Security Best Practices of Intel® Active Management Technology and Intel® Standard Manageability Q&A August 2022

Intended Audience

This Q&A is for Intel customers who plan to deploy and activate Intel® Active Management Technology (AMT) and Intel® Standard Manageability.

Content Summary:

This Q&A focuses on security practices around provisioning Intel® AMT and Intel® Standard Manageability, its security considerations, and security practices in the following areas:

- Intel® AMT and Intel® Standard Manageability provisioning via Manual Configuration
- IDE-R/USB-R and Serial over LAN
- HTTP digest Authentication schema
- Remote provisioning
- Wireless Intel® AMT and Intel® Standard Manageability
- End User Privacy

Key Messages

- Intel recommends following security best practices including running with the least privileged access, and keeping firmware, security software & operating systems up to date.
- Intel makes every effort to protect our platforms from attack and takes reports of issues seriously investigating each to determine merit and opportunities to further enhance system security.
- There are published best known methods and recommended security configurations that mitigate most issues raised in this Q&A.

Contacts: For technical assistance, please contact Intel Customer Support at http://vprosupport.intel.com

Questions and Answers:

Q1. Why this Q & A?
A1. This Q & A is to articulate best practices in securing Intel® Active Management Technology (AMT) and Intel® Standard Manageability security capabilities and to further clarify certain misperceptions of Intel® AMT and Intel® Standard Manageability security vulnerabilities, which would require the attacker to have physical access to the device and OS administrator credentials to attempt this exploit.

Q2. Are there security concerns with Intel Active Management Technology?
A2. The Intel® vPro™ platform and its included Intel® Active Management Technology (AMT) and Intel® Standard Manageability has supplied differentiated hardware-assisted security and manageability capabilities to over 100 million systems over the last decade. When Intel receives a report of a potential security vulnerability in our products, we begin evaluation of the report. We confirm the potential vulnerability, assesses the risk, determine the impact, and assign a processing priority. After vulnerability confirmation, the priority determines issue handling throughout the remaining steps in the process. For severe issues requiring immediate mitigation steps, communication occurs through https://www.intel.com/security.

Q3. Are there security vulnerabilities in your product(s)?
A3. Intel recognizes our role in improving the security of the computing platform. Intel actively works to identify and resolve security vulnerabilities. In the event that vulnerabilities are identified, the Intel Product Security Incident Response Team (PSIRT) works across Intel and with the security community to understand the vulnerability and the underlying issue. The Intel PSIRT has the responsibility to communicate with our suppliers, customers, and end users.

Public communications from the Intel PSIRT are available at https://www.intel.com/security.

Q4. If Intel knew of a security issue with its products would you disclose that issue?
A4. Intel is committed to addressing security vulnerabilities affecting our customers and providing responsible guidance on the solution, impact, severity and mitigation. The latest information about product security issues is available on our portal https://www.intel.com/security.

Q5. What prevents malicious software from using Intel® Active Management Technology (AMT) and Intel® Standard Manageability to exploit a PC and what authentication mechanism is used to prevent an unauthorized person from gaining access?
A5. Access and communications between Intel® Active Management Technology (AMT) and Intel® Standard Manageability and authorized management consoles can be fully encrypted using TLS. Even if authorized management consoles are not “encrypted”, the communication with Intel AMT requires valid credential setup during configuration, either digest authentication or Kerberos authentication are supported. It is also possible to setup Intel® AMT and Intel® Standard Manageability to require a client x509v3 certificate (aka TLS mutual authentication) to provide additional security. Intel® AMT and Intel® Standard Manageability Client Initiated Remote Access (CIRA) can be setup so that access to Intel® AMT and Intel® Standard Manageability is always via a client initiated TLS tunnel. In addition, IT administrators' access can be limited to only certain remote features and full privilege can be granted only to those with Admin rights. Intel AMT and Intel® Standard Manageability also includes an Access Monitor feature that allows only an authorized Auditor to clear out logs to help deter malicious insider attacks. The log also includes critical events that cannot be cleared even by an authorized Auditor.

Q6. Does Intel recommend local access to Intel® Active Management Technology (AMT) and

Intel® Standard Manageability for operations?
A6. Intel® Active Management Technology (AMT) and Intel® Standard Manageability provides a distinction between local user accounts for SW that accesses Intel AMT and Intel® Standard Manageability via the local host interface versus remote user accounts for accessing Intel® AMT and Intel® Standard Manageability from a remote management console. Intel strongly recommends the remote management user account not be accessed from the local host interface. Doing so may expose the remote account credential to the operating system software.

Q7. Is Intel® Active Management Technology (AMT) and Intel® Standard Manageability disabled by default on Intel vPro platforms? If not, can it be disabled or have any default passwords changed by end users not part of the IT-supported network?
A7. Depending on the customers' request, Intel vPro platforms can be delivered by OEMs in one of the following Intel Intel® Active Management Technology (AMT) and Intel® Standard Manageability states:

- Un-provisioned and ON in BIOS or
- Un-provisioned and OFF in BIOS or
- Un- provisioned and permanently OFF in BIOS

The Intel® AMT and Intel® Standard Manageability firmware does not search for a configuration server when being plugged in the network for the first time; this capability is not supported. Intel recommends when receiving a new Intel® AMT and Intel® Standard Manageability capable platform with Intel® AMT or Intel® Standard Manageability turned ON in the BIOS, that the default BIOS password, as well as the default Intel® Management Engine BIOS Extension (Intel® MEBx) password be changed.

