

Intel® Active Management Technology Validation Tools

User Guide

October 2009

Revision 0.90

Intel Confidential



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.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described 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.

This document contains information on products in the design phase of development.

All products, platforms, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. All dates specified are target dates, are provided for planning purposes only and are subject to change.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

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 www.intel.com/technology/platform-technology/intel-amt/

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Intel, Intel vPro, and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

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

Copyright © 2007-2008, Intel Corporation. All rights reserved.



IMPORTANT—READ BEFORE COPYING, INSTALLING OR USING.

Do not use or load this software or any associated materials (collectively, the “Software”) until you have carefully read the following terms and conditions. By loading or using the Software, you agree to the terms of this Agreement. If you do not wish to so agree, do not install or use the Software.

LICENSE—Subject to the restrictions below, Intel Corporation ("Intel") grants you the following limited, revocable, non-exclusive, non-assignable, royalty-free copyright licenses in the Software.

The Software may contain the software and other property of third party suppliers, some of which may be identified in, and licensed in accordance with, the “license.txt” file or other text or file in the Software:

DEVELOPER TOOLS—including developer documentation, installation or development utilities, and other materials, including documentation. You may use, modify and copy them internally for the purposes of using the Software as herein licensed, but you may not distribute all or any portion of them.

RESTRICTIONS—You will make reasonable efforts to discontinue use of the Software licensed hereunder upon Intel’s release of an update, upgrade or new version of the Software.

You shall not reverse-assemble, reverse-compile, or otherwise reverse-engineer all or any portion of the Software.

Use of the Software is also subject to the following limitations:

You,

(i) are solely responsible to your customers for any update or support obligation or other liability which may arise from the distribution of your product(s)

(ii) shall not make any statement that your product is "certified," or that its performance is guaranteed in any way by Intel

(iii) shall not use Intel's name or trademarks to market your product without written permission

(iv) shall prohibit disassembly and reverse engineering, and

(v) shall indemnify, hold harmless, and defend Intel and its suppliers from and against any claims or lawsuits, including attorney's fees, that arise or result from your distribution of any product.

OWNERSHIP OF SOFTWARE AND COPYRIGHTS—Title to all copies of the Software remains with Intel or its suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You will not remove, alter, deface or obscure any copyright notices in the Software. Intel may make changes to the Software or to items referenced therein at any time without notice, but is not obligated to support or update the Software. Except as otherwise expressly provided, Intel grants no express or implied right under Intel patents, copyrights, trademarks, or other intellectual property rights. You may transfer the Software only if the recipient agrees to be fully bound by these terms and if you retain no copies of the Software.

LIMITED MEDIA WARRANTY—If the Software has been delivered by Intel on physical media, Intel warrants the media to be free from material physical defects for a period of ninety (90) days after delivery by Intel. If such a defect is found, return the media to Intel for replacement or alternate delivery of the Software as Intel may select.

EXCLUSION OF OTHER WARRANTIES—EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Intel or its suppliers do not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained in the Software.

LIMITATION OF LIABILITY—IN NO EVENT SHALL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.



Contents

1 Introduction 7

1.1 Terminology 7
1.2 Reference Documents 8

2 Preface 9

2.1 Intel® Management Engine (Intel® ME) 9
2.2 Intel® AMT 9

3 Tools 11

3.1 Overview 11
3.1.1 Manufacturing Line Validation Tools 11
3.1.2 Image Editing Tools 11
3.1.3 Integration Validation Tools 12
3.1.4 Requirements 12
3.1.5 Tools Summary 13

4 Intel® AMT System Validation Tool — Local (AMTVTL) 15

4.1 Requirements 15
4.2 Usage 15
4.3 Intel® Anti-Theft Technology -setPT 16
4.4 Agent Presence Demo 17

5 Intel® AMT System Validation Tool— Remote (AMTVTR) 19

5.1 Requirements 19
5.2 Usage 19
5.2.1 Intel® Anti-Theft Lock/Unlock Demo 21
5.2.2 AMTVTR Redirection Demo 21
5.2.3 Redirection Demo Using TLS 23
5.3 Example 24
5.3.1 Example 1 – Opening an SOL session 24
5.3.2 Example 2 – Opening an IDE-R Session 25
5.3.3 Example 3 – System Defense Demo 25
5.3.4 Example 4 - Agent Presence Demo 25

