HP Business Notebook Intel® vPro™ setup and configuration

2011 Business Notebook Models

Technical white paper

Table of contents

Executive summary

Select HP ProBook and EliteBook models use Intel vPro processor technology to simplify PC management and reduce IT related expenditures. Intel vPro processor technology uses Intel Active Management Technology (AMT), which allows for improved management of PC systems and better security. AMT provides Out-of-Band (OOB) remote access to a system regardless of the system power state or operating system condition as long as the system is connected to a power source and a network. AMT is a hardware and firmware platform resident solution relying upon the Management Engine (ME) within the Mobile Intel QM67 Express Chipset.

By default, the AMT is inactive. It must be setup and configured in the system before it can be used. The setup and configuration process is also known as provisioning. There are two methods of AMT setup and configuration:

- Manual mode
- Enterprise mode

This whitepaper details manual mode and enterprise mode setup and configuration for the client PC along with the usage of a Setup and Configuration Server (SCS) in enterprise mode. Please consult your Management Console ISV provider for details regarding installation procedures for a Setup and Configuration Server. Basic knowledge of Intel AMT and networking are required. Please refer to the Intel website www.intel.com/technology/vpro/index.htm for other whitepapers and technical information regarding Intel vPro Technology.

Supported models and background

Intel vPro Processor technology is an available option on select HP Business Notebook models introduced in 2011. Supported models are listed below.

- HP EliteBook 8460p Notebook PC
- HP EliteBook 8560p Notebook PC
- HP ProBook 6360b Notebook PC
- HP ProBook 6460b Notebook PC
- HP ProBook 6560b Notebook PC

Table 1 shows AMT versions and when they were introduced.

Table 1. AMT versions and when they were introduced into HP notebook models

Year	AMT version	Intel chipset	HP Models
2007	2.5	Intel 965	HP Compaq 2510p, 2710p, 6910p, 8510p, 8510w, 8710p and 8710w
2008	4.0	Intel PM45 Express	HP EliteBook 2530p, 2730p, 6930p, 8530p, 8530w and 8730w
2010	6.0	Mobile Intel QM57	HP EliteBook 2540p, 2740p, 8440p, 8440w, 8540p, 8540w and 8740w
2011	7.1	Intel QM67	HP EliteBook 8460p, EliteBook 8560p, ProBook 6360b, ProBook 6460b and ProBook 6560b

Intel Active Management 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. It is generally performed only once for the lifetime of the system. When AMT is enabled, it can be discovered by management software over a network.

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

AMT system phases

There are three Phases of AMT setup and configuration:

- Factory
- In-Setup
- Operational

The Factory phase is the initial stage as the system comes from the factory. No AMT Setup and Configuration has been done. The only way to access AMT in Factory phase is through the MEBx. This phase will end for manual mode systems once the default password has been changed. Enterprise mode systems also require the Provisioning ID (PID) and Provisioning Passphrase (PPS) to be set.

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

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

Manual (SMB) mode – AMT Setup and Configuration with MEBx

Manual mode is for customers who do not have independent software vendors (ISV) management consoles or the necessary network and security infrastructures to use encrypted Transport Layer Security (TLS). Manual mode AMT setup and configuration is a manual process done through the Intel ME BIOS Extension (MEBx).

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

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

MEBx password guidelines

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

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

  Some examples:
  - 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

Manual 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 whitepaper details HP recommended settings on options, some of which may be the same as the default selection. Even though the default setting is set and used for certain options, it is good practice to double check important options.

1. Hit Ctrl-P during POST to enter Management Engine BIOS Extension (MEBx) Setup.

   This option is by default not shown during the HP splash screen. It can be displayed during POST if set in F10-Setup.
2. Enter the default password.

   The default password is "admin". Passwords are case sensitive. The user must change the default password before any changes can be made in the MEBx.
3. Change the password for the MEBx.

