



White Paper
Intel® Centrino® with vPro™
Technology
Intel® Core™2 Processor with
vPro™ Technology

Simplifying the Provisioning Process

Understanding the interaction of Intel® Active
Management Technology and the IT
infrastructure during the provisioning process



Introduction

Intel® Core™2 processor with vPro™ technology and Intel® Centrino® with vPro™ technology includes a core component called Intel® Active Management technology (Intel® AMT). Intel® AMT extends management capabilities for in-band and out-of band management. As a security measure, these features may not be active when received from the Original Equipment Manufacturer (OEM) vendor. Intel® AMT must be activated (or provisioned) in order to benefit from these additional management capabilities.

This paper focuses on four key aspects of enterprise mode provisioning of Intel® AMT systems.

- Overview of the provisioning sequence
- Preparing the provisioning environment
- Authenticating the client management engine
- Completing the provisioning sequence

This paper identifies the basic elements of the provisioning process, network infrastructure interaction, and related dependencies, and is not intended to provide a full overview of the provisioning process for Intel® AMT devices. It will help the desktop management and the network management teams understand the requirements to activate Intel® AMT successfully. This process, known as enterprise provisioning, is a simple and self-sustaining process once the upfront planning and infrastructural preparations are accomplished.

More details are included in the Intel® AMT Setup and Configuration Service Installation and User Manual.ⁱ

Overview of the Provisioning Sequence

Provisioning refers to steps required to configure the Intel® Management Engine securely within the enterprise client environment. Similar to an un-configured client operating system, initial trusted information and environmental configuration data is needed by the Intel® Management Engine. The Intel® Management Engine may be operational whether or not the client operating system is configured and operational.

A few basic steps must be completed to properly configure the Intel® Management Engine:

1. Setup of a supporting enterprise infrastructure and services for the provisioning sequence
2. Enabling Intel® AMT features on the client
3. Creation and distribution of authentication credentials or pre-shared secrets to the Intel® Management Engine and configuration service (e.g. ProvisionServer)
4. Intel® Management Engine locating the configuration service to which it will authenticate
5. Completing the authentication process with the configuration profile sent to the Intel® Management Engine.

The Intel® AMT system has a TCP/IP stack that is separate from that of the operating systemⁱⁱ which allows for client management when the operating system or supporting software agents are unavailable. For terminology purposes, this is referred to as out of band management.

During the provisioning process, Intel® AMT will interact with the DHCP and DNS servers to direct communications to the provisioning or configuration service commonly referred to as ProvisionServer. The pre-shared secrets are used to authentication and encrypt the session during the configuration or provisioning process.

The following diagram provides a simplified view of the sequence

1. Pre-shared secretsⁱⁱⁱ are generated or associated to the ProvisionServer.
2. The pre-shared secrets are distributed to the Intel® Management Engine.^{iv}
3. With the Intel® Management Engine in setup mode, an IP address and associated DHCP options are obtained.
4. The Intel® Management Engine requests resolution of "ProvisionServer" based on the specified DNS domain
5. The "hello" packet is then sent to the ProvisionServer for authentication and the provisioning process completes

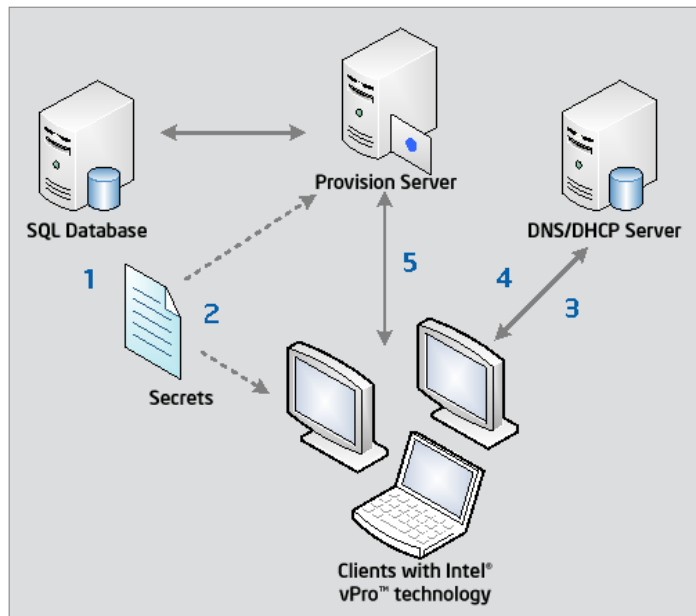


Figure 1 - Simplified enterprise provisioning sequence for client systems with Intel® vPro™ technology.

