Technical white paper

Setting up and configuring Intel AMT in HP Business Notebooks, Desktops, and Workstations

Detailed instructions for the IT professional

Table of contents

Executive summary

Select HP models use Intel® vPro processor technology to simplify PC management and reduce IT-related expenditures. A key element of vPro is Intel Active Management Technology (Intel AMT), a platform-resident solution that includes both hardware and firmware, and relies on the Management Engine (ME) integrated into supported Intel chipsets.

Intel AMT provides out-of-band (OOB) remote access to individual systems regardless of power state or operating system condition – as long as the system is connected to a power source and a network. By default, Intel AMT is inactive; it must be setup and configured in order to enable its capabilities. There are two options for setup and configuration (also known as provisioning):

- Manual mode
- Enterprise mode, using a setup and configuration server (SCS)[1]

This white paper details the manual setup and configuration of a client PC (Intel AMT system), as well as discussing options and providing guidelines for enterprise-mode setup and configuration. Refer to the Intel website www.intel.com/technology/vpro/index.htm for other white papers and technical information on Intel vPro Technology.

Intended audience: This white paper is intended for IT administrators familiar with setting up and configuring manageability features. Basic knowledge of Intel AMT and networking are required.

Introduction

Select HP Workstation, Desktop and Business Notebook PCs utilize Intel vPro Technology to simplify PC management, enhance security, and reduce IT-related expenditures. Intel vPro includes a range of technologies and components, including the following:

- Intel Core™ i5 or i7 processor
- Intel Active Management Technology (Intel AMT), which provides remote access to the PC for management tasks; this hardware- and firmware-based platform relies on the Management Engine featured in certain Intel chipsets
- Remote configuration capabilities
- Wired and wireless connectivity

Resident on each client PC, Intel AMT enables out-of-band (OOB) remote access to the PC, regardless of the system power state or operating system condition – as long as the PC is connected to a power source and a network. By default, Intel AMT is shipped in an inactive state and must be setup and configured[2] in the system before it can be used.

The following methods can be used for Intel AMT setup and configuration:

- Manual mode
- Enterprise mode, using a setup and configuration server (SCS)

Note
The SCS is a software application that is integrated into the remote console being used to manage client PCs. Consult the particular independent software vendor (ISV) for information on deploying an SCS.

---

[1] The SCS is a software application that is integrated with the central management console. Consult the console's independent software vendor (ISV) for information on deploying an SCS.
[2] The setup and configuration process is also known as provisioning.

Support

Intel AMT technology is available on the following select HP models:

Note
Remote access to a client PC can be wired or wireless, depending on the particular HP model.

Note
Wired Intel AMT is supported with Integrated Intel 1217LM Gigabit Network Connection. Wireless Intel AMT is supported with Intel Centrino Advanced-N 6205 or Ultimate-N 6300 802.11a/b/g/n/ac adapters.

- Desktops
  - Wired or wireless: HP EliteDesk 800 G1 Ultra-Slim, Small Form Factor, and Microtower PCs; EliteOne 800 G1 All-in-One PCs
- Workstations
  - Select models

Setting up and configuring Intel AMT

Before it can be used, Intel AMT must be setup and configured, which involves the following activities:

- Setup – Generally performed once in the lifetime of a system, Intel AMT setup involves the steps necessary to enable Intel AMT, such as setting up the system and enabling network connectivity. After Intel AMT has been enabled, it can be discovered by management software over a network.
- Configuration – After setting up Intel AMT, you can now configure a range of options that may be changed many times over the system's lifecycle, such as enabling the system for Serial-Over-LAN (SOL) or IDE-Redirect (IDE-R). Changes can be made to the system locally or through a remote console.

Setup and configuration phases

The setup and configuration process involves the following phases:

- Factory

  In Factory phase, the system is initially as received from the factory; no Intel AMT setup and configuration has been performed. In this phase, you can only access Intel AMT locally, through the Intel Management Engine BIOS Extension (MEBx).[3]

  Factory phase ends when the following occurs:

  – Manual mode – You have changed the default password.

  – Enterprise mode – You have changed the default password and set the Provisioning ID (PID) and Provisioning Passphrase (PPS).
- In-Setup

  The In-Setup phase is used to set most Intel AMT options,[4] either manually or automatically, using an SCS.
- Operational

  The Operational phase is the final phase. Intel AMT has been fully setup and configured, making the system ready for normal use.

Manual mode setup and configuration

The Manual mode for Intel AMT setup and configuration is intended for customers that do not have an SCS or the necessary network and security infrastructures to use encrypted Transport Layer Security (TLS). Here, setup and configuration is performed manually through the MEBx.

Because less infrastructure is required, Manual mode is easier to implement than Enterprise mode; however, Manual mode is less secure because network traffic is unencrypted.

Note
HP recommends performing a Manual mode setup and configuration in a closed network.

The remainder of this section provides prerequisites and guidelines for Manual mode setup and configuration.

Note
The MEBx is not HP-specific and contains options that are not used by HP. Do not change unused options from their default state.

---

[3] The MEBx is an optional ROM module that is provided by Intel to HP for inclusion in the HP system BIOS.
[4] This process is also known as provisioning.

Creating a password

To reduce vulnerability to a dictionary attack, MEBx enforces the following minimum criteria for a password:

- 8 – 32 characters long
- Upper- and lower-case Latin characters (for example: A, a, B, b)
- At least one digit (for example: 0, 1, 2, … , 9).
- One of the following non-alphanumeric characters:
  - Exclamation !
  - At @
  - Number #
  - Dollar $
  - Percent %
  - Caret ^
  - Asterisk *

  Note that the underscore character (_) is considered alpha-numeric.

  The following characters are not allowed:
  - Quotation mark “
  - Apostrophe ‘
  - Comma ,
  - Greater than >
  - Less than <
  - Colon :
  - Ampersand &
  - Space

BIOS prerequisites

For best performance and to take advantage of AMT 9.x features, make sure the PC meets the following prerequisites:

- System BIOS 1.00 or later
- Intel AMT Management Engine firmware (ME FW) level 9.0.5.1367 or later
- MEBx 9.0.0.0024 or later

The system BIOS and ME FW must be updated individually. For more information on flashing the system BIOS and ME FW, refer to the BIOS Flash white paper. Use the following steps to locate the document that applies to your particular system:

1. Go to www.hp.com.
2. Select **Support & Drivers**.
3. Select **Support & Drivers**.
4. Select **Product Support & Troubleshooting**.
5. Enter the particular product name/number and click **Search**.
6. Select the **Manuals** link under **Resources**.
7. Select **White Papers**.

Note
Intel AMT 9.x allows certain versions of ME FW to be downgraded to earlier versions, which may be useful for troubleshooting purposes.

Setup and configuration procedure

When you explore MEBx options for the first time (Factory phase), default settings are in place. This white paper details the settings recommended by HP, some of which may be the same as the default selections.

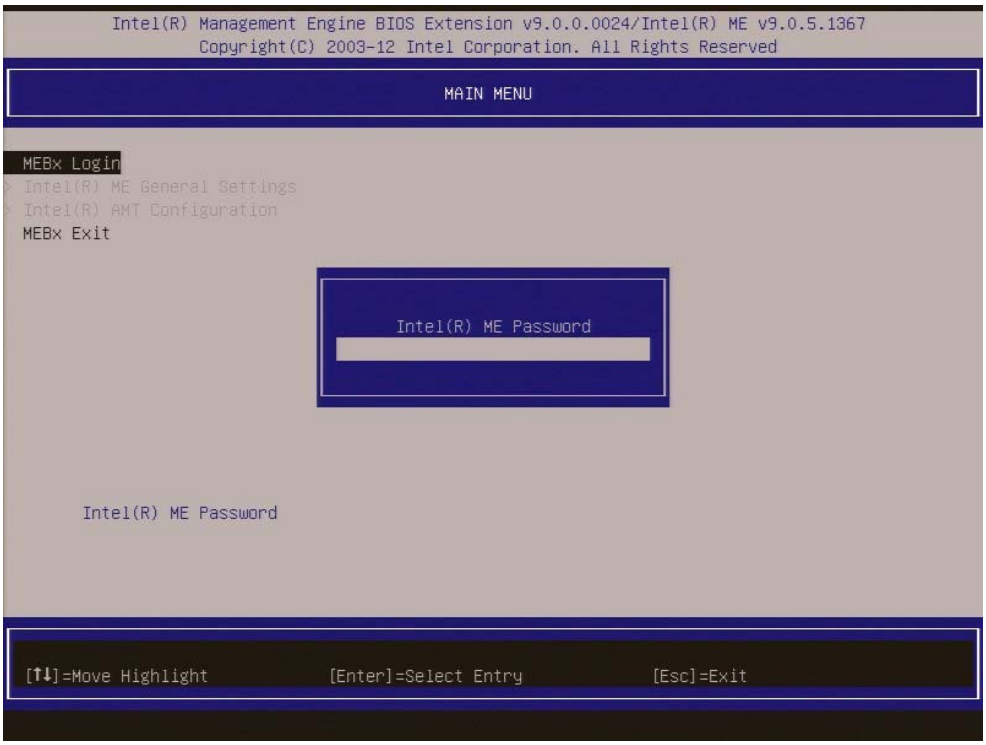
Even though the default setting is used for many options, it is good practice to double-check important options.

For setup and configuration, perform the following procedure:

1. Enter the main menu for MEBx setup (shown in Figure 1) by selecting **Esc** from the startup menu. Alternatively, you could press **F6** (notebook PCs) or **Ctrl-P** (desktop PCs) during POST.

Note
For desktop PCs, by default, the **Ctrl-P** prompt is not displayed on the HP splash screen. This prompt can be displayed during POST if set in F10 Setup.
Workstation PCs do not provide a BIOS option to display the Ctrl-P prompt.

Figure 1. Selecting the MEBx password



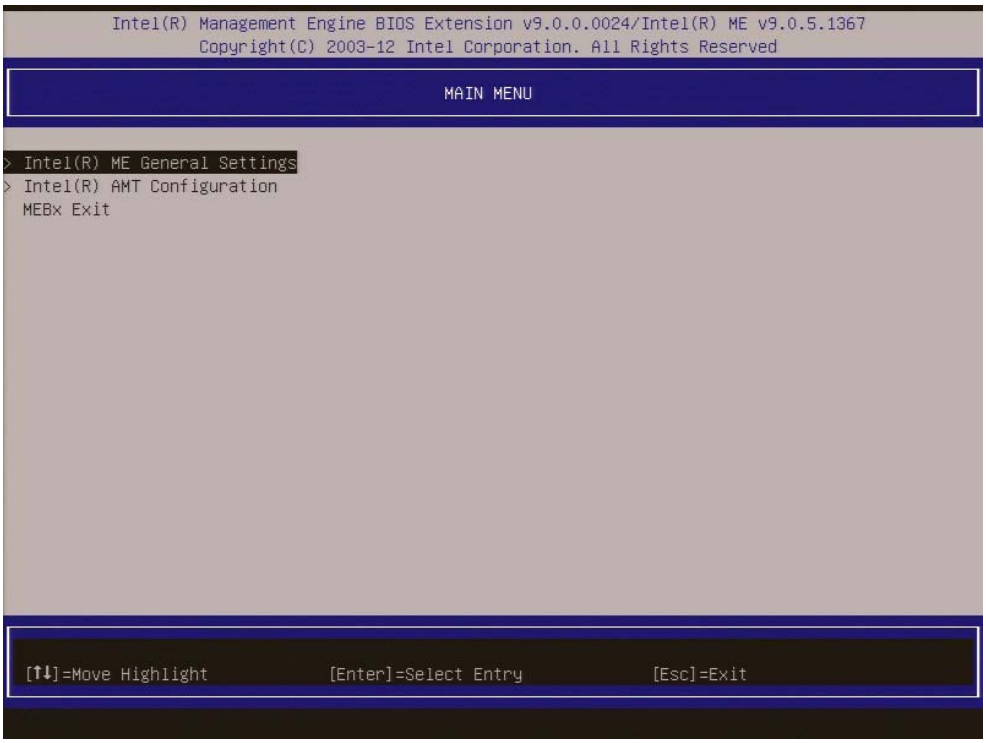
2. Select **MEBx Login** and enter the case-sensitive, default password (**admin**), which must be changed before making any changes in the MEBx.
3. Provide a strong, new MEBx password using the criteria listed in Creating a password. Repeat the password for verification.

   Changing the password establishes Intel AMT ownership and moves the system from Factory to In-Setup phase. As a result, ME and Intel AMT options are now accessible within the MEBx; the system can be accessed via the Intel AMT WebUI (WebUI).

Note
For information on using the WebUI, refer to Using the WebUI.

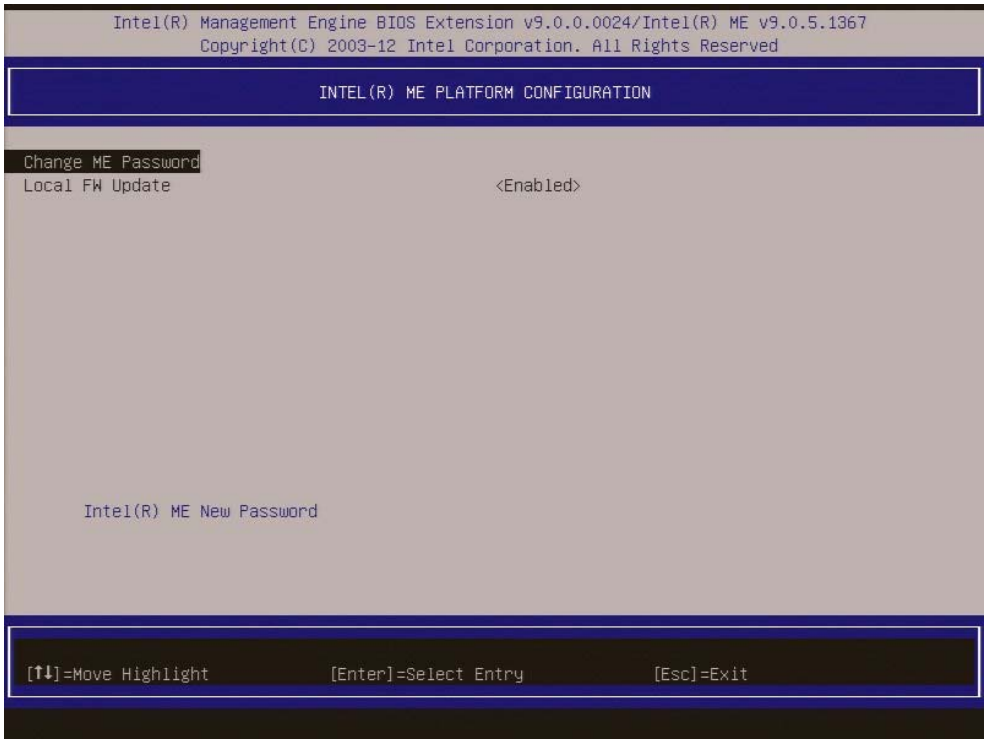
4. From the MEBX main menu, select **Intel ME General Settings**, as shown in Figure 2.