6 Setup and Configuration Application (Configuration Server) 27

6.1 Tool Requirements 27
6.2 Usage 28
6.3 PSK/PID File Format 28
6.4 Sample TLS Certificates 29
6.4.1 Configuring an Intel® AMT System in Enterprise Mode 29
6.4.2 Modifying the PSK Repository 29
6.4.3 USBfile.exe 30
6.4.4 Configure Setup Parameters 30
6.4.5 Preparing Intel® AMT Devices 31
6.4.6 Install Sample Certificates 31

Appendix A Error Codes 33

A.1 Common Tool Errors – Applies to all Tools 33

A.1.1 Host and Network Interface Errors 33

A.1.2 Network Interface Errors 35

A.1.3 SDK Specific Errors 37

A.2 Intel® ME Interface Errors – Applies to all Tools 37

Tables

Table 1. Tool Summary 13
Table 2. PSKRepository.xml format 29



Revision History

Revision Number	Description	Revision Date
0.3	Pre-Alpha	11/16/2007
0.6	Alpha 1	03/07/2008
0.61	Alpha 2	04/05/2008
0.7	Alpha 3	05/15/2008
0.72	Beta	05/22/2008
0.80	PV	07/15/2008
0.81	Updated AMTVR for Danbury changes	09/26/2008
0.90	Updated Lock/unlock options for AMTVTR and AMTVTL	10/30/2008

§



1 Introduction

The software tools described in this document are designed to assist in qualifying and verifying the implementation of Intel® AMT technology on a new platform. A brief overview of the tools follows.

1.1 Terminology

Term	Description
BIOS	Basic Input-Output System
Complete SPI Image	Complete SPI image contains a Descriptor, BIOS, GbE and ME region
FW	FirmWare, specifically firmware executing on the ME.
GbE	Gigabit Ethernet
IDE-R	IDE Redirection
Intel® AMT	Intel® Active Management Technology.
Intel® MEI	Intel® Management Engine Interface
Intel® QST	Intel® Quiet Speed Technology. Embedded hardware and firmware solution that allows for algorithmic relationship between system cooling fans and temperature monitors so as to reduce noise without losing thermal efficiency.
Intel® TPM	Intel® Trusted Platform Module—Compliant with TPM 1.2 Specification
ME	Intel® Management Engine
MEBx	Intel® Management Engine BIOS Extension
NVM	Non-volatile Memory
OOB	Out-of-Band
OS	Operating System
SNMP	Simple Network Management Protocol
SOAP	Standard Object Access Protocol
SOL	Serial Over LAN
TLS	Transport Layer Security
UI	User Interface
UUID	Unique Universal Identifier

1.2 Reference Documents

Document	Document No./Location
OEM Bring Up Guide	Release kit
Intel® AMT Web UI Guide	Release kit
Users Guide to the Setup and Configuration Application	Release kit "iAMT tools\iamtconfiguration"
Intel® I/O Controller Hub 10 (ICH10) Family datasheet	<TBD>
Intel® AMT SDK	http://softwarecommunity.intel.com/isn/home/manageability.aspx

§

2 Preface

2.1 Intel® Management Engine (Intel® ME)

The new hardware architecture available in Intel® VPro™ platforms offers a number of advanced features, such as:

- A separate processing engine, the Intel® Management Engine (Intel® ME) located in the MCH, which serves as a processor for Intel® AMT capabilities, including out-of-band (OOB) operation.
- Dedicated memory space within main memory where ME code may be executed and ME run-time data stored.
- A LAN controller that supports OOB activity.