As noted in the above diagram, the success of the Intel® AMT client is dependent upon key infrastructure components and interactions. In addition to provisioning of the Intel® Management Engine, the operational aspects of the solution will most likely require adjustments to the associated IT governance and processes. For these reasons, a successful deployment of Intel® Core™2 processor with vPro™ technology is best realized by the collaborative efforts of client, server, infrastructure, operations, and other teams.

Preparing the Provisioning Environment

Automated and central provisioning of Intel® AMT devices is supported by a web service or server referred to as ProvisionServer. The configuration of this service requires connectivity to a database which holds the configuring service settings and configured client settings. The configuration service settings include pre-shared secrets to authenticate clients to the service, configuration profiles which the target clients will receive, access control to the service console, and so forth.

Once properly configured, the provisioning service responds to network packets being sent from the Intel® AMT clients. These packets are known as "hello" packets. The hello packets need to navigate the corporate network infrastructure to reach the provisioning service. The received requests contain a portion of a pre-shared secret which will be discussed in the next section.

Once requests are received and validated, the provisioning service awaits the manual or automated inputs necessary to determine the correct client identification mapping, configuration profile, and related information to complete the provisioning process.

Based on the above information, the following infrastructural and service preparations are required:

- Provisioning service has been installed within the enterprise environment
- Users have been granted sufficient rights to administer the service
- Pre-shared secrets have been generated and associated to the service and target clients
- At least one Intel® AMT client configuration profile has been defined within the provisioning service for most ISV applications.

White Paper: Simplifying the Provisioning Process

- A provisioning script or method to obtain and assign the necessary properties has been defined^v
- The correct network ports are open for the provisioning sequence. Intel® AMT utilizes ports 16992-16995, which are assigned to Intel. Network 9971 is the default provisioning port.
- "ProvisionServer" DNS Alias or CNAME record has been generated to direct resolution to the provisioning service
- Resolution of the DNS entries for the ProvisionServer have been confirmed
- Client DNS objects are supported and updated in the environment.

Most of the steps and processes are defined within specific client management solutions which support clients with Intel® vPro™ technology or within the [Intel® Setup and Configuration manual](#). Two key focus points will be addressed in the remainder of this section: DHCP and DNS.

DHCP: Dynamic IP addressing is most common for client computing systems and will be the focus point for this paper in regards to provisioning PCs with Intel® vPro™ technology. The same physical port is used for Intel® Management Engine and client operating system TCP/IP network stacks, enabling the Intel® Management Engine to snoop DHCP related traffic destined for the client operating system. This allows the Intel® Management Engine to assume the same IP address as the client operating system. Intel® Management Engine can also negotiate an IP address if the client operating system TCP/IP stack is not available or functional.

In addition to the default DHCP reply of IP address and subnet mask, the following DHCP options are recommended for clients with Intel® vPro™ technology:

- DHCP option 3 - Router or Gateway address. Used for routing TCP/IP traffic requests
- DHCP option 6 - DNS server IP address. To resolve ProvisionServer entry
- DHCP option 15 - DNS domain name. Locate the correct ProvisionServer instance.

DNS: As mentioned above, when the Intel® Management Engine enters setup mode, it needs to communicate with the Intel® AMT Setup and Configuration Service. A

manual entry can be placed in the Intel® Management Engine to direct the request to a specific IP address. However, most enterprise environments prefer to use an automated provisioning method instead of manual entry of the address. If an IP address is not entered into the Intel® Management Engine, then the device will send out a query to resolve the name "ProvisionServer" to the Setup and Configuration server. DNS is used to resolve the request. An Alias or CNAME record in the DNS can be used to point "ProvisionServer" to the correct physical instance. This approach provides flexibility if the actual system running the service instance changes.