Figure 2. Selecting the Local FW Update option



5. Select **Local FW Update** from the Intel ME Platform Configuration menu.

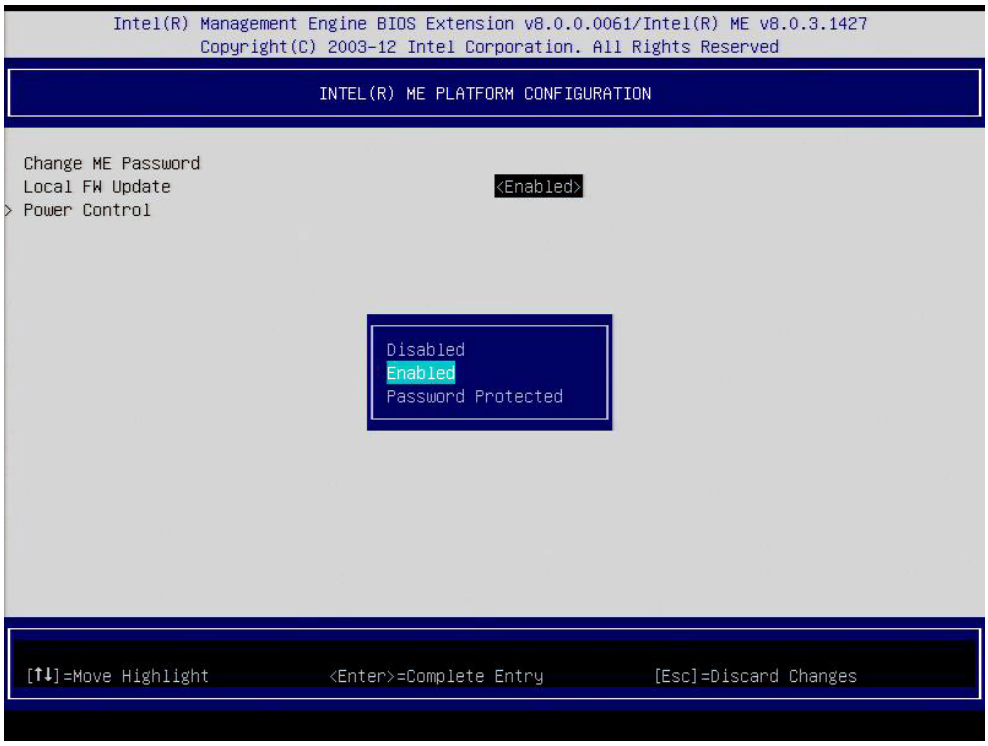
Figure 3. Selecting the **Local FW Update** option



6. As shown in Figure 4, HP recommends enabling **Local FW Update**, which is the default setting.

   Unless otherwise specified, the system BIOS allows ME FW to be updated locally without password protection. If desired, you can modify the **Local FW Update** setting to enable password protection.

Figure 4. **Local FW Update** has been enabled



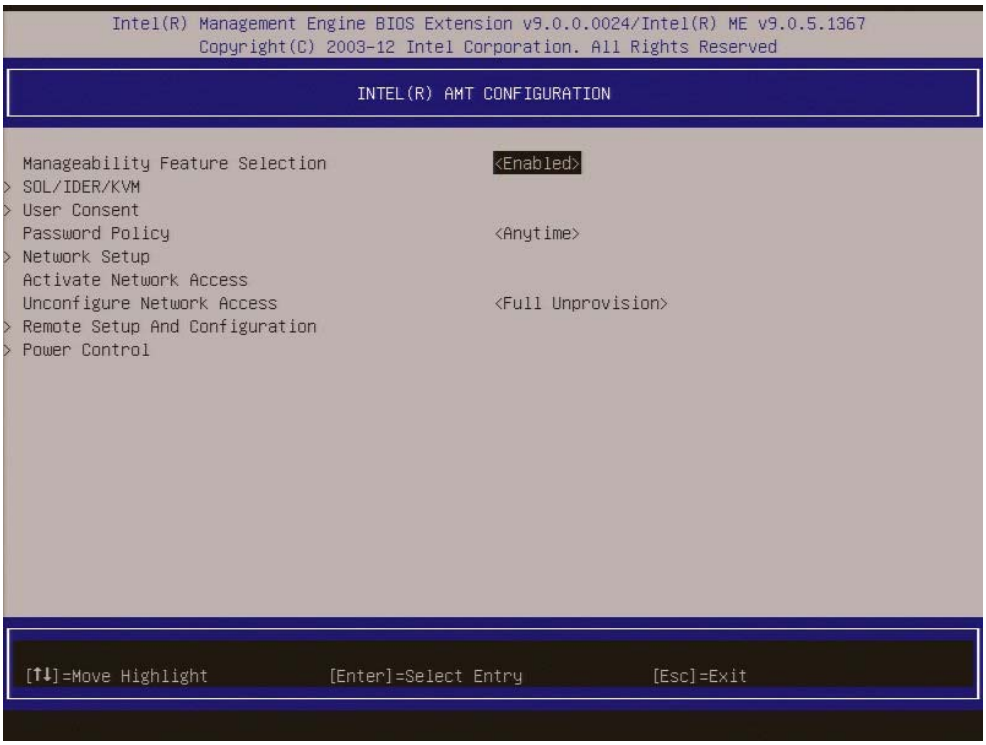
7. Return to the MEBx Main Menu (Figure 1).
8. Select **Configure Intel AMT**.

9. From the Intel AMT Configuration menu (shown in Figure 5), select **Manageability Feature Selection**.

   This option allows Intel AMT to be enabled (recommended) or disabled. By default, HP systems are set to enable Intel AMT.

   Note that disabling **Manageability Feature Selection** also disables all remote management capabilities and unprovisions any Intel AMT settings.

Figure 5. Enabling Intel AMT via the **Manageability Feature Selection** setting



10. From the Intel AMT Configuration menu, select **SOL/IDER/KVM**.

The SOL/IDER/KVM screen appears, as shown in Figure 6. Review the following settings:

- **Username and password**: **Enabled** (Recommended setting; default)

  When enabled, this setting allows users and passwords to be added via the WebUI; if it is disabled, only the administrator has MEBx remote access.
- **SOL**: **Enabled** (Recommended setting; default)

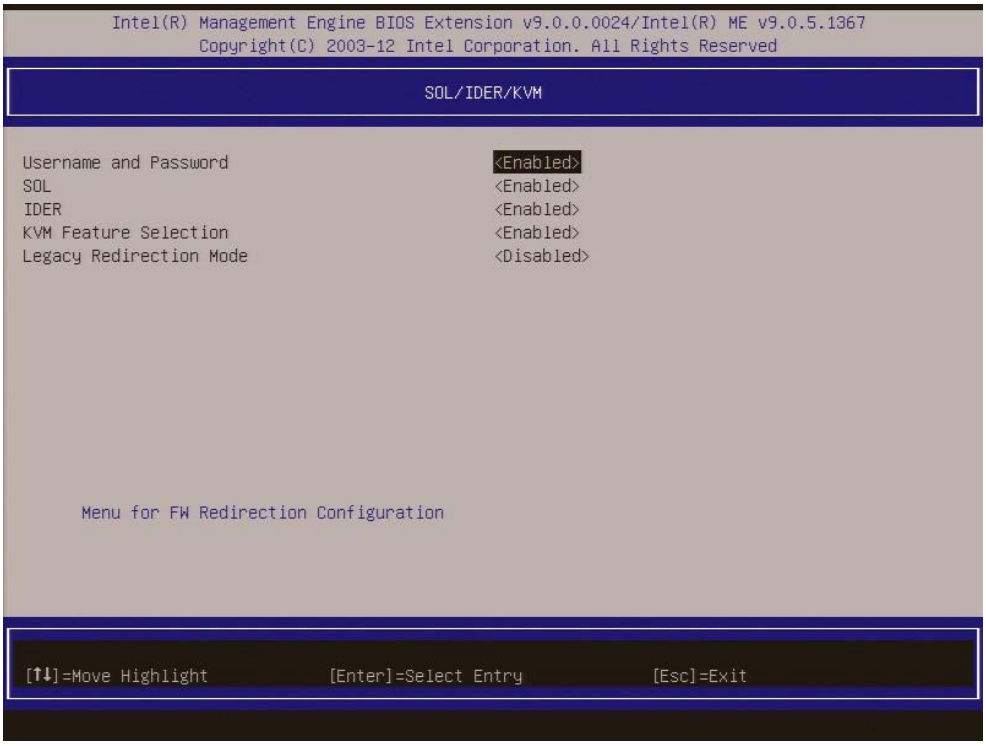
  This setting enables or disables Serial-over-LAN (SOL) functionality.
- **IDER**: **Enabled** (Recommended setting; default)

  This setting enables or disables IDE Redirection (IDE-R) functionality.
- **Legacy Redirection Mode**: **Disabled** (Recommended setting; default)

  This setting allows the redirection feature to work with a pre-Intel AMT 6.0 SCS.
- **KVM Feature Selection**: **Enabled** (Recommended setting; default)

  This setting enables or disables the keyboard/video/mouse feature.

Figure 6. Configuring SOL/IDER/KVM settings



11. From the Intel AMT Configuration menu, select **User Consent**.

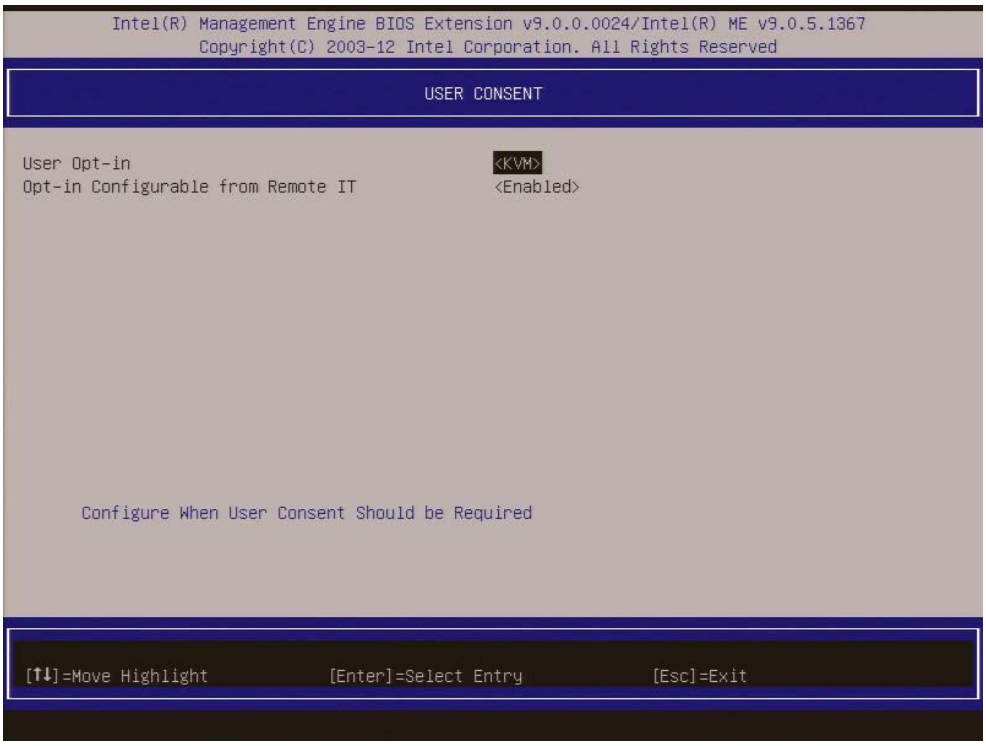
    The User Consent screen appears, as shown in Figure 7. Review the following settings:

    – **User Opt-in**: **KVM** (Setting is user-dependent; **KVM** by default)

    – **Opt-in Configurable from Remote IT**: **Enabled** (Setting is user-dependent; **Enabled** by default)

      This setting enables or disables a remote user's ability to select user opt-in policy. If set to disabled, only the local user can control the opt-in policy.

