

Default Setting = None.

This option shows the current provisioning TLS mode. The three options are: None, PKI, and PSK.

This option is only for display, no changes can be made here.

b. Select **Provisioning Record.**

Default Setting = Not Present

This option shows provision record data of the system.

The provisioning 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
- Hash Algorithm
- Serial Number
- ISDefault Bit
- Time Validity Pass
- FQDN
- Provisioning IP
- Date of Provisioning

This option is only for display, no changes can be made here.

c. Select **Provisioning Server IP**.

i. Enter Provisioning Server IP

Default Setting = 0.0.0.0, Recommended Setting = Network Dependent

ii. Enter Port.

Default Setting = 0, Recommended Setting = 9971

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 SCS is at 9971.

Some ISVs may require additional settings, such as the SCS port number and SCS IP address. Contact your Management Console ISV for more details.

d. Select **Provisioning Server FQDN**.

i. Enter Provisioning Server FQDN

Default Setting = None, Recommended Setting = Network Dependent

ii. Enter Port.

Default Setting = 0, Recommended Setting = 9971

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.

e. Select **TLS PSK**.

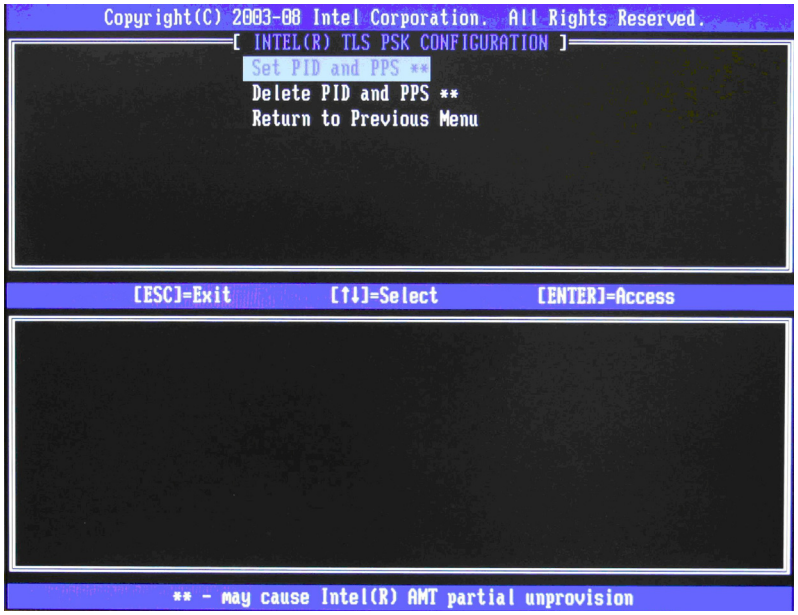


Figure 10 Intel TLS PSK Configuration Screen

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

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. Go to the OEM TLS-PSK section for details.

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

iii. Select **Return to previous menu**.

e. Skip **TLS-PKI**. This option is for Remote Configuration (RCFG) also known as Zero Touch Configuration (ZTC). This option only appears in the Factory or In-Setup phase. Go to the RCFG section for more information.

f. Select **Return to previous menu**.

17. Skip **Un-Provision**. This option returns the system to factory defaults. See the Return to Default section for more information about unprovisioning.

18. **Skip VLAN**.

    Default Setting = Disabled, Recommended Setting = User Dependent

    This option enables or disables VLAN support. If VLAN is enabled, then the VLAN tag must be provided (1-4094).

19. Select **SOL/IDE-R**, and then select **Y**.

    a. A message window indicates that the system resets after configuration.

    b. Select **Username and Password**, and then select **Enabled**.

        Default Setting = Enabled, Recommended Setting = Enabled

        This option allows you to add users and passwords from the WebGUI. If the option is disabled, then only the administrator has MEBx remote access.

    c. Select **Serial Over LAN**, and then select **Enabled**.

        Default Setting = Enabled, Recommended Setting = Enabled

    d. Select **IDE Redirection**, and then select **Enabled**.

        Default Setting = Enabled, Recommended Setting = Enabled

20. Select **Password Policy**.

    Default Setting = Default Password Only, Recommended Setting = Default Password Only

    This option determines if the local MEBx password can be modified from a remote console.

Option	Effect
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.

21. Select **Remote Firmware Update**, and then select **Enabled**.

    Default Setting = Enabled, Recommended Setting = Enabled

    This option enables or disables the ability to remotely update the ME firmware.

22. Skip **Set PRTC**.

    Default Setting = None, Recommended Setting = Current Date and Time

    This option sets the PRTC (Protected Real Time Clock). It is used with TLS mutual authentication, which checks for the client certificate for expiration based on its PRTC. PRTC has a valid date range of 1/1/2004 to 1/4/2021.