If multiple DNS suffixes or domains exist within an enterprise environment, use DHCP Option 15 to help the Intel® Management Engine identify the correct DNS suffix resolution. Multiple DNS records may be needed to correctly resolve to the appropriate ProvisionServer instance based on the DNS domain suffix. The figure below shows how a multi-domain setup might be configured for clients in remote DNS domains to locate the actual provisioning service. The DNS suffix is vital in helping the Intel® AMT device lookup the "ProvisionServer". If this option is missing or not set to match the DNS configuration then automatic provisioning may fail because Intel® AMT cannot resolve ProvisionServer to an IP address^{vi}.

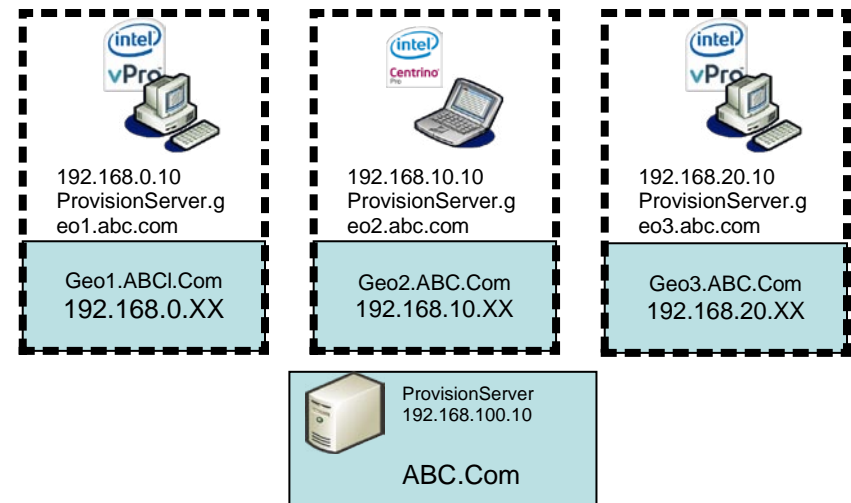


Figure 2 - The three geographies or locations of an enterprise will have a local DNS instance redirecting provisioning traffic to the true physical ProvisionServer within the root DNS domain

A simple way to test whether the hello packets will be able to reach the provision server is to ping the provision server using the fully qualified domain name. For example, from the geo1.abc.com domain, pinging “ProvisionServer” and “ProvisionServer.geo1.abc.com” should resolve to the appropriate IP address hosting the service.^{vii} This simple test will show whether an Intel® AMT system placed on a network segment will be able to reach the provision server. Another helpful method to determine whether the hello packets have reached the provision server is to check the logs on the server. This may require verbose logging of events and should be used only for short periods to determine what is occurring for troubleshooting purposes. All versions and implementations of the setup and configuration application that we are aware of have some type of log that will indicate whether a hello packet has been received.

Once the infrastructural components are prepared and operational, the authentication sequence is ready to occur. If the authentication sequence is not initiating, a check of the supporting infrastructure and associated services is recommended. The next section will briefly discuss the pre-shared secret options.

Network Infrastructure Rules

- DHCP server must provide AMT clients with an IP Address, a Subnet Mask, a Default Gateway, a DNS Domain-Name and a DNS Server IP Address.
- Intel® AMT clients must be able to successfully resolve the name “ProvisionServer.<Domain-Suffix>” to an IP address of the provisioning service using the DNS Server IP Address and DNS Domain-Name values received from the DHCP server in Step 1.
- Intel® AMT client hello packets and provisioning server responses must be capable of traversing the network. Default network ports are 9971 for provisioning, and 16992-16995 for Intel AMT traffic.

Authenticating the Intel® Management Engine

Intel has provided two secure methods to authenticate Intel® AMT clients to the provisioning service. An earlier diagram and sequence made reference to pre-shared secrets. These secrets are associated to the method or approach of enterprise provisioning with the following summary:

- **TLS-PSK:** Transport Layer Security Pre-shared key. Commonly referred to as pre-shared key or One-Touch. Refers to a pre-shared public and private key between the ProvisionServer and the client.
- **TLS-PKI:** Transport Layer Security Public Key Infrastructure. Commonly referred to as Remote Configuration (RCFG) or Zero Touch Configuration (ZTC). This process utilizes a certificate associated with the ProvisionServer. The associated certificate hash must be listed within the Intel® Management Engine BIOS Extension (MEBx)^{viii}.