2.2 Intel® AMT

An Intel® AMT-enabled system provides the following functionality:

- Highly available out-of-band remote management:
  - Provides remote management capabilities in all system power and health states
  - Runs on auxiliary power.
- Operating System independence:
  - Runs outside the context of the OS
  - Functions in exactly the same manner, irrespective of the installed OS
  - Immunity from OS configuration issues.
- Tamper Resistance:
  - An Intel® AMT agent bound to the PC and configured by IT
  - Resistant to end-user modification or disabling
  - Robust network and local host interface security.
- Capabilities:
  - Discover—hardware and software inventory
  - Heal—remote control, event management, IDE Redirection(IDE-R), and Serial Over LAN (SOL)
  - Infrastructure—firmware update, Setup and Configuration, network and security administration, local communication over SOAP/TLS, and mutual authentication
  - Protect—System Defense for network outbreak containment and detection with agent presence.

§





3 Tools

3.1 Overview

The software tools described in this document are designed to assist in qualifying and verifying the implementation of Intel® AMT technology on a new platform. A brief overview of the tools follows.

3.1.1 Manufacturing Line Validation Tools

Manufacturing line validation tools allow for testing of the Intel® AMT technology immediately after platform silicon is generated. These tools are written to operate quickly and on simple operating systems such as:

- MS-DOS* 6.22
- Windows* 98 DOS
- FreeDOS*
- DRMK DOS*

The Windows version is written to run on Windows* XP (SP1/2) and Windows Vista*.

MEManuf and MEManufWin—these tools validate the Intel® AMT device functionality on the manufacturing line.

3.1.2 Image Editing Tools

- Flash Image tool—combines the GbE, BIOS and ME firmware into a single image that can be programmed by the Flash Programming Tool or any third-party flash programming device.
- FWUpdate—updates the firmware code of a flash device that has already been programmed with a full firmware image.
- Flash Programming tool—programs the flash device on the Intel® AMT device. This tool can program individual regions, or the entire flash device.

3.1.3 Integration Validation Tools

Integration validation tools are used by system integrators to check and validate various aspects of Intel® AMT technology functionality.

- AMTVTL—Uses the LMS and the MEI interface to verify functionality.
- AMTVTR—queries the Intel® AMT subsystem for a remote feature and reports on whether this feature is available or not. Remote features include event manager, remote control, hardware assets, network administration, security administration, System Defense, storage and storage administration, agent presence and remote interface.
- MEInfo and MEInfoWin—queries the Intel ® ME and returns information such as BIOS, FW, and Intel® MEI driver versions.

3.1.4 Requirements

Manufacturing line validation tools run on:

- MS-DOS* 6.22
- Windows* 98 DOS
- Windows* XP (SP1/2)
- Windows Vista*.

Integration validation tools run on Windows (Windows XP SP1/2 and Vista).

Integration validation tools that run locally on the Intel® AMT device require one or more of the following services to be installed:

- Intel® AMT Local Manageability Service (LMS)
- Intel® MEI driver
- Intel® TPM driver.

Check individual tool descriptions for the exact requirements.



3.1.5 Tools Summary

Table 1. Tool Summary

Tool Name	Feature Tested	Runs on Intel® AMT System	Runs on Management System
MEManuf and MEManufWin	Connectivity between Intel® AMT Devices	X	
MEInfo	Firmware Aliveness; Outputs certain Intel® AMT parameters	X	
AMTVTL	Test agent presence and general firmware information.	X	
AMTVTR	Remote administrative features		X
Flash Programming Tool	Programs the image onto the flash device of the Intel® AMT system	X	
Flash Image Tool	Prepares the image files to be programmed onto the flash programming tool	X	X
Firmware Update	Updates the firmware code while maintain the values previously set	X	

§



4 Intel® AMT System Validation Tool — Local (AMTVTL)

The Intel® AMT system Validation Tool Local (AMTVTL) is used to verify the functionality of local Intel® AMT storage, agent presence and general firmware information.

Note: The Web GUI, ME Verification Tool Local, and AMT System Validation Tool Remote do not cover the checking of all features of an Intel® AMT device.

Intel® AMT system validation local tool checks only the local access to NVM storage.

4.1 Requirements

AMTVTL runs on a Windows (XP SP1/2, XP 32/64, Vista 32bit/64bit). It is a command-line executable and must be run locally on the Intel® AMT device.

