



Guide

Intel® Centrino® with vPro™ Technology

Intel® Core™2 Processor with vPro™ Technology

Intel® vPro™ and Intel® Centrino® Pro Processor Technology Quick Start Guide

Based on Intel® Active Management Technology and HP Out-of-Band Manager v 4.0

Version 0.3

April 2009



Contents

Preface	3
Intended Audience.....	3
What This Document Contains	3
Process Overview	4
Section 3 - Deploying Intel® vPro Using Enterprise Standard Mode	
Provisioning	5
Process Flowchart.....	5
Intel vPro Enterprise Setup and Configuration Flow	6
Step 1: Configure Existing IT Infrastructure.....	7
Step 2: Verify Intel vPro Client Windows Drivers.....	8
Step 3: Install Intel SCS and HP OOBM Management Console.....	9
Step 4: Configure Intel vPro Client Authentication Settings	10
Step 5: Discover Intel vPro Clients through the Management Console	15
Step 6: Test Intel vPro Client Functionality in HP OOBMC.....	16
Step 7: Post Configuration.....	17
Appendix A: Troubleshooting	19
Appendix B: Glossary of Terms used in this guide	20

Preface

This document provides the high level steps required to deploy desktop and notebook PCs with Intel® vPro™ technology. It does not provide step-by-step procedures for completing those high level steps, but instead provides links to more detailed information where such step-by-step procedures may be found.

Note: Hewlett Packard* Out of Band Management (HP OOBM) software only supports Intel vPro Enterprise mode provisioning. HP OOBM supports both the standard and advanced modes of Enterprise mode provisioning. To get users started quickly, this guide will focus on Enterprise standard mode only. For the TLS advanced configuration, please refer to the HP OOBM manual.

Intended Audience

This Quick Start Guide is intended for Information Technology (IT) professionals, system integrators, and other technical specialists with experience deploying computer systems and networking technologies in an Information Technology environment. It is not intended for general audiences.

What This Document Contains

Section	Description
Process Overview	Provides a brief overview of the overall deployment process; lists high level steps, including decisions to be made, which are explained in more detail in subsequent sections.
Deploying Intel vPro Using Enterprise Standard Mode Provisioning	Provides the overall steps to deploy Intel vPro based systems into your IT environment using Enterprise Standard mode provisioning.
Appendix A: Troubleshooting	Provides information on correcting problems that may arise during deployment.
Appendix B: Glossary	Provides a list of terms used in this document and their definitions.

Process Overview

Intel® Active Management Technology¹ (Intel® AMT) provides significant flexibility in order to meet the needs of various customer environments. This flexibility requires that customers make a number of decisions when planning and implementing their deployment of Intel AMT enabled systems.

The overall deployment process is shown below:

- Install or validate infrastructure components (DNS, DHCP, SQL Server, etc.).
- Ensure required Windows* drivers (for SOL and IDE-R) are installed on Intel vPro clients.
- Install Intel® SCS and HP OOBM software.
 - Intel SCS and Intel vPro Setup: provides steps for setting up and configuring the SCS Provisioning Server and the Intel vPro device.
 - OOB Management Console Installation: specifies system requirements and tells you how to install, configure, and start the OOB Management Console.
- Configure your management console to manage Intel vPro clients.
- Discover Intel vPro clients in your management console.
- Test Intel vPro client management functionality in your management console.
- Perform post configuration steps (IT support process changes, maintenance procedures, etc.).