The table below shows the types of keys available for each of the Intel® AMT firmware versions and which provisioning methods are supported.^{ix}

Intel® AMT Firmware	Manual	One-touch	RCFG	OEM Pre-Load	Certificate Type
2.0	Yes	Yes	No	No	TLS-PSK
2.1	Yes	Yes	No	Yes	TLS-PSK
2.2	Yes	Yes	Yes	Yes	TLS-PSK or TLS-PKI
2.5	Yes	Yes	No	Yes	TLS-PSK
2.6	Yes	Yes	Yes	Yes	TLS-PSK or TLS-PKI
3.0	Yes	Yes	Yes	Yes	TLS-PSK or TLS-PKI

TLS-PSK. TLS-PSK uses pre-shared keys (PSK) that are stored on the ProvisionServer and on the Intel® AMT client. The provisioning keys are generated and associated to the client systems. There are four methods used to place these pre-shared keys on the client.

1. **Manual:** An individual accesses the MEBx by pressing Ctrl-P during the system boot process before the operating system starts loading. The password for the Intel® Management Engine would be changed and then the pre-shared keys (e.g. the PID and PPS) entered into it. This approach may introduce errors in the key sequence if the entries are incorrect.
2. **USB one-touch:** The Intel® Setup and Configuration application can create a transfer file called setup.bin. This file is then transferred to a USB flash drive^x and inserted into an Intel® AMT system. Upon powering the system, the setup.bin file will be accessed and the next available record containing the pre-shared keys will be transferred to the client.
3. **Pre-provisioning service:** For a negotiated cost per system, a post manufacturing process can be applied to write the pre-shared key data to the clients. Those providing the service will then provide a copy of the pre-shared key data to the customer for importing into the ProvisionServer

TLS-PKI Provisioning Certificate. With RCFG a TLS-PKI certificate, often referred to as the Intel® AMT client setup certificate, is placed on the ProvisionServer and a matching certificate hash is on the Intel® AMT client. There are two methods used for placement of these certificates on the client:

Intel has worked with leading certificate vendors to pre-load a set of certificate hash values within the MEBx. The certificate associated to the ProvisionServer can be purchased from these vendors. With this scenario, Intel® AMT clients do not need to be “touched” in order to load the certificate information. Instructional information on using Remote Configuration is available on [Intel® vPro™ Expert Center](#).^{xi}

A company could also decide to obtain a certificate from another source, such as their own internally trusted corporate Public Key Infrastructure (PKI). When this choice is made, a matching hash will need to be placed on the client. Four options of adding the certificate hash to the client are available:

1. **Manual:** Entering of the 40 character certificate hash or thumbprint within the MEBx interface. Up to three certificate hashes can be added post manufacturing.
2. **One-Touch:** Using a utility called USBfile, you can generate a custom setup.bin file with certificate hash information. Up to three certificate hashes can be added to an Intel® AMT system that supports remote configuration and version 2 of the setup.bin file.
3. **OEM pre-load:** Before locking the MEBx, an OEM has the ability to add persistent certificate hashes. Space is provided for 23 persistent hashes, which cannot be removed once the system is deployed. In addition, the OEM can perform a pre-load similar to the above options for the non-persistent store certificate hashes, with space for only three.
4. **Pre-provisioning service:** For a negotiated price, an external service can load the preferred certificate hashes using options 1 or 2 above.

TLS-PKI Certificate Rules:

- The certificate hash must have the same Domain portion of the CN as the certificate on its provision server.
- The certificate hash must match the certificate for the provision server (i.e. a Verisign G1 Hash must be matched with a Verisign G1 certificate on the provision server).
- The certificate must be loaded and associated to the correct ProvisionServer
- The computer OEM will have a set of hashes “pre-loaded” as a standard part of the Intel® Management Engine BIOS. Make sure you understand which certificate hashes are included in your OEM product.

Hello Packet Initiation. Once the pre-shared secrets are defined and distributed to the client systems and an IP address is determined for the ProvisionServer, the client is able to announce the intent to authenticate to the provisioning service. The hello packets will be sent for up to six hours while attempting to connect to the ProvisionServer.^{xii} After six hours, the network interface is closed.

To reopen the network interface, which restarts the hello packet sequence, the following options are available:

1. Remove and reapply power to the system. This will power off the MEBx. When powered on in setup mode, the MEBx will restart the hello packet sequence
2. Use of the Intel provided reference utility – Remote Configuration Tool (RCT). More information will be shared in the next section.
3. Use of a client management agent to restart the hello packet sequence.