Figure 7. Configuring user consent



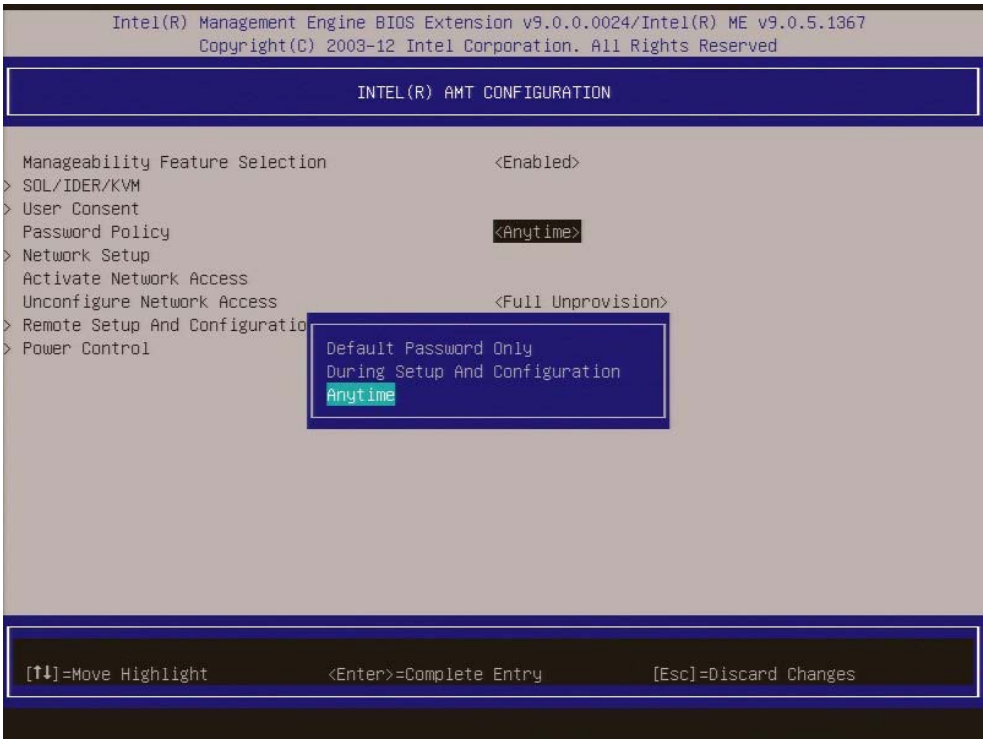
12. Review the **Password Policy** setting shown in the Intel AMT Configuration screen.
    This setting specifies when it is possible to change the MEBx password over the network.

Note
The MEBx password can always be changed locally through the MEBx user interface.

As shown in Figure 8, options are:

- **Default Password Only**
  You can change the MEBx password via the network interface if the default password has not yet been changed.
- **During Setup and Configuration**
  You can change the MEBx password via the network interface during the setup and configuration process but at no other time. Once setup and configuration is complete, the password cannot be changed via the network interface.
- **Anytime** (recommended; default setting)
  You can change the MEBx password via the network interface at any time.

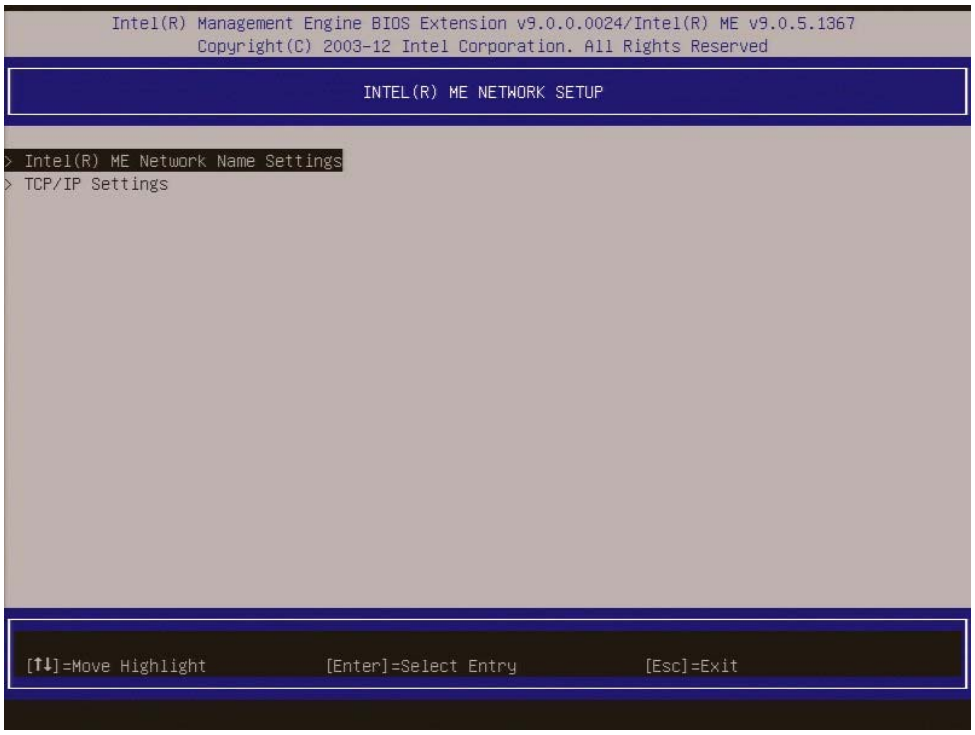
Figure 8. Setting the password policy



13. Select **Network Setup** from the Intel AMT Configuration menu.

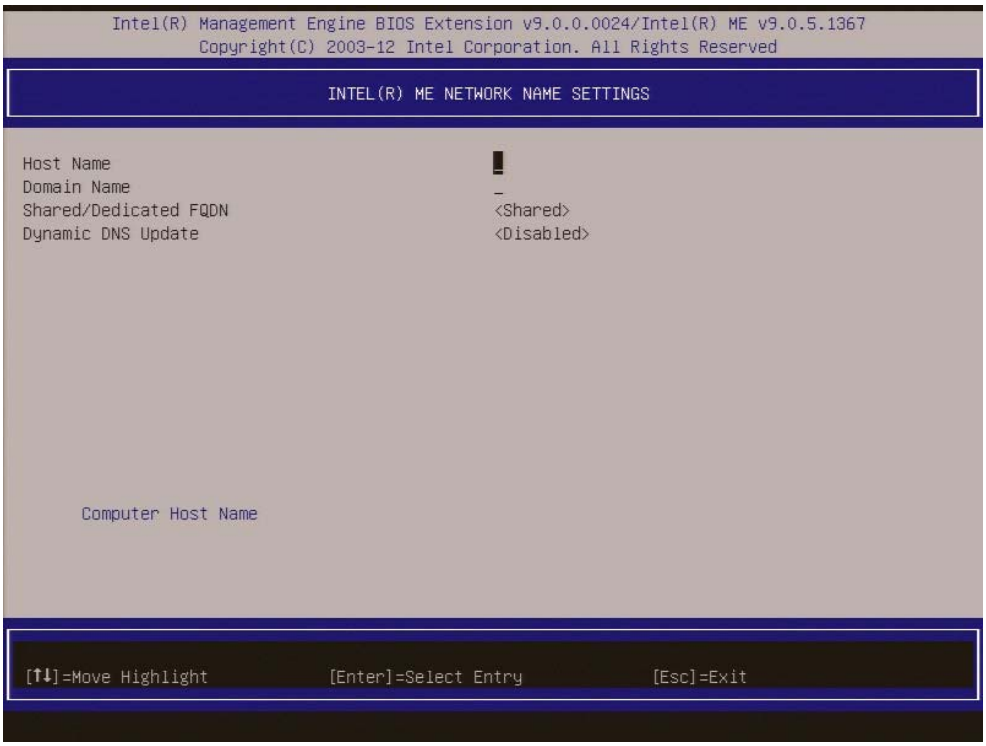
    The Intel ME Network Setup screen appears, as shown in Figure 9, allowing you to configure Intel AMT so that it can be accessed by a remote system.

Figure 9. Initiating the setup of the ME network



14. Select **Intel ME Network Name Settings** from the Intel ME Network Setup menu.
    The Intel ME Network Name Settings screen appears, as shown in Figure 10.

Figure 10. Setting up the ME network names



Review the following settings:

– **Host Name**: (Setting is user-dependent; there is no default)
  Host names can be used in place of the system's IP address for any application that requires this address.

Note
Spaces are not acceptable in a host name.
Make sure there is not a duplicate host name on the network.

– **Domain Name**: (Setting is network-dependent; there is no default)
  If a domain name is not specified, then the default domain name of **Provisionserver** will be used when connecting to the SCS.
  If a domain name is not specified and the domain name for the SCS is not **Provisionserver**, you must set up an alias in the DHCP server to redirect the connection for **Provisionserver** to the appropriate domain.
  If a domain name is specified, then that domain will be used. However, if there is no response after four DNS queries to the specified domain, **Provisionserver** will be used instead.

– **Shared/Dedicated FDQN**: **Shared** (Recommended setting; default)
  This setting determines whether the Intel ME Fully Qualified Domain Name (FQDN) – that is, the HostName. DomainName – is shared with the operating system or is in a separate domain.

– **Dynamic DNS Update**: **Disabled** (Recommended setting; default)

If Dynamic DNS (DDNS) update is enabled, the firmware will actively try to register its IP addresses and FQDN in DNS using DDNS update protocol. You must set the appropriate host and domain names; in addition, the MEBx menu displays the following options:

- **Periodic Update Interval**: Specify a time from 20 to 1,440 minutes
- **TTL** (time-to-live): Specify a time in seconds

If DDNS update is disabled, the firmware will make no attempt to update DNS using DHCP option 81 or DDNS update protocol.

If DDNS update has not been set (that is, it is neither enabled nor disabled), the firmware will use DHCP option 81 for DNS registration; it will not directly update DNS using DDNS update protocol.

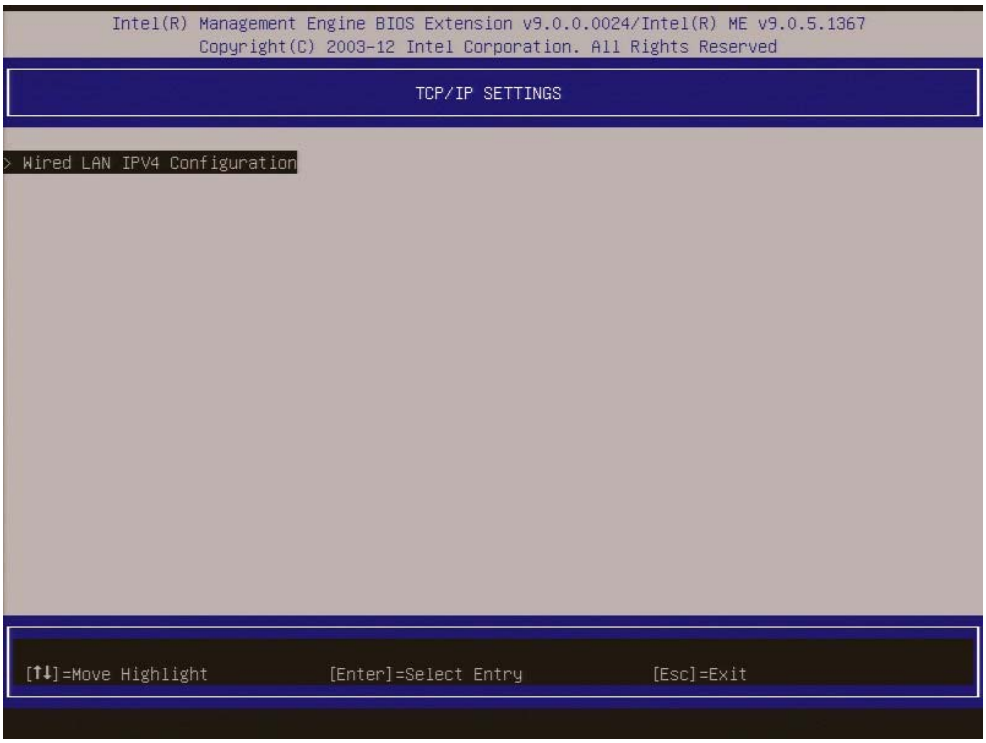
15. At the Intel ME Network Setup menu (Figure 9), select **TCP/IP Settings**. The TCP/IP Settings screen appears, as shown in Figure 11.

    Intel AMT 9.x supports Internet Protocol version 4 (IPv4) and IPv6 interfaces, which are set up differently:

    – **IPv4**: See Configuring IPv4.

    – **IPv6**: The IPv6 option has been removed from the MEBx in Intel AMT 9.x. IPv6 (wired or wireless[5]) can be configured from an SCS or the WebUI. See Configuring IPv6.

Figure 11. Configuring TCP/IP settings

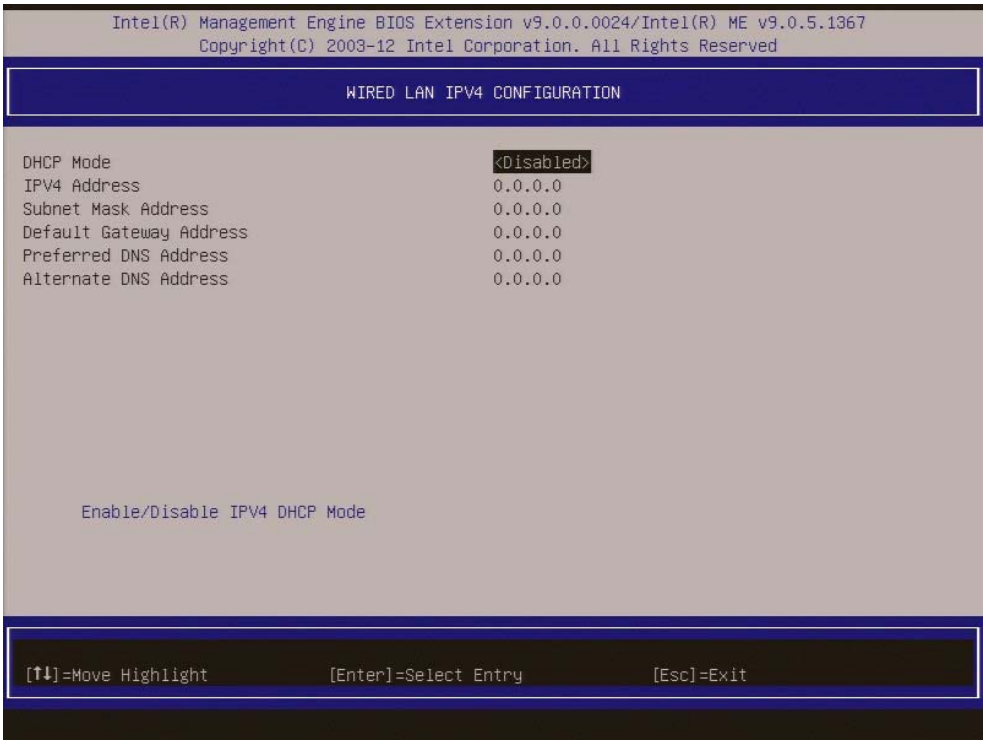


[5] Wireless Intel AMT support is not provided on HP Workstation PCs.

Configuring IPv4

Select **Wired LAN IPV4 Configuration** and then configure the parameters shown in Figure 12.

