Guide

Intel® vPro™ Processor Technology
Intel® Centrino® Pro Processor Technology

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

Based on Intel® Active Management Technology Setup and Configuration Service

Version 1.0
July 2, 2007

Acknowledgments:

Thanks go out to all those who have contributed to this article in many different ways.

Primary Author: Michael Seawright, Intel Corporation
Major Contributors: Steve Davies, Intel Corporation
Steve Kahn, Intel Corporation
Terry Cutler, Intel Corporation
Bill York, Intel Corporation

Table of Contents

Executive Summary

Intel® Active Management Technology[1] (Intel® AMT) provides various configuration options for customers to use when deploying Intel® vPro™ and Intel® Centrino® Pro processor technology-enabled systems into their environment. This document will provide a step-by-step approach of what needs to be done to successfully deploy Intel AMT systems. It will not provide step-by-step instructions for each specific process as those are typically well documented in other Original Equipment Manufacturer (OEM) or Independent Software Vendor (ISV) articles. This document will provide references to the Microsoft SMS* add-on by Intel and the Altiris Out of Band Management Solution* applications. Both applications use the Intel® Setup and Configuration Service (SCS) as the foundation for provisioning an Intel AMT client. Other ISV applications that utilize SCS will follow a similar thought process.

Intel AMT provides significant flexibility in order to meet the needs of various customer environments. This flexibility leads to a number of decisions that have to be made as a customer plans and implements their deployment of Intel AMT-enabled systems. Some of the decisions can be made quickly depending on customer infrastructure and requirements. This document will highlight some of the clear-cut questions and provide links of where to go if further detail is required.

The order of some items can happen in parallel. For example, you could verify that the router will allow traffic through port 9971 (infrastructure setup) at the same time you are configuring the Intel AMT drivers on the client. For simplicity, we will proceed with the following approach:

- First decision. Decide whether to use SMB or Enterprise provisioning mode

We'll then divide into two sections, one for SMB and the other for Enterprise. The following major steps are followed in each section:

1. Install or validate infrastructure components (DNS, DHCP, SQL Server, etc.)

2. Install any components for your given management console solution

3. Configure Intel AMT client BIOS

4. Configure Intel AMT client Windows* drivers

5. Discover Intel AMT clients through the Management Console

6. Test Intel AMT client functionality

7. Post configuration

For Additional Information: Most sections will have a reference to additional information. Below are URLs where you can locate the documents referenced throughout the paper.

- Altiris® Out of Band Management Solution™ 6.1 SP1 Reference Guide
  http://www.altiris.com/upload/outofbandref_002.pdf
- Intel® Active Management Technology Setup and Configuration Service Installation and User Manual
  http://cache-www.intel.com/cd/00/00/32/09/320963_320963.pdf

Section 1: Provisioning Mode and Management Console

Provisioning Mode, SMB or Enterprise: The first decision to be made is whether to use the Small Business (SMB) or the Enterprise provisioning mode. There are several factors that will weigh into this decision, such as size of organization, security requirements, and IT infrastructure. The following set of questions can help make this decision clear.

Question	Yes	No
1. Do your security requirements require that all traffic from a management console to the AMT device be encrypted?	You must choose Enterprise	Both Enterprise and SMB have a non-secure option
2. Do your security guidelines require that you frequently change passwords and other management tasks from a central management console?	If yes, you should choose Enterprise	Password changes are more difficult with SMB
3. Is your infrastructure setup to support either Static IP or Windows Workgroups?	Choose SMB. They are not supported in Enterprise	Enterprise or SMB are options
4. Do you have frequent client changes (employee turnover, employee location changes, etc.) that would require client PCs to be re-imaged or be given a different computer name?	Enterprise recommended due to central "re-do"	Either Enterprise or SMB would work in a static environment
5. Not all management consoles support both SMB and enterprise mode. To date, all support at least SMB, but may not yet support Enterprise. Does your management console vendor support Enterprise mode?	You can choose between SMB and Enterprise	You must choose SMB mode until Enterprise becomes available
6. Do you require the use of Windows logon credentials to manage the Intel AMT device? By using Windows credentials you are able to simplify the administrative burden compared to using Digest authentication, which is the other option. Please note: In order to use Windows credentials it is necessary to extend the Microsoft Active Directory schema.	Enterprise is the only choice that supports Windows credentials	Enterprise or SMB are options

Through this short set of questions, if it is still not clear whether to use SMB or Enterprise mode, please refer to the more extensive document noted above. If you have decided that SMB mode is the correct decision, please proceed to Section 2 – SMB Mode. If your choice is Enterprise mode, please proceed to Section 3 – Enterprise Mode

Management Console: It is generally understood that a management console by an Independent Software Vendor (ISV) will be used. There are a number of ISVs that support Intel AMT. This document assumes that the customer either has experience with a console from a supporting ISV, or is in the planning process to purchase one. Although Intel AMT can be managed through a WebUI, it is not recommended to do this for a large-scale deployment. Combining the features of Intel AMT with that of a management console creates a very compelling return on investment and it is suggested that a management console be used as the management interface to the AMT functionality.
Please refer to the documentation from your chosen management console to determine whether they support both SMB and Enterprise mode. Some may only support SMB mode.

