

Secure Provisioning for PCs with Intel® 945/955 Express Chipset and Intel® Active Management Technology

White Paper



Legal Notice

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.

Intel products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

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

The Intel products discussed in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting www.intel.com.

Intel® is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

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

Copyright © 2005, Intel Corporation



Revision History

Date	Revision	Comments
June 2005	1.0	Initial release
September 2005	1.1	Revised release.

Contents

Intel® Active Management Technology Security Overview	1
Overview of Related Security Technologies	2
Transport Layer Security	2
HTTP Digest Authentication	2
Access Control	2
Provisioning Intel AMT Systems	3
Technology Implementation in Intel AMT	3
TLS	3
HTTP Digest Authentication	4
Password Strength	4
Realms	5
Login “Backoff” Mechanism after failed login attempts	5
Third Party Data Store (3PDS)	5
Intel AMT Provisioning Overview	5
Enterprise IT Provisioning (TLS secured)	7
Provisioning for Small Businesses	10
Recommended Best Practices	12
Provisioning should be done on an isolated wired network for enterprise systems	12
Username/Password pairs should be unique on each Intel AMT system	12
Provisioning Server should be able to leverage a Secure Password Management Infrastructure	12
Use of Strong Passwords	13
Change the default Admin account name	13
TLS should be turned ON for all communication with Intel AMT systems in the enterprise	13
PRNG secret keys should be unique	13
Ensure secure communication between the Provisioning Server and the TLS Certificate Authority (CA) Server	14
The TLS Certificate Authority Server must generate certificates that are appropriately populated	14
Manage the Intel AMT certificates using a PKI infrastructure	14
Provisioning server should forget the secret and private keys after provisioning them into Intel AMT systems	15
Protect the access to the data stored in the 3rd Party Data Store	15
Encrypt any sensitive data being stored in the Third-Party Data Store	15
Backup and Restore of data stored in the Third-Party Data Store	15



Intel® Active Management Technology Security Overview

Intel® Active Management Technology (Intel® AMT) allows IT to better Discover, Heal, and Protect their networked computing assets using new platform capabilities and popular 3rd-party management and security applications. Intel AMT stores hardware and software information in non-volatile memory and allows IT to Discover the assets, even while PCs are powered off*. With Intel AMT, remote consoles do not rely on local software agents, helping to avoid accidental data loss. Intel AMT provides out-of-band management capabilities to allow IT to remotely Heal systems after OS failures. Alerting and event logging help IT detect problems quickly to reduce downtime. Intel AMT helps to Protect your network by making it easier to keep software and virus protection consistent and up-to-date across the enterprise. 3rd party software can store version numbers or policy data in non-volatile memory for off-hours retrieval or updates.

Intel AMT is comprised of several features, including:

- Out of Band (OOB) system access allows remote management of PCs regardless of system power* or OS state
- Remote troubleshooting and recovery significantly reduces desk-side visits to increase the efficiency of IT technical staff
- Proactive alerting decreases end-user downtime and minimizes time to repair
- Remote hardware and software inventory increases speed and accuracy over manual inventory tracking to reduce asset accounting costs
- 3rd party non-volatile storage eliminates reliance on local software agents to store and retrieve data to help prevent accidental data loss

Intel AMT is designed to deploy these capabilities in a safe and secure manner. Intel AMT is a hardware and firmware based solution utilizing persistent non-volatile storage, making Intel AMT resistant to tampering or accidental data loss. To help ensure that only authorized users have access to critical features, and to protect against network attacks and/or technology misuse, Intel AMT employs robust access control and privacy mechanisms.

In order to take best advantage of these security mechanisms, Intel AMT must be carefully provisioned and implemented. This document describes the security mechanisms and discusses various deployment guidelines for Intel AMT deployment.

Some of the highlights of Intel AMT security are:

- Transport Layer Security (TLS) protocol to secure communications over the OOB network interface. The TLS implementation uses RSA keys with modulus lengths of 1536 bits.
- HTTP Digest Authentication protocol as defined in RFC 2617. The Remote Management application authenticates users (i.e. operators/administrators) who manage Intel AMT systems.
- Access-controlled storage of critical management data, via a non-volatile data store in the Intel AMT hardware.
- A pseudo-random number generator within the firmware of the Intel AMT system that generates high quality session keys for secure communication.