Once the hello packet is received and the pre-shared secrets are validated, the client authentication process has started. The completion of the authentication process occurs during the final steps as an encrypted session is established for the purposes of provisioning and the configuration settings are sent to the client system.

Completing the Provisioning Sequence

With the Intel® Management Engine associated to the ProvisionServer, the final configuration step is to assign an Intel® AMT profile to the target Intel® AMT device. This process requires the following:

- Successful authentication via TLS-PSK or TLS-PKI as referenced previously
- An Intel® AMT client profile has been created containing the necessary target environment configuration data for security, network, power policy, and so forth.^{xiii} Profiles are created by the Intel® Setup and Configuration application.
- The profile has been assigned to the target Intel® AMT client device.
- The device UUID^{xiv} obtained from the hello packet must match the UUID and associated operating system FQDN^{xv} as determined by one of the methods below.

Completion of the above steps can be accomplished manually for lab or testing purposes. However, various scripts are available to automate the repeated steps of authentication, profile assignment, and configuration completion. Most integrated client management solutions which support Intel® AMT have already defined and installed these configuration scripts. If unsure which configuration script is used for an Intel® SCS environment, open the Intel® SCS console^{xvi} and check the Intel® AMT properties setting under the General tab.

For environments using the Intel® Setup and Configuration Service, the following sample scripts and utilities are provided within the full download with additional explanation inside the installation manual referenced at the beginning of this document.

- **Database script** – An auxiliary database instance is created to capture matching UUID and FQDN data for the target Intel® AMT clients. This could allow for predetermination of a client and associated Intel® AMT configuration for deployment staging scenario. For systems already deployed, a client side scripts obtains the UUID and FQDN from the system. A server side script references the auxiliary database to match the UUID received via the hello packet to that which the client side script obtained. The server script can also be customized to determine default Intel® AMT client profile and Microsoft Active Directory organizational unit (OU).
- **Server Script** – Using Windows Management Instrumentation (WMI), the ProvisionServer server obtains the UUID and FQDN from the client operating system. Once obtained, the alignment with the UUID from the hello packet is performed and the configuration completes. An auxiliary database is not used. However, similar to the above Database server script, this script can be customized to determine the default Intel® AMT client profile and Microsoft Active Directory* OU.
- **Remote Configuration Tool (RCT)** – Provided with the latest Intel® SCS download as a reference tool and used with Intel® AMT systems supporting both TLS-PSK and TLS-PKI configuration approaches. This utility utilizes a separate virtual web directory instance added during the installation (e.g. AMTSCS_RCFG). The tool is supported with Intel® SCS 3.1.7 or higher, and is

White Paper: Simplifying the Provisioning Process

executed locally on the target client system. More information on the tool is available in the Intel® SCS installation manual.

When all configuration steps are in place, including authentication of the Intel® Management Engine to the ProvisionServer and provisioning automation scripts, a sequence of events will occur. The log sequence below is read from bottom to top to convey actions from time of hello packet until changes are committed.

Table: Configuration Service Logs for Successful Provisioning Sequence

Time	Description	UUID
21:54	Exit normally processing provisioning worker.	4C4C4544-00FF-FF10-80FF-
21:54	Commit changes.	4C4C4544-00FF-FF10-80FF-
21:54	Change admin password.	4C4C4544-00FF-FF10-80FF-
21:54	Generate a new PID for Intel® AMT device UUID: HLLQ-045Q.	4C4C4544-00FF-FF10-80FF-
21:54	Set power policies.	4C4C4544-00FF-FF10-80FF-
21:54	Successfully removed existing 802.1x wired profile.	4C4C4544-00FF-FF10-80FF-
21:54	Set ACL.	4C4C4544-00FF-FF10-80FF-
21:54	Remove existing 802.1x wired profile.	4C4C4544-00FF-FF10-80FF-
21:54	Set Kerberos options.	4C4C4544-00FF-FF10-80FF-
21:54	Set enabled interfaces.	4C4C4544-00FF-FF10-80FF-
21:54	Set TLS options.	4C4C4544-00FF-FF10-80FF-
21:54	Set Ping Response.	4C4C4544-00FF-FF10-80FF-
21:54	Set the host name to dell755.	4C4C4544-00FF-FF10-80FF-
21:54	Set domain name to pro.intel.com.	4C4C4544-00FF-FF10-80FF-
21:54	Synchronize clock on Intel® AMT device.	4C4C4544-00FF-FF10-80FF-