The following components that must be working correctly in order to perform this test:

- LMS
- The Intel® MEI driver.
- The feature tested must be supported by the system

Note: These LMS and Intel® MEI cannot be tested directly.

4.2 Usage

If the SKU does not support the feature under test, AMTVTL will return a failure. Please make sure the system supports the features under test before using AMTVTL

The executable is invoked by:
AMTVTL.exe [-host <Hostname/IP>] [–user <username>] [–pass <password>] [-TLS] [–cert <certificate>] [-feat ALL| LS| AP| RC| SD| EM| NA| SA| AP| WC]

Options consist of the following:

user <username>—the username used to access to Intel® AMT features on the local machine. If Kerberos authentication is used, the username and password should not be entered.

-pass <password>—the password corresponding to the username used to access to Intel® AMT features on local machine. If Kerberos authentication is used, the username and password should not be entered.

-TLS—must be entered if TLS mode is enabled. If TLS mode is enabled a host name must be provided. The hostname provided must be the same as the hostname used in the TLS certificate in the firmware.

-host <hostname>—the host name as it is appears in the MEBX. If TLS/Kerberos is used, the TLS certificate name must be used as the hostname.

-cert <certificate>—the common name of the client certificate is provided here. The certificate is used only when Mutual Authentication is enabled and in TLS mode. If TLS is used the hostname provided must be the same as the hostname used in the TLS certificate in the firmware.

-eoi is used for legacy support for local test. If EOI is NOT specified, WS-MAN will be used.

-setPT – Creates the credential file needed to unlock a system.

-feat <feature>—specifies the feature to be tested. Feature can only be one of the following options:

Ls—local storage

Ap— agent presence. This test should be used in conjunction with AMTVTR. The –*aptool* option from AMTVTR should be executed before using this option

Gi—general information test. General information test returns:

- BIOS Version
- FW Version
- Build Number
- Configuration mode
- TLS mode
- Hardware Crypto Status
- Network Interface Status
- SOL settings
- IDE-R settings
- FW Update settings
- Configuration State

All—test all of the features mentioned above, except agent presence test (ap)

Note: If the user name and password are not supplied, AMTVTL will prompt the user for hostname.

AMTVTL will return success or failure based on the availability of the tested features. In case of failure, AMTVTL will give a meaningful error message, such as the following:

```
PTSDK_STATUS_HARDWARE_ACCESS_ERROR: The Library has identified a HW Internal
error.
```

4.3 Intel® Anti-Theft Technology -setPT

AMTVTL can create a credential file to unlock a locked system. Without this credential file a locked system can not be unlocked



The command below will create the credential file needed to unlock a system

```
AMTVTL –setPT credentials.xml

This will create the file credentials.xml. This file can be used with AMTVTR
to unlock a locked system. This file MUST be created before the system is
locked. A credential file can NOT be created after a system has been locked.
```

4.4 Agent Presence Demo

The Aptool demo from AMTVTR (AMTVTR –aptool) must be evoked before running.

The agent presence (AP) demo in AMTVTL will create a local agent to send out a heartbeat message. After the user presses a key, the heartbeat messages will no longer be sent. After a short time period, a system defense filter will be triggered. This will stop all network traffic. Network traffic will resume when the agent presence option is called again by AMTVTL, or when the AMTVTR agent presence tool is closed

The agent presence demon flow is as follows:

1. AMTVTR –aptool : Creates a watchdog event and a system defense filter. When the heartbeat messages from the agent stop, the system defense filter is triggered.
2. AMTVTL –ap : A local agent is created and sends heartbeat messages to AMTVTR.
3. After pressing any key on the Intel® AMT system, ATMVTL –ap will close and heartbeat messages will stop
4. AMTVTR watchdog timer is trigg.ered and system defense filter is activated. All network traffic from the Intel® AMT system is blocked.
5. Network traffic will resume when:
    a. AMTVTL –ap is called again (Heartbeat messages resume)
    b. AMTVTR policy is removed (-cleanup)

§



5 Intel® AMT System Validation Tool— Remote (AMTVTR)

Intel® AMT system Validation Tool Remote (AMTVTR) is used to check the functionality of a remote Intel® AMT feature which may not be available through the Web GUI. Note that the Web GUI, AMT system Validation Tool local, and AMT system Validation tool Remote do not cover checking of all features of an Intel® AMT device.