Overview of Related Security Technologies

Transport Layer Security

The Transport Layer Security (TLS) protocol provides communication security and privacy over the Internet and enterprise networks. The protocol supports server and client channel authentication. The TLS protocol is application independent, allowing other protocols like HTTP to be transparently layered on top. The TLS protocol is able to negotiate encryption keys as well as authenticate the server before data is exchanged by higher-level applications. The TLS protocol maintains the security and integrity of the transmission channel by using encryption, authentication and message authentication codes.

The TLS protocol establishes a secure channel of communication between the client and server, and consists of two phases: (1) server authentication and (2) an optional client authentication. In the phase one, the server, sends its certificate and its cipher preferences, in response to a client's request. The client then generates a master key, which it encrypts with the server's public key, and transmits the encrypted master key to the server. The server recovers the master key and authenticates itself to the client by returning a message authenticated with the master key.

In the optional second phase, the server sends a challenge to the client. The client authenticates itself to the server by returning the client's digital signature on the challenge, as well as its public-key certificate. A variety of cryptographic algorithms are supported by TLS. Subsequently, the client and server use keys derived from the master key to encrypt and authenticate the exchange of data between themselves.

The TLS protocol is defined in RFC2246 and RFC3546 in which more details can be found.

HTTP Digest Authentication

The HTTP protocol provides for two authentication mechanisms: the HTTP Basic authentication, and the more secure HTTP Digest authentication. These mechanisms are detailed in RFC 2617.

HTTP Basic Authentication protocol provides for a challenge-response authentication mechanism that may be used by a server to challenge a client, and by a client to provide authentication information back to the server. In this scheme, the client sends its user-ID and password to the server, and the server will authorize the client only if it can validate the user-ID and password. Otherwise, the server responds with an error code. The user-ID and password are sent across the wire, without any encryption, which makes the basic authentication scheme less secure than then HTTP Digest Authentication.

The HTTP Digest Authentication scheme is more secure than the HTTP Basic Authentication Scheme, because the password is never sent from the client to the server in the clear. In the Digest Scheme, the server challenges the client with a random value (called a *nonce*). A valid response contains a checksum of the username, the password, the given nonce value, and some other data. In this way, the password is sent over the wire as a hash to prevent interception and reuse. Upon receiving the response, the server computes the checksum using the same inputs, and compares the computed checksum with the one received from the client. If they match, then the client is authenticated.

Access Control

Access control is the mechanism by which systems grant or revoke the right to access particular data, or perform particular actions. Typically, a user must first authenticate or log in to a system, using some authentication credentials such as a username and a password. Then the Access Control mechanism determines which operations the user may access by comparing the user's ID to an Access Control List (ACL) or database. An access control list specifies the privilege attribute(s) needed to access the object, as well as the permissions



that can be granted with respect to the protected object to principals that possess privilege attribute(s).

Intel AMT allows individual usernames and passwords to be assigned to various Realms. A realm is a set of functions that are isolated from the rest of the functions. This allows an IT administrator to grant access to different features for different employees, if needed. In general, it is a best practice to grant the least needed privileges to a given user.

Provisioning Intel AMT Systems

When an Intel AMT system is purchased from a PC vendor, and powered-on for the first time, it should be provisioned with all the data and technology resources required to configure Intel AMT appropriately. This ensures that the full spectrum of Intel AMT system manageability features can be used to manage the system. These technology resources include unique and secure user-ID and password, secret keys, Access Control Lists and public key certificates.

Technology Implementation in Intel AMT

TLS

Intel AMT uses TLS to secure its communication over the network. Applications on Intel AMT systems work in the TLS server mode, while applications on other devices, host or Management Console, work in the TLS client mode, and initiate communications to applications on the Intel AMT system. Intel AMT supports the mandatory first phase of authentication (i.e., server authentication), where the Intel AMT system sends its certificate to the client for validation. However, the optional second phase of client-side authentication is not supported. Client authentication is achieved using the HTTP Digest Authentication mechanism.

To support these applications, a minimum of four simultaneous TLS sessions are available. At least one TLS session is always reserved so that the remote management application can always be accessed. The remaining TLS sessions can be used by any combination of the remaining applications (e.g., two Third Party Data Store TLS sessions and one SOL TLS session). To facilitate access by all applications, appropriate timeout mechanisms are employed for each TLS session.

TLS in the Intel AMT system contains an RSA certificate or certificate chain and the RSA private key that corresponds to the leaf certificate in the chain. The public key certificate and the private keys are used for TLS server authentication during the TLS handshake.