Figure 12. Configuring the network for IPv4



- **DHCP Mode**: **Enabled** (Recommended setting; default)

  If DHCP is enabled (recommended), skip to Step 16.

  If DHCP is disabled, complete steps (i) – (v) of Implementing wireless connectivity for Intel AMT to configure an IPv4 static IP address for Intel AMT.
- **IPV4 Address**: (Network-dependent; default is **0.0.0.0**)

  Specify the desired static IP address (such as **192.168.0.1**). Ensure that each Intel AMT system has a unique IP address. Multiple systems sharing the same IP address may result in network collisions that would cause the systems to respond incorrectly.
- **Subnet Mask Address**: (Network-dependent; default is **255.255.255.0**)
- **Default Gateway Address**: (Network-dependent; default is **0.0.0.0**)
- **Preferred DNS Address**: (Network-dependent; default is **0.0.0.0**)
- **Alternate DNS Address**: (Network-dependent; default is **0.0.0.0**)

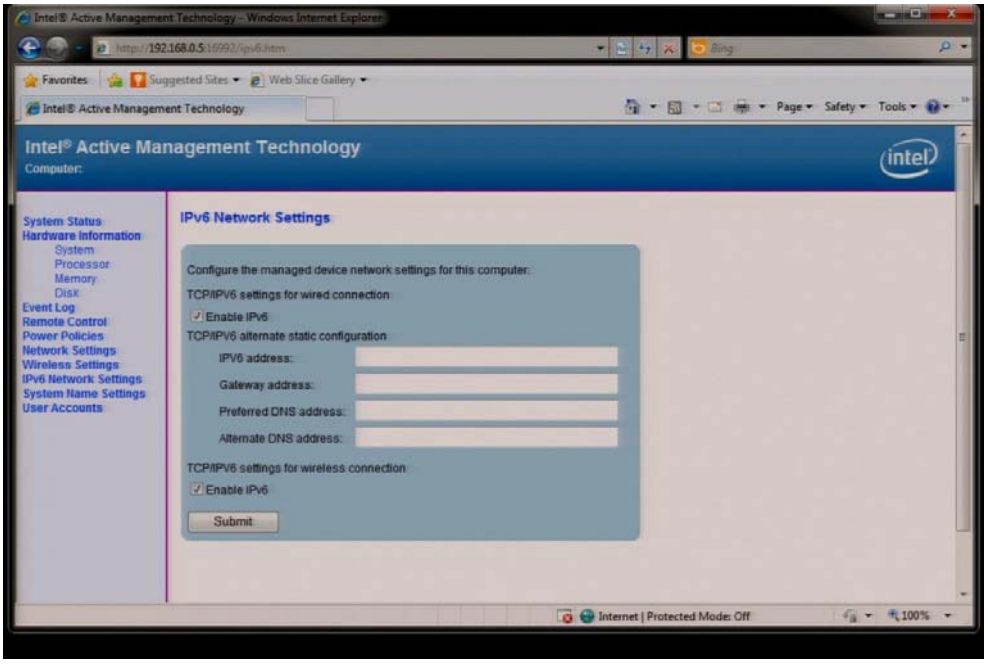
Configuring IPv6

Both wired and wireless[6] IPv6 can be enabled via an SCS or, as in this example, the WebUI.

Review the **TCP/IPv6** settings for **wired** and **wireless** connections, as shown in Figure 13:

- **Enable IPv6 (wired)**: **Enabled** (Recommended setting; default setting is **Disabled**)
- **Enable IPv6 (wireless)**: (Implementation-dependent; default setting is **Disabled**)

Figure 13. Configuring wired and wireless networks for IPv6 via the WebUI



Implementing wireless connectivity for Intel AMT

Consider the following caveats:

- For desktop PCs, wireless Intel AMT is supported on EliteDesk 800 G1 Ultra Slim, Small Form Factor, and Microtower systems, and EliteOne 800 G1 All-in-One systems using the Intel Centrino Advanced-N 6205 mini PCI wireless LAN card or the add-on PCI Express x1 option card with Intel Centrino Advanced-N 6205.
- For business notebook PCs, wireless Intel AMT is supported on Intel Centrino Advanced-N 6205/6235 and Intel Dual Band Wireless-N 7260 802.11 adapters, and Intel Dual Band Wireless-AC 7260 802.11a/b/g/n/ac adapters; wired Intel AMT is supported on Integrated Intel 1217LM and 1218LM Gigabit Network Connection.
- Intel AMT only supports DHCP and does not support static IP addresses.
- Wired and wireless Intel AMT traffic cannot travel on the same subnet concurrently.

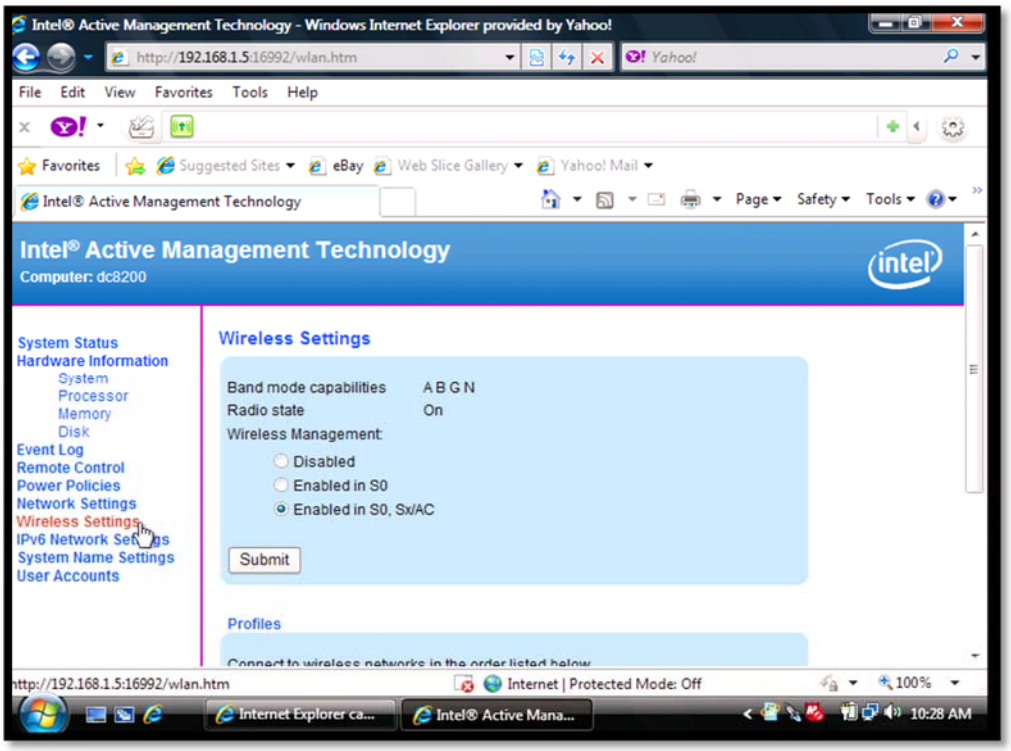
[6] Wireless Intel AMT support is not provided on HP Workstation PCs.

If you wish to use wireless Intel AMT connectivity, you must first connect to the Intel AMT system from a remote system using wired LAN in order to create a wireless profile. Carry out the following steps:

i. Using the WebUI (for example), select the **Wireless Settings** option to configure the wireless management settings, as shown in Figure 14.

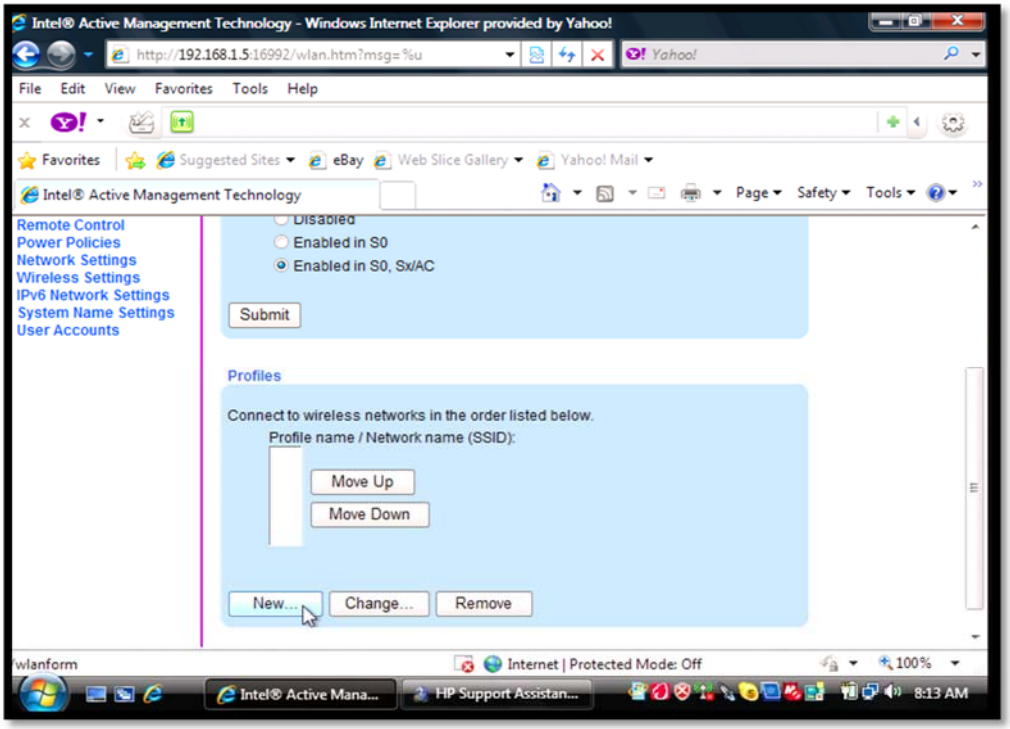
ii. Select the **Wireless Settings** option to configure wireless power policy. Set **Enabled in S0, Sx/AC**.

Figure 14. Specifying wireless power policy



iii. In the **Profiles** field box (Figure 15), click **New** to create a new wireless profile.

Figure 15. Selecting **New** to create a new wireless profile

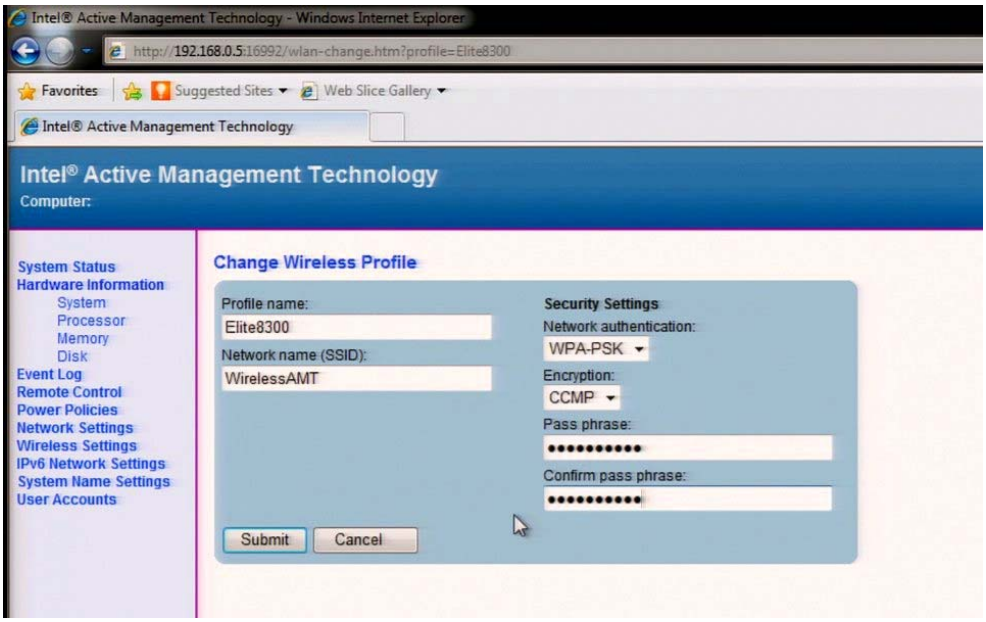


iv. Enter the following data for the new wireless profile, as shown in Figure 16:

- **Profile name**: (any name)
- **Network name (SSID)**: (the wireless network SSID name)
- **Network authentication**: (implementation-dependent; default is **WPA-PSK**)
- **Encryption**: **CCMP** (recommended setting; default)
- **Pass phrase**: (wireless network pass phrase)

On completion, click **Submit**.

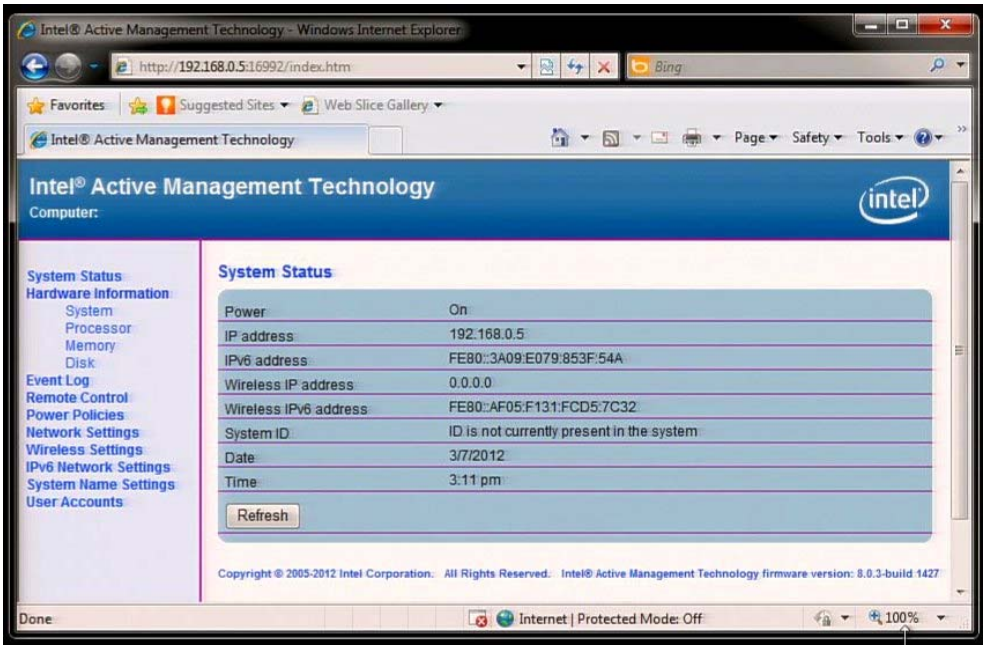
Figure 16. Configuring a new wireless profile



v. Select **System Status** to display the Wireless IP address, as shown in Figure 17.