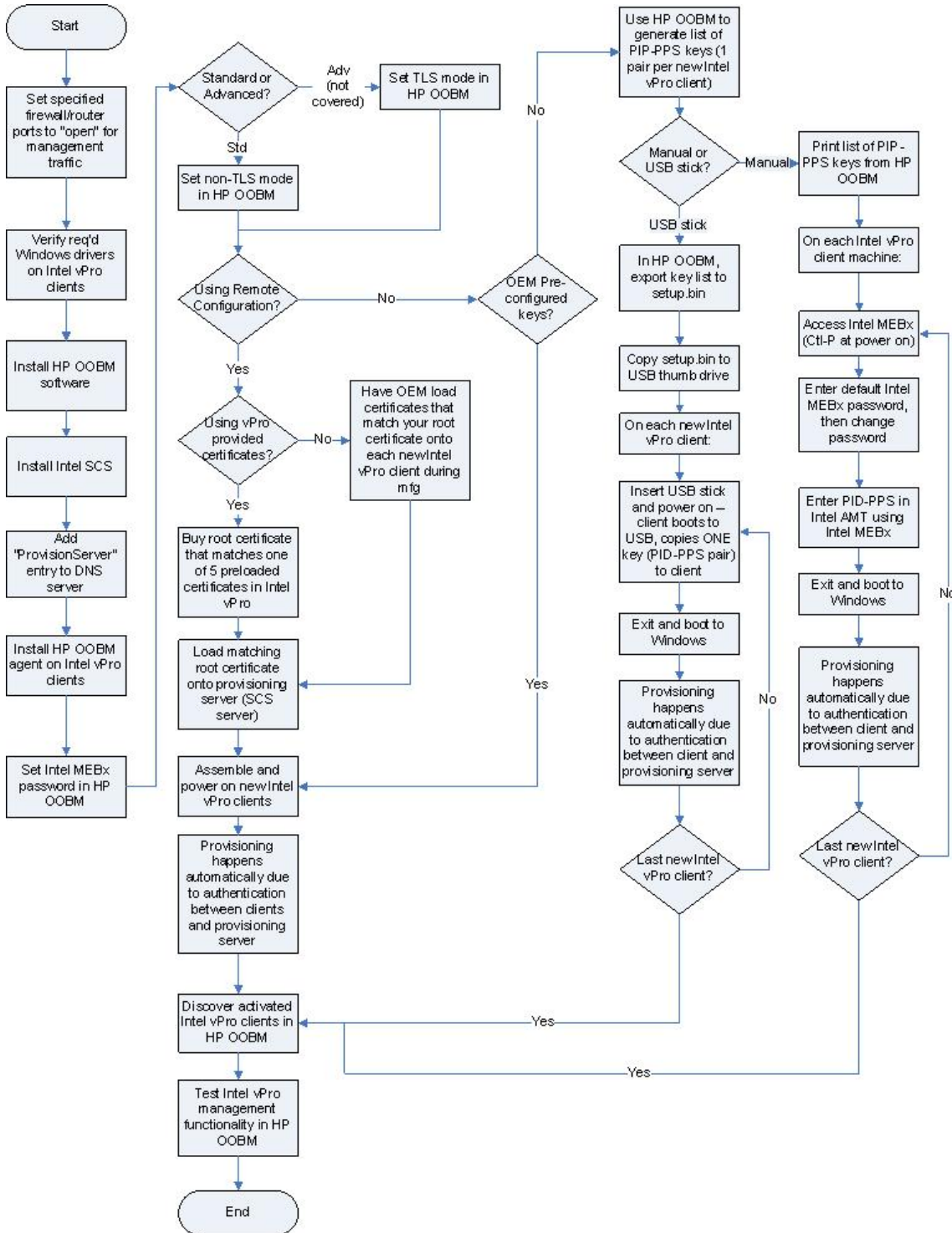
1. **Intel® Active Management Technology (Intel® AMT)** is a hardware-based technology that facilitates remote out-of-band management of computers by use of a small secondary processor located on the motherboard.

This out of band (OOB) controller has embedded firmware that runs on the Intel® Management Engine (Intel® ME), a separate small ARC architecture processor built into either the North Bridge or NIC of the motherboard. The Intel AMT firmware is stored in the same SPI flash memory component used to store the BIOS and is generally updated along with the BIOS.

Section 3 - Deploying Intel® vPro Using Enterprise Standard Mode Provisioning

Process Flowchart

The following picture shows the overall process flow for provisioning Intel vPro client systems in Enterprise (Standard and Advanced) mode. The steps for Enterprise Standard mode are described in further detail in this section.



Intel vPro Enterprise Setup and Configuration Flow

Prior to executing the steps for configuring the Intel vPro components (Intel AMT and Intel ME) in Enterprise standard mode, it is first important to understand the overall flow of the Enterprise mode configuration process

In Enterprise mode, an Intel vPro machine receives its configuration settings over the network, once it has been prepared with some initial setup information. The following diagram shows the modes or states that an Intel vPro device passes through before it becomes operational.

Intel vPro Configuration States:

1. Factory State

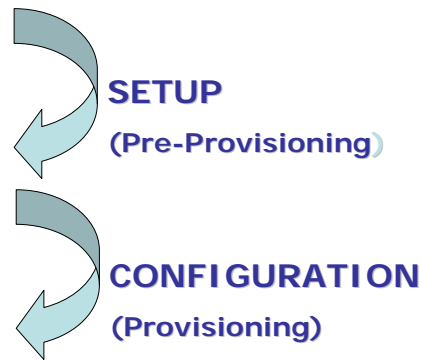
- AMT disabled
- No network configuration
- No security credentials

2. Setup State

- AMT enabled
- Basic network configured
- Admin credentials loaded

3. Configured State

- AMT fully configured (e.g power policies)
- Security credentials fully loaded
- Ready for remote management



Factory State: An Intel vPro machine comes from the OEM in Factory State. In this state Intel AMT is un-configured and not available for use by management applications. When an operator enters information via the Intel Management Engine BIOS extension (Intel MEBX) manually or with the aid of a USB storage device, the Intel vPro machine makes the transition into the setup state. See Step 3 – Configure AMT Client BIOS for instructions on how to prepare an Intel vPro machine to receive its configuration settings from a Setup and Configuration Server (SCS) which is part of HP OOBM distribution.