The following features are checked by the AMTVTR:

- Event Manager (Note that access to the Event Log must be on NVM, not through the listener)
- Remote control (boot optional)
- HW assets
- Network admin
- Security admin
- System Defense
- Storage and Storage Admin
- Agent Presence Remote Interface
- Simple Identity
- Audit Log
- Redirection (SOL/IDE-R)

5.1 Requirements

AMTVTR runs on Windows XP SP1/2, XP 32/64, Vista 32bit/64bit, and Server 2003. It is a command-line executable and can be run on a remote computer connected to an Intel® AMT device.

The following components that must be working correctly in order to perform this test:

- LMS
- The Intel® MEI driver.
- The feature tested must be supported by the system

5.2 Usage

If the SKU does not support the feature under test, AMTVTR will return a failure. Please make sure the system supports the features under test before using AMTVTR

The executable is invoked by:

AMTVTR.exe [-host <Hostname/IP>] [–user <username>] [–pass <password>] [-TLS] [-EOI] [-DASH] [–cert <certificate>] [-feat ALL| STO| HWINV| RC| SD| EM| NA| SA| AP| WC| SI| ALOG] [-boot] [-aptool -cleanup] [-redirect] [-sysd –interface [WLAN |LAN| both] -cleanup]

-host <Hostname/IP>—the hostname (hostname displayed in the MEBX) or the IP address (Intel® AMT IP address) of the remote Intel® AMT machine specified in a dotted decimal notation ddd.ddd.ddd.ddd (for example, 134.176.185.2). If TLS mode is used, the hostname must be used

-user <username>—the username to authenticate for access to Intel® AMT features on a remote machine. If Kerberos authentication is used, the username and password should not be entered.

-pass <password>—the password corresponding to the username to authenticate for access to Intel® AMT features on a remote machine. If Kerberos authentication is used, the username and password should not be entered.

-TLS—must be entered if TLS mode is enabled.

-EOI – Used to test legacy commands. If this option is not used WS-MAN protocol will be used. This can not be used with “-dash” option

-DASH – Specifies DASH protocol to be used instead of WS-MAN. If this option is not specified WS-MAN protocol will be used. This can not be used with “-eoi” option

-cert <certificate>—the common name of the client certificate. The certificate is used only when Mutual Authentication is enabled and in TLS mode. If TLS is used, the hostname provided must be the same as the hostname used in the TLS certificate in the firmware.

-feat—run the feature to be tested. Only one out of the following options may be used with each call to the program:

- ALL—check all features
- STO—test the Storage interfaces. This also tests writing to and reading from the flash.

Note: If there are any EACL entries with Enterprise Name = Intel2, using the sto option will erase this entry.

- HWINV—enumerates the hardware inventory and retrieves hardware inventory details.

Note: When additional asset data information is not captured by the Intel® AMT device due to container space limitations, an appropriate warning will be displayed.

- SD—checks the System Defense feature. Enumerates System Defense filters and policies.
- EM—reads the event log records and log timestamp. Note: A warning will be displayed in a case where no event entries exist.
- RC—get the current and supported power states of the Intel® AMT device
- NA—get TCP/IP parameters
- SA—get firmware and configuration mode



- AP—enumerate console watch dog timers
- WC—test wireless profiles that are currently added.
- SI – Simple Identity (only supported in DASH)
- ALOG – Audit Log test

boot—using this option in conjunction with the all or the rc option, the system will perform a power cycle test.

Aptool – Launches agent presence demonstration. This option needs to be executed before running the AP option with AMTVL. Please see Agent Presence Demo section below for more information

-cleanup – Removes the Agent presence policy created by AMTVTR

-CPT – Creates a credential file that will allow a system to be unlocked if ownership has been established

Lock/Unlock – Lock will halt the system at the Intel® Anti-Theft Technology screen if Intel® AMT is enabled. To allow the system to boot the user should use the unlock option with a platform token XML.