The cipher suites and associated certificate types and key exchange algorithms supported are listed below:

Cipher Suite	Certificate Type and Key Exchange Algorithm
TLS_RSA_WITH_AES_128_CBC_SHA	RSA
TLS_RSA_WITH_RC4_128_SHA	RSA
TLS_RSA_WITH_NULL_SHA	RSA

The TLS implementation uses RSA keys with modulus lengths of 1536 bits, and public exponent values of 10001h (65537 decimal).

HTTP Digest Authentication

Intel AMT uses the HTTP Digest Authentication Scheme for authentication of the client (such as the Remote Console), before allowing access to the system. A challenge is sent to the client, and a response containing the digest of the password and other information, must be returned.

The Intel AMT system stores the MD5 hash of the username, password, and the HTTP realm. The HTTP realm incorporates the Intel AMT machine ID, which is unique for every system (also known as a Universal Unique Identifier, UUID). This makes the hash value stored on every Intel AMT system unique.

Should an attacker break into the Intel AMT system's flash memory and seizes this hash value, it is of no use in attacking other Intel AMT systems, even if the passwords of those Intel AMT systems happen to be the same.

The cryptographic hashing also ensures that the passwords cannot be reverse engineered by gaining access to the hash value.

The steps involved in the HTTP Digest authentication technique are detailed in Figure 1, below:

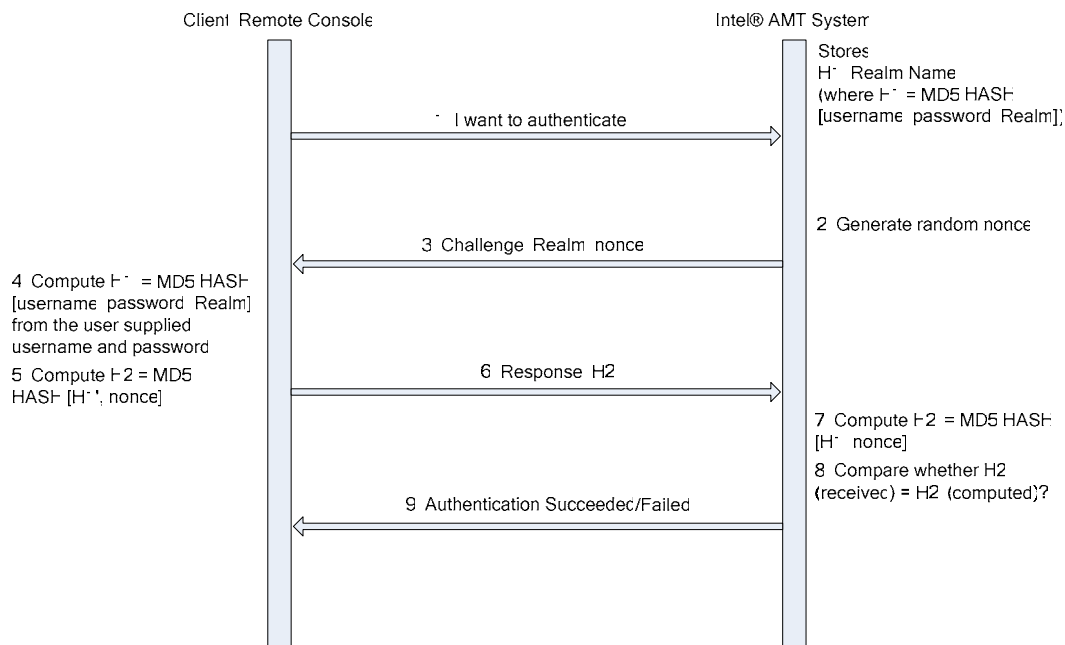


Figure 1: HTTP Digest Authentication

Password Strength

Intel AMT requires that passwords used for authentication to the Intel AMT system meet the following minimum criteria:

1. Must be at least 8 characters long. Characters allowed are 7-bit ASCII characters in the values of 32-126 inclusive. The characters '“', '‘', '‘', and ' : ' are not allowed.
2. Must have at least one digit character (e.g. '0', '1',... '9')
3. Must have at least one 7-bit ASCII non-alphanumeric character (e.g. '!', '\$', ',')
4. Must contain both lower case and upper case Latin characters



5. Must contain both lower-case Latin ('a', 'b', ...'z') and upper case Latin ('A', 'B',... 'Z'), or non ASCII characters (UTF+00800 and above)

These restrictions enforced by Intel AMT help to reduce susceptibility of passwords to offline dictionary attacks.