Setup State: When an Intel vPro machine enters Setup State it waits for delivery of its configuration settings from the SCS. After it enters setup mode, the Intel vPro machine periodically sends messages to the SCS. When the SCS receives messages from the Intel vPro machine, it responds by delivering the configuration settings and placing the device in Operational State.

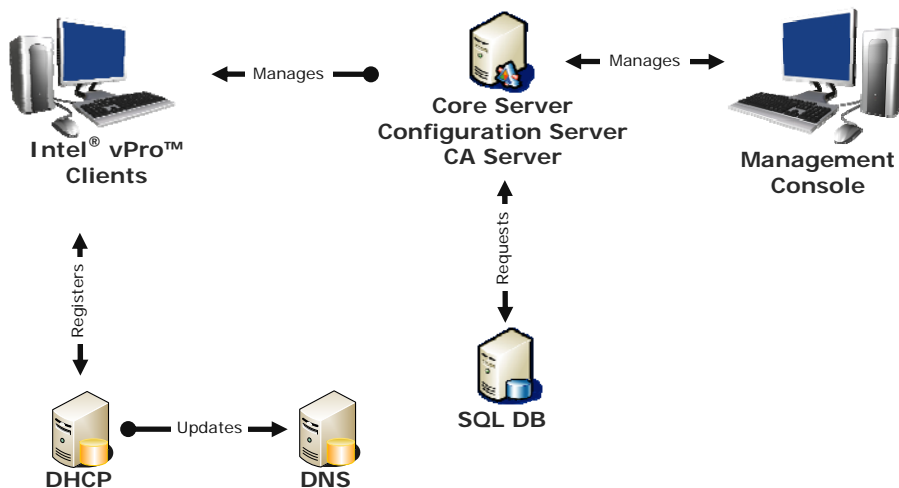
Operational State: The Intel vPro machine enters Operational State once its configuration settings have been supplied and committed. At this point the Intel vPro machine is ready to interact with HP OOBM management applications.

Step 1: Configure Existing IT Infrastructure

In order for an Intel vPro machine to be manageable, it must become known to the management console. The process by which this occurs is called “provisioning”. Enterprise setup (pre-provisioning) requires a series of steps that are performed on both the Intel vPro clients and the SCS in order to prepare the client for provisioning over the network by the SCS (which acts as the provisioning server for the Intel vPro clients).

Intel vPro Integration Points with IT Infrastructure Components

The following diagram shows the interaction with the different network elements. Each will be discussed briefly in order to understand the integration requirement.



DHCP Server: When an Intel vPro machine enters setup state, the default IP addressing scheme is DHCP (that is, use DHCP to obtain an IP address). The Intel® Management Engine (Intel® ME) also uses the DHCP server to help dynamically update the DNS server with its network address information. The DHCP server must support Option 81 to register network address information into the DNS server on behalf of the Intel ME. Option 15 should also be enabled in the DHCP Scope Options to allow the DNS to resolve host queries after IP address changes.

DNS Server: The DNS Server is used by network devices such as Management Consoles to locate address information for Intel vPro clients in order to contact them and manage them. The Intel vPro clients may also use the DNS server during the provisioning configuration phase to locate the provision server and request their configuration information, as explained below.

Once configured to the setup state, Intel AMT makes a DNS request for the name "ProvisionServer" (unless you choose to configure the client's BIOS manually). If the requested name cannot be resolved by the DNS server, then a second request is made for "ProvisionServer.DomainName." Intel AMT expects to either find the IP address of the provision server in this way, or by having it set explicitly in the Intel MEBX configuration process (Step 4: Configure Intel vPro Client Authentication Settings, page 10). The Intel Management Engine BIOS Extension (Intel MEBX) is an option ROM module extension to the system BIOS, provided to the OEM by Intel. The Intel MEBX allows you to configure settings that

control the operation of the Management Engine which runs on the Intel AMT client. For more information on Intel MEBX, see the *Intel Management Engine BIOS Extension User's Guide*.

Step 1a: Manually register the "provision server" entry into the DNS server.

Manually register the "provision server" entry into the DNS server.

Step 1b: Set Firewall/Router Ports Open for Management Traffic

Intel AMT requires certain ports to be "open" in order to allow management traffic through them. The Intel AMT ports are 16992 (non-TLS), 16994 (non-TLS redirection), – these are IANA-assigned ports which Intel purchased. They cannot be changed. Port 9971 is used in Enterprise mode to listen for "Hello" packets. This port is configurable in the SCS console.