Redirect – Launches an interactive IDE-R and SoL demo. SOL and IDE-R must be enabled in the MEBX for this option to function.

Sysd – Launches an interactive system defense demo. This demo will create a system defense policy on the specified interface (LAN or WLAN)

-interface [LAN | WLAN| both] – Specifies which interface to enforce the system defense policy

-cleanup – Removes the system defense policy created by AMTVTR

5.2.1 Intel® Anti-Theft Lock/Unlock Demo

Intel® Anti Theft Technology will prevent the system from booting to the OS or any other media when Intel® Anti-theft technology is enabled and the lock option is set by AMTVTR. The unlock command will allow the system to boot normally. Before a system can be unlocked the user must generate the proper credential token file.

This following command will prevent the system from booting:

- AMTVTR –host amt.intel.com –user admin –pass Admin`12 –lock

This following command will allow the system to boot normally:

- AMTVTR –host amt.intel.com –user admin –pass Admin`12 –unlock credential.XML

Please see above (Section 4.3 Intel® Anti-Theft Technology –setPT) for details to create the credential token file.

5.2.2 AMTVTR Redirection Demo

After entering launching the redirection demo, the user will be asked to make a selection from the following menu:

a: Open SOL Session
b: Close SOL Session
c: Open IDER Session

d: Close IDER Session
e: Regular boot.
f: SOL boot.
g: SOL boot to BIOS setup
h: IDER Floppy boot.
i: IDER CD boot.
j: SOL + IDER Floppy boot.
k: SOL + IDER CD boot.
m: Enable Redirection listener
n: Disable Redirection listener
l: Display Menu Option
x: Exit

choose an option>

Pressing an invalid entry or the letter “L” will display the menu.

A: Open SOL Session: This will launch the PuTTY* terminal emulator in a separate window. Through this window keyboard input will be sent to the Intel® AMT system, and all text based information from the Intel® AMT enabled system will be viewable in this window. Only one SOL session may be open at any time.

After AMTRedirection launches PuTTY, configure the settings as follows:

- Right-click on the PuTTY window title bar, and select "Change Settings..."
- Select "Terminal" and change both "Local Echo" and "Local Line Editing" to "Force Off".
- Select "Terminal-Keyboard", change the sequence sent by the Function keys and keypad to be "VT100+" and the sequence sent by the Backspace key to be "Control-H".
- Select "Session" and "Save" to save these settings for future sessions. (Optional)

Click "Apply" for the settings to take effect.

Note: The Redirection listener must be enabled before opening an SOL session in Enterprise mode.

B: Close SOL Session: Will close the SOL session that was previously opened.

C: Open IDER Session: When this option is invoked, the user will be prompted to choose disk or image for floppy device. When floppy disk is chosen, the appropriate drive letter should be entered. If image file is chosen, the appropriate filename with relative path of image file should be entered. This is followed by the same queries for CD-ROM device, where if CD is chosen, the appropriate drive letter should be entered. If image file is chosen, the appropriate filename with relative path of image file should be entered.

Note: opening IDER session with AMVTR automatically exposes the virtual CD/Floppy devices to the host by enabling IDE Client registers. One should “Scan for hardware changes” in Device Manager to actually see and use these devices in My Computer. Only one IDER session may be open at any time using this particular instance of the program.

Only *.IMG files are supported for floppy disk image files and *.ISO files are supported for CD ROM image files.

D: Close IDER Session: Will close the IDE-R session that was previously opened.



Note: Closing the IDER session leaves the Client IDE registers enabled, i.e. the virtual devices are still exposed to the host even though there is no open IDER session.

E: Regular Boot: Will cause the Intel® AMT enabled system to perform a regular boot as described in the BIOS.

F: SOL Boot: Will cause the remote session to perform a regular boot with the SOL option. An SOL session must be open before using this menu option.

G: SOL Boot to BIOS Setup: Will cause the remote system to boot directly to the BIOS Screen with SOL. An SOL session must be open before using this menu option.

