Intelligent Systems

Intel® Active Management Technology Embedded Host-based Configuration in Intelligent Systems

Easy activation of Intel® vPro™ technology remote manageability without trade-offs in security, functionality, and cost

EXECUTIVE SUMMARY

Intel® Active Management Technology (Intel® AMT) is used by businesses of all types to reduce cost-of-ownership of their client platforms. As the remote manageability component of Intel® vPro™ technology, Intel AMT is especially valuable for retail end-users who operate unattended embedded intelligent clients including point-of-sale terminals, digital signs, and self-service devices such as kiosks and ATM machines.

Host-based Configuration (HBC) in Client Control Mode (CCM), introduced with Intel AMT Release 7, significantly simplifies the activation process. This host-based, in-band provisioning method is as simple as running a local patch with administrator privilege, but it requires certain tradeoffs. With HBC-CCM, the system defense feature is unavailable, and for security reasons it requires mandatory user consent for KVM and redirection features.

Intel AMT Release 9, supported in 4th generation Intel® Core™ processors, introduces a new option for provisioning unattended intelligent devices called Embedded Host-based Configuration (EHBC). While EHBC is available for all market segments, it is especially targeted to meet the requirements of intelligent devices that benefit from HBC CCM but also require security features, and due to their unattended nature have no user to provide the consent actions needed for HBC CCM.

EHBC simplifies activation and deployment of Intel AMT in intelligent clients, without tradeoffs involving security, usability, functionality, or cost.

Intel AMT is especially valuable for retail end-users who operate unattended embedded intelligent clients including point-of-sale terminals, digital signs, and self-service devices such as kiosks and ATM machines.

Introduction

Like other networked devices, intelligent devices in retail that are easy to manage, reliable, and secure can provide significantly lower total cost of ownership (TCO). ATMs, point-of-sale stations, gas station pumps, and intelligent digital signs are all examples of retail applications that benefit from remote manageability enabled by Intel Active Management Technology.

With billions of intelligent devices now deployed worldwide, and growing numbers in retail, it is impractical to send technicians to each device to load routine security updates, or keep the devices continuously turned-on for off-hour patches. Intel AMT makes it possible to query, restore and protect devices remotely, even when they are powered off, experiencing software failures, or not functioning.

Intel AMT implements a unique capability in Intel chipsets that allows management consoles to access, manage, diagnose, and fix the systems out-of-band remotely, regardless of system's power and/or health state. In addition, there are special security mechanisms built into hardware to protect the device and to ensure the communications link between the IT management console and the embedded system is fully secure.

There are many different versions of Intel AMT. Prior to Intel AMT Release 6.0, setup and control of Intel AMT had to be

The Distribution model meets the needs of many IT environments, such as retail, that prefer to push an agent to the platform to perform IT-mandated activities locally.

performed manually, or out-of-band over a network. Automated provisioning required the use of either a secret pre-shared key (PSK), or a server certificate derived from one of the commercial root certificates or local certificate authority. The setup and configuration process required a sophisticated enterprise network with adequate server support, as well as an IT organization to keep it all working.

Host-based Configuration (HBC) in CCM mode was introduced to simplify the provisioning process. However, the user consent requirement remained an obstacle to deploying Intel AMT for unattended intelligent devices.

HBC Simplified: Embedded Host-based Configuration

Embedded Host-based Configuration (EHBC) is a capability extension to HBC that greatly reduces the complexity of configuring intelligent systems to achieve the remote manageability benefits of Intel vPro technology, but without a user consent requirement or the need to compromise cost, security, or functionality.

EHBC is new with the release of Intel AMT 9 (back-ported to Intel AMT 8.1.20). It is targeted to meet the requirements of intelligent systems that require security features, and due to their embedded nature have no user to provide the consent actions required for HBC.

With EHBC, similar to HBC in CCM mode, the configuration is easy and can be accomplished like a normal software or patch delivery job. There is no need for IT personnel to touch the Intel® Management Engine BIOS Extension (Intel® MEBX), and there is no requirement for a Setup and Configuration server to connect with the Intel vPro client over the network. The Distribution model meets the needs of many IT environments, such as retail, that prefer to push an agent to the platform to perform IT-mandated activities locally.