Note
Wireless Intel AMT only supports IPv6 addresses.

Figure 17. Verifying that you have configured a wireless IP address

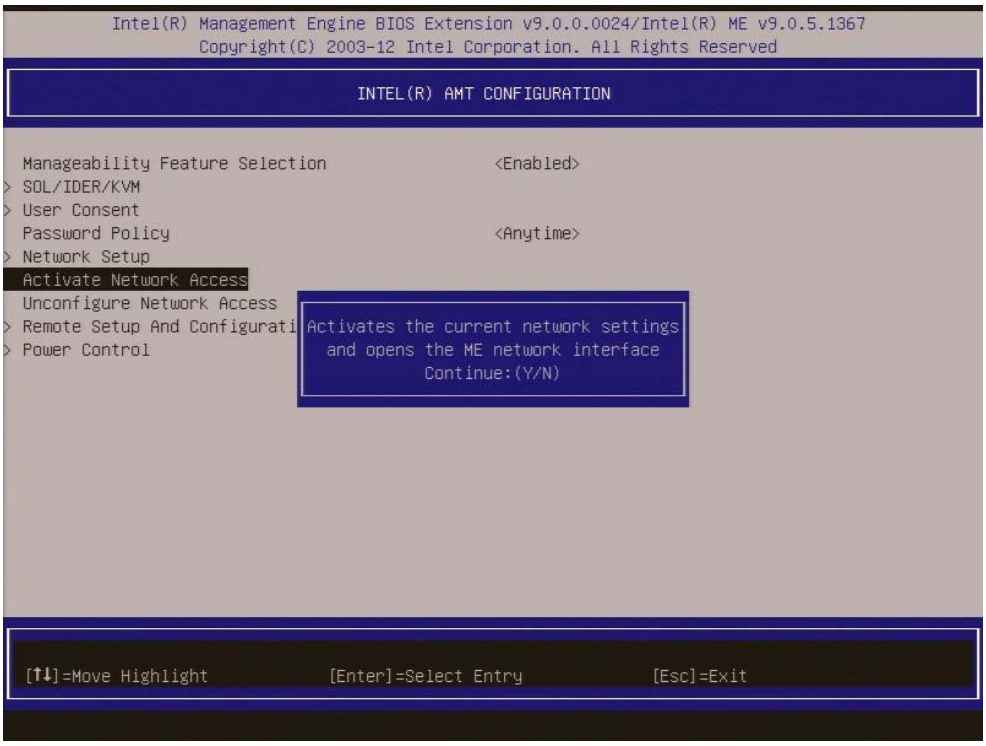


A remote system should now be able to access the ME.

16. Having completed the network setup, select **Activate Network Access** from the Intel AMT Configuration menu, as shown in Figure 18. This setting causes the ME to transition to the newly-provisioned state if all required settings have been configured.

    The **Unconfigure Network Access** option causes the ME to transition to the pre-provisioned state. For more information, refer to Unprovisioning an Intel AMT system or Making a full return to factory default settings.

Figure 18. Transitioning the ME to the newly-provisioned state



17. When MEBx displays **Update Network Settings** in the **General Settings** menu, press **Enter**.
18. At the MEBx CAUTION prompt, press **Y**.

19. Select **Power Control** from the Intel AMT Configuration menu (shown in Figure 19). Select the appropriate **Intel AMT ON in Host Sleep States** setting, as shown in Figures 20 and 21.

Figure 19. Selecting Power Control

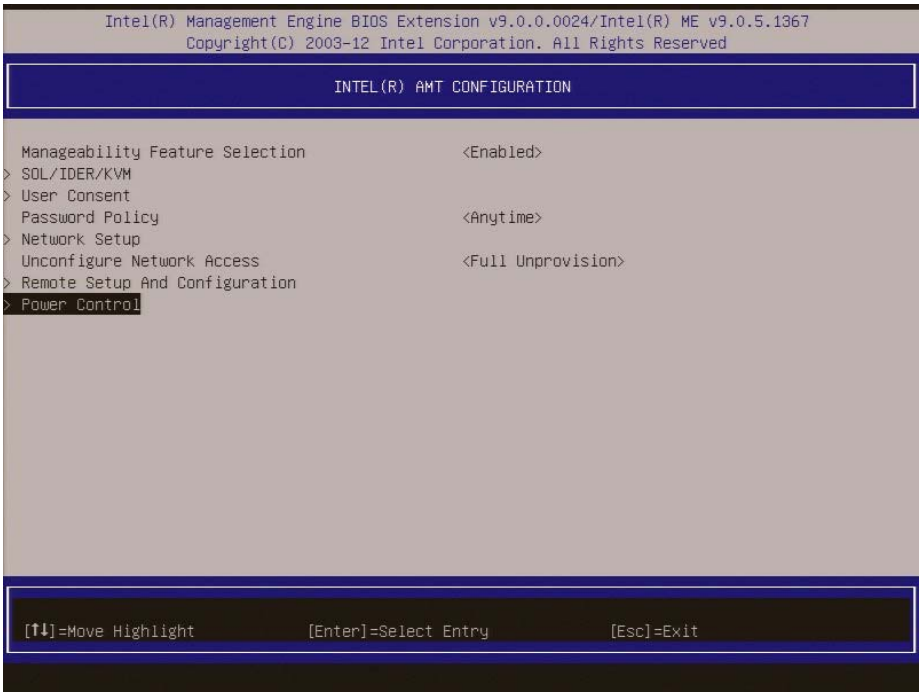


Figure 20. Current **Intel AMT ON in Host Sleep States** setting

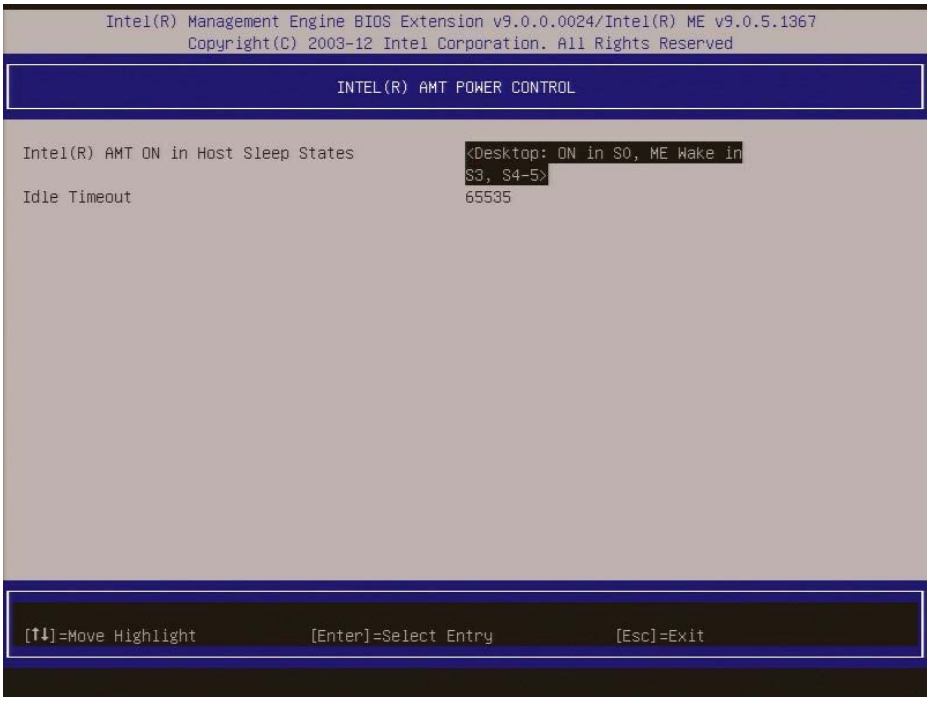
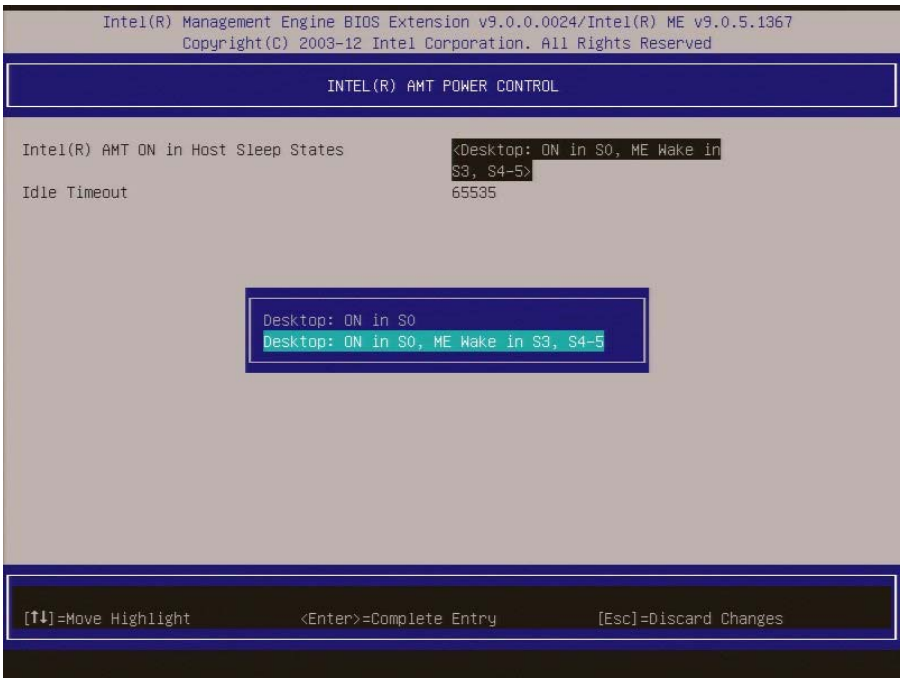


Figure 21. Options for **Intel AMT ON in Host Sleep States** setting



Recommended setting: **Desktop: ON in S0, ME Wake in S3, S4-5**

Note

After you activate network access (Step 16), **Intel AMT On in Host Sleep States** is automatically set to **Desktop: ON in S0, ME Wake in S3, S4-5**.

Note

For more information on sleep states and Wake-On-ME, refer to Appendix B: Overview of power, sleep, and global states and Appendix C: Wake-On-ME overview, respectively.

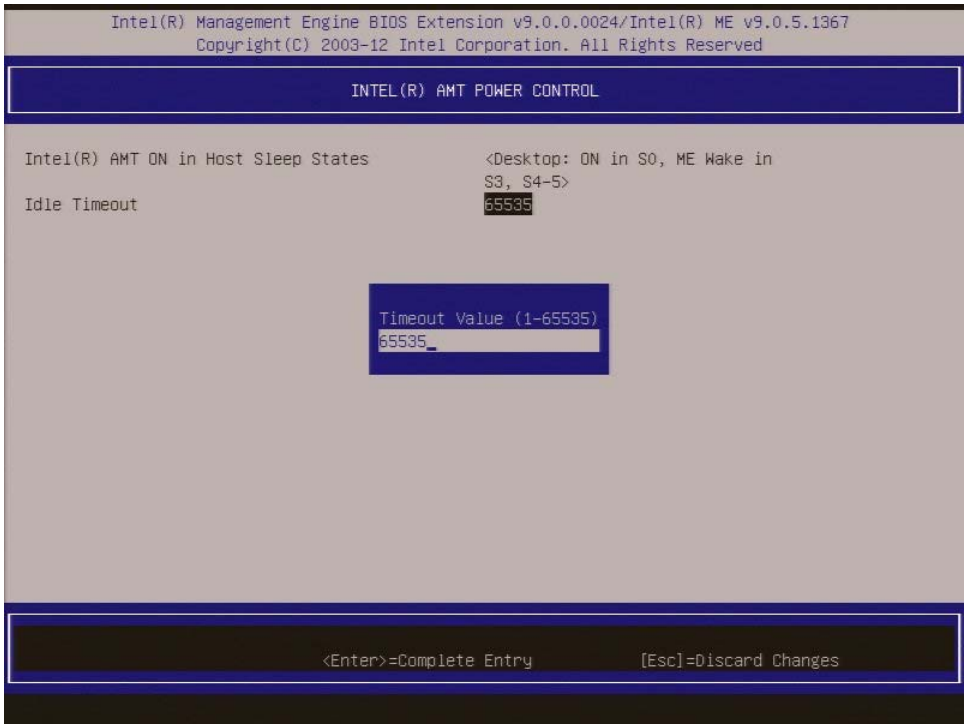
---

20. Select the appropriate **Idle Timeout value** for Wake-On-ME in minutes, as shown in Figure 22.
    - **Idle Timeout**: **65535** (Recommended setting; default)

    The timeout must be set to a non-zero value for the ME to take advantage of Wake-On-ME.

    The timeout is not used when the system is in active state (S0); it is only used when the **AMT ON in Host Sleep States** setting is configured to allow Wake-On-ME.

Figure 22. Selecting the **Idle Timeout** value



21. Press the ESC key to return to the MEBx Main Menu and select **MEBx Exit** to exit the MEBx setup and save settings. The system will reboot.

Once the system reboots, it changes from Intel AMT In-Setup phase to Operational phase. Now, the system can be remotely managed through the WebUI or a remote console and can be provided to the end-user for regular use.

Using the WebUI

The WebUI is a browser-based interface that provides limited support for remote system management. It is often used to verify that Intel AMT setup and configuration has been performed properly on a system. Obtaining a successful connection between a remote system and the system running the WebUI indicates proper Intel AMT setup and configuration on the remote system.