Note: The "Boot to BIOS" option must be set to true in the firmware image.

H: IDER Floppy Boot: Will cause the remote machine to boot from the floppy device in the management console. An IDE-R session must be open before using this menu option.

I: IDER CD Boot: Will cause the remote machine to boot from the CD ROM device in the management console. An IDE-R session must be open before using this menu option.

J: SOL + IDER Floppy boot: This will cause the Intel® AMT host to boot from the bootable remote floppy disk/image in the Management Console. In addition, text and keyboard redirection will be enabled, i.e. text-based information will be redirected from Intel® AMT machine to Management Console, as well as keyboard redirection from Management Console to Intel® AMT machine can be performed (pressing Del to enter BIOS for example). Both SOL and IDER sessions must be opened before using this option.

K: SOL + IDER CD boot: This will cause the Intel® AMT host to boot from the bootable remote CD disk/image in the Management Console. In addition, text and keyboard redirection will be enabled, i.e. text-based information will be redirected from Intel® AMT machine to Management Console, as well as keyboard redirection from Management Console to Intel® AMT machine can be performed (pressing Del to enter BIOS for example). Both SOL and IDER sessions must be opened before using this option.

M: Enable Redirection Listener: This will enable the Redirection service listener.

Note: By default, the Redirection listener is disabled in Enterprise mode and enabled in Small Business mode.

N: Disable Redirection Listener: This will disable the Redirection service listener.

Note: By default, the Redirection listener is disabled in Enterprise mode and enabled in Small Business mode.

L: Display Menu Option: Display the above menu option.

X: Exit: Will exit the menu option and close any open sessions.

Any Other Option: Displays the above menu option

5.2.3 Redirection Demo Using TLS

Before the redirection demo can be performed using a TLS connection the **MC.INI** needs to be modified. The **MCI.INI** file is located in the AMTVTR folder. A [SECURITY] section needs to be added to the **MC.ini** file.

For TLS Server side authentication mode:
Add CA_FILE key in MC.ini under [SECURITY] section. Value for this key must be the path to a root certificate - file containing Certificate Authority certificates.

Example:

[COMMON]…

[SECURITY]

CA_FILE = cacert.cer

For TLS Mutual authentication mode:

1. Create trusted root certificate in PEM format (See "Redirection Library Design Guide" document for instructions about creating PEM certificate).

2. Additional to CA_FILE key add also PRIVATE_CERT and CERT_PASS keys. PRIVATE_CERT value is a path to a file containing a private certificate in PEM format. CERT_PASS value is a string specifying the password protecting the certificate file specified in PRIVATE_CERT.

Example:

[COMMON]…

[SECURITY]

CA_FILE = cacert.cer

PRIVATE_CERT = remote_client.pem

CERT_PASS = 1234

Note: File path name can be either absolute or relative to the directory from which the application is run.

5.3 Example

5.3.1 Example 1 – Opening an SOL session

Before an SOL session can be open, please make sure SOL is enabled in the MEBX menu and your system is SOL capable.

C:\ AMTVTR –host 192.168.0.15 –user admin –pass Admin`12 –redirect
M
A
F

This will display the Redirection menu. By default the redirection listener is disabled. This will prevent un-authorized SOL session from being open. Before an SOL session can be



opened the re-direction listener must be enabled (option M). Once the redirection listener is enabled, SOL sessions can be opened (option A). Once an SOL session is opened the user can test SOL boot and SOL boot to BIOS only.

To test SOL plus IDE-R, an SOL session and IDE-R session must be opened.

Only 1 (one) SOL session may be open at a time.

5.3.2 Example 2 – Opening an IDE-R Session

Before an IDE-R session can be open, please make sure IDE-R is enabled in the MEBX menu and your system is IDE-R capable. Both floppy and CD devices must be specified to open and IDE-R session. An image file may be used instead of a physical drive.

C:\ AMTVTR –host 192.168.0.15 –user admin –pass Admin`12 –redirect
M
A
C

Only 1 (one) IDE-R session may be opened at a time. Before the session can be opened the user will be prompted to enter image filename or the drive letter of the physical device for the floppy and CD drive.