Section 2 – SMB Mode

Step 1: Determine IT Infrastructure Integration

The SMB mode has few integration points with the IT infrastructure compared to Enterprise Mode. It is important that you understand how each works.

DHCP or Static IP Client: Some computing environments require a static IP address on all clients (automated teller industry, for example). When a static IP environment is required, the infrastructure would be required to have a manual update of the “hosts” table typically in a DNS server and at the client. These settings are required for the client IP packets to be properly routed throughout the network. If static IP addressing is required, it is recommended that you use SMB mode. Keeping the hosts table updated is difficult and thus not a supported configuration in Enterprise mode.

With static IP, the Intel AMT client must have two IP addresses, one for the host OS and one for the Management Engine (ME). Static IP also requires a separate host (computer) name for the host OS and the ME.

If DHCP is supported, a single IP address and host name can be shared between the host OS and the ME. It is recommended that the client DHCP be configured to support Option 81. This option permits the client to provide its fully qualified domain name (FQDN) as well as instructions to the DHCP server on how it would like the server to process DNS dynamic updates (if any) on its behalf.

Firewall/Router Ports: Intel AMT requires certain ports to be “open” in order to allow management traffic to go through them. The Intel AMT ports are 16992 (non-TLS), 16993 (TLS), 16994 (non-TLS redirection), 16995 (TLS redirection) – these are IANA-assigned ports which Intel purchased, they cannot be changed. An additional port (9971) is used in the enterprise provisioning process, but is not required for SMB mode.

Management Console Dependencies: Please refer to the documentation of your chosen management console to determine whether other integration requirements exist for SMB mode.

Step 2: Install or Validate Management Console has Correct Intel AMT Support

Most management consoles have a slightly different process and/or set of components that are used to support SMB or Enterprise mode. Please refer to the documentation of your console vendor to determine that you have the proper components installed and configured properly to support SMB mode.

Step 3: Configure Intel AMT Client BIOS – SMB

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.

For more information (examples):

- 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=

Entering the Management Engine BIOS extensions (MEBx): The MEBx is an option ROM module provided to the OEM by Intel that is an extension to the system BIOS. The MEBx allows you to configure settings that control the operation of the Management Engine which runs on the Intel AMT client. We've seen two different methods to enter the MEBx.

- Ctrl+P. When booting the Intel AMT enabled system, after the BIOS entry screen has passed, another screen will display which prompts you to enter Ctrl+P which will then enter you into the management engine BIOS.
- BIOS. Some local OEMs have chosen to have the MEBx be a portion of their regular BIOS menu system. In this case follow the keystrokes to enter their BIOS settings (usually pressing F2 or Del).
  Default MEBx Password: Upon entering the MEBx for the first time, you will be required to enter the default password, which is "admin."

Change the MEBx Password: When you enter the MEBx for the first time, you will be prompted to change the password. The 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 (!, @, #, $, %, ^, &, *)

IP Addressing Scheme: SMB mode supports both Static IP and Dynamic Host Protocol Configuration (DHCP) for an IP addressing scheme. DHCP is the most commonly utilized scheme today and provides the easiest integration with Intel AMT. If DHCP is your choice, simply ensure that the DHCP value is set properly in the MEBx, which will typically be ("DHCP Disabled? No").

With static IP, the Intel AMT client must have two IP addresses, one for the host OS and one for the Management Engine (ME). Static IP also requires a separate host (computer) name for the host OS and the ME. To select static IP you will select "DHCP Disabled? Yes." You'll then be prompted to enter the IP information including IP address, subnet mask, default gateway, and primary and secondary DNS server.

A host name must be entered into the ME whether you choose static IP or DHCP within SMB mode. It is not necessary to enter the Domain name into the ME for SMB mode.

MEBx Recommendations: There are a number of parameters that are available for you to change in the MEBx. All fields will have a default setting that may slightly vary depending on manufacturer. However, there are some values you'll need to choose. For example, if your infrastructure supports Static IP, you'll need to change one entry that disables the DHCP and then fill in the entries for the Static IP address.

In the table, there are a few sections you'll need to pay particular attention to for SMB mode.

- Intel AMT Configuration Mode: Set to SMB
- Configuration Server Options: Not needed because these apply only to enterprise mode
- Intel AMT Hostname: In SMB mode this is required. If you use DHCP, this must match computer name in the host OS. If static IP is selected, this name must be unique from the computer name in the host OS.
- AMT Domain Name: This will match the Domain Name in the Host OS
- DHCP Enabled: It is recommended that you use DHCP, but in SMB, both DHCP and Static IP are supported.

Please refer to documentation provided by your hardware manufacturer to determine which settings you might need to change.

For more information:

- HP dc7700 Business PC - http://www.icare.hp.com.cn/TechCenter_StaticArticle/37022/44474.pdf

Step 4: Validate Intel AMT Client Windows Drivers

There are a few Intel AMT drivers for the client platform. It is recommended that the latest versions are obtained from the respective OEM driver and download support pages. The drivers and firmware are digitally signed by Intel, one of many security features for the platform. The operating system level drivers could easily be integrated into the client image. Drivers are compatible with Microsoft® Windows versions including 2000, XP, and Vista.