Realms

Intel AMT supports multiple realms that can be assigned to any individual usernames. The following realms are available:

- Event Manager
- Power Up/Down
- Network and Intel AMT Admin
- ISV Storage
- ISV Storage Admin
- Hardware Asset
- IDE-R/SOL (Remote Boot/Console Redirection)

Login “Backoff” Mechanism after failed login attempts

Intel AMT prevents online attacks to the Intel AMT systems by including a “backoff” mechanism, triggered by a certain number of successive failed login attempts. If an attacker tries to login to the Intel AMT system by guessing a password, and Intel AMT detects ten successive login failures, further login attempts are disallowed for a period of time. The timeout period starts at 5 seconds and reaches 80 seconds during continuous attack. After one hour of no attack the “backoff” mechanism is reset. This feature substantially impedes a system attack using password guessing.

Third Party Data Store (3PDS)

Intel AMT provides third-party applications with a mechanism to store data in a non-volatile data store. Controlled access to the data can subsequently be granted to other applications on the same platform or from an authorized remote platform. Intel AMT provides this capability through a set of commands that operate over a local host interface Keyboard Controller Style (KCS), or OOB over a network interface.

3PDS commands are protected by controls which are enforced by Intel AMT Firmware. ACL lists are used to provide access to, and permit allocation of, non-volatile memory (NVM) for applications. Applications must register themselves to enable the commands used in accessing and managing the 3PDS.

The structure, meaning and sensitivity of data placed into the 3PDS are transparent to the 3PDS Storage Manager. As a result, applications are responsible for any security mechanisms necessary to protect their stored data (e.g., encryption of sensitive data or keys).

Intel AMT Provisioning Overview

For Intel AMT to be useful in the market, it must be deployable into a wide variety of environments. These environments vary from large enterprises with trained IT staff who securely manage multi-site networks, to small businesses with a few part-time administrators who manage a single building network. Intel AMT is designed with a complete set of

provisioning and management functions to meet the deployment needs of administrators in each of these environments.

All provisioning operations are conducted using a combination of the BIOS-based Intel AMT Configuration Screen and the Intel AMT firmware, communicating over the network interface. To help Intel AMT know how to operate in its destination environment, two provisioning modes of operation are provided, Enterprise mode and Small Business mode. Typically, the default mode is set to Enterprise mode; however the PC vendor may preset the mode of operation value when they build the PC. This value can be changed after successful login through either the Intel AMT BIOS Configuration Screen or the network interface.

Enterprise IT Provisioning (TLS secured)

The Enterprise provisioning mode is designed to serve the needs of large enterprises with trained IT staff in securely managing multi-site networks. When supported with the proper network infrastructure services, this mode can provide automated, secure, one-touch provisioning for Intel AMT platforms as shown in Figure 2.

The required network infrastructure services include:

- DHCP service
- DNS Service
- TLS Certificate Authority Service
- Provisioning Service¹

Intel AMT systems arrive at a customer's site from the PC vendor's factory and are placed into inventory in an IT staging area. The staging area features an isolated wired LAN with DHCP, DNS, and Provisioning servers. The wired LAN must be isolated from the rest of the enterprise network(s) to prevent disclosure of security-related parameters while they are being uploaded to Intel AMT systems.² The Provisioning Server should also support a secured connection over a second interface to a TLS Certificate Authority server. Intel AMT systems in the Enterprise provisioning mode will typically have DHCP enabled by default.