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

4. Go into the Intel ME General Settings.
5. FW Update Settings

   Local FW Update
   Default Setting : Enabled
   Recommended Setting : Enabled

   By default, the system BIOS allows for local ME FW updates without the password protected. However, the administrator can modify the Local FW Update setting with the Password Protected.
6. Set PRTC

   Default Setting : None
   Recommended Setting : Current Date and Time

   This option sets the PRTC (Protected Real Time Clock). Setting the PRTC value is used for virtually maintaining PRTC during the power-off (G3) state. PRTC has a valid date range of 1/1/2004 to 1/4/2021.
7. Power Control
   a. Intel ME ON in Host Sleep States.
      Default Setting : Desktop: ON in S0
      Recommended Setting : Desktop: ON in S0, ME Wake in S3, S4-5

      The ME On in Host Sleep State mode will automatically set to Desktop: ON in S0, ME Wake in S3, S4-5 after Activating the Network Access (step 9)

   b. Idle Timeout
      Default Setting : 65535
      Recommended Setting : 65535
      This option sets the timeout value for Wake-On-ME. The default timeout value is 65535 from the factory and it is in units of a minute. HP recommends a setting of 65535 for most applications. . Certain console vendor's product falsely detects an AMT system as disconnected if the software has to wait for the ME to wake and respond. If the console software being used does not have this issue, HP recommends a setting of 1 which allows the ME to go to sleep after approximately 1 minute of inactivity. This allows for maximum power savings when the ME is enabled to be on in S3, S4, or S5. The timeout value can be set in decimal and hexadecimal notation. It must be set to a non-zero value for the ME to take advantage of Wake-On-ME. This value is not used when the system is in an active state – S0. This value is used only if the ME ON in Host Sleep State setting is set to allow ME WoL. See Appendix C for an explanation of Wake-On-ME / ME WoL.

8. Return to MEBx Main menu. Select Previous menu and press enter to go back to the MEBx Main menu
9. Go into the Intel AMT Configuration.
10. Check the Manageability Feature Selection.

    Default Setting : Enabled
    Recommended Setting : Enabled
    This option allows Intel AMT to be enabled or disabled. By default, HP notebook PCs are set to enable Intel AMT. Note that setting the Disabled option will disable all remote management capabilities. Setting Disabled will also unprovision any AMT settings.
11. Check SOL/IDER/KVM
    a. Username & Password
       Default Setting : Enabled

Recommended Setting : Enabled
Select Enabled.

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

b. SOL

Default Setting : Enabled
Recommended Setting : Enabled
Select Enabled.

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

c. IDER

Default Setting : Enabled
Recommended Setting : Enabled
Select Enabled.

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

d. Legacy Redirection Mode.

Default Setting : Disabled
Recommended Setting : Disabled
Select Disabled.

This option allows the Redirection feature to work with the pre-AMT 6.0 remote consoles.

e. KVM Configuration

Default Setting : Enabled
Recommended Setting : Enabled

12. User Consent

a. User opt-in.

Default Setting : KVM
Recommended Setting : User Dependent

b. Opt-in Configurable from Remote IT

Default Setting : Enabled Remote Control of KVM Opt-in Policy
Recommended Setting : User Dependent

Disable Remote Control of KVM Opt-in Policy – This option disables the Remote User's ability to select User OPT-IN Policy. In this case only the local user can control the opt-in policy.
Enable Remote Control of KVM Opt-in Policy - Enables Remote User's ability to select User OPT-IN Policy.

13. Password Policy.

Default Setting : Default Password Only
Recommended Setting : Default Password Only

Select Default Password Only. This option determines when the user is allowed to change the Intel MEBX password through the network. The Intel MEBX password can always be changed via the Intel MEBX user interface.

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

14. Network Setup.

Intel ME Network Name Settings

a. Host Name
Enter a Host Name
Default Setting : None
Recommended Setting : User Dependent

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

b. Domain Name
Enter a domain name
Default Setting : None
Recommended Setting : Network Dependent

The domain name is blank by default. If it is not populated, then the default domain of "Provisionserver" will be used when connecting to a Setup and Configuration Server. If the name of the S&CS is not "Provisionserver" and the domain name is blank, then an alias must be set up in the DHCP server to redirect the connection for "Provisionserver" to the proper S&CS domain name. If the domain name field is populated, then that will be the domain used. However, if there is no response after four DNS queries to the named domain, then that domain name will no longer be used and the default "Provisionserver" will be used.

c. Subnet Mask Address
Share/Dedicated FQDN
Default: Setting: Shared
Recommended Setting: Shared

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

d. Dynamic DNS Update
Default: Setting: Disabled
Recommended Setting: Disabled

If Dynamic DNS Update is enabled then the firmware will actively try to register its IP addresses and FQDN in DNS using the Dynamic DNS Update protocol. If DDNS Update is disabled then the firmware will make no attempt to update DNS using DHCP option 81 or Dynamic DNS update. If the DDNS Update state (Enabled or Disabled) is not configured by the user at all then the firmware will assume its old implementation where the firmware used DHCP option 81 for DNS registration but did not directly update DNS using the DDNS update protocol. For selecting "Enabled" for Dynamic DNS Update it is required that the Host Name and Domain Name must be set. When DDNS Update option is enabled, the MEBx menu will display "Periodic Update Interval" and "TTL" options.