EHBC accelerates the return on Intel vPro technology investments, making many management use cases possible and accelerating time to positive ROI.

Configuration Methods and Intel® Active Management Technology Versions

Intel AMT provides users with considerable system configuration flexibility with respect to security, functionality, complexity tradeoffs, and deployment cost. Table 1 lists the configuration methods available for the different versions of Intel AMT.

Configuration Method	Intel® Active Management Technology Versions
Host-based Configuration	CCM, 6.2 and higher & ACM, 7.0 and higher
SMB/Manual Configuration	2.0 and higher
SMB/Manual with USB Key Configuration	4.0 and higher
One Touch Configuration (PSK)	2.1 and higher
Remote Configuration (PKI)	2.2, 2.6. 3.0 and higher
Factory provisioning	4.2 and higher

Table 1. Intel® Active Management Technology Configuration Methods

Control Modes
After configuration, Intel AMT-enabled devices are put into one of two control modes:

Client Control Mode (CCM) is the level of functionality provided when configuring Intel AMT using Host-based Configuration, without touching the machine or providing additional credentials beyond OS administrative (Admin) credentials. Intel AMT-enabled devices in this mode have the following limitations:

- System Defense features are not available.
- User consent is required for all redirection operations and changes to the boot process.
- Permission from the auditor user (if defined) is not required to un-configure Intel AMT.
- To ensure that untrusted users cannot get control of the Intel AMT system, some Intel AMT configuration functions are blocked.

The Intel AMT user consent mechanism directly displays a message that the host platform cannot detect. The message contains a random passcode that the platform user must pass along to the operator who wants to perform one of the above functions from a remote console. This limitation cannot be bypassed in Client Control Mode. It is important for security, but it requires a display and a user to be physically present to read the displayed passcode. Users can move a platform configured using Host-based Setup and Configuration from Client Control mode to Admin Control mode, where the user consent and related restrictions are removed, by providing a client certificate that corresponds to a certification authority (CA) root hash, similar to remote configuration.

Admin Control Mode (ACM) is the functional level achieved with any of the legacy configuration methods (PKI, PSK, manual, UPDPARAM), or Host-based Configuration that supplies a certificate chain in addition to the OS Admin credentials, to corroborate the identity of the caller. In this mode all Intel AMT features are available.

Host-based Configuration (HBC)
HBC is a feature of Intel AMT 7.0 that has been partially back-ported to Intel AMT 6.2 (in CCM mode only).

HBC provides two basic methods to configure an Intel AMT-enabled device: the Client Control Mode (CCM) method and the Admin Control Method (ACM) method. In addition, HBC allows CCM to be upgraded to ACM.

HBP CCM allows an application running locally with Admin privileges on the Intel AMT system to configure the Intel AMT device in Client Control Mode. Configuration is done via an XML configuration profile. The application and the profile can be sent to an Intel AMT-enabled device in a deployment package and run with a script.

HBP ACM could be reached by supplying a certificate chain to corroborate the identity of the caller. The same requirement exists for the upgrade flow.

SMB/Manual Configuration (Through Intel® Management Engine BIOS Extension (Intel® MEBX) or USB Key):
The SMB/Manual configuration method allows configuration of Intel AMT devices with basic settings. Configuration is performed locally at the Intel AMT system by an IT administrator using one of the following options:

- Intel AMT 4.0 and higher versions can be configured using a USB key containing a configuration file. A confirmation of the operation is required by the operator of USB key to secure the process.
- All Intel AMT generations can be configured manually from the BIOS using the Intel Management Engine BIOS Extension (Intel MEBX) interface that is accessible with the Intel AMT in-boot interface. This interface is secured via a preset administrator's password that has to be changed the first time the Intel MEBx password is entered.

Users can move a platform configured using Host-based Setup and Configuration from Client Control mode to Admin Control mode, where the user consent and related restrictions are removed, by providing a client certificate that corresponds to a certification authority (CA) root hash, similar to remote configuration.