Below are short descriptions of the drivers and firmware.

- **Intel® Management Engine Interface (MEI) driver** -- Driver providing a secure local communications interface between the host operating system and the management engine (ME) via the Management Engine Interface (MEI).
- **Serial-over-LAN (SoL) driver** -- This 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** – The 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 management console agent is also installed, although not required.

For more information:

- See Step 3 above. Most client drivers and MEBx updates are contained on the same support web page by the OEM

Step 5: Discover Intel AMT Clients Through Management Console

The discovery of the Intel AMT enabled devices will vary depending on how the ISV has enabled this in their software. We've seen a couple of steps that are common among most of the vendors.

- **Device Discovery**: In this phase, the management console has a discovery mechanism to find the Intel AMT-enabled devices. This can be accomplished by a scan of an IP address range or other discovery mechanisms within the ISV application.
- **Database Integration**: Once the Intel AMT device is discovered, then it needs to be "imported" into the management console database. This could be a manual or an automatic method.

Each ISV will have variations of how these steps are performed, thus we don't go into detail on how they are accomplished. Please refer to the documentation by the chosen ISV to see how this step is handled within their application.

Step 6: Test Intel AMT Client Functionality

After the device has been discovered and added to the console database, it is wise to test the functionality of the Intel AMT device. Each ISV will have their own user guide which will provide a step-by-step approach of how to use each function. We suggest that you look at the following functions as a minimum to test that the configuration has been successfully completed:

- Asset Information
- Wake-up
- Remote control operations
- Serial over LAN (SOL) and IDE Redirection Operations

To test whether the Intel AMT system has been configured outside of the ISV management console, you can access the Intel AMT platform with a web browser. This can be used to view and update platform parameters. An administrator with user rights can remotely connect to the Intel AMT device by entering the IP address and assigned port number 16992 into the address bar of the web browser.
Example: http://192.168.0.1:16992

The following web browsers are supported:

- Internet Explorer* 6.0 SP1
- Netscape* 7.2 for Windows and Linux
- Mozilla Firefox* 1.0 for Windows and Linux
- Mozilla 1.7 for Windows and Linux

The web browser will establish a TCP connection to the Intel AMT system and access the top-level Intel AMT configuration web page. To view this information, you will be prompted to authenticate by logging in with the configured username and password. You then have access to see such things as:

- System Status
- Hardware Information
- Event Log
- Remote Control
- Network Settings
- User Accounts

Step 7: Post Configuration

Upon completion of the configuration steps, there are some additional actions you may choose to take.

Access Control Lists (ACL): The ME password is also used to log into the ME from a WebUI interface the first time. From this WebUI you are able to create additional users (access control lists – ACL) with different passwords and give users various rights to manage the Intel AMT device. Access can be limited to the following or with administrator rights you can manage all:

- Hardware Information
- Event Log
- Remote Control
- Update Firmware

Please keep in mind that in SMB mode, the ACLs are administered one at a time on each Intel AMT system. For a large organization, this would prove to be problematic and use of Enterprise mode rather than SMB mode should be considered.

Adding Devices: Keep in mind that as new Intel AMT clients are added to the network you'll need to run the same process identified above to discover the device and then add it to your management database. This should be added into any standard maintenance procedures you might have.

Process Changes: With the new capabilities available through Intel AMT devices, you should work with the management console to determine how to best utilize the new features. For example, you should document the process to re-image a PC that has blue screened at a remote site. Write down the process that the help desk agent should follow to do a remote boot and redirection to a stable image for the client. Such process changes are important for you to see the real value of the Intel AMT features.

Other Tasks: This section will be used as other follow up tasks are defined.

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.

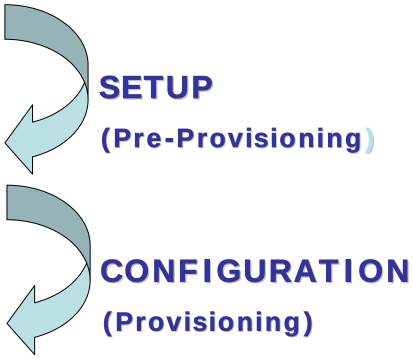
Section 3 – Enterprise Mode

Intel AMT Enterprise Setup and Configuration Flow

Prior to showing the steps that are needed to execute an Enterprise mode configuration, it is first important to understand the sequence of steps required to complete the process. An Intel AMT device receives its configuration settings over the network, after it is first prepared with some initial setup information. The following diagram shows the modes or stages that an Intel AMT device passes through before it becomes operational.

Intel AMT 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 Mode: Intel AMT comes from the OEM in Factory Mode. In this mode Intel AMT is un-configured and not available for use by management applications. When an operator enters information via the Intel AMT BIOS extension manually or with the aid of a USB storage device, Intel AMT makes the transition into setup mode. See Step 3 – Configure AMT Client BIOS for instructions on how to prepare an Intel AMT device to receive its configuration settings from a Setup and Configuration Application (SCA).