Step 1c: Database Server Integration:

Intel vPro machines will have information about them (inventory) stored in a repository used by the management console. With HP Software management products, Microsoft SQL 2005 is the primary choice.

Step 2: Verify Intel vPro Client Windows Drivers

The following Intel AMT drivers, which are digitally signed by Intel and compatible with Microsoft Windows* operating systems (including Windows 2000, Windows XP, and Windows Vista*), are required on the Intel vPro client platform. Obtain these drivers from your client system manufacturer's driver and download support pages (most client drivers and Intel MEBX updates are contained on the same support web page by the OEM).

- **Intel Management Engine Interface (Intel MEI) driver** -- Provides a secure local communications interface between the host operating system and the Intel ME via the Intel MEI.
- **Serial-over-LAN (SoL) driver** -- Enables a COM port for VT100 or ANSI remote sessions prior to graphic interface when the operating system loads. You can view and send commands to a remote client prior to the operating system loading, including entering into the BIOS, viewing POST, etc.
- **Local Management Service (LMS) driver** –Provides an interface enabling local management software agents to communicate with the Intel Management Engine using the same high-level protocols as those used for remote management (e.g. XML, SOAP). When first loaded, the driver will cause a pop-up to occur to confirm that Intel AMT is running. The pop-up can be disabled. As the Intel AMT firmware is updated, this driver is most likely to require a coordinated update as new features are enabled. The driver also checks for consistency of the Intel AMT hostname and the operating system host name.

It is recommended that the HP OOBMC client agent also be installed, although it is not required. This agent will communicate with the Intel AMT watchdog timer on the client local system in order to provide the agent present functionality. The agent software “oobmlocalagent.msi” is located in LocalAgent sub-directory in the HP OOBM software distribution. A manual installation is recommended for a small number of test systems. There are other ways to install this agent software automatically, which are described in the HP OOBM Console Guide (OVCOutOFBandMgtConsoleGuide.pdf) under Chapter 2, “Installing the Local Agent”.

Step 3: Install Intel SCS and HP OOBM Management Console

The following two software packages need to be installed:

- Setup and Configuration Server (SCS): includes the installation executables ATMConfServer.exe for the server portion and AMTConsole.exe for the console. For details on the SCS installation, please refer to “Intel_AMT_SCS_Installation_Guide.pdf” Part 9-10. Note that the SCS software is available in the HP OOBMC distribution under the SetupConfService folder.
- HP Out-of-Band Management Console (HP OOBMC): Please refer to the HP OOBMC guide (OVCOutOFBandMgtConsoleGuide.pdf) Chapter 3 “Installing the OOBM Management Console” for details on installing the HP OOBM software.

After the SCS and OOBMC are installed, a vPro profile needs to be created. A profile allows configuration of multiple Intel AMT platforms with certain configuration properties. A profile defines the security settings of the communication with the platform, the network environment, and more. For a quick start, a basic profile is created with minimum settings. For the detail and screen shots, please refer to “Intel_AMT_SCS_Console_Guide.pdf” Part 4 “Creating and Changing Profiles”.

1. In the Console tree, right-click the Profiles element and choose Add Profile. Alternatively, in the Welcome window, click Create a Profile. The Profile Creator wizard opens.
2. Click Next. The New SCS Profile Wizard opens, displaying the Before You Begin section, which contains information on creating profiles.
3. In the Basic Settings section, click General and enter Profile Name and Description area.
4. Checked ACL in the Profile Components section, the wizard displays the Access Control List (ACL) settings.
 - a. To add a new user, Click Add. The ACL Details window opens.
 - b. To create a digest users, Select Digest User in the User Type section. Enter the user name and password, and confirm the password. Then, select PT_administration right to this user and Apply the setting.

During the Intel vPro system provision stage, the Intel vPro systems need to be connected through a wired network. For Intel Centrino vPro systems, the WiFi option needs to be added so that the wireless systems can be managed after being provisioned. Please refer to Intel_AMT_SCS_Console_Guide “Configuring WiFi” section for the detail.

Step 4: Configure Intel vPro Client Authentication Settings

In Enterprise mode, configuring the authentication settings on the Intel vPro clients can be performed in either of the following three ways:

- Remote Configuration (Intel AMT 3.0 or higher) – Step 4A below
- OEM pre-configuration – Step 4B below
- One-touch configuration (using a USB thumb drive or manual entry) – Step 4C below

Step 4A: Remote Configuration (Intel AMT 3.0 or higher) – Factory State to Configured State

Remote Configuration uses matching certificate hashes on the Intel vPro clients and the provisioning server to authenticate interaction between the clients and the server. Once the client and server authenticate each other (i.e., the certificate hashes match), the provisioning server automatically begins provisioning the client.