- Periodic Update Interval: Enter a desired interval between 20 minutes – 1440 minutes
- TTL: Enter desired time in seconds

15.TCP/IP Settings.

AMT 7.1 supports IPV4 and IPV6 interface. Follow steps 15a-15f to configure for IPV4 and 15g-15h for IPV6.

a. Wired LAN IPV4 Configuration
   DHCP Mode
   Default Setting : Enabled
   Recommended Setting : Enabled

   DHCP can be used if it is available (TCP/ IP settings will be configured by a DHCP server). If DHCP is disabled, then steps 15b through 15f are required to configure the IPv4 static IP address for Intel AMT.

b. IPV4 Address
   Enter a static address
   Default Setting : 0.0.0.0
   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.

c. Subnet Mask
   Enter subnet mask
   Default Setting : 255.255.255.0
   Recommended Setting : Network Dependent

   Example: 255.255.255.0

d. Default Gateway Address
   Leave as default value and hit Enter
   Default Setting : 0.0.0.0
   Recommended Setting : Network Dependent

   Leave as 0.0.0.0 if this option is not needed.

e. Preferred DNS Address

Leave as default value and hit Enter
Default Setting : 0.0.0.0
Recommended Setting : Network Dependent

Leave as 0.0.0.0 if this option is not needed.

f. Alternate DNS Address
Leave as default value and hit Enter
Default Setting : 0.0.0.0
Recommended Setting : Network Dependent

g. Wired LAN IPV6 Configuration
Select Enabled option for IPV6IPV6 Feature Selection

If DHCP is disabled, then steps 15b through 15f are required to configure the IPV6 static IP address

i. IPV6 Interface ID Type
Default Setting : Random ID
Recommended Setting : Random ID

RANDOM ID - The IPV6 Interface ID is automatically generated using a randomnumber as described in RFC 3041. This is the default.
Intel ID - The IPV6 Interface ID is automatically generated using the MAC address.
Manual ID - The IPV6 Interface ID is configured manually. Selecting this type requires that the Manual Interface ID is set with a valid value.

ii. IPV6 Address
AMT 7.1 supports IPV6 network interface.

Enter a static IPV6 address
Default Setting : None
Recommended Setting : Network Dependent

Example: 2001:db8::1428:57ab

iii. IPV6 default Router
Enter the IPV6 Default Router address
Default Setting : None
Recommended Setting : Network Dependent

Example: 2001:db8::1428:57ab

iv. Preferred DNS IPV6 Address
Enter the Preferred DNS IPV6 Address
Default Setting : None
Recommended Setting : Network Dependent

Example: 2001:db8::1428:57ab

v. Alternate DNS IPV6 Address
Enter the Alternate DNS IPV6 Address
Default Setting : None
Recommended Setting : Network Dependent

Example: 2001:db8::1428:57ab

h. Wireless LAN IPV6 Configuration

Select Enabled option for IPV6 Feature Selection. If DHCP is disabled, then steps 15b through 15f are required to configure the IPV6 static IP address

i. IPV6 Interface ID Type.
Default Setting : Random ID
Recommended Setting : Random ID

RANDOM ID - The IPV6 Interface ID is automatically generated using a random number as described in RFC 3041. This is the default.
Intel ID - The IPV6 Interface ID is automatically generated using the MAC address.
Manual ID - The IPV6 Interface ID is configured manually. Selecting this type requires that the Manual Interface ID is set with a valid value.

16. Activate Network Access.

From the Intel ME Platform Configuration menu, select 'Activate Network Access'. Activate Network Access causes the Intel ME to transition to the POST provisioning state if all required settings are configured. The 'Un-configure Network Access' option will cause the Intel ME to transition to PRE provisioning state. Press the Enter key when MEBx displays "Update Network settings in the General Settings menu". Press 'Y' at the MEBx prompt.