Setup Mode: When an Intel AMT device enters Setup Mode it waits for delivery of its configuration settings from a Setup and Configuration Server (SCS). After it enters setup mode, the Intel AMT device periodically sends messages to the SCS. When the SCS receives messages from the Intel AMT device, it responds by delivering the configuration settings and placing the device in Operational Mode.

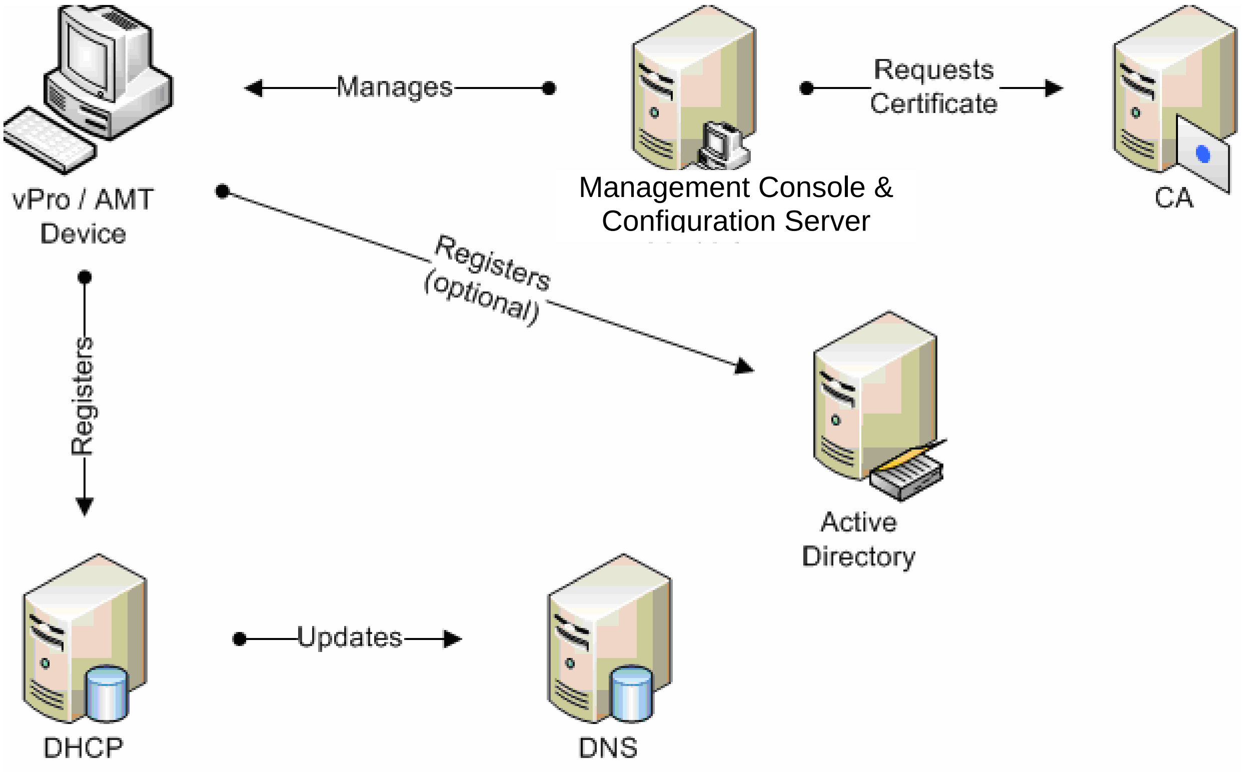
Operational Mode: Intel AMT enters Operational Mode once its configuration settings have been supplied and committed. At this point Intel AMT is ready to interact with management applications.

Step 1: Determine IT Infrastructure Integration

In order for an Intel AMT system to be manageable, the device must become known to the management console. The process by which this occurs is called provisioning. Enterprise setup requires a series of steps that include the client and a Setup and Configuration Server (SCS). Enterprise setup utilizes the network infrastructure to provide automated one-touch setup and configuration for Intel AMT platforms.

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

Intel AMT Integration Points with IT Infrastructure Components



DHCP Server: When an Intel AMT device enters setup mode, the default for IP addressing is for it to obtain an IP address from a DHCP server. The Management Engine (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 ME.

DNS Server: The DNS Server is used by network devices such as Management Consoles to locate address information for Intel AMT clients in order to contact them and manage them. The Intel AMT clients may also use the DNS server during the configuration phase to locate the provision server and request their configuration information. If the provision server IP address was not manually entered during the Intel AMT MEBx setup process, then the Intel AMT MEBx makes a DNS request for the name "ProvisionServer." 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 AMT MEBx configuration process.

It is required to manually register the “provision server” entry into the DNS server.

Firewall/Router Ports: Intel AMT requires certain ports to be "open" in order to allow management traffic to go through them. The Intel AMT ports are 16992 (non-TLS), 16993 (TLS), 16994 (non-TLS redirection), 16995 (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 at both the SCS console and the Intel AMT client.