Provisioning Enterprise One-Touch

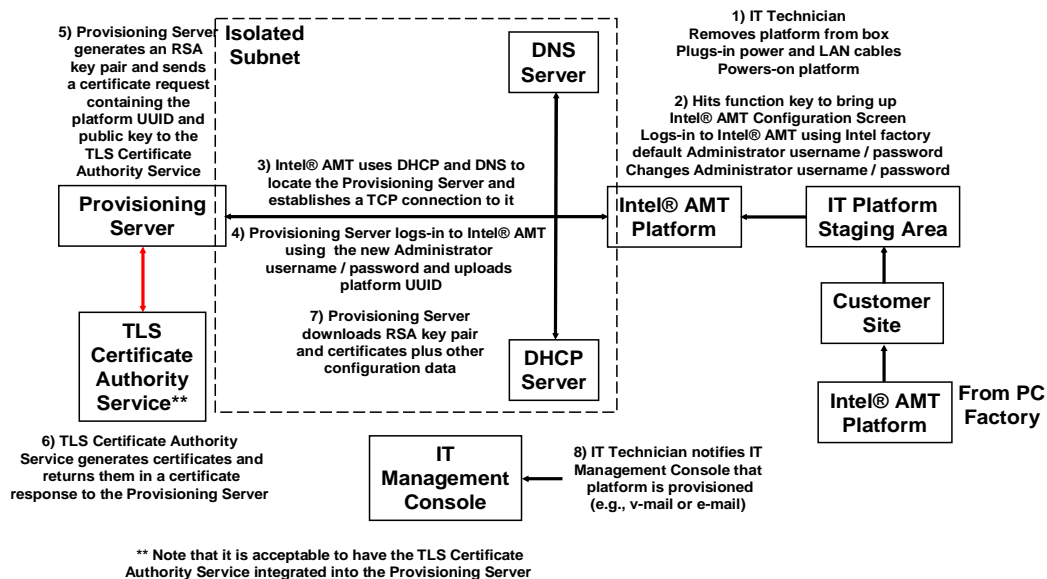


Figure 2: Intel AMT Enterprise One-Touch Provisioning

¹ This is a software service that performs all the necessary tasks to successfully provision Intel AMT systems, before they are put in use. Provided by ISVs who support Intel AMT in their enterprise software applications.

² See the Best Practices section for more information on this attack.

Steps to provision Intel AMT systems for enterprises:

Steps 1 and 2 require specific action by the IT staff:

1. An IT Technician removes a PC from inventory, places it into a provisioning rack, plugs in power and isolated LAN cables, and turns on the platform power.
2. The IT Technician uses a keyboard function key, defined by the PC manufacturer, to invoke the Intel AMT BIOS Configuration Screen.
 - a. The IT Technician logs-in to the Intel AMT platform using the Intel factory default administrator username / password. This default username and password is provided in the box/manual of the system.
 - b. When this first log-in occurs, the IT Technician is required to change the factory default username and password to a new password.¹
 - c. Once the default username / password have been changed, the IT Technician logs-out of Intel AMT.

Steps 3 to 7 are performed automatically by the Intel AMT system or other servers in the provisioning infrastructure:

3. The Intel AMT system then sends a request to the DHCP server for an IP address. The DHCP server returns a reply containing the IP address for the Intel AMT system, the DNS Domain Name, and the IP address of the DNS server.
 - a. Using this information, the Intel AMT system sends a request to the DNS server for an IP address of the Provisioning Server.
 - b. The DNS server returns a reply containing the IP address of the Provisioning server.
 - c. Using this information, the Intel AMT system establishes a TCP connection to the Provisioning Server.
4. The Provisioning Server logs in to the Intel AMT system using the new administrator username / password and the Intel AMT platform sends UUID.
5. The Provisioning server generates an RSA key pair and sends a certificate request containing the platform UUID and the public key to the TLS Certificate Authority Service.
6. The TLS Certificate Authority service generates certificates and returns them in a certificate response to the Provisioning Server (Note: The TLS Certificate Authority service may be integrated into the Provisioning Server).
7. The Provisioning server uploads the RSA key pair and certificates plus any other configuration data to the Intel AMT system. This other data includes items such as:
 - Fully Qualified Domain Name (FQDN) of the Intel AMT system
 - DNS IP address (for non-isolated network)
 - Pseudo Random Number Generator (PRNG) Secret Key
 - Current Date and Time

¹ The requirement to change the default password prevents provisioning masquerade attacks based on a presumably well-known factory default username / password. See the Best Practices section for more information on this attack.



- Access Control Lists (Username / Password)
- Access Control List (Enterprise Names)

Once all of the configuration data has been uploaded, the Provisioning server sends a reset command to the Intel AMT Management Engine processor to complete the provisioning process.

Step 8 requires action by the IT staff:

8. At this point, the IT Technician notifies an IT Management Console (e.g., via e-mail) that this Intel AMT platform is provisioned and available to be managed. The Intel AMT platform can now be deployed into the production Enterprise network.

The steps described above represent the ideal One-Touch Enterprise provisioning model. However, there are a few points to note, as below, in certain situations:

- If all of the desired network infrastructure services are not available in the isolated wired subnet (e.g., DHCP server), this provisioning mode can still be supported. However, the IT Technician may be required to manually enter some of the data into each Intel AMT platform.
- After powering-on the Intel AMT platform, the IT Technician will change the factory default username / password. If DHCP is not available, the IT Technician will set the DHCP Enable parameter to FALSE, enter the DNS Domain Name, and enter IP addresses for the Intel AMT system and the DNS server. The IT Technician will then log-out of Intel AMT and the system will proceed with the provisioning operations as described above.
- If both DHCP and DNS are not available, then the IT Technician will set the DHCP Enable parameter to FALSE; if available, enter IP addresses for the Intel AMT system and the Provisioning server. The IT Technician will log-out of Intel AMT and the platform will proceed with the provisioning operations as described above.