17. Exit MEBx Menu.

Select the Previous Menu option to get back MEBx Main Menu and select Exit to exit the MEBx Setup and save settings. The system will reboot. Once the system reboots, it will go from In-Setup phase to Operational phase. AMT is fully operational. Once in the Operational phase, the system can be remotely managed through the Intel AMT WebGUI or ISV remote console and can be provided to the end-user for regular use.

NOTE
For more information about remote setup and configuration please see the MEBx and Hashes section in this document.

Enterprise mode setup and configuration

Enterprise mode is for large corporate customers. A Setup and Configuration Server (SCS) is required for enterprise mode setup and configuration. The SCS is also known as a Provisioning Server as seen in the MEBx. An 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 Pre-Shared Key (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 PSK.

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

Here is a brief outline of the initial communication between an AMT client system and an SCS:

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

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

There are several independent software vendors (ISV) offering Setup and Configuration Servers on the market. Here are some examples:

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

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 Manual Mode – AMT setup and configuration for MEBx menus and full text. The following are quick steps for AMT setup.

1. Get into the MEBx by pressing Ctrl-P during POST.
2. Enter the default password "admin".
3. Change the MEBx password, follow strong password guidelines.
4. Go into Intel ME Platform Configuration.
5. Check the Intel ME State Control, select Enabled.
6. Check the Intel ME Firmware Local Update Qualifier, select Always Open.
7. Go into Intel ME Power Control.
    a. Go into ME ON in Host Sleep States, select Option 2 *(Desktop: ON in S0, ME Wake in S3, S4-5*)
8. Go into the Intel ME General Settings.

   The Intel ME Platform Configuration screen has more options than could be displayed in one page. More options are available if you scroll down the menu.

9. Password Policy

   Default Setting : Default Password Only
   Recommended Setting : Default Password Only

This option will determine 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.

10. Go into Network Setup & select Host Name.
    a. Enter a host name
       Default Setting : None
       Recommended Setting : User Dependent

       Spaces are not accepted in the host name.

11. Go into Network Setup and select TCP/IP.
    a. Wired LAN IPV4 Configuration
       i. DHCP Mode
          Default Setting : DHCP Enabled
          Recommended Setting : User Dependent

          Select Enabled.

          For the purpose of this whitepaper, DHCP is enabled.

    b. Wired LAN IPV6 Configuration

    Select Enabled option for IPV6 Feature Selection

       i. IPV6 Interface ID Type.
          Default Setting : Random ID
          Recommended Setting : Random ID

       ii. IPV6 Address.
          Enter a static IPV6 address
          Default Setting : None
          Recommended Setting : Network Dependent

          Example: 2001:db8::1428:57ab

       iii. IPV6 default Router.
          Enter the IPV6 Default Router address
          Default Setting : None
          Recommended Setting : Network Dependent

          Example: 2001:db8::1428:57ab

       iv. Preferred DNS IPV6 Address

Enter the Preferred DNS IPV6 Address
Default Setting : None
Recommended Setting : Network Dependent

Example: 2001:db8::1428:57ab

v. Alternate DNS IPV6 Address
Enter the Alternate DNS IPV6 Address
Default Setting : None
Recommended Setting : Network Dependent

Example: 2001:db8::1428:57ab

12. Skip Activate Network Access.
13. Skip Un-Configure Network Access.
14. Go into Remote Setup And Configuration.

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

a. Current Provisioning Mode.
Default Setting : PKI

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. 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. Provisioning Server IPV4/IPV6.
i. Enter Provisioning Server IPV4/IPV6 address
Default Setting : 0.0.0.0

Recommended Setting : Network Dependent

This option is used in Enterprise mode when an Intel AMT Setup and Configuration (Provisioning) Server is available. It points to the IP address of the SCS.

If the IP is left as the default, the ME will look for "ProvisionServer" on DNS. The default port for many SCS is at 9971.

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

d. Provisioning Server FQDN.
   i. Enter Provisioning Server FQDN
   Default Setting : None
   Recommended Setting : Network Dependent

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

e. Go into TLS PSK.

   i. Go into Set PID and PPS.
   Default Setting : None
   Recommended Setting : System Dependent

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

   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. Return to previous menu.

f. 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.

g. Return to previous menu.