Management Console Dependencies: Please refer to the documentation of your chosen management console to determine whether other integration requirements exist for SMB mode.

Active Directory Integration (optional): An optional integration point for the Intel AMT device is the Microsoft Active Directory (AD). This integration allows the management console to use the Kerberos authentication to securely manage Intel AMT credentials which simplifies single logon and administration. Currently (June, 07), the only management console that supports this integration is the Intel AMT add-on for SMS. The Setup and Configuration Service (SCS) installation includes scripts used by the administrator to:

- Extend the Active Directory schema to support the Intel ME class
- Populate the Intel ME attributes

During the configuration stage, Intel SCS

- Creates an Active Directory object representing the Intel AMT device
- Creates an attribute for connecting the AD computer object to the Intel AMT object

VB Scripts that are supplied with Intel AMT Setup and Configuration Server:

- Run BuildSchema.VBS (no parameters)
    - Extends AD schema
- Run CheckSchema.VBS
    - Verifies AD schema extended
- CreateUsers.VBS
- Creategroups.VBS
- CreateACL.VBS
    - These three scripts are used to create the required users, groups, and ACLs and provide necessary administrative rights to the ME objects in the Active Directory.

For proper operation, Microsoft hotfixes 899900 and 908209 are required for Kerberos to work with Intel AMT. The fixes can be downloaded from the Microsoft website and need to applied to all servers and consoles that will be communicating with Intel AMT devices. Windows Server 2003 Service Pack 2 (SP2) includes these fixes and do not require them to be applied. Windows Server XP requires the hotfixes. Investigation into the status of these with Vista remains open at date of printing.

For further information:

- Intel AMT SCS: Pages 7, 12-13, 17, 35, 98-99

.NET Framework 2.0 Integration: .Net is a prerequisite for Microsoft SQL Server 2005 and SQL Server Express. If either of these databases are going to be used the lNET framework will need to be installed. This is an easy installation that requires the user to only launch the installation package and follow the steps.

For further information

- Intel AMT SCS: Page 19
- Altiris OOBM Reference: Page 80

Database Server Integration: Intel AMT devices will have information about them (inventory) stored into a repository used by the management console. This engine will vary based on the needs of the console. We will use as our example using Microsoft SQL server for the integration discussion. Please check the requirements of the individual management console to determine which database will be appropriate for your needs. This will include knowing which version of the database is supported. For example, with the SMS add-on for Intel AMT, SQL Server Express, SQL Server 2005, and SQL Server 2000 (SP3) are supported.

During the integration or setup phase of the management console a new database is created that corresponds with the Setup and Configuration Application (SCA). The management console will create a connection to this database that can be secured or unsecured. For example, the SMS add-on for Intel AMT uses a secure HTTPS connection and LANDesk Server Manager uses an insecure HTTP connection. This is a choice of the console manufacturer on what is required.

After installation of the SCS database into SQL, you'll want to check to see that the proper access method is selected. For the SMS add-on for Intel AMT it would be required to select "Mixed Mode" for authentication (SQL Server and Windows authentication). Determine what authentication is required for your management console.

For more information

- Intel AMT SCS: Pages 20-24
- Altiris OOBM Reference: Pages 80-83

Certificate Authority Integration (optional): Transport Layer Security (TLS) is used to provide privacy and data integrity between communicating applications. It allows for Client/Server applications to communicate in a way to prevent eavesdropping, tampering, or message forgery. TLS is only available in enterprise mode provisioning with an Intel AMT device. A Certificate Authority (CA) is used to issue the certificates to the proper trusted devices within the network. The certificates can be stored in Active Directory, the management console database, or in the Intel AMT client, depending on the usage model and implementation.

CA integration is a very complicated subject. However, in an attempt to simplify the process we will show you the common flow of the certificate elements. You can then apply this common knowledge to the management console vendor's implementation of TLS.

The foundation of a CA is called the Root CA. The Root CA is a "trusted" source. This root CA could be purchased from an outside vendor, such as Verisign. If this were the case, Verisign has specific recommendations on how to keep your Root certificate secure. Certain polices and procedures are recommended to do this. Along with the Root CA, you can have sub-ordinate CAs. This allows you to have a distributed certificate network.
A PEM file is stored on the management console which defines the chain of authority; ie. the issuing CA, the signing CA, and then the trusted root CA.

In order to use TLS a root CA must be established. If one does not exist in your organization, the management console will recommend how to create this. In some cases, the root CA will be installed with the management software if you choose to use TLS during the installation. In other cases, you may be required to install the Microsoft Certificate Authority Server.

Each Intel AMT device that needs to communicate using TLS requires a Server Authentication certificate. A certificate is automatically requested from the CA on behalf of the Intel AMT client by the Setup and Configuration Service (SCS) when the Intel AMT client is configured to use TLS. The certificate is downloaded to the Intel AMT client by SCS and stored into NVRAM on the client. When a management console attempts to establish communication with the Intel AMT client, the client provides its certificate to the management console to verify its identity and allow a secure channel to be created. The management console must be configured to trust certificates issued by the CA that issued the certificate to the Intel AMT client.