With Remote Configuration, you have two choices:

- Use your own root certificate, if you already have one
- Use one of the certificate hashes provided with Intel vPro (i.e., already on the client systems)

Using your own root certificate: If you already have a root certificate on your SCS server, then you need to do one of the following:

- instruct your Intel vPro client manufacturer (OEM) to place a matching certificate hash on each Intel vPro client during manufacture
- manually enter the matching certificate hash using the Intel MEBX on each Intel vPro client before deployment

If you instruct your OEM to load the certificate hashes onto your Intel vPro clients, the clients will already have a certificate hash that matches the existing root certificate on your provisioning server when they arrive. This will allow Intel vPro clients to establish a secure communication channel to exchange the certificate information to ensure the authenticity of the Intel vPro clients. But the provisioning process still depends on the Intel vPro Technology Activator to initiate the process.

The Intel® vPro™ Technology Activator Utility is the next generation of the Remote Configuration tool. A Windows executable that runs locally on an Intel AMT enabled platform, the Activator does the following:

- Simplify the process of configuring the Intel vPro systems via Intel SCS
- Facilitate initial Intel AMT configuration or policy change
- Address the following scenarios:
 - Intel vPro failure to find the Setup and Configuration server in the network
 - Expiration of Intel vPro 'hello' messages
- The configuration server must get the parameters necessary to start the Intel vPro configuration process

- Intel vPro system becomes unreachable if OS/AMT host names go out of sync
- Some Intel vPro systems are shipped with management mode disabled. Remote Configuration must be enabled by a local software tool

For more information about the Activator, see the [Intel® vPro™ Technology Activator Utility user guide](http://software.intel.com/en-us/articles/intel-vpro-technology-activator-utility/), which is available at <http://software.intel.com/en-us/articles/intel-vpro-technology-activator-utility/>.

Skip to Step 5: Discover Intel vPro Clients through the Management Console, on page 15.

Using one of the certificates provided with Intel vPro: If you want to use one of the certificates provided with Intel vPro, you will need to purchase a matching root certificate, and load it onto your SCS server. Once a matching root certificate is present on the provisioning server, the Intel vPro clients will automatically authenticate themselves with the provisioning server at power on, and will then automatically be provisioned by the provisioning server.

The certificates are purchased from one of the approved Certificate Authority (CA) vendors, such as VeriSign, Comodo, Go Daddy, and Starfield. Check with your OEM to see which of these CA vendors they support. The detail steps to purchase the certificate is available at <http://communities.intel.com/docs/DOC-1916>.

Once the pending certificate request has been completed with the .CER file provided, the target website used for this process has been assigned the issued certificate. In addition, a backup copy of the certificate is recommended.

In SCS 5.0, which is part of the HP OOBMC 4.0 distribution, the loadcert.exe is no longer needed. Therefore it is not necessary to run the last step “Run LoadCert.exe to Complete the Certificate Process” of the certificate import procedure described in the <http://communities.intel.com/docs/DOC-1916>.

For more about how remote configuration works, please refer to Intel_AMT_SCS_Console_Guide.pdf, Appendix A.

If you want to use one of the certificates provided with Intel vPro, the clients will already have a certificate hash that matches the purchased root certificate on your provisioning server. This will allow Intel vPro clients to establish a secure communication channel to exchange the certificate information to ensure the authenticity of the Intel vPro clients. But the provisioning process still depends on the Intel vPro Technology Activator to initiate the process, which is described in the previous section “**Using your own root certificate**”. For more information about the Activator, see the Intel® vPro™ Technology Activator Utility user guide, which is available at the following website:

<http://software.intel.com/en-us/articles/intel-vpro-technology-activator-utility/>.

Skip to Step 5: Discover Intel vPro Clients through the Management Console, on page 15.

Step 4B: OEM Pre-configuration – Factory State to Configured State

Most OEMs are willing to provide the service of changing the Intel vPro client from factory state to setup state by entering the password and client authentication information into the Intel MEBX on each client system for you. This often requires an additional fee to the OEM. This method is most useful when an Intel vPro client machines are to be delivered directly to the end user from the manufacturer.

The authentication information (security keys) can be provided to the OEM for loading into the client system's BIOS (via the Intel MEBX), or the OEM could provide you with a list of keys they generated. The keys must match between the Intel vPro machines and the management console. The management consoles have an option to import and export keys to facilitate this transaction.

If you ordered your Intel vPro client systems pre-configured with Intel MEBX password and client authentication information already loaded by the OEM, then they are already in a Setup state. When you connect the client systems to the network and power them on they will automatically authenticate themselves with the provisioning server and provisioning will occur (assuming you performed Steps 1-3 above). Then they will be in a Configured state, ready to be discovered and managed by the management console.