15. FW Update Settings

a. Local FW Update.
   Default Setting : Enabled

Recommended Setting : Enabled

By default BIOS allows to update the ME firmware without password protected, the administrator can select the Password Protected (the user must provide the password in order to upgrade the ME firmware.

16. Skip Set PRTC
17. Power Control
    a. Intel ME ON in Host Sleep States.
       Default Setting : Desktop: ON in S0
       Recommended Setting : Desktop: ON is S0, ME Wake in S3, S4-5
    b. Idle Timeout
       Default Setting : 65535
       Recommended Setting: :65535

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

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

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

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

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

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

18. Go into AMT Configuration menu

    Check the Manageability Feature Selection.
    Default Setting : Enabled
    Recommended Setting : Enabled
19. Check SOL/IDE-R under Intel AMT Configuration menu.
    a. A message window telling the user that the system resets after configuration will appear.
       i. Select Y.

    b. Username and Password
       Default Setting : Enabled
       Recommended Setting : Enabled

       i. Select Enabled.

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

c. Serial Over LAN
Default Setting : Enabled
Recommended Setting : Enabled

i. Select Enabled.

d. IDE Redirection
Default Setting : Enabled
Recommended Setting : Enabled

i. Select Enabled.

f. Legacy Redirection Mode.
Default Setting : Disabled
Recommended Setting : Disabled
Select Disabled.

This option allows the Redirection feature to work with the pre-AMT 7.0 remote consoles (need to set to Enabled).

20. Check KVM Configuration.

KVM feature Selection.
Default Setting : Enabled
Recommended Setting : Enabled

21. User Consent

a. User opt-in.

Default Setting : User Consent is required for KVM session
Recommended Setting : User Dependent

b. Opt-in Configuration from remote IT

Default Setting : Enabled Remote Control of KVM Opt-in Policy
Recommended Setting : User Dependent

Disable Remote Control of KVM Opt-in Policy – This option disables the Remote User's ability to select User OPT-IN Policy. In this case only the local user can control the opt-in policy.
Enable Remote Control of KVM Opt-in Policy - Enables Remote User's ability to select User OPT-IN Policy

22. Return to MEBx Main menu. And select Exit.

a. Select Y.

This will exit the MEBx Setup and save settings.

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

24. System will reboot.
25. Turn off system and remove power.

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

26. User plugs system into a power source and connects the network.

    Only use the integrated Intel NIC. Intel AMT does not work with any other NIC solution.

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

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

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

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

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

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

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

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

30. Setup and Configuration Server logs into AMT system with the username and password, and provisions all required data items:
    a. New PPS and PID (for future Setup and Configuration)
    b. TLS certificates
    c. Private keys
    d. Current date and time
    e. HTTP Digest credentials
    f. HTTP Negotiate credentials

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

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

Enterprise mode provisioning methods

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

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

Legacy AMT setup and configuration

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

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

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

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

IT TLS-PSK setup and configuration

IT TLS-PSK AMT setup and configuration is usually done in the IT department of a corporation. You will need a Setup and Configuration Server and network and security infrastructure to use this method.

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

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

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

OEM TLS-PSK setup and configuration

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

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

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

In the second stage, the customer receives the In-Setup systems and the PID, PPS, and password information. The PID, PPS, and password information is integrated into the customer Setup and Configuration Server. 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 Setup and Configuration Server port number and IP address. Contact your Management Console ISV for more details.

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

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

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

USB drive key setup and configuration

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

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

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

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 a Setup and Configuration Server through the console.
3. The Setup and Configuration Server will:
    a. Generate the appropriate amount of passwords, PID and PPS sets.
    b. Store them in its database.
    c. Return the information to the management console.
4. The management console writes the password, PID and PPS sets to a Setup.bin file in the USB drive key.
5. Technician takes the USB drive key to the staging area where new AMT platforms are located.
    a. Unpack and connect platforms if necessary.
    b. Insert USB Drive Key into a platform.
    c. Turn on that platform.