Provisioning for Small Businesses

The Small Business provisioning mode is designed to serve the needs of small businesses with a few part-time administrators managing a small network – for example, in a single building. In its most basic form, this mode uses no network infrastructure services. All that is needed to provision an Intel AMT system in this mode is a PC with a web browser as shown in figure 3.

Intel AMT platforms arrive at a customer's site from a PC vendor and are placed into the administrator's office. No isolated wired subnet is expected to be used for provisioning in this mode since the entire network is to be treated as an isolated network.

Provisioning Small Business

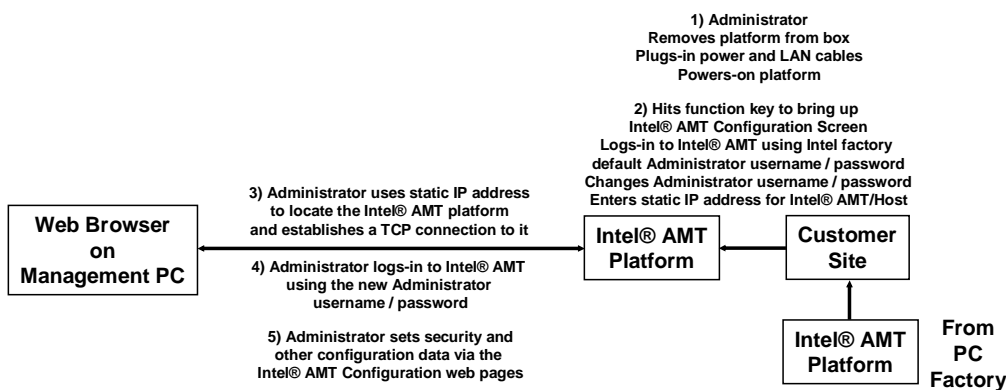


Figure 3: Intel AMT Small Business Provisioning

Steps to provision Intel AMT systems for Small Businesses (all the following steps require action on the part of the IT staff):

1. When a new Intel AMT platform is needed, the administrator removes a platform from its box, places it onto a table or desk, plugs in power and wired LAN cables, and turns on the platform power.
2. The administrator uses a keyboard function key, defined by the PC manufacturer, to bring up the Intel AMT BIOS Configuration Screen.
 - a. The administrator logs-in to the Intel AMT system using the factory default administrator username / password. This default username and password is provided in the box/manual of the system.
 - b. When this first log-in occurs, the administrator is required to change the factory default username and password to a newly chosen one.



- c. Once the default username / password has been changed, the administrator enters an IP address for the Intel AMT system.
 - d. The administrator logs-out of Intel AMT, and the platform will wait for the Management PC to connect to it over the wired network interface to complete provisioning.
3. Using the web browser on the Management PC, the administrator enters the IP address and port of the Intel AMT system into the address bar of the web browser (e.g. "http://192.168.1.100:16992" where the IP address of the AMT system is "192.168.1.100").
 - a. The Management PC establishes a TCP connection to the Intel AMT platform and accesses the top-level Intel AMT embedded web page and is prompted to log-in.
 4. The administrator logs-in using the new administrator username/password.
 5. The administrator enters the required configuration data into the various Intel AMT Configuration web pages. This data includes items such as:
 - Fully Qualified Domain Name (FQDN) of the AMT system
 - DNS IP address
 - Default gateway IP address
 - Access Control Lists (Username / Password)

Once all of the configuration data has been uploaded, the Intel AMT system can now be deployed into the Small Business network.

The steps described above represent the most basic Small Business provisioning model. If some network infrastructure services are available, this provisioning mode can still be supported. However, the administrator will need to add/change additional parameters on the Configuration web pages to make use of these services (e.g., enabling DHCP), as described above in the section "Enterprise IT Provisioning" describing how to configure platforms for static IP address environments.