Skip to Step 5: Discover Intel vPro Clients through the Management Console, on page 15.

Step 4C: One-Touch Configuration of Intel vPro Client - Factory State to Setup State

The Intel vPro clients need authentication information configured on them so that they can authenticate themselves to the provisioning server; otherwise the server won't provision them. This authentication information is made up of a Provisioning ID (PID) and a Provisioning Pass-phrase (PPS). Together they are referred to as a PID-PPS pair. The server maintains a list of valid PID-PPS pairs, which is matched against any incoming PID-PPS pair from a client requesting provisioning. If the client's PID-PPS matches one of the entries in the server's list, that client is provisioned.

Step 4C-1: Confirm Latest BIOS Version: It is important that you use the latest BIOS and firmware version from the Original Equipment Manufacturer (OEM). Please visit their website to determine the latest versions. If an update is needed, follow the instructions provided by the OEM to implement the update.

Examples of OEM BIOS updates

- HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareIndex.jsp?lang=en&cc=us&prodNameId=3232116&prodTypeId=12454&prodSeriesId=3232030&swLang=13&taskId=135&swEnvOID=1093>
- Lenovo: <http://www-307.ibm.com/pc/support/site.wss/MIGR-67881.html>
- Dell: http://support.dell.com/support/downloads/driverslist.aspx?c=us&l=en&s=gen&ServiceTag=&SystemID=PLX_PNT_P4_745C&os=WW1&osl=en&catid=&impid=

Step 4C-2: Create PID-PPS security keys in SCS. Before you can configure the PID-PPS information on the Intel vPro clients, you need to generate that information in the SCS console.

To create TLS-PSK security keys in SCS, do the following:

1. In the Advanced element, right-click TLS-PSK Configuration Keys and choose Add Security Keys. The Security Key Settings window opens.
2. Specify the following information where applicable:
 - Number of keys to store: The number of keys that you want to create (up to 1024 keys)
 - Manufacturing default MEBx password: the MEBx password that was entered in the firmware by the manufacturer.
 - New MEBx Password: Choose the type of new MEBx password:
 - Fixed Password: To use the same password with all the keys, choose this and enter the password that you want to use.
3. Click OK. The Intel SCS creates a list of Security Keys. See the MEBx Settings pane to configure the number of keys generated. Each record consists of an 8 byte PID, a 32 byte PPS and the administrator's password.

Step 4C-3: Configure Intel vPro Clients Using a USB Thumb Drive: In this method, the new password and the PID/PPS keys are exported from the management console onto a USB thumb drive.

To export the list of keys to a USB drive:

1. Attach a USB drive to a USB port on the server on which the Console is running.
2. In the Advanced element, right-click TLS-PSK Configuration Keys and choose Export Keys to USB Drive.
3. In the USB Drive list, choose the drive to which you want to export the keys.
4. To export existing keys, select the Export option. Then specify the number of keys that you want to store on the drive (up to 1024 keys). Click **Next** to export the keys and finish this procedure.

Note: *You can only use the USB key to transfer the PID/PPS information to the Intel MEBX one time per client system. A bit is set on the client once the transfer has been made and the client will not allow an additional transfer to occur unless the bit is reset. To reset this bit, you would need to clear the client Intel Management Engine by performing a Full Un-Provision in the Intel MEBX (reset to factory defaults).*

USB Thumb Drive Notes: You should use a USB 2.0 thumb drive and 2 GB or less. Format the USB drive in FAT 16 through any Windows client. *This must be in FAT 16, not FAT 32.* The file (setup.bin) that is created by the export function noted above MUST be the first file on the drive, to function properly. Once this file is on the drive, other files can then be added as needed.

You may need to try several USB drives to find one that works, and you may need to try both the front and back USB ports on the client system. Refer to the USB Provisioning Matrix for a list of tested drives: <http://communities.intel.com/docs/DOC-1247#USB2>

Once you have configured your clients using the USB thumb drive, skip to Step 5: Discover Intel vPro Clients through the Management Console, on page 24.

Step 4C-3a: Manual Configuration of the Intel vPro Clients (alternative to USB drive method): Use this method to manually enter the password and PID-PPS credentials for each Intel vPro client machine.

A minimal amount of information is required to change the Intel vPro client from Factory Mode to Setup Mode. The information required includes:

- Change Intel MEBX password (change from factory default). The default password is “admin.” The new ME password must meet “strong” password criteria which include:
 - Be between 8 and 32 characters long
 - Contain both upper and lower case Latin characters
 - Have at least one numeric character
 - Have at least one ASCII non-alphanumeric character (!, @, #, \$, %, ^, &, *)
- Provisioning ID (PID) and Provisioning Pass-Phrase (PPS). These are used to perform the necessary steps of authenticating a new client and initiating the provisioning process. This uses Transport Layer Security (TLS) Pre-shared Key (PSK) for authentication.