23. Select **Idle Timeout.**

    Default Setting = 1, Recommended Setting = 1

    This option sets the timeout value for Wake-On-ME.

The default timeout value is 1 from the factory and is in units of a minute. A value of 0 means the Wake-On-ME feature is disabled and the ME will not go to sleep when not being used in a non-active system. HP recommends a setting of 1 which allows the ME to go to sleep after 1 minute of inactivity.

The timeout value can only be set in decimal notation, which is a minor change from the dc7700p that allowed both 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: Wake-On-ME Explained" on page 35** for an explanation of Wake-On-ME/ME WoL.

24. Select **Return to previous menu**.
25. Select **Exit**, and then select **Y** to exit the MEBx Setup and save settings. The system displays an Intel ME Configuration Complete message (only once) and reboots.
26. Turn off the system and remove power. The system is now in In-Setup Mode and is ready for deployment.
27. Plug the system into a power source and connect the network. Use the integrated Intel 82566DM NIC. Intel AMT does not work with any other NIC solution.

    When power is reapplied to the system, the system immediately looks for a Setup and Configuration Server. If the system finds this server, 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 contains the following information:

    - PID
    - UUID (Universally Unique Identifier)
    - IP address
    - ROM and firmware version numbers

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

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

    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, use TLS if the infrastructure is available. If you do not use TLS, then HTTP Digest will be used for mutual authentication. HTTP Digest is not as secure as TLS.

    Setup and Configuration Server logs into AMT system with the user name and password and provisions all required data items:

    - New PPS and PID (for future Setup and Configuration)

- TLS certificates
- Private keys
- Current date and time
- HTTP Digest credentials
- HTTP Negotiate credentials

You can set other options depending on S&CS implementation.

The system goes from In-Setup phase to Operational phase, and AMT is fully operational. Once in the Operational phase, you can remotely manage the system and you can provide the system to end-users for regular use.

Provisioning Methods

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

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

Legacy

If you want TLS, execute legacy method of AMT set up and configuration on an isolated network separate from the corporate network. An S&CS server requires a secondary network connection to Certification Authority for TLS configuration.

Customers perform legacy AMT set up and configuration. The customer initially receives systems in the Factory phase with AMT disabled. These systems must 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.

IT TLS-PSK

IT TLS-PSK AMT Setup and Configuration is usually performed in a company's IT department.

The following are required:

- Setup and Configuration Server
- Network and security infrastructure

AMT systems in the Factory phase are given to the IT department, which is responsible for AMT set up and configuration. The IT department can use any method to enter in AMT setup information, after which 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 must occur over a network. The network can be encrypted using Transport Layer Security Pre-Shared Key (TLS-PSK) protocol. Once the systems connect to an S&CS, Enterprise mode Configuration occurs.

OEM TLS-PSK

OEM TLS-PSK AMT set up and configuration occurs 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, which will AMT 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 Administrator password, PID, and PPS to use for the order, which HP will use 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 you need 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 AMT Setup systems in the factory and securely provide pre-shared keys. HP offers a secured service that will eliminate manual AMT Setup of each unit at the customer site. Contact HP for more information about this valuable service.

USB Drive Key Set Up and Configuration

You can set up and locally configure password, PID, and PPS information with a USB drive key. This feature allows an IT technician to manually setup and configure systems without the problems associated with manually 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 technician request local setup and configuration records from an S&CS through the console.
3. The S&CS:

   a. Generates the appropriate passwords, PID, and PPS sets.

   b. Stores this information in its database.

   c. Returns 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 technician takes the USB drive key to the staging area where new AMT platforms are located. The technician:

   a. Unpacks and connects platforms, if necessary.

   b. Inserts the USB drive key into a platform.

   c. Turns on that platform.
6. The system BIOS detects the USB drive key.

   a. If found, the BIOS looks for a Setup.bin file at the beginning of the drive key. Skip to Step 7.

   b. If no USB drive key or Setup.bin file is found, then boot normally. Ignore Steps 7-11.

7. The system BIOS displays a message that automatic setup and configuration will occur.
   a. The first available record in the Setup.bin is read into memory. The process:
      i. Validates the file header record.
      ii. Locates the next available record.
      iii. Invalidates current record so it cannot be used again.
   b. The process places the memory address into the MEBx parameter block.
   c. The process calls MEBx.
8. MEBx processes the record.
9. MEBx writes a completion message to display.
10. The IT technician powers down the system. The system is now in In-Setup phase and is ready to be distributed to users in an Enterprise mode environment.
11. Repeat Step 5 if necessary (more than one system).

Refer to your management console supplier for more information on USB drive key set up and configuration.

USB Drive Key Requirements

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

- It must be greater than 16MB.
- 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

Remote Configuration (RCFG) was formerly known as Zero Touch Configuration (ZTC).