The WebUI is accessible from the following web browsers:

- Microsoft Internet Explorer 6 SP1 or newer
- Mozilla Firefox

Remote system management capabilities include:

- Hardware inventory
- Event logging
- Remote system reset
- Updating network settings

- Adding new users and passwords
- Updating ME firmware

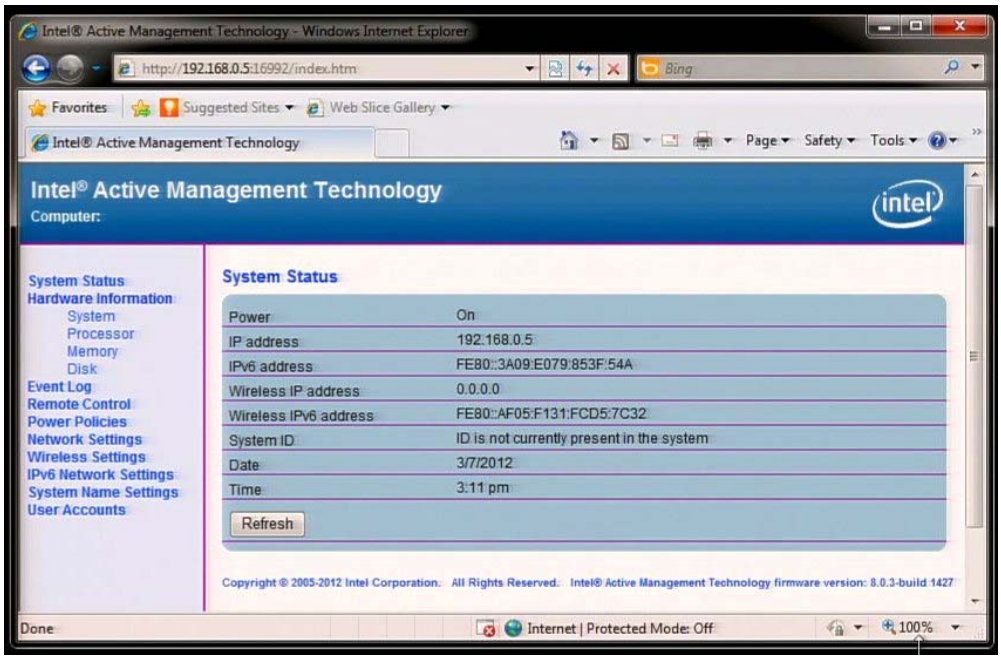
WebUI support is enabled by default for Manual mode setup and configuration.

Connecting with the WebUI in Manual mode

1. Power on an Intel AMT system that is in its operational phase.
2. Invoke a web browser on a separate system (such as a management PC) that is on the same subnet as the Intel AMT system.
3. Connect to the Intel AMT system using the IP address and port specified in the MEBx.
   - By default, the port is 16992
   - If DHCP has been specified, then use the Fully Qualified Domain Name (FQDN) for the ME, which is a combination of the hostname and domain as in the following examples:
     - **IPv4 address**: http://192.168.0.1:16992
     - **Host names** (see Host Name) http://hpsystem.hp.com:16992
     - **IPv6 address**: http://[2001:ABC::ABC]:16992

   The remote system makes a TCP connection to the Intel AMT system and accesses the top-level web page embedded within the ME.
4. Enter your username and password. The default username is **admin**, while the password is the one specified during ME setup. After login, the System Status screen appears, as shown in Figure 21.

Figure 21. The WebUI System Status screen



5. Review the system information and make any necessary changes.

Note

You can use the WebUI to change the MEBx password (see Creating a password) for the remote system.
Changing a password in the WebUI or SCS results in the creation of two passwords for Intel AMT setup and configuration, with the new credential being known as the **remote MEBx password**.
The remote MEBx password only works remotely with the WebUI or SCS. The local MEBx password does not change.
If you create a remote MEBx password, you must now keep track of two passwords.
When the MEBx password is initially set in Intel AMT setup, it serves as both a local and remote password. In this scenario, passwords are synchronized; if you create a remote password, the passwords are now out of sync.

6. Exit.

Enterprise mode setup and configuration

This section provides instructions and guidelines for Intel AMT setup and configuration (provisioning) in Enterprise mode.

Intel AMT is designed to support a range of SMB and enterprise provisioning scenarios that involve tradeoffs between security, cost, and convenience. At one end of the spectrum, it is possible to manually configure Intel AMT in a matter of minutes on a local machine. Alternatively, it is possible to configure a vast array of machines with Intel AMT in a large enterprise environment without physically touching these machines once; moreover, they can be configured in such a way that the process is trusted and secure, and not vulnerable to being attacked or snooped on by malware or prying eyes.

SMBs can perform all setup and configuration tasks manually, with no need for third-party software. However, enterprise IT departments typically automate the provisioning process by allowing Intel AMT systems to connect over the network to a setup and configuration server (SCS) application (such as Symantec Notification Server, LANDesk Management Suite, or Microsoft System Center Configuration Manager) that is integrated with the remote management console. Provisioning can then be achieved by establishing a secure Transport Layer Security (TLS) tunnel between the Intel AMT system and SCS, and then automatically downloading the necessary provisioning information to the Intel AMT system. Various levels of security are supported, including public-key infrastructure (PKI) and pre-shared key (PSK) implementations.

Intel AMT can support a range of provisioning scenarios:

- Direct shipment – The Intel AMT system is shipped from the OEM to the end-user; provisioning takes place locally – either manually or via an SCS.
- IT staging area – For larger customers, systems are shipped to an IT staging area where they undergo provisioning before being given to end-users.
- OEM-customized system – The OEM may apply a custom image to the client; no provisioning would then be required at the customer's site; alternatively, the OEM may pre-configure various Intel AMT settings. See also OEM TLS-PSK provisioning.

Intel AMT offers a range of options for carrying out the actual provisioning:

- Manual setup and configuration – The Manual mode for Intel AMT setup and configuration is intended for customers that do not have an SCS or the necessary network and security infrastructures to use TLS. Here, setup and configuration is performed manually through the MEBx, as described in Manual mode setup and configuration.
- Legacy provisioning – As soon as the Intel AMT system is powered on for the first time, it begins sending out "hello" messages looking for an SCS. When the SCS is found and authentication has taken place, the SCS provisions the Intel AMT system. This zero-touch method may place a significant burden on the network, depending on the number of systems being provisioned concurrently.

Note
Zero-touch provisioning uses the default MEBx setup.

- Remote provisioning – With remote provisioning (also known as remote configuration or host-based configuration), the Intel AMT system has an OS up-and-running, as well as a local Intel agent – the Intel AMT Configuration Utility (ACU_configurator). As soon as the system is powered up, it begins sending "hello" messages to request provisioning. However, if the system is not provisioned within six hours, the "hello" messages stop; you would then need to re-use the agent to initiate remote configuration.

  Remote provisioning uses the TLS-PKI method and can be zero-touch at the client side. For more information, refer to Using the TLS-PKI method.
- Delayed remote provisioning – The Intel AMT system has its OS up-and-running and a local agent has been installed. Provisioning, which can take place whenever convenient so as not to burden the network, is initiated when the local agent contacts the SCS.

  For more information, refer to Using the TLS-PKI method.
- TLS-PSK provisioning – For stronger security, TLS-PSK can be used for remote provisioning. For more information, refer to Using the TLS-PSK method.
  - OEM-TLS-PSK provisioning – HP supports zero-touch TLS-PSK provisioning by pre-configuring key Intel AMT settings at the factory. For more information, refer to OEM TLS-PSK provisioning.

- **Using a USB drive key** – A USB drive key can be used for zero-touch provisioning. With this method, password, PID, and PPS information is loaded to the MEBx on system boot using a specially formatted **setup.bin** file. After this information has been loaded, the Intel AMT system starts requesting provisioning. For more information, refer to Using a USB drive key for provisioning.

Using the TLS-PSK method

TLS-PSK provisioning requires the Intel AMT system to possess a pre-shared key (PSK) in order to support authentication with the SCS. While the distribution of pre-shared keys adds complexity and cost, this method provides strong security.

To support PSK provisioning, Intel AMT and the SCS share a Provisioning ID (PID)/Provisioning Passphrase (PPS) set, which forms the PSK. Security can be further enhanced by allocating a unique PID/PPS set to each Intel AMT system.

Note
Without dashes, PIDs have eight characters, while PPSs have 32 characters. Since there are dashes between every set of four characters, PIDs have a total of 9 characters, while PPSs have a total of 40 characters.

As soon as a PID/PPS set has been delivered to the ME – either manually via the MEBx or using a USB Key – the Intel AMT system starts looking for an SCS. The Intel AMT system continues to look for an SCS every time it is powered up until provisioning has occurred.

The provisioning process is as follows:

1. Assuming an agent has been pushed to the Intel AMT system, the system automatically looks for an SCS as soon as power is applied.
2. If an SCS is found, the Intel AMT system sends it a "hello" message.

   DHCP and DNS must be available for the SCS search to automatically succeed. If DHCP and DNS are not available, then you must manually enter the IP address of the SCS into the Intel AMT system's MEBx.

   The "hello" message contains the following information:

   – PID
   – UUID (Universally Unique Identifier)
   – IP address
   – ROM and FW version numbers

The "hello" message is transparent to the user; there is no feedback mechanism to tell you messages are being broadcast..

Note
The initial "hello" message is unencrypted; however, all subsequent communications between Intel AMT system and SCS can be encrypted with TLS.

---

3. The SCS uses the information in the "hello" message to initiate a TLS connection (if supported) to the Intel AMT system using TLS PSK.

Note
TLS is optional. However, if the infrastructure is available, you should use TLS for secure, encrypted transactions.
If TLS is not available, less secure HTTP Digest is used for mutual authentication.

The SCS looks up the appropriate PPS in its database[7] and uses the PPS and PID to generate the premaster secret.

[7] Based on the PID

4. The SCS logs into the Intel AMT system and provisions all required data items, including the following:
   - New PPS and PID for future configuration
   - TLS certificates
   - Private keys
   - Current date and time
   - HTTP Digest credentials
   - HTTP Negotiate credentials

   Other options can be set depending on the particular SCS implementation.

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

Enabling TLS-PSK provisioning
For information on enabling TLS-PSK provisioning on an Intel AMT system, refer to Enabling TLS-PKI or TLS-PSK.

OEM TLS-PSK provisioning

To reduce the burden on local IT staff, the information required to enable TLS-PSK provisioning can be pre-configured at the factory. OEM TLS-PSK provisioning is performed in the following stages:

1. During OEM manufacturing
2. At the customer's location

During OEM manufacturing

During manufacturing, HP sets up Intel AMT[8] and ships the customer a system that is already in In-Setup phase.

If desired, the admin password, PID, and PSS can be generated during manufacturing and transferred to the customer in a separate, secure fashion. Alternatively, customers can provide their own admin password, PID, and PPS to be used by HP for a particular order.

At the customer's location

The customer receives In-Setup systems along with the PIDs, PPSs, and password information needed by the SCS. The systems are connected to the network and powered up, allowing remote provisioning to take place automatically.

Note
Some SCSs may require additional settings, such as a port number and IP address. Contact the ISV for more information.

If desired, the SCS can generate a new PID/PPS combination to replace the combination configured by HP.

Using a USB drive key for provisioning

This is a zero-touch provisioning method that eliminates the errors that can occur when manually typing entries. Password, PID, and PPS information is loaded to the MEBx on system boot using a specially formatted setup.bin file. After this information has been loaded, the Intel AMT system starts requesting provisioning.

Prerequisites

A USB drive key must meet the following requirements to support USB drive key setup and configuration:

- It must be greater than 16 MB in size.
- The sector size must be 1 KB.
- It must not be formatted to boot.
- The setup.bin file must be the first file landed on key.

[8] This is a custom, fee-based service. Contact HP for more information.

Using the key

The following are typical stages in the use of a USB drive key:

1. An IT technician inserts a USB drive key into the system hosting the SCS.
2. Through the SCS, the IT technician requests local setup and configuration records.
3. The SCS generates the appropriate passwords and PID/PPS sets and stores them in its database.
4. The SCS writes the passwords and PID/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 for new Intel AMT platforms and performs the following actions:
   i. Unpack a system and connect it to the network.
   ii. Insert the USB drive key into the system.
   iii. Power on the system.
6. The system BIOS checks for the presence of a USB drive key.
   – If a key is detected, the BIOS looks for a setup.bin file; if this file is found, the BIOS continues with Step 7.
   – If a key is not detected – or if a key is detected but no setup.bin file is found – the system boots normally; no Intel AMT setup and configuration is performed.
7. The system BIOS displays a message indicating that automatic setup and configuration will occur and takes the following actions:
   i. Read the first available record in the setup.bin file into memory, validate the file header record, locate the next available record, and invalidate the current record so it cannot be used again.
   ii. Place the file's memory address into the MEBx parameter block.
   iii. Call MEBx.
8. MEBx processes the record from memory.
9. MEBx writes a completion message to be displayed.
10. The IT technician powers down the system. At the time, the system is in In-Setup phase and is ready to be distributed to the user in an Enterprise mode environment.
11. Return to Step 5 for additional Intel AMT systems.

Note

Refer to the ISV for your SCS for more information on USB drive key setup and configuration.

Using the TLS-PKI method

Remote provisioning of Intel AMT systems is achieved using the TLS-PKI method.

Note

By default, HP EliteDesk 800 G1 Business PCs are shipped ready for remote provisioning (that is, no changes to the MEBx are required). The MEBx is pre-configured to support PKI; thus, all that is required to initiate provisioning is an agent that can be pushed over the network to Intel AMT systems whenever convenient.

TLS-PKI provisioning uses Public Key Infrastructure with Certificate Hashes (PKI-CH) protocol to maintain security; a DHCP environment is required.

Thus, no pre-shared key is required with TLS-PKI provisioning; instead, authentication is mutual. The Intel AMT system maintains default hashes in firmware for a number of certificates; alternatively, you can add your own hashes (see Appendix D: Supported certificates). Hashes are integrated into the "hello" messages sent to the SCS, which must have compatible certificates in order for authentication to take place.

Creating a secure connection between the Intel AMT system and SCS requires a certificate, which is used for encryption rather than authentication. If you do not wish to use a third-party certificate, you can use the SCS to create a self-signed certificate. The SCS uses the public key from the certificate to encrypt the session key it generates and sends to the Intel AMT system, which can decrypt the session key using its private key.