To manually update the Intel vPro clients with new Intel MEBX passwords and valid PID-PPS security keys, do the following on each client system:

1. Start the client system, then press Ctrl-P during startup to enter the Intel MEBX.
2. Change the Intel MEBX password to a “strong” password (use the same password for each client system).
3. Select **Intel AMT Configuration**, then **Setup and Configuration**, then **TLS-PSK**, then **Set PID and PPS**.
4. Enter one of the PID-PPS combinations from the list of PID-PPS pairs you generated in SCS console (Step 4C-2 above).
5. Exit the Intel MEBX and reboot the client system to the Windows OS.
6. Repeat for each Intel vPro client.

Note: *Once the client boots to Windows, it will automatically authenticate itself with the provisioning server and provisioning will occur.*

See the *Intel Management Engine BIOS Extension (Intel MEBX) User's Guide* for detailed information about configuring the Intel ME and Intel AMT using the Intel MEBX.

Skip to Step 5: Discover Intel vPro Clients through the Management Console, on page 15.

Step 5: Discover Intel vPro Clients through the Management Console

After provisioning the vPro device in one of ways described in the previous section, you can view it in the vPro SCS console.

1. Open the vPro SCS Console.
2. Expand the Intel AMT Systems branch and select the target vPro device. The target vPro device is displayed with its provisioning status.
3. Depending on the provisioning approach, there are two different provisioning status associated with vPro systems.
 - a. If the Intel vPro system is provisioned with the remote configuration method described in the 4A, the system status will transition from unprovisioned to provision state automatically using a PKI key.
 - b. If the Intel vPro system is provisioned with the other methods, there are several steps to complete the provision process.
 - i. Select an unprovisioned Intel vPro client using a Pre-Shared Key (PSK). Enter the Intel AMT machine's Fully Qualified Domain Name (FQDN) in the relevant fields. If there are multiple systems shown at the same time, administrator needs to manually find out which UUID matches to which FQDN.
 - ii. From the Profile list, choose the profile that you want to use to configure the Intel AMT system
 - iii. Click OK to save the setting. Then, the status of the Intel vPro system will change from unprovisioned state to provisioned state. Since the handshaking between the Intel vPro system and Intel SCS takes time, the state transition can take a few minutes to complete.

Step 6: Test Intel vPro Client Functionality in HP OOBMC

After the device has been discovered and added to the management database, it is a good idea to test the functionality of the Intel vPro machine. To do that, you must login to the HP OOBM console as an administrator (see HP OOBM Console User Guide [OVCOutOfBandMgtConsoleGuide.pdf](#) Chapter 3 “Starting the OOB Management Console” section and Chapter 5 “Getting Started Managing OOB Devices” for detail). Once you have logged in to the HP OOBM console as an administrator, perform the following steps to test the Intel AMT client functionality.

Step 6a: Test Intel vPro Client Functionality From HP Software

At a minimum, look at the following Intel vPro Options to test that the Intel AMT configuration has been successfully completed:

- discover the Hardware Assets on all of the provisioned OOB devices on your network.
Remote Boot Manager – Power On/Off
- Remote Boot Manager using Console Redirection (Serial over LAN /SOL) and IDE Redirection

For further information on testing these features, refer to [OVCOutOfBandMgtConsoleGuide.pdf](#) Chapter 6 “OOB Management Use Case Scenarios”.

Step 6b: Test Intel AMT Client Functionality Using Intel AMT Web Console

1. On the management console system, login as an administrator created in Step 3 with user rights.
2. Open a web browser and enter the IP address and assigned port number (16992 for non-TLS) in the browser address bar (example, <http://192.168.0.1:16992>).

The following web browsers are supported:

- Internet Explorer* 6.0 SP1 or later
 - Netscape* 7.2 for Windows and Linux
 - Mozilla Firefox* 1.0 for Windows and Linux
 - Mozilla 1.7 for Windows and Linux
3. Once the Intel AMT Configuration Web Page is displayed, login using the Intel MEBX username and password. You can then view the following client management information:
 - System Status
 - Hardware Information
 - Event Log
 - Remote Control
 - Network Settings
 - User Accounts

Step 7: Post Configuration

Once you've deployed and configured your Intel vPro client machines, there are still some additional actions you should consider.

Adding New Devices:

As new Intel vPro clients are added to the network you will need to perform the deployment process described above to activate Intel AMT on the new devices, discover the new devices, and then add them to your management database. This procedure should be added to your standard maintenance procedures.