Security can be further enhanced by using Mutual TLS. In this scenario, both the Intel AMT client and the management console are required to have certificates to verify their identity. When the management console attempts to establish communication with the Intel AMT client, the client provides its certificate to the management console and will also request a certificate from the management console in order to verify the identity of the management console before establishing a secure channel.

The high-level steps to follow would be:

- Create root certificate on your certificate authority
- Create a Server certificate to place on the Intel AMT device
- With Mutual TLS, you will also create a Client Authentication certificate to be placed on the management console

Each management console vendor handles this process differently. We will not attempt to show the actual steps, but we have found this process to be well documented by each of the management console vendors.

For more information:

- Intel AMT SCS: Pages 26-34
- Altiris OOBM Reference: Pages 84-85

Multi-Tiered Certificate Authority and Redirection: Certificate authorities can be configured in a hierarchy with the Root CA and subordinate CAs. When this configuration is utilized, there are some operations that need to know how to "walk the chain" of authority. Such an operation would be Serial over LAN (SOL) and IDE redirection (IDE-R) functions. A file is created called a "PEM" file that contains all the certificates in the chain. This will then be used by the client requesting a TLS session.

For more information:

- Intel AMT SCS: Pages 104-105

Microsoft IIS Integration: Your management console vendor may require a secure communication (SSL/HTTPS) to interface with the Microsoft IIS server. Most management console vendors have some sort of a web service interface. It may be accessed securely through HTTPS or not secured through HTTP. For example, with the Intel AMT SCS console, a secure connection is required to IIS. Therefore, the IIS server needs to be a trusted "Server" and receive a certificate from the CA. The SCS console will receive a certificate to authenticate to IIS.

For further information:

- Intel AMT SCS: Pages 31-33
- Altiris OOBM Reference: Pages 85-88

Step 2: Install or Validate Management Console has Correct Intel AMT Support

Most management consoles have a slightly different process and/or set of components that are used to support SMB or Enterprise mode. Please refer to the documentation of your console vendor to determine that you have the proper components installed and configured properly to support Enterprise mode.

Step 3A: Configure Automated Client Settings

The Setup and Configuration Application (SCA) allows the remote configuration of several MEBx settings. These settings will be pushed over the network to the Intel AMT client during the provisioning operation. The SCA is typically part of the management console, but can be a separate application as well.

Define General Parameters: There are a few parameters that can be applied to all Intel AMT devices when they receive the configuration from a Setup and Configuration Application (SCA).   Refer to your management console application on how these options are presented. Values that can be configured include:

- TCP Listen Port – This is the port that receives the “hello” packets from the Intel AMT device
- Integration with Active Directory
- Get New Intel AMT Properties From: Database or Script choices
- Service Maintenance Parameters

For further information:

- Intel AMT SCS: Pages 62-64
- Altiris OOBM Reference: Page 50

Create Client Profiles: Profiles determine which features are enabled on an Intel AMT device, what authentication mechanism will be used, and which users have access to device features. Depending on ISV implementation, one or many profiles may be defined. Each profile can be assigned to one or more Intel AMT devices. Profile settings will typically include the follow areas:

- User name and password (Intel AMT administrator name)
- Network settings: Ping allowed, VLAN, Enabled interfaces – WebUI, SOL, IDE-R, TLS Settings
- Certificates: CA Server Name, CA Type, Certificate Template
- Mutual Authentication (M-TLS) settings
- Access Control List (ACL) settings: Digest or Kerberos user
- Power Policy settings

Certificate Settings: Intel AMT devices can store a TLS certificate which will be used by the management console to provide secure authentication to the device. A certificate server must be present in the network to provide these certificates. Some ISV implementations require the Fully Qualified Domain Name (FQDN) of the certificate server to be defined.

Mutual Authentication: Some management consoles support mutual TLS (MTLS) authentication or two-way authentication settings. If MTLS is selected, a list of trusted root certificates will need to be imported into the database and Client Authentication certificates may need to be requested from the CA for each management console and installed onto those management consoles.

Access Control Lists (ACLs): In Enterprise mode you are able to configure (ACLs) that grant rights to administer the Intel AMT device. You are able to limit management to any of the following categories:

- Hardware Information
- Event Log
- Remote Control
- Update Firmware

ACLs can be administered centrally through integration with active directory by using Kerberos authentication. It is important for the ACLs to be kept updated so access to the Intel AMT devices can be properly controlled. The initial password for ACL authentication will be the MEBx password. When a profile is pushed to the MEBx a new password can be assigned to match the ACL. This password (aka Intel AMT credential) is different than the MEBx password.

Power Policy Settings: The ME can be configured to be on or off depending on the sleep state of the host computer.