After configuration in either case, the Intel AMT device is put in one of the following modes:

- Small Medium Business (SMB) Mode — devices with Intel AMT 5.x and prior generations are put in this mode. Advanced (optional) Intel AMT features, including secure communication with transport layer security (TLS), are not available to devices in this mode.
- Manual Mode — devices with Intel AMT 6.x and higher are put in this mode. All Intel AMT features are available to devices in this mode, if a third-party application can configure them.

One Touch Configuration (PSK)
To achieve a higher level of security, the One Touch Configuration method is performed out-of-band using a configuration server. This method uses a Pre-Shared Key (PSK) for authentication and encryption. The PSK protocol provides secure communication based on a symmetric encryption key that has been shared in advance between the Intel® Management Engine (Intel® ME) firmware on an Intel AMT device and a remote configuration server.

In most cases, physical access to the Intel AMT system is necessary to import the key to the system either manually, via a USB key, or by the OEM.

Remote Configuration (PKI)
To achieve a higher level of security, the Remote Configuration method is performed out-of-band using a configuration server. This mechanism eliminates the need for human intervention (zero touch) and uses digital signatures based on public key infrastructure (PKI) certificates to secure the connection and validate the identities of both parties.

The public key, of an x509 certificate matching the domain name used by the enterprise network, is shared through a digital certificate signed by a trusted authority, known as a certification authority (CA). The CA generates digital certificates that can identify an individual or an organization.

To use this method, the Intel AMT device must have at least one active root certificate hash defined in the Intel MEBx. Several provisioning root certificate hashes from authorized external CA vendors, including VeriSign*, GoDaddy*, Comodo*, and Starfield*, are already included in the Intel ME firmware. The manufacturer could also add customer's internal CA root certificate hash to the Intel ME firmware, if desired, before the computer is shipped.

Provisioning at Manufacturing
An Intel AMT-enabled system 4.x or higher generation can also be provisioned at the manufacturing line by an OEM or board vendor, based on a customer request. This method requires the UPDPARAM tool and a special BIOS that temporarily configures the system before the main BIOS is loaded. A different UPDPARAM tool is provided in the Intel ME firmware kit for each generation of Intel AMT.

Host-based Configuration CCM Security Issues

Host-based Configuration Client Control Mode allows a program running locally on the platform to move Intel AMT to a setup state. All of the configuration commands that previously needed to be sent over the network can be sent locally. The enterprise server needs only to push a setup agent to the platform. All actions occur locally, and a certificate is not required to start the process. The only requirement is to have administrative privileges on the host operating system.

This is considered not secure because a virus with Admin privileges could perform setup and configuration and use security features such as KVM or redirection to control or take over the system. Therefore, a platform configured using host-based configuration is placed in Client Control Mode. But in this mode Intel AMT is subject to the limitations described previously.

Intel AMT Release 9 introduces Embedded Host-based Configuration (EHBC) that is also back-ported to Intel AMT release 8.1.20 and beyond. With this option, performing host-based setup transitions the platform directly to Admin Control Mode without the requirement of providing a certificate. This eliminates the user consent requirement and enables full ACM mode functionality.

EHBC is available for all market segments but it is primarily targeted to meet the requirements of intelligent devices that would benefit from HBC CCM but also require security features, and due to their unattended nature have no user to provide the consent actions needed for HBC CCM.

It is important to note that EHBC-enabled devices must be provisioned before deployment and never deployed un-configured. To address security, the EHBC feature is disabled by default and can only be enabled by OEMs or board vendors during BIOS/firmware image-build using a special flag. The use case for systems enabled with EHBC is new device deployments, with the assumption that the systems will be configured in a secure staging location prior to deployment and connection to the public network.

It is important to note that EHBC-enabled devices must be provisioned before deployment and never deployed un-configured.

Note that with Embedded Host-based Configuration, there is no need for a keyboard or mouse, which many intelligent systems do not have.

EHBC could be permanently disabled after being enabled at manufacturing, using a command by the customer if for any reason the usage model for the EHBC enabled device changes after device delivery to the end user. It is up to the customer to follow deployment guidelines to avoid possible security risks.