Recommended Best Practices

To realize the full potential of Intel AMT while maintaining the best possible security, the following best practices are recommended for provisioning of Intel AMT systems:

Provisioning should be done on an isolated wired network for enterprise systems

When Intel AMT systems are provisioned in an enterprise, Intel recommends that the provisioning be done on a network that is physically isolated from the enterprise operations network. The isolated sub-network should only contain trusted users. Provisioning over an isolated sub-network will prevent unscrupulous users from watching network traffic and gain access to security-related parameters (such as RSA private keys, PRNG Secret Key, etc.) when they are being uploaded to Intel AMT systems.

An unscrupulous user with access to sensitive security parameters, could compromise communication between the Management Console and an Intel AMT system, to gain access to the Intel AMT features and abuse them (e.g. turn off the system, or install/uninstall software on that system, etc.).

Username/Password pairs should be unique on each Intel AMT system

Intel AMT uses the username / password to authenticate IT administrators for managing Intel AMT systems. It is recommended that IT administrators use unique passwords when provisioning each Intel AMT system.

A malicious employee with knowledge of one username / password pair for an Intel AMT system could not only compromise that system, but any other system with the same username / password.

In an enterprise, where IT administrators have to provision (and manage) hundreds or thousands of Intel AMT systems, a password management system/process becomes a necessity. This is discussed in more detail in the next section.

Provisioning Server should be able to leverage a Secure Password Management Infrastructure

ISV's who are developing software for Provisioning Servers are strongly encouraged to integrate a secure password management infrastructure into the Provisioning Service. This will make password management easier and more secure for IT users. Examples could be leveraging the Microsoft Active Directory infrastructure, or any other X.500/LADP directory infrastructure having adequate security to protect the set of username / password pairs. Even the use of a Relational Database may serve the purpose, as long as adequate security can be built around it to protect the username / password pairs.

These Password Management mechanisms would then securely store the username / password pairs for each Intel AMT system, yet provide them to the IT administrator when they need to manage systems. If the Management Console has an integrated Password Management capability, the Management Console can authenticate itself to an Intel AMT system by automatically selecting the correct username / password and supplying it to the Intel AMT system via the HTTP Digest Authentication protocol.

Use of Strong Passwords

Password Management Infrastructures should have the capability to generate high entropy passwords.¹ Even in the absence of a Password Management System, it is strongly recommended that the Provisioning Server have this capability, so that high quality passwords are generated. Leaving the generation of passwords to the humans is prone to result in weak passwords (such as common names of people, places, words, etc.) that are subject to dictionary attacks.

Intel AMT requires that passwords meet the following minimum criteria:

1. At least 8 characters long. Characters allowed are 7-bit ASCII characters in the values of 32-126 inclusive. The characters '“', '‘', ' ’' and ' : ' are not allowed.
2. At least one digit character (e.g. '0', '1',... '9')
3. At least one 7-bit ASCII non-alphanumeric character (e.g. '!', '\$', ',')
4. Contains both lower-case Latin ('a', 'b', ... 'z') and upper case Latin ('A', 'B',... 'Z')

The minimum requirements do not prevent an administrator from using passwords such as “George_1”, “George_2”, “George_3”, etc., each of which is relatively weak and prone to discovery. Once a few passwords are obtained, a pattern may be discovered.

Random strings such as “HoS8V@y\$” and “u\$8s#R9a” are examples of stronger passwords.

Change the default Admin account name

Users of Intel AMT should change the default account name for the “Admin”. It is recommended not to use commonly occurring account names for administrators such as “Admin”, or “Administrator”. This prevents a malicious person on the network from easily guessing the account name. Though it is the knowledge of the secret password that protects the user, and prevents others from impersonating the administrator, it is advisable to choose non-obvious admin account names for better security.

TLS should be turned ON for all communication with Intel AMT systems in the enterprise

Intel AMT provides two modes of TLS operation, TLS on and TLS off. Intel strongly recommends that TLS be turned on at all times, thereby protecting the communication of sensitive data between Intel AMT systems and the management console.

TLS provides channel authentication and encryption to prevent “man-in-the-middle” attacks, where an attacker monitors the network activity between a remote console and Intel AMT platform and takes over the connection, once established, to take control of the platform by sending malicious commands.

PRNG secret keys should be unique

Intel AMT hardware contains a Pseudo Random Number Generator (PRNG), which is used to generate runtime keys for secure communication. The PRNG algorithm utilizes a secret key which is used to initialize it, and enable it to generate a series of random numbers. One of the properties of this algorithm is that the series of (pseudo) random numbers generated by this algorithm will always be the same, as long as it is initialized with the same secret key. It is therefore strongly recommended that the Provisioning Server generates unique PRNG secret keys to be provisioned into each Intel AMT system.