6. The system BIOS will detect for a USB drive key.
    a. If found, the BIOS will look for a Setup.bin file at the beginning of the drive key.
        i. Go to Step 7.
    b. If no USB drive key or Setup.bin file is found, then boot normally.
        ii. Ignore Steps 7-11.
7. The system BIOS will display a message that automatic setup and configuration will occur.
    a. The first available record in the Setup.bin will be read into memory.
        iii. Validate the file header record.
        iv. Locate the next available record.
        v. Invalidate current record so it cannot be used again.
    b. Place the memory address into the MEBx parameter block.
    c. Calls MEBx.
8. MEBx processes the record.
9. MEBx writes completion message to display.
10. The IT technician powers down the system.
    a. The system is in In-Setup phase at this time.
    b. It is ready to be distributed to user 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 setup and configuration.

Remote Configuration

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

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

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

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

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

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

Delayed network access, as the name implies, is remote configuration at a later time when an OS has been installed on the AMT system. In this implementation, setup and configuration is started when a

remote console application initiates the process by communicating with the ME through the HECI driver. This requires a functional OS and agent to be installed on the AMT system. Optionally, OTP authentication can be used. The remote console provides the OTP to the AMT system and to the SCS.

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

Remote configuration timeouts in HP systems

HP notebook PCs are shipped from the factory with the Remote Configuration Timer set to 0 (no Hello message broadcasting). In order to enable ME to broadcast Hello messages, an Activator local agent must be used.

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

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

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

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

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

Remote configuration 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(R) 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 OS and local agent must be installed on the AMT system.

MEBx and Hashes

AMT 7.0 has a feature in MEBx that allows IT administrators to manually activate a hash and add up to three additional certificate hashes. To enter the Remote Configuration screen in the MEBx:

1. Hit CTRL-P for the MEBx and enter the MEBx password.
2. Go into the Intel AMT Configuration option.
3. Go into the Setup and Configuration option.
4. Choose the TLS PKI option

a. Remote Configuration Enable/Disable

Default Setting : Enabled
Recommended Setting : Enabled
This option enables or disables Remote Configuration.

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

c. Manage Certificate Hashes
This option shows the hashes in the system including the name of the hash and whether it is active or not. If no hashes are in the system, then an option to add one is available. If hashes are available, then an option to delete one or more is available. To add a hash:
   i. Hit the Insert key
   ii. Type in a name for the hash
   iii. Type in the fingerprint of the hash
   iv. Choose to set this hash active or not

Hashes can be made active, not active, default, or not default in this screen.

d. Return to Previous Menu

List of Supported CA Certificates

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

- VeriSign Class 3 Primary CA-G1
  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-G2
  SHA1 Fingerprint: 85 37 1C A6 E5 50 14 3D CE 28 03 47 1B DE 3A 09 E8 F8 77 0F
- 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 known as Unprovisioning. An AMT setup and configured system can be unprovisioned through the ME Platform Configuration Screen and the Un-Configure Network Access option. Depending on how the system was previously provisioned, one or both unprovisioning options may appear.

1. Go into Unconfigure Network Access menu.
   a. Select the needed Unprovision mode.

      Full unprovisioning is available for Manual and Enterprise mode provisioned systems. It will return all AMT Configuration settings to factory defaults. All certificate hashes

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

b. Un-provisioning message will appear. This usually takes about one minute.
c. After unprovisioning is done, control is passed back to the AMT Configuration screen.

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

2. Return to previous menu.
3. Exit.
    a. Select Y.
4. System will reboot.

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

Full Return to Factory Defaults

All MEBx settings can be returned to the factory default by clearing CMOS. This includes resetting the password to the default "admin". 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.

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 PC that is also on the same subnet as the AMT PC.
3. Connect to the IP address specified in the MEBx and port of the AMT system.
    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 (IPV4 address)

    Example B: http://hpsystem.hp.com:16992 (from Steps 15 and 16h)

    Example C: http://[2001:ABC::ABC]:16992 (IPV6 address)

4. The management PC makes a TCP connection to the AMT system and accesses the top level AMT embedded webpage within the management engine of the AMT system.
5. Enter username and password. The default username is "admin" and the password is the one set during AMT Setup in the MEBx.

IMPORTANT

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

6. Review system information and/or make any necessary changes.
7. Exit.

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 displayed if set in F10 Setup.

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix B: Power / Sleep / Global states explained

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

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

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

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

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

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

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

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

M3 is the ON state for the ME when the system is in a non-S0 state. 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 M3 state.

Appendix C: Wake-On-ME explained

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

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.

For more information

To learn more about HP business notebooks, contact your local HP sales representative or visit www.hp.com/go/notebooks.

4AA2-xxxxENW, Created February 2011