How EHBC Works

OEMs build intelligent devices using a firmware image that enables this special feature. This special build is for customers who plan to use Intel AMT manageability features and who have already decided to configure Intel AMT on all new systems. Note that the default firmware image disables this feature. It is enabled only for customers who understand the potential security risks.

End-users perform Host-based Configuration ACM using the network port to deploy the local configuration application to the platform. Note that with Embedded Host-based Configuration, there is no need for a keyboard or mouse, which many intelligent systems do not have. OEMs will recommend that end-users or system builders and integrators perform host-based setup in a secure staging area before deployment and as soon as possible after receipt of the platform. Following this recommendation will minimize the window of opportunity for a virus to configure the system.

Conclusion

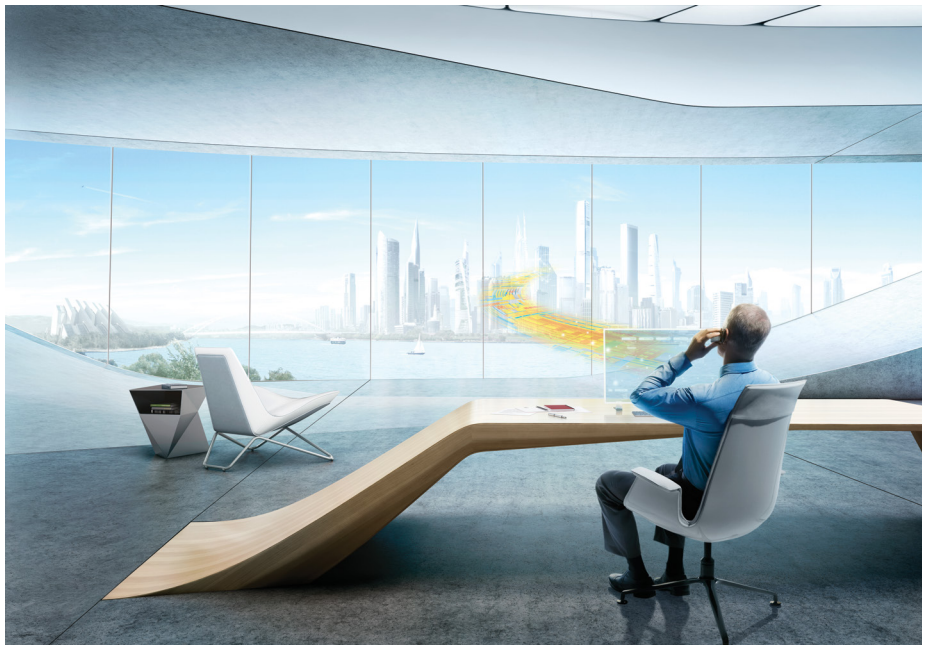
With Intel AMT Release 9, the special version of Intel AMT firmware designed for Embedded Host-based Configuration (EHBC) provides substantial advantages for intelligent system builders and integrators. With EHBC, configuration of Intel vPro technology clients can be accomplished like a normal software delivery or patch delivery job without restricting features or requiring mandatory user consent.

5

These benefits are especially important for retail enterprises and other computing environments that require high levels of security in intelligent devices such as intelligent digital signage, gas pumps, vending machines, and kiosks/ATM machines.

- With Admin Control Mode enabled, users have access to all Intel AMT features without the user consent limitations. All the benefits of Intel AMT, including remote restart, hardware KVM, alarm clock, redirection and others, can be used in intelligent devices.
- Remote platforms can be managed and maintained without the need for local user intervention.
- Because of reduced security protection and the risk coming from viruses that may have Admin privileges, this configuration is recommended only for applications where Intel AMT will be deployed, and the systems would be configured within a secure staging area prior to deployment. Purchasing organizations must be advised to setup and configure their systems in such a secure and controlled area to eliminate possible risks.

EHBC makes it much easier to deploy Intel AMT to achieve total cost of ownership benefits, without the need to make tradeoffs in security or functionality.



For more information about Intel AMT for intelligent systems, please visit http://edc.intel.com/Intel-Product-Technologies/AMT

intel®
Intelligent Systems

Printed in USA 0513/BR/ICMCRC/PDF ♻ Please Recycle 328979-001US