Time	Description	UUID
21:54	Set rng key on Intel® AMT device.	4C4C4544-00FF-FF10-80FF-
21:54	Start configuring the Intel® AMT device UUID: 4C4C454400FFFF1080FFFC04FFF0000.	4C4C4544-00FF-FF10-80FF-
21:54	Provisioning Intel® AMT device UUID: 4C4C454400FFFF1080FFFC04FFF0000.	4C4C4544-00FF-FF10-80FF-
21:53	Incoming connection from 192.168.1.100:16994	UUID 4C4C454400FFFF1080FFFC04FFF0000.

Conclusion

Understanding how Intel® AMT devices use the IT infrastructure to automate the provisioning process will speed the ability to use the valuable out of band management features. Not all IT infrastructures are the same and thus it is important to understand how Intel® AMT provisioning operates to effectively setup these devices. Collaboration between client, network, security, and server infrastructure teams is highly recommended to ensure all have a mutual understanding and assigned roles to the overall success of the improved client management and security.



www.intel.com

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

Copyright © 2007 Intel Corporation. All rights reserved.

Intel, the Intel logo, Intel® AMT, Intel vPro, Centrino, Centrino Inside and vPro Inside are trademarks of Intel Corporation in the U.S. 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/>

http://softwarecommunity.intel.com/isn/downloads/Manageability/Intel_AMT_SCS_Installation_and_User_Manual.pdf

- ii In a DHCP client environment, if the operating system is running and performs a DHCP lease request, the Intel ME will assume the same IP address. If the operating system is not operational, the Intel ME will request a DHCP lease if in a setup or configured state.
- iii The secrets can include either matching provisioning keys or matching certificate with associated hash.
- iv With the latest firmware for Intel® vPro™ technology, version 3.x, some pre-shared secrets are present in the Intel® Management Engine from the manufacturer. See the section below which refers to TLS-PKI for further information.
- v More on the provisioning automation scripts will in the latter section – “Completing the Provisioning Sequence”
- vi The static IP address of the ProvisionServer may also be entered into the Intel® Management Engine if needed. This would require a one-touch through a USB key (Intel® AMT 3.x) or a manual entry (Intel® AMT 2.x).
- vii Some network administrators or environments may not allow ping packets, which utilize ICMP. Other methods of resolution could include nslookup, tracert, or associated commands to ensure the DNS entry resolves to the correct IP address for ProvisionServer.
- viii Certificate hashes can also be specified via version 2 setup.bin files. More information is available at <http://communities.intel.com/docs/DOC-1210>.
- ix For more information on versioning and capabilities, please refer to <http://communities.intel.com/openport/blogs/proexpert/2007/08/23/intel-amt-versions-and-features>
- x More information on the setup.bin file is available at <http://communities.intel.com/thread/1181>
- xi For an overview article on Remote Configuration, please review <http://communities.intel.com/openport/blogs/proexpert/2007/08/29/remote-configuration-what-is-it-how-does-it-work-when-will-it-be-available>. For video and materials on the setup, please review <http://communities.intel.com/docs/DOC-1182>
- xii Intel® AMT 3.0 or higher systems with TLS-PKI enabled will automatically initiate hello packet sequence as the pre-defined certificate hashes are already loaded, thus the system is in a setup state. This first sequence will occur for 24 hours, after which the network interface will close. Subsequent attempts will defer to the six hour sequence.
- xiii For a complete list of Intel AMT client profile settings and options, please refer the AMT user guide distributed with the Intel® Setup and Configuration Service (<http://softwarecommunity.intel.com/articles/eng/1025.htm>)
- xiv Universally Unique Identifier is assigned by the device manufacturer according to the system board and is stored in the device firmware. Intel® AMT obtains this UUID from the system BIOS and stores in the Intel® Management Engine firmware.
- xv Fully Qualified Domain Name is assigned in the operating system properties. It is comprised of the operating system host name and DNS suffix. The FQDN may change during the lifecycle of a client system thus requiring a reprovision of the Intel® Management Engine to match accordingly.
- xvi Available within the full Intel® SCS download available at <http://softwarecommunity.intel.com/articles/eng/1025.htm>