Since the Intel AMT system is already running an OS, provisioning can take place at any time. The local agent contacts the SCS, which responds by telling the Intel AMT system to provide a one-time password (OTP).[9] Once a TLS connection has been established, the SCS can begin provisioning the Intel AMT system.

The OTP is created and encrypted by the ME and is then sent to the SCS.

Delayed network access
TLS-PKI provisioning utilizes delayed network access; that is, provisioning does not commence as soon as the Intel AMT system is first powered up. In this implementation, provisioning can be initiated after an OS has been installed and a local agent has been pushed over the network to the Intel AMT system.

In this implementation, remote provisioning begins when the SCS is able to communicate with the ME through the Intel Host Embedded Controller Interface (HECI) driver, which requires a functional OS and agent to be installed on the Intel AMT system.

Note
Consult the management console ISV for more information on OS agents that provide delayed remote provisioning support.

Enabling TLS-PKI provisioning
For information on enabling TLS-PKI provisioning on an Intel AMT system, refer to Enabling TLS-PKI or TLS-PSK.

Setting the remote configuration timeout
HP EliteDesk 800 G1 Business PCs are shipped with a Remote Configuration Timer that is set to 0, which effectively disables "hello" message broadcasting. Enabling the ME to broadcast "hello" messages requires the use of an Intel local agent.

Note
The remote configuration timeout was omitted from subsequent HP Compaq Elite 8x00 and EliteDesk 800 Business PCs.

Note
Consult the management console ISV for more information on delayed remote configuration timeouts.

The local agent typically configures ME to broadcast "hello" messages for six hours while the ME is active and the system is connected to a network. If there no response from an SCS within the timeout period, the network interface that is sending out "hello messages" is disabled. It can be re-enabled by one of the following methods:

- Re-initiating provisioning via the local agent
- Partial unprovisioning through the MEBx (for more information, refer to Unprovisioning an Intel AMT system

Prerequisites and caveats for TLS-PKI
TLS-PKI provisioning requires the following prerequisites to be met:

- The OS must be present on the Intel AMT system.
- Both the Intel AMT system and SCS must be on a DHCP server. The SCS must either be named Provisionserver or must have an alias in DNS and be on the same domain as the Intel AMT system.
- The Intel AMT system must have at least one pre-programmed active root certificate hash.

[9] A one-time password is not required with PSK.

- The SCS must have a server certificate with the appropriate object identifier (OID) or organizational unit (OU):
  - Unique Intel AMT OID value in the **Extended Key Usage** field is **2.16.840.1.113741.1.2.3**
  - OU value in **Subject** field is **Intel Client Setup Certificate**

    This OU value is case-sensitive and must be entered exactly as shown.
- If support for delayed provisioning is required, an OS and local agent must be installed on the Intel AMT system.

Enabling TLS-PKI or TLS-PSK

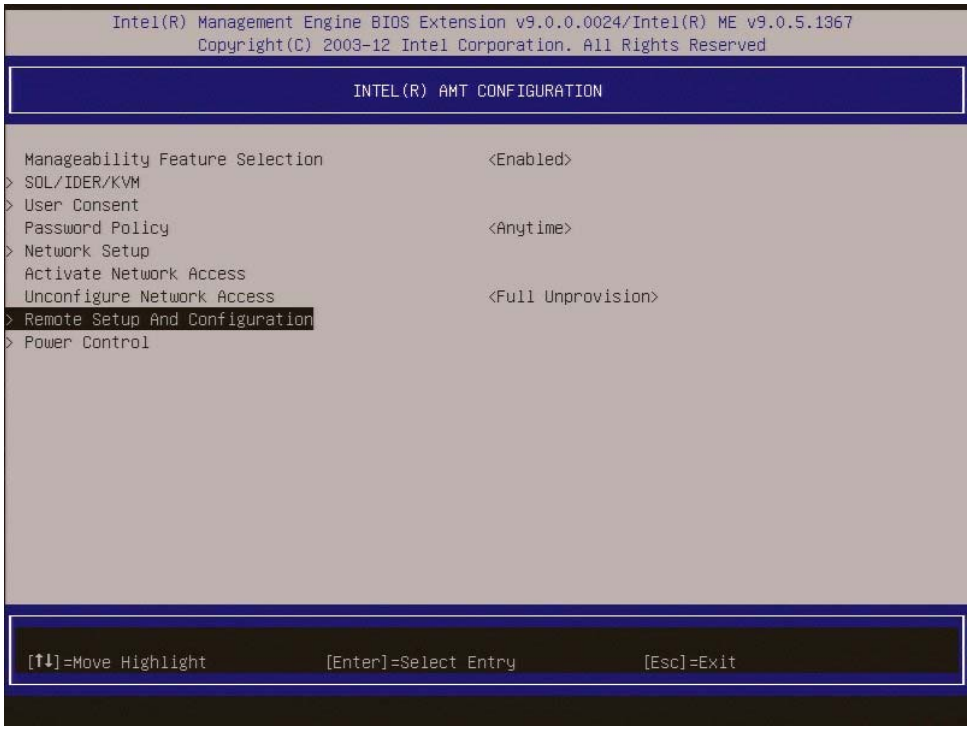
Remote provisioning via TLS-PKI or TLS-PSK may require you to manually specify certain network and security settings on the Intel AMT system unless you use a USB key to provide the appropriate information.

Carry out the following steps to manually configure an Intel AMT system that is already in In-Setup phase:

1. Select **Remote Setup and Configuration** from the Intel AMT Configuration menu, as shown in Figure 22.

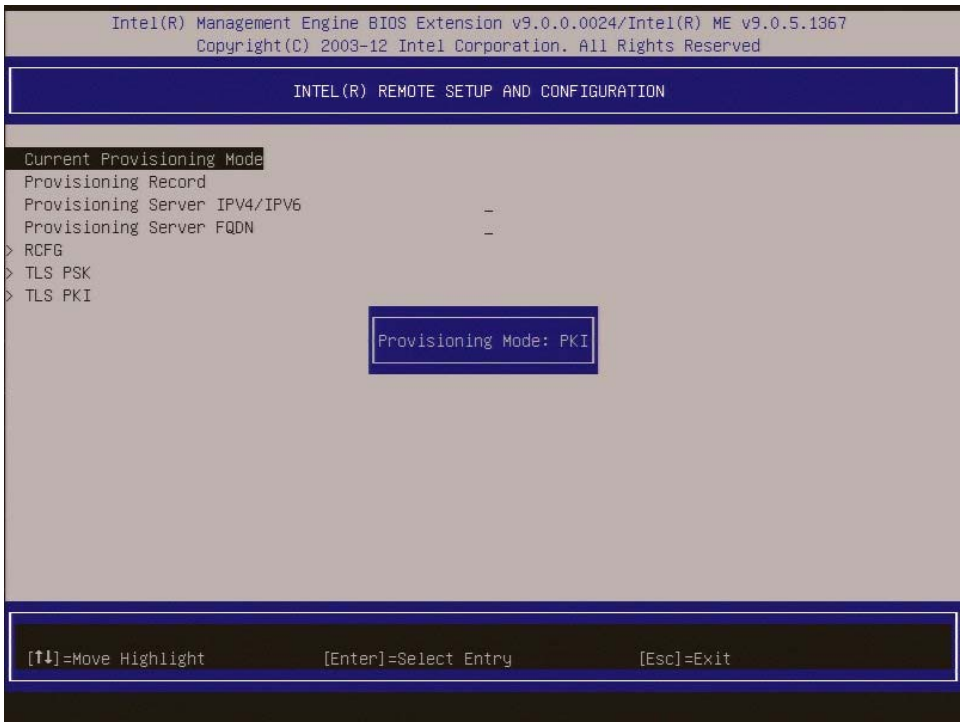
Note
Skip the **Activate Network Access** and **Unconfigure Network Access** menu items.

Figure 22. Transitioning from Intel AMT setup to configuration



2. Review the Intel Automated Setup and Configuration menu items (shown in Figure 23).

Figure 23. Menu used to enable remote provisioning



– **Current Provisioning Mode**

  This menu item is used to display the provisioning mode currently selected. Options are:

  - None
  - PKI (default)
  - PSK

  No changes can be made at this menu.

– **Provisioning Record**

  This menu item is used to display the data in the system's provisioning record. The default setting is **Not Present**; no changes can be made at this menu.

  The record for a system with **PKI provisioning** includes the following data:

  - Provisioning Mode
  - DNS
  - Host Initiated
  - Hash Data
  - Serial Algorithm
  - ISDefault Bit
  - Time Validity Pass
  - FQDN
  - Provisioning IP
  - Date of Provisioning

  The provisioning record for a system with **PSK provisioning** includes the following information:

  - Provisioning Mode
  - Provisioning IP
  - Date of provisioning

– **RCFG**

Remote Configuration (RCFG) is an Intel AMT feature that allows a single OEM OS image to provision systems securely, without the need to manually modify Intel AMT options.

RCFG has the following requirements:

- Public Key Infrastructure with Certificate Hashes (PKI-CH) protocol to maintain security
- DHCP environment
- OS present on the Intel AMT system

– **Provisioning Server IPv4/IPv6**

This menu item is used in Enterprise mode to point to the IP address of the SCS. The default is **0.0.0.0**.

If the IP address is left at its default value, the ME will look for **ProvisionServer** on the DNS.

Some SCS products may require additional settings, such as the port number[10] and IP address. Contact the particular ISV for more information.

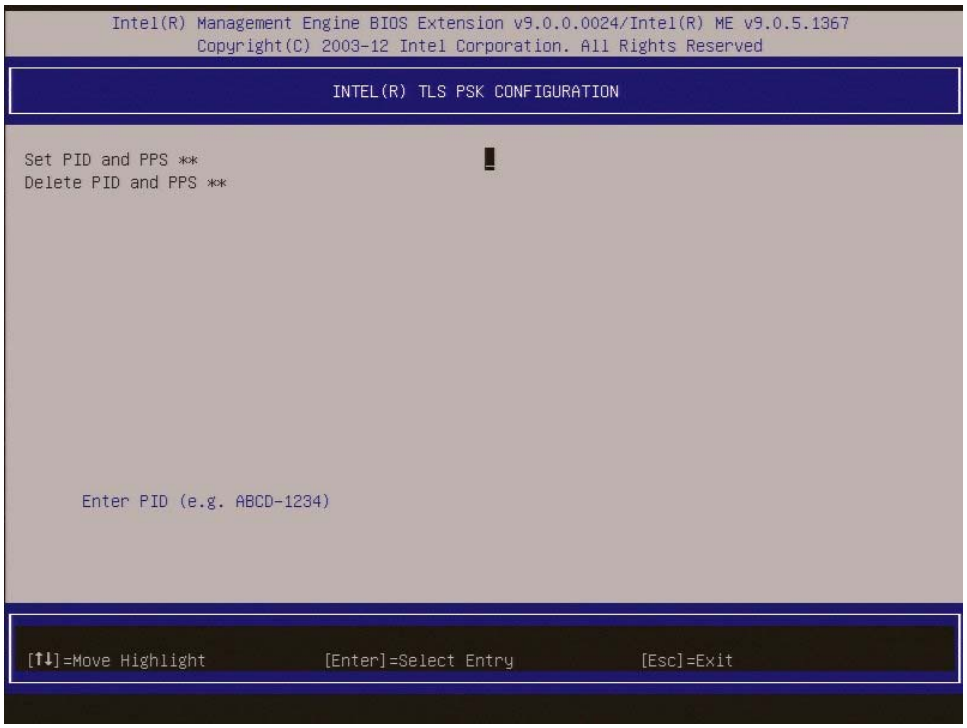
– **Provisioning Server FQDN**

This menu item is used in Enterprise mode to specify the Fully Qualified Domain Name (FQDN) of the SCS, which is network-dependent. There is no default.

– **TLS PSK**

Select this menu item in order to configure TLS-PSK via the Intel TLS PSK Configuration screen, shown in Figure 24.

Figure 24. Configuring TLS–PSK provisioning



Options are:

– **Set PID and PPS**

This option allows you to specify a provisioning ID (PID) and provisioning passphrase (PPS). Values are system-dependent; there is no default.

Without dashes, PIDs have eight characters, while PPSs have 32 characters. Since there are dashes between every set of four characters, PIDs have a total of 9 characters, while PPSs have a total of 40 characters. If you do not wish to enter the PID or PPS manually, you can use a USB key that contains the appropriate information (see Using a USB drive key for provisioning).

[10] The default port for many SCSs is 9971.

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

Legacy (zero-touch) provisioning uses a default certificate; no PID or PPS are needed. PKI is active in the base image, which contains 15 pre-installed certificates.

- Delete PID and PPS

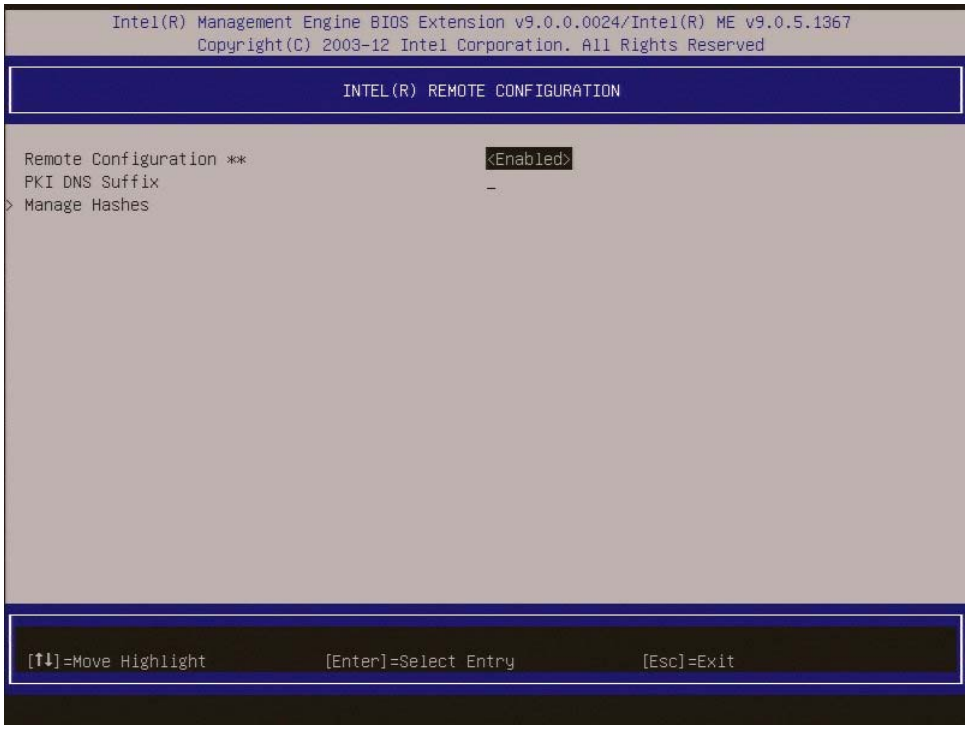
  This option is used to delete the current PID and PPS entries and should be skipped.