For further information:

- Intel AMT SCS: Pages 65-73
- Altiris OOBM Reference: Pages 50-54

Configure Setup and Configuration Security Keys: Setup and configuration of Intel AMT 2.0/2.1/2.5 devices is done using the TLS-PSK (Pre-Shared Key) protocol to provide a secure method of configuration. The protocol requires a security key installed both in the Intel AMT device and in the SCS database. Setup at the Intel AMT device is addressed in the next section. Each management console that supports Enterprise mode will have a function which creates a security key containing a provisioning ID (PID) and provisioning passphrase (PPS) combination that will be used to authenticate Intel AMT devices. The console will display the values for manual entry into the Intel AMT device, or most have a method to export the security keys to a USB thumb drive for one-touch configuration. The export function contains the PID/PPS keys and will also change the factory default MEBx password to the new password. Remember, the new MEBx password must follow strong password standards.

Note. Do not confuse the TLS security keys that are part of management console interaction with the Intel AMT device and the TLS-PSK keys that are used during setup and configuration. These are separate keys. One the TLS-PSK keys are used during the setup and configuration stage, they are not used again unless an Intel AMT device is re-provisioned, whereas, the other TLS keys are used for all communications from the management console to the Intel AMT device.

For further information:

- Intel AMT SCS: Pages 74-76
- Altiris OOBM Reference: Pages 54-58

Step 3B: Configure Intel AMT Client BIOS – Enterprise

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.
For more information (examples):

- 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=

Configuration Method: With Enterprise mode you have the flexibility to choose a pre-provisioning method. A minimal amount of information is required to change the MEBx from Factory Mode to Setup Mode. The information required includes

- Change Intel AMT 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.

Enterprise mode provides the following choices in entering this information.

- **Manual Entry**: This method is used to manually enter the initial credentials for the Intel AMT device to complete the provisioning process. Open the Management Engine BIOS extension (MEBx), which is an option ROM Module provided to the OEM by Intel that is an extension to the system BIOS. The MEBx allows you to configure settings that control the operation of the Management Engine which runs on the Intel AMT client   We've seen two different methods to enter this Option ROM.
    - Ctrl+P. When booting the Intel AMT enabled system, after the BIOS entry screen has passed, another screen will display which prompts you to enter Ctrl+P to enter into the Management Engine BIOS.
    - BIOS. Some Local OEMs have chosen to have the MEBx be a portion of their regular BIOS menu system. In this case follow the keystrokes to enter their BIOS settings (usually pressing F2 or Del).

  When you enter the MEBx for the first time, you will be prompted to change the password. As noted above the default password (admin) must be changed to a strong password.

  Next, you will select the AMT Configuration option, then Provisioning Configuration (actual terminology may vary by manufacturer).

Provisioning Mode:	Enterprise
Provisioning Server Port:	9971 (you can change this but it is not recommended)
PID	Enter 8-character key
PPS	Enter 24-character key
Provisioning Server Address:	Enter the IP address of the SCA server (not required if "provisionserver" has been added to the DNS server)

  The PID/PPS keys will be generated by the Setup and Configuration Application (SCA). You will need to have a matching pair on the SCS and the client.

- **OEM pre-provisioned**: Most OEMs can provide you a service to change the MEBx from factory mode to setup mode by entering the information into the MEBx for you. This often requires an additional fee to the OEM. This method is most useful when an Intel AMT device is delivered directly to the end user from the manufacturer. The security keys could be provided by the customer to the OEM for integration, or the OEM could provide the customer with a list of keys they generated. The keys must match between the Intel AMT devices and the management console. The management consoles have an option to import and export keys to facilitate this transaction.
- **USB One-touch**: In this method, the new password and the PID/PPS keys are exported from the management console onto a USB thumb drive. The USB drive is then inserted into each Intel AMT system during boot up and the information is transferred to the ME. This method is most useful when a configuration area is used prior to deploying new systems to the end user.

  Note. You can only use the USB key once to transfer the PID/PPS information to the MEBx. A bit is set once the transfer has been made and it won't allow for an additional transfer, unless the bit is reset. To reset this bit, the client BIOS would have to be cleared (reset to factory defaults).

For further information:

- Intel AMT SCS Pages 53-57
- Altiris OOBM Reference: Pages 27-30

IP Addressing Scheme: Enterprise mode only supports Dynamic Host Protocol Configuration (DHCP) for an IP addressing scheme. Ensure that the DHCP value is set properly in the MEBx, which will typically be ("DHCP Disabled?   No").

MEBx Recommendations: There are a number of parameters that are available for you to change in the MEBx. All entries have been pre-set by the manufacturer to a default setting, which may vary. As mentioned above, in Enterprise mode a minimal amount of information is required to change from factory mode to setup mode. The process of provisioning which changes the Intel AMT device to the operational state is handled by the Setup and Configuration Service (SCS) and the infrastructure. More of this will be discussed in the Setup and Configuration Application (SCA) profile section.

The minimum amount of information required in the MEBx for the system to begin sending “hello” packets (described later) is:

- New MEBx password
- PID/PPS keys

Step 4: Validate Intel AMT Client Windows Drivers

There are a few Intel AMT drivers for the client platform. It is recommended that the latest versions are obtained from the respective OEM driver and download support pages. The drivers and firmware are digitally signed by Intel, one of many security features for the platform. The operating system level drivers could easily be integrated into the client image. Drivers are compatible with Microsoft® Windows versions including 2000, XP, and Vista.