Q8. What is the Intel® Management Engine BIOS Extension (Intel® MEBX)?
A8. The Intel® Management Engine BIOS Extension (Intel® MEBX) is an additional BIOS menu present only on Intel® Active Management Technology (AMT) and Intel® Standard Manageability systems. This menu is displayed if the local user presses a special key combination (usually Ctrl-P) during system POST. In some platforms, Intel® MEBX is integrated into BIOS menu. In such systems, during system boot, access BIOS menu (OEM dependent) and select MEBX. The Intel® MEBX can be used to locally configure Intel® AMT or Intel® Standard Manageability.

Q9. How do I change the default Intel® Management Engine BIOS Extension (Intel® MEBX) password?
A9. Before the Intel® Management Engine BIOS Extension (Intel® MEBX) can be used, the default password must be changed. see Q7 above for guidance. The Intel® MEBX can also be changed remotely during the Intel® Active Management Technology (AMT) or Intel® Standard Manageability configuration process. To configure Intel AMT and Intel® Standard Manageability remotely you can leverage the Intel® Endpoint Management Assistant (Intel® EMA) to configure the system into Admin Control Mode. Client Control Mode does not support changing the Intel® MEBX password.

Q10. Are there security vulnerabilities in Manual Configuration of Intel® Active Management Technology (AMT) and Intel® Standard Manageability provisioning via Intel® Management Engine BIOS Extension (Intel® MEBX)?
A10. The Intel® Active Management Technology (AMT) and Intel® Standard Manageability manual configuration methods let you provision an Intel® AMT and Intel® Standard Manageability system with basic settings, but they do require local access to the device in order to boot to the Intel® Management Engine BIOS Extension (Intel® MEBX). If the Intel® MEBX default password was never changed, an unauthorized person with physical access to the system could manually provision Intel® AMT and Intel® Standard Manageability via the Intel® MEBX using the default password. Once configured, Intel® AMT

and Intel® Standard Manageability allows remote access to the Intel® AMT and Intel® Standard Manageability feature set on the local area network (LAN). If the system's manufacturer has followed Intel's recommendation to protect the Intel® MEBX menu with the system BIOS password, this physical attack would be mitigated.

Q11. Has Intel provided guidance to system manufacturers to reduce the potential vulnerability of unauthorized Intel® Active Management Technology (AMT) and Intel® Standard Manageability provisioning via Manual Configuration?
A11. Yes, Intel has provided recommendations to system manufacturers in September 2015 to protect the Intel® Management Engine BIOS Extension (Intel® MEBX) with the system BIOS password.

Q12. Is there a method to detect if an unauthorized attacker has access to my Intel® Active Management Technology (AMT) and Intel® Standard Manageability system?
A12. Intel® Active Management Technology (AMT) and Intel® Standard Manageability provides event log and audit log capabilities that can provide detail on use of Intel® AMT and Intel® Standard Manageability capabilities. However, users with the Intel® AMT and Intel® Standard Manageability password have the ability to clear event logs or fill logs in an attempt to obfuscate their activity. Intel® AMT and Intel® Standard Manageability also includes an Access Monitor feature that allows only an authorized Auditor to clear out logs to help deter malicious insider attacks. The log includes critical events that cannot be cleared even by an authorized Auditor. Starting with 11th Generation Intel® Core™ processor-basedplatforms (release 15.0), the Intel® AMT and Intel® Standard Manageability Audit Log can be retrieved also via a host interface that is available regardless of Intel® AMT and Intel® Standard Manageability provisioning state. The use of the Intel® AMT and Intel® Standard Manageability "KVM remote control" feature provides a prominent and mandatory flashing border indicating an active KVM session; however, this relies on the local user being present to observe it.

Q13. Are there security vulnerabilities in IDE-R and Serial over LAN?
A13. In legacy systems (Intel® Active Management Technology (AMT) and Intel® Standard Manageability 5.x and older), passwords could be visible when performing SOL/IDER only when TLS is disabled. In Intel® AMT and Intel® Standard Manageability 6.0 and later versions, Intel has further hardened these features by supporting an additional authentication scheme.

Q14. Are there security vulnerabilities in an HTTP digest authentication scheme?
A14. HTTP digest authentication requires a username and password as forms of identification. It is theoretically possible to uncover the Intel® Active Management Technology (AMT) and Intel® Standard Manageability credentials that are exchanged during HTTP digest authentication, when using non-TLS mode. Thus, Intel strongly recommends that customers use TLS mode to benefit from its enhanced security in communication. The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. Alternatively, Kerberos-based authentication schemes can be used if TLS is not applicable.

Q15. Are there security vulnerabilities in Intel® Active Management Technology (AMT) and Intel® Standard Manageability related to Remote Provisioning?
A15. A complex sequence of successful CA infrastructure and domain hacks would be required to purchase and install a compromised certificate. In addition to the certificate, you will need to gain access to the network by setting up a rogue DHCP server and also have administrative rights to the clients in order to perform remote provisioning tasks.

Q16. Are there security vulnerabilities in wireless Intel® Active Management Technology (AMT) and Intel® Standard Manageability related to 802.11?

A16. There are generic security concerns on all 802.11 compliant products (Intel® Active Management Technology (AMT), Intel® Standard Manageability and non-Intel® AMT). Intel has implemented Intel® AMT and Intel® Standard Manageability configurations preventing connections to open networks, enforcing a password policy for PKI profiles; Intel® AMT and Intel® Standard Manageability configuration only allows an Intel® AMT and Intel® Standard Manageability authorized user to add a wireless profile. Additionally, 802.1x authentication and 802.11i encryption are both supported for secure WLAN connections.

Q17. Where can I find additional information on privacy-sensitive functions and capabilities of Intel® Active Management Technology (AMT) and Intel® Standard Manageability?

A17. Intel publishes a supplemental privacy statement for Intel® Active Management Technology (AMT) and Intel® Standard Manageability at https://www.intel.com/content/www/us/en/privacy/intel-active-technology-vpro.html