  After configuring TLS-PSK, return to the previous menu.

- TLS PKI

  Select this menu item in order to configure TLS-PKI via the Intel Remote Configuration screen,[11] shown in Figure 25.

Figure 25. Configuring TLS-PKI provisioning



Options are:

- Remote Configuration

  This option enables (recommended; default) or disables TLS-PKI provisioning.

- PKI DNS Suffix

  This option allows the PKI DNS suffix for the SCS to be specified.

- Manage Hashes

  This option shows the hashes that are in the system, providing names and status (active/inactive). If there are no hashes in the system, you are given the option to add hashes; if hashes are available, you are given the option to delete one or more. For more information on supported certificates, refer to Appendix D: Supported certificates.

[11] Intel refers to TLS-PKI provisioning as remote configuration.

In Intel AMT 9.x, the MEBx allows you to manually activate a hash and use up to three additional certificate hashes. To add a hash:

i. Press the **Insert** key in the **Manage Hashes** menu.

ii. Enter a name and fingerprint for the hash.

iii. Specify the status of the hash (active or not active; default or not default).

After configuring TLS-PKI, return to the previous menu.

3. Return to the MEBx Main Menu.
4. Select **MEBx Exit** to exit the configuration procedure and save settings.

   The system displays a single Intel ME Configuration Complete message and reboots.
5. Turn off the system and remove power. At this point the system has migrated from Factory phase to In-Setup phase.

After you plug the system into a power source and make the network connection, the automated migration from In-Setup phase to Operational phase can commence.

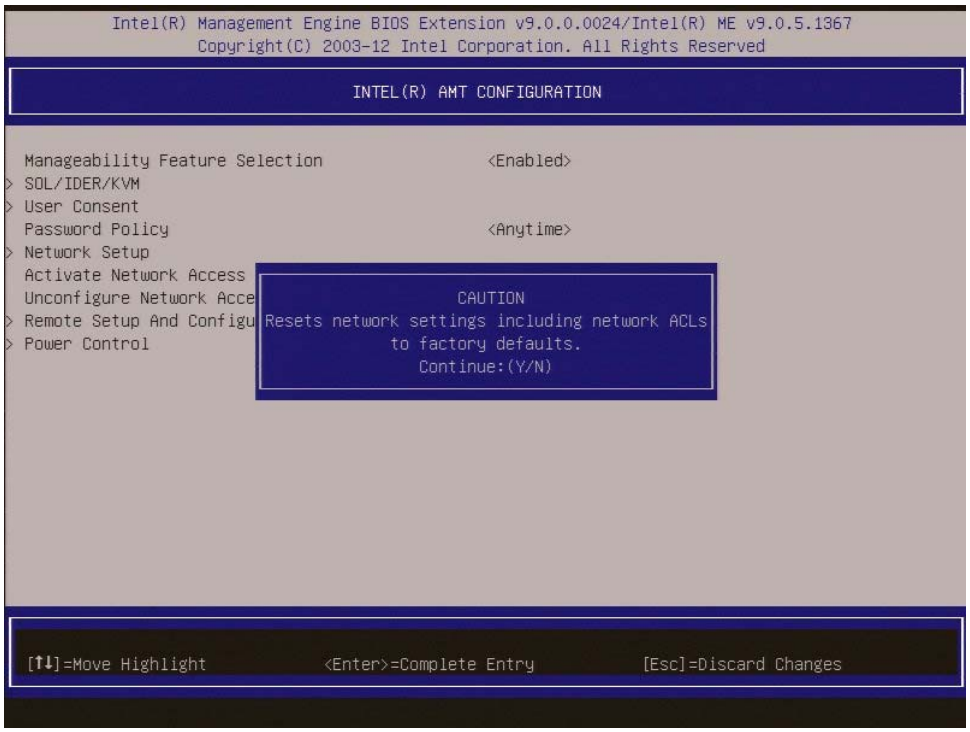
Note

Only use the integrated Intel NIC to make the network connection. Intel AMT does not work with other NIC solutions.

Unprovisioning an Intel AMT system

If desired, you can unprovision an Intel AMT system that has been setup and configured. Use the **Unconfigure Network Access** option on the Intel AMT Configuration menu, as shown in Figure 26.

Figure 26. Selecting the **Unconfigure Network Access** option



Having selected **Unconfigure Network Access**, you can select one or both of the following unprovisioning options depending on how the Intel AMT system has been provisioned:

- **Full unprovisioning**

  Available for systems provisioned in Manual or Enterprise mode, full unprovisioning returns all Intel AMT configuration settings to their factory defaults. All certificate hashes are deleted; the default hash is made active.

  This option does not reset all ME configuration settings (such as network settings) or the MEBx password.

- Partial unprovisioning

  Only available for systems provisioned in Enterprise mode, partial unprovisioning returns all Intel AMT configuration settings to their factory defaults with the exception PID, PPS, and PKI-CH settings.

  This option does not reset ME configuration settings or the MEBx password.

  Partial unprovisioning re-opens the network interface for six hours of “hello” message broadcasts.

Approximately a minute after you select the desired unprovisioning option, the caution shown in Figure 26 appears.

On completion, control is passed back to the Intel AMT Configuration screen. Notice that the **Activate Network Access** option (Figure 8) is again available.

After return to the previous menu and exiting, the system will reboot.

Making a full return to factory default settings

F10 setup provides an option that allows you to fully unprovision the ME to factory defaults. Use the **Unconfigure AMT/ME** option, which is located under the **Advanced/AMT Configuration** menu.

The unconfigure option clears CMOS, thus returning all MEBx settings to factory defaults; for example, the password is reset to **admin**.

Following the unconfigure, the system must 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 I access the MEBx locally?
A: The MEBx can be locally accessed by selecting **Esc** from the startup menu. Alternatively, you could press **F6** (notebook PCs) or **Ctrl-P** (desktop PCs) during POST.

Q: Why isn't the **Ctrl-P** prompt displayed during POST?
A: By default, the **Ctrl-P** prompt is hidden from desktop PC users during POST; however, this prompt can be displayed if set in F10 Setup.
Workstation PCs do not provide a BIOS option to display the **Ctrl-P** prompt during POST.

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

Q: Why doesn't the MEBx accept my new password?
A: All MEBx passwords, other than the default password, must comply with strong password guidelines. See the Creating a password section for more details.

Q: If the password is inknown, can the system be recovered?
A: Clearing CMOS resets all MEBx options including the password, which reverts to its default setting, **admin**.

Q: How can all MEBx options be restored to factory defaults?
A: See the Making a full return to factory default settings section.

Q: What happens if the wrong password is entered multiple times?
A: After the password has been entered incorrectly three times, the system reboots. You can go back into the MEBx after the reboot and attempt to enter the password again.

Q: Can the WebUI be used locally (on the Intel AMT system) to access the MEBx on the system?
A: No. WebUI access must originate from an outside network to a specific IP and port.

Q: Why can't a new password set with the WebUI be used locally in the MEBx?
A: The password set with the WebUI is a remote password and can only be used when accessing the MEBx remotely; it does not work with the MEBx locally. The local password must be used for local access the MEBx.

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

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

Q: Where can I get an SCS?
A: You can use HP Client Configuration Manager; alternatively, ISVs such as Altiris offer SCSs. Check with your management console supplier to see if they offer this service.

Q: Can Intel AMT be set for a static address while the OS is set for DHCP or vice versa?
A: Although possible, these scenarios are not supported setting by Intel and may cause unexpected system behavior.

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

Q: What is the difference between the ME and Intel AMT?
A: The ME is the controller that, along with Intel Protected Audio Video Path (PAVP) capability, is used to manage Intel AMT. Note that clearing Intel AMT settings does not affect the ME settings, which are separate.

Q: Why doesn't Wake-On-ME function after I've set the idle timeout?
A: The Wake-On-ME feature only works if the **ME ON in Host Sleep State** setting has been set to allow ME WoL and the system has been fully provisioned.

Q: Does Intel AMT provide wireless LAN support?
A: For desktops, all EliteDesk and EliteOne platforms support wireless Intel AMT using the mini PCI Express Intel Centrino Advanced-N 6205 Wireless LAN or HP PCI Express x1 add-on card with Intel Centrino Advanced-N 6205 Wireless LAN.

Certain HP Business Notebook PCs and Mobile Workstations featuring the appropriate adapters can support wireless Intel AMT. See Support.

Wireless Intel AMT is not supported on HP Workstation PCs.

Appendix B: Overview of power, sleep, and global states

Under the Advanced Configuration and Power Interface (ACPI) specification, a PC may be in one of the following power states (also known as Sleep (Sx) or Global (Gx) states).

- S0

  S0 (also known as G0) is the On state, during which the PC is fully functional. All system devices and the operating system, if available, are running.
- S3

  S3 is the Standby (Microsoft® terminology) or Suspend-to-RAM state. The memory subsystem and V_{aux} power rail remain powered, while the remainder of the PC – including the processor – is not powered. After resuming from S3, the system context is still intact because system memory was powered at all times.
- S4

  S4 is the Hibernate (Microsoft terminology) or Suspend-to-Disk state. The system context is saved to the hard drive as a hibernation file; when the PC resumes from S4, the system context is restored from this file.

  During S4, V_{aux} remains powered; all other subsystems – including system memory and the processor – are not powered.
- S5

  S5 (also known as G2) is the Soft Off state and is identical to S4, except that the system context is not saved. When the PC resumes from S5, it powers up and goes through POST.
- G3

  G3 is the Mechanical Off state, during which all PC subsystems are powered off. The easiest way to achieve this state is by removing utility power from the PC by unplugging the power cord.

ME power states

The ME has its own power states (Mx), as follows:

- M0

  M0 is the On state for the ME; the PC is in S0 state. The ME is fully powered and running.
- M3

  M3 is the On state for the ME; the PC is in a non-S0 state. The ME is fully powered and running.
- Moff

  Moff is the Off state for the ME; the PC is in a non-S0 state.

The ME can be set to stay powered-on and active in all Sx states. In this scenario, if the PC is in S0, then the ME will be in the corresponding M0 state; however, if the system is in S3, S4, or S5, the ME remains active but migrates to M3 state.

Appendix C: Wake-On-ME overview

Wake-On-ME, also known as ME Wake-on-LAN (ME WoL), is a feature that allows the ME to go into a low power state when it is not being used but awaken if required. The ME counts down from the amount of time set in **Idle Timeout** before going to sleep.

The following condition must be met for Wake-On-ME to function:

- The system is in a sleep state (S3, S4, or S5)
- **Intel ME On in Host Sleep States** is set to allow Wake-On-ME WoL

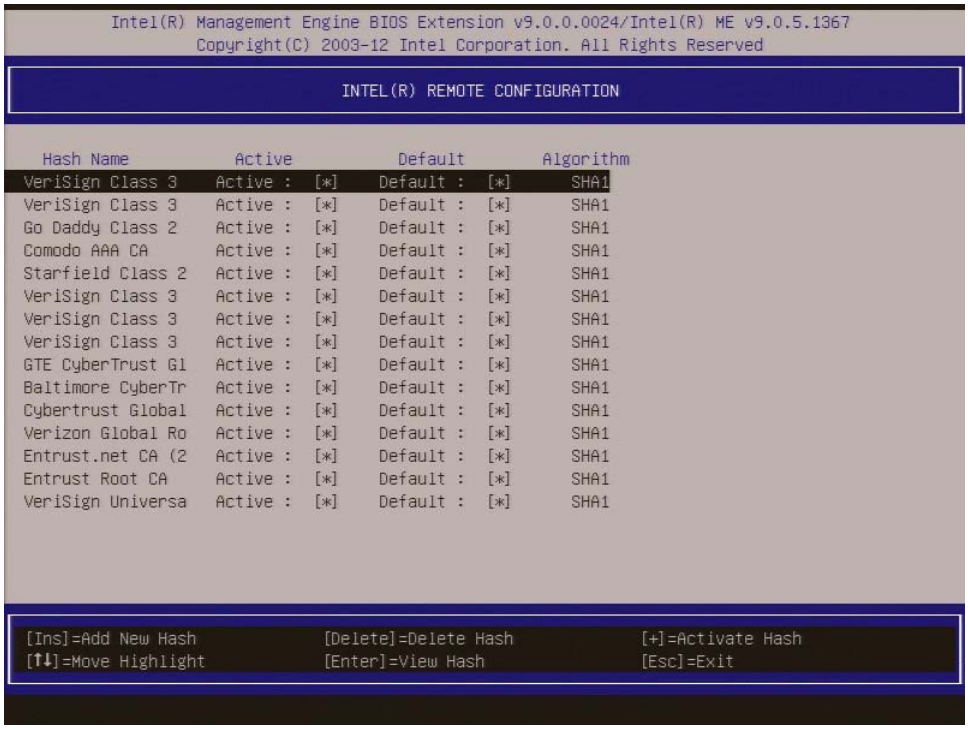
Appendix D: Supported certificates

The following are supported certificate authorities and certificates (see also Figure D-1):

Note
Not all certificates may 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

Figure D-1. Supported certificate authorities and certificates



Resources, contacts, or additional links

Intel vPro Technology
www.intel.com/technology/vpro/index.htm

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

P/N 742409-001, June 2013