Updating Procedures to Include Intel AMT Features:

Work with your management console to determine how best to utilize the new capabilities available to you through your Intel vPro devices. Further, it is a good idea to update your procedures to utilize Intel vPro features, such as those procedures your help desk staff follow when helping users. For example, you will want to update the process to re-image a PC that has blue screened at a remote site using the new Intel AMT features now available in your management console.

Using Agent Presence (AP):

Agent Presence (AP) monitors for the existence of agents. The HP Software client agents must be installed on the client PC in order to use AP. The detailed procedures are described in the HP OOBM Console User Guide (OVCOutOfBandMgtConsoleGuide.pdf) Chapter 6 "Monitoring Security Software" section.

System Defense (SD):

System Defense (SD) does not require any agents to be installed on the Intel AMT client machine. System Defense policies may be configured on a per-machine basis.

There are four pre-defined SD policies:

- An FTP access policy which will trigger SD if an FTP access is made either to or from the Intel AMT client machine.
- A UDP flood policy which will trigger SD if Intel AMT sees at least 20,000 UDP packets per second and will monitor for a Denial-of-service attack.
- An SYN flood policy which will trigger SD if Intel AMT sees at least 20,000 IP packets per second and will monitor for a Denial-of-service attack.

- A Kill All NICs policy which will stop all network traffic except for HP Software management, Intel AMT, DNS, and DHCP traffic, thus isolating the client system from the network except for system management functions.

Once SD triggers an alert, the alert is displayed in the OOBM log. OOBM and Intel AMT limit network access by replacing the current client policy with the Kill All NICs policy when SD is triggered. Once the machine is remediated, the Kill All NICs policy is removed and the previous policy is re-applied. The administrator must manually perform the actual remediation of removing the virus or spyware, or fixing whatever caused the SD to be triggered. The detail procedures are described in the HP OOBM Console User Guide (OVCOutOfBandMgtConsoleGuide.pdf) Chapter 6 "Virus Infection Detection and Recovery" section.

Congratulations! You are now on your way to more productively managing a powerful computer system. This can improve your productivity and provide a valuable return on your investment.

Appendix A: Troubleshooting

The SCS service and the SOAP API issue error messages and information messages that are displayed in the console log. The messages actually displayed will be based on the filter selection on the Log page. There is a table lists the possible messages, causes, and a suggested action to remedy the situation, in case of an error. The detail information is available in the "Intel_AMT_SCS_Troubleshooting_Guide.pdf".

The troubleshooting guide also describes various issues and suggests solutions or debugging procedures.

Appendix B: Glossary of Terms used in this guide

BIOS: Basic Input Output System

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name Service.

Enterprise Mode: Provisioning model used for larger organizations

Intel® AMT: Intel® Active Management Technology allows Web Service calls to Intel desktops and notebook clients for out-of-band management and services.

Intel® Centrino® Pro processor technology: Intel processor technology that provides a higher level of security and management to mobile computers.

Intel® ME: Intel® Management Engine

Intel® MEBX: Intel® Management Engine BIOS Extension

Intel® vPro™ Processor Technology: Intel processor technology that provides a higher level of security and management to desktop computers.

ISV: Independent Software Vendor

LMS: Local Management Service driver. Provides an interface enabling local management software agents to communicate with the Intel Management Engine using the same high-level protocols as those used for remote management (e.g. XML, SOAP).

OEM: Original Equipment Manufacturer. Notation used to designate the PC manufacturer.

PID: Provisioning ID. First portion of security key used in provisioning Intel vPro machines.

PKI: Public Key Infrastructure

PKI CH: Public Key Infrastructure – Certification Hash

PPS: Provisioning Pass phrase. Pre-shared key used in provisioning Intel vPro machines.

PSK: Pre-shared key

SMB Mode: Small (and Medium) Business model used for provisioning an Intel vPro machine

TLS: Transport Layer Security

Intel® vPro™ and Intel® Centrino® Pro Processor Technology Quick Start Guide

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

Copyright © 2009 Intel Corporation. All rights reserved.

Intel®, the Intel logo, Intel. Leap ahead™, the Intel Leap ahead™ Logo, Centrino®, the Centrino® logo, Intel® Core™, vPro™, the vPro™ logo, Intel SpeedStep™, Pentium®, and Celeron® are registered trademarks of Intel Corporation in the United States and other countries.

Intel® Active Management Technology requires the computer system to have an Intel® AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see <http://www.intel.com/technology/manage/iamt/>



INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights.

Intel may make changes to specifications and product descriptions at any time, without notice.

Intel® Active Management Technology requires the platform to have an Intel® AMT-enabled chipset, network hardware and software, connection with a power source, and a network connection.