RCFG is the ability to use a single OEM image to provision systems securely without the need 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
- Timed network access

One or more hash root certificates are embedded into the AMT firmware. 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. The amount of time is configurable by the OEM.

Remote Configuration: Bare-Metal vs. Delayed

There are two ways to implement Remote Configuration: Bare-Metal and Delayed.

Bare-Metal, as the name implies, is remote configuration of the AMT system without an operating system; in other words, only the hardware. In this implementation, Setup and Configuration is started (Hello message broadcast) as soon as the ME is active and the system is connected to a network. This means that the AMT system is configured without the use of a local agent and does not use One Time Password (OTP) authentication.

Delayed, as the name implies, is remote configuration at a later time when an operating system 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 operating system agents for Delayed remote configuration support.

Remote Configuration Time-outs in HP Systems

The HP Compaq 8000 Elite Business PCs are shipped out of the factory in Bare-Metal mode with the ME set to broadcast Hello messages for 255 hours when the ME is active and the system is connected to a network.

If no SCS responds to the Hello messages within the time-out 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 Prerequisites

RCFG requires certain prerequisites before it can be used.

- 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.
- The AMT system must have at least one pre-programmed active root certificate hash.
- The SCS must have a server certificate with the proper OID or OU values.
  - OID value in the Extended Key Usage field = **2.16.840.1.113741.1.2.3**

    This is the unique Intel AMT OID.
  - OU value in Subject field = **Intel Client Setup Certificate**

    This OU value is case sensitive and must be entered exactly as shown.
- In the case of a Delayed Setup and Configuration, an operating system and local agent must be installed on the AMT system.

MEBx and Hashes

AMT 5.0 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 then type the MEBx password.
2. Select **Intel AMT Configuration**.
3. Select **Setup and Configuration**.
4. Select **TLS PKI**.

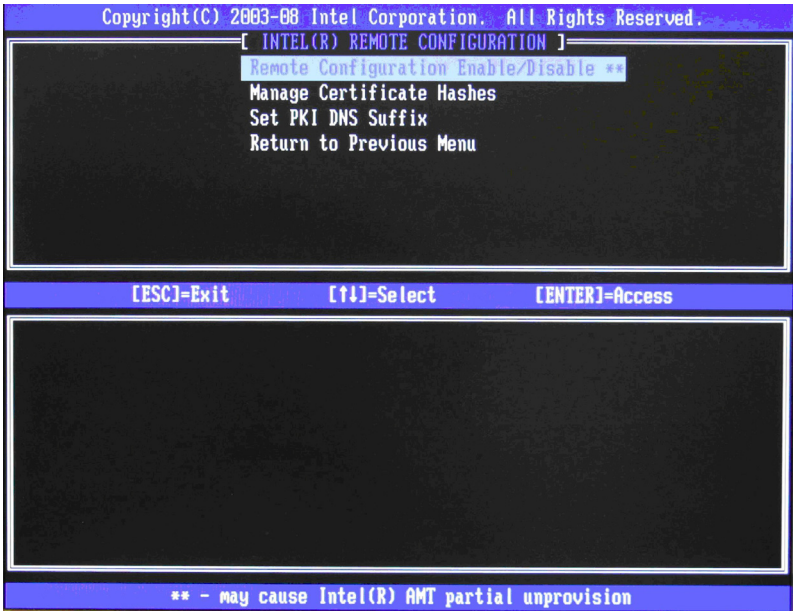


Figure 11 Intel Remote Configuration Screen

1. Select **Remote Configuration Enable/Disable**.

   Default Setting = Enabled, Recommended Setting = Enabled

   This option enables or disables remote configuration.

2. Skip **Manage Certificate Hashes**.

   This option shows the hashes in the system, including the name of the hash and whether it is active.

   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 **Insert**.

   b. Type a name for the hash.

   c. Type the fingerprint of the hash.

   d. Select whether this hash is active. Hashes can be made active, not active, default, or not default in this screen.

3. Set **PKI DNS Suffix**. This option allows you to enter the PKI DNS Suffix of the SCS.

4. Select **Return to the Previous Menu**.

List of Supported CA Certificates

The following list provides supported Certificate Authorities and certificates. Not all certificates are populated in certain configurations.