¹ High Entropy passwords are passwords that are difficult to guess; such as “w7_uH9xb”. These are words that are not common names, or other words in the language, and hence cannot be found in a dictionary.

Failure to provision according to the above recommendation will cause all Intel AMT systems to generate the same series of random numbers (and hence the same series of keys, used for secure communication). Thus, if someone knows this series (and hence the resulting keys) for one Intel AMT system, then the keys for all of the other systems communicating over the network are also known.

Ensure secure communication between the Provisioning Server and the TLS Certificate Authority (CA) Server

The Provisioning Server communicates with the TLS CA server to obtain Digital Certificates for the RSA public keys that it generates. It is strongly recommended that the Provisioning Server use secure methods (such as those described in RFC 2511 - Internet X.509 Certificate Request Message Format) to supply the required information to the TLS CA server to obtain Digital Certificate(s).

One of the key points to keep in mind is that the Provisioning Server must, under no circumstance, pass on the RSA private key to the TLS CA server directly. It should only pass on a Proof of Possession of the RSA Private Key to the TLS CA server.

It is also strongly recommended that the connection between the Provisioning Server and the TLS CA server be on a separate network interface (when the TLS CA server is not on the isolated network), than the one the Provisioning Server is using for the isolated provisioning network.

The TLS Certificate Authority Server must generate certificates that are appropriately populated

Certificates generated for Intel AMT systems by the TLS CA (which is a separate Server or integrated into the Provisioning Server) must have their fields appropriately populated. This includes:

CN = Fully Qualified Domain Name (FQDN),

UI¹ = the platform UUID

DN = a subsystem identifier (Intel AMT System)

Manage the Intel AMT certificates using a PKI infrastructure

The best method of managing Intel AMT certificates is through the use of commercial Public Key Infrastructure software. This may be limited to the use of a Certificate Server to generate certificates, or it may take a step further to include other PKI components such as a Certificate Revocation Lists (CRL) published at a CRL Distribution Point, Key Management, re-issuance, etc. These modules could be run from a separate Certificate Management Server or integrated into the Provisioning Server.

From the standpoint of Intel AMT, one of the important aspects of managing certificates via a PKI is revocation of certificates. Certificates issued to Intel AMT systems may need to be revoked before they expire for two reasons: (1) the private key has been compromised (i.e., someone else also knows the private key, other than the Intel AMT system, or (2) the private key is no longer in possession of the Intel AMT system (e.g., loss, due to corruption of the key in the flash storage area, or erasure due to error). Therefore, it is highly recommended that a revocation mechanism be put in place to ensure that entities with malicious intent do not misuse compromised or lost certificates.

¹ Unique Identifier (RFC 2459; section 4.1.2.8)



Provisioning server should forget the secret and private keys after provisioning them into Intel AMT systems

The Provisioning Server should erase all references to the PRNG secret key, and the RSA private key (that were generated during the provisioning process), as soon as they have been provisioned into Intel AMT systems.

Private or secret key values may remain in the Provisioning Server memory and, malicious programs or users could generate a memory dump and search for the key values. Consequences of having these secret or private keys fall into the wrong hands could result in a security breach.

Protect the access to the data stored in the 3rd Party Data Store

Applications that use 3PDS should protect access to the application data by leveraging the access control features of the Intel AMT 3PDS Manager. This provides the first line of security for application data, and protects access to the data from other applications and malicious attackers. Several commands are provided by the 3PDS Manager that create access controls for stored data including a provision for group access permissions.

Encrypt any sensitive data being stored in the Third-Party Data Store

ISVs are responsible for protecting the data stored by their applications. The structure, meaning, and sensitivity of the data placed into the 3PDS are transparent to Intel AMT. Furthermore, Intel AMT does not ensure privacy of the data via encryption or other means.

If an ISV application uses the 3PDS to store sensitive data (such as keys, passwords, etc.), it is strongly recommended that the application(s) protect the stored data using encryption prior to storage. Encrypting sensitive data before storing it in the 3PDS significantly reduces the likelihood of an attacker obtaining the data.

Backup and Restore of data stored in the Third-Party Data Store

Application developers, who are developing applications that use the 3PDS, should keep a backup copy of the Application ID, data store configuration, as well as any stored data. This will facilitate data restoration in the event of data loss from the 3PDS. Intel AMT does not provide data back up services for 3PDS data.