Below are short descriptions of the drivers and firmware.

- **Intel® Management Engine Interface (MEI) driver** -- Driver providing a secure local communications interface between the host operating system and the Management Engine (ME) via the Management Engine Interface (MEI).
- **Serial-over-LAN (SoL) driver** -- This 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** – The 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 management console agent is also installed, although not required.

Step 5A: Client Provisioning. From Setup to Configured State

When the Intel AMT device has had the BIOS enabled through the above process it begins to send “hello” packets over the network. The Setup and Configuration Server (SCS) listens for these packets. Upon receipt the SCA will authenticate the Intel AMT device with the PID and PPS keys and use the PPS to establish a secure channel which is used to download the configuration information to the Intel AMT client. Once authenticated the Intel AMT device is considered in setup state. Depending on the parameters set in the general parameters and profile, the Intel AMT device can receive the additional settings. If your SCA allows the use of scripts, this process can be automated. If not, it may be necessary to manually apply profile settings to the Intel AMT device. Once these settings are applied to the MEBx, it is considered in the operational state and an entry is made in the SCA database.

Step 5B: Discover Intel AMT Clients through Management Console

When the SCA has the new Intel AMT device in its database it may or may not be in the database for the management console. For example, with the Intel SMS add-on a process must be followed to move an Intel AMT device into the management database.

For more information:

- Intel AMT Add-on for SMS: Page 7

Step 6: Test Intel AMT Client Functionality

After the device has been discovered and added to the console database, it is wise to test the functionality of the Intel AMT device. Each ISV will have their own user guide which will provide a step-by-step approach of how to use each function. We suggest that you look at the following functions as a minimum to test that the configuration has been successfully completed:

- Asset Information
- Wake-up
- Remote control operations
- Serial over LAN (SOL) and IDE Redirection Operations

To test whether the Intel AMT system has been configured outside of the ISV management console, you can access the Intel AMT platform with a web browser. This can be used to view and update platform parameters. An administrator with user rights can remotely connect to the Intel AMT device by entering the IP address and assigned port number 16992 into the address bar of the web browser.

Example: https://192.168.0.1:16993 Validate a TLS connection
http://192.168.0.1:16992 Validate a non-TLS connection

The following web browsers are supported:

- Internet Explorer* 6.0 SP1
- Netscape* 7.2 for Windows and Linux
- Mozilla Firefox* 1.0 for Windows and Linux
- Mozilla 1.7 for Windows and Linux

The web browser will establish a TCP connection to the Intel AMT system and access the top-level Intel AMT configuration web page. To view this information, you will be prompted to authenticate by logging in with the configured username and password. You then have access to see such things as:

- System Status
- Hardware Information
- Event Log
- Remote Control
- Network Settings
- User Accounts

Step 7: Post Configuration

Upon completion of the configuration steps, there are some additional actions you may choose to take and some regular processes you'll want to monitor.

Access Control Lists (ACL): The ME password is also used to log into the ME from a WebUI interface the first time. From this WebUI you are able to create additional users (access control lists – ACL) with different passwords and give users various rights to manage the Intel AMT device. Access can be limited to the following or with administrator rights you can manage all:

- Hardware Information
- Event Log
- Remote Control
- Update Firmware

Adding Devices: Keep in mind that as new Intel AMT clients are added to the network you'll need to run the same process identified above to discover the device and then add it to your management database. This should be added into any standard maintenance procedures you might have.

Process Changes: With the new capabilities available through Intel AMT devices, you should work with the management console to determine how to best utilize the new features. For example, you should document the process to re-image a PC that has blue screened at a remote site. Write down the process that the help desk agent should follow to do a remote boot and redirection to a stable image for the client. Such process changes are important for you to see the real value of the Intel AMT features.

Other Tasks: This section will be used as other follow up tasks are defined.

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: Glossary of Terms used in this guide

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

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

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).

MEBx: Management Engine BIOS extension

ME: Management Engine

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

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

ISV: Independent Software Vendor

SMB Mode: Small (and Medium) Business model used for provisioning an Intel AMT device

Enterprise Mode: Provisioning model used for larger organizations

DNS: Domain Name Service.

DHCP: Dynamic Host Configuration Protocol

BIOS: Basic Input Output System

TLS: Transport Layer Security

PID: Provisioning ID. First portion of security key used in provisioning Intel AMT devices.

PPS: Provisioning Pass phrase. Pre-shared key used in provisioning Intel AMT devices.

PSK: Pre-shared key

MEI: Management Engine Interface (MEI) driver

SoL: Serial over LAN driver

LMS: Local Management Service driver

ACL: Access Control Lists

SCS: Setup and Configuration Service

SCA: Setup and Configuration Application

OOBM: Out of Band Management Solution. Altiris application that accesses Intel AMT devices.

CA: Certificate Authority

NVRAM: Non-volatile Random Access Memory

IDE-R: IDE Redirection

Appendix B: Important Product and Legal Information

- Copyright © 2007 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 trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- 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.
- * Other names and brands may be claimed as the property of their respective owners.