- VeriSign Class 3 Primary CA-G1
  - SHA1 Fingerprint: 74 2C 31 92 E6 07 E4 24 EB 45 49 54 2B E1 BB C5 3E 61 74 E2
- VeriSign Class 3 Primary CA-G3
  - SHA1 Fingerprint: 13 2D 0D 45 53 4B 69 97 CD B2 D5 C3 39 E2 55 76 60 9B 5C C6
- Go Daddy Class 2 CA
  - SHA1 Fingerprint: 27 96 BA E6 3F 18 01 E2 77 26 1B A0 D7 77 70 02 8F 20 EE E4
- Comodo AAA CA
  - SHA1 Fingerprint: D1 EB 23 A4 6D 17 D6 8F D9 25 64 C2 F1 F1 60 17 64 D8 E3 49
- Starfield Class 2 CA
  - SHA1 Fingerprint: AD 7E 1C 28 B0 64 EF 8F 60 03 40 20 14 C3 D0 E3 37 0E B5 8A

Return to Default

Return to Default is also know as Unprovisioning. An AMT Setup and Configured system can be unprovisioned. It is done through the AMT Configuration Screen and the Un-Provision option.

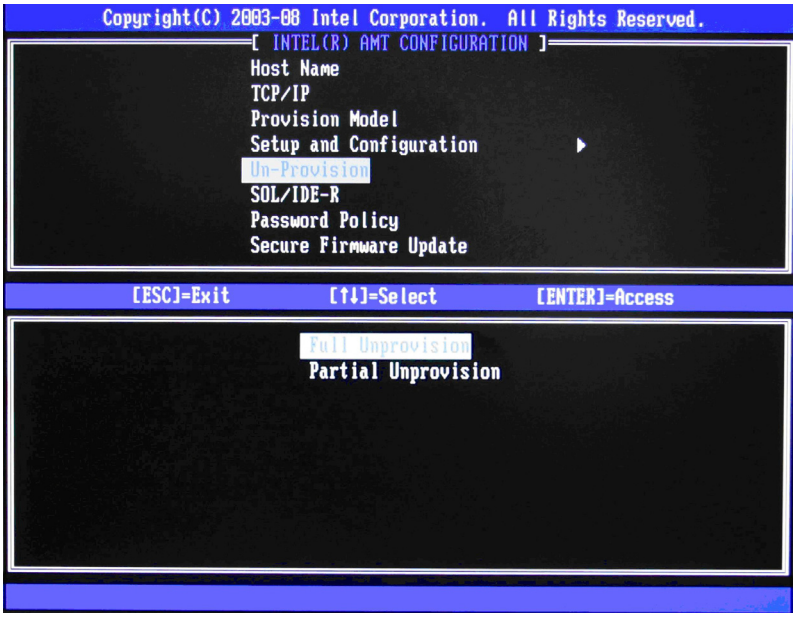


Figure 12 Intel AMT Unprovisioning Screen

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

1. Select **Un-Provision**, and then select the appropriate unprovision mode.

   Full unprovisioning is available for SMB 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 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.

2. Select **Return to previous menu**.
3. Select **Exit**, and then select **Y**.

The system reboots.

A partial unprovisioning will re-open the network interface for six hours of Hello message broadcasts.

Full Return to Factory Defaults

All AMT settings can be returned to the factory default by clearing CMOS. This includes resetting the password to the default "admin". This is a behavior change from the HP Compaq dc7800p Business PC, where a CMOS change only clears the AMT settings and the password.

The system will need to be set up 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 user name 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 AMT 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. 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 Out of Band 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?

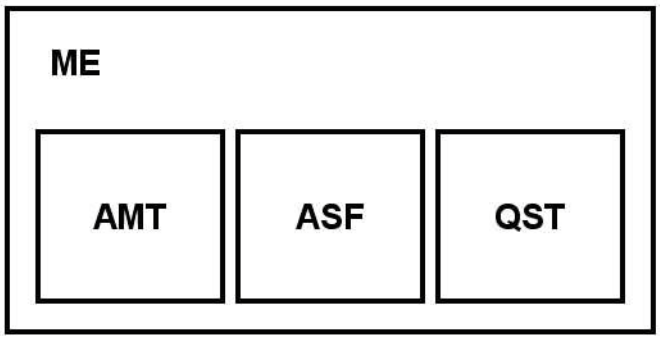
A: The ME is the controller that manages AMT along with ASF and QST. Notice that clearing AMT settings does not affect ME settings since the ME is a separate entity.

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.

Q: Is a graphical representation of the ME and AMT available?

A: Yes.



Appendix B: Power / Sleep / Global States Explained

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

- **S0** is the ON state. The computer 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 Vaux power rail remains powered, while the rest of the system, including the processor, is not powered. When the system resumes from S3, the system context remains intact because 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. Vaux 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 powers 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 AC power from the system by 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.
- **M1** 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 remain active, but it will be in M1 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**.
- **Idle Timeout** setting is set to a non-zero value.

The system must be in a sleep state (S3, S4, or S5) for Wake-On-ME to function. 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.

Idle Timeout must be set to a non-zero value. If it is set to zero, then the Wake-On-ME feature is disabled and the ME will not go to sleep when not being used.

434476-005, 12/2009