After an IDE-R session is open, both devices will appear in windows if the user refreshes the device list.

5.3.3 Example 3 – System Defense Demo

The system defense demo will create a system defense profile that will block all packets.

C:\ AMTVTR –user admin –pass Admin`12 –sysd

This will prompt the user to enable the profile. After the profile is enabled, all packets will be blocked, but the ME will still remain active.

The profile will remain even after system reset occurs. To remove the profile the user should disable when prompted or use the cleanup option

C:\ AMTVTR –user admin –pass Admin`12 –sysd -cleanup

5.3.4 Example 4 - Agent Presence Demo

The Aptool demo from AMTVTR (AMTVTR –aptool) works with the agent presence (ap) option from AMTVTL

The agent presence (APTool) in AMTVTR will create a watchdog event and a system defense filter. The watchdog event will be triggered when the heartbeat messages from ATMVTL stop. When the watchdog event is triggered the system defense filter is enforced and all network traffic from the Intel® AMT system is blocked. Network traffic will resume when the heartbeat messages are received again or when the policy is removed.

The agent presence demon flow is as follows:

1. AMTVTR –aptool : Creates a watchdog event and a system defense filter. When the heartbeat messages from the agent stop, the system defense filter is triggered
2. AMTVTL –ap : A local agent is created and sends heartbeat messages to AMTVTR
3. After pressing any key on the Intel® AMT system, ATMVTL –ap will close and heartbeat messages will stop
4. AMTVTR watchdog timer is triggered and system defense filter is activated. All network traffic from the Intel® AMT system is blocked
5. Network traffic will resume when:
    a. AMTVTL –ap is called again (Heartbeat messages resume)
    b. AMTVTR watchdog policies are removed (-cleanup)

§

6 Setup and Configuration Application (Configuration Server)

Before management applications can access an Intel® AMT device, the device must be populated with various configuration settings, such as:

- Usernames and passwords
- Network parameters
- Transport Layer Security (TLS) certificates
- Keys necessary for secure communications.

This can be done in one of two ways. Either the device can be set up manually as described in the OEM Bringup Guide, or the setup can be done through the use of the Setup and Configuration Application. For more details on the full functionality of this application, refer to the Setup and Configuration User Guide located in the same folder as the application executable. (For example, iAMT Tools\iamtConfiguration\)

6.1 Tool Requirements

The Setup and Configuration Application runs on Windows* Server 2000 and Windows Server 2003 using a command line interface with the following conditions:.

- Mutual authentication requires that the Intel® AMT device has a trusted_root certificate installed.
- If a DHCP server is not available, then the Intel® AMT device must be configured to use static IP addressing.
- If a DNS server is not available, then the SCS IP address must be explicitly set through either the MEBx or AMTNVM.

All of the files that are included in the subdirectories add features to the configuration server. For more details on all of these features, refer to the Setup and Configuration User's Guide. As a minimum, the following files are required to run the Setup and Configuration Application:

ConfigurationServer.exe—the SCA executable.

BAT Files—before the configuration server can run, certain files need to be present. These BAT files check for the presence of the required files, hence all of the BAT files included in the folders are required for the Server to function.

Library files—the following is a list of library files that must be in the same folder as the Setup and Configuration executable:

- libeay32.dll
- msvcr71.dll
- ssleay32.dll

psk.repository.xml—this file contains a set of PID-PPS key pairs for each Intel® AMT device. The PID is an eight character entry of the form: XXXX-XXXX. The PPS is a thirty-two character quantity of the form: AAAA-BBBB-CCCC-DDDD-EEEE-FFFF-GGGG-HHHH. A sample of the file can be found in the Configuration\ConfigScripts subdirectory in the Setup and Configuration Application folder.

default.conf.xml—this file contains the desired configuration settings for any Intel® AMT devices that are to be configured by the SCA. These settings will be applied to all instances of Intel® AMT devices unless the user creates a unique file for each device. The unique file should be named <UUID>.conf.xml where <UUID> is the actual UUID of the Intel® AMT device. A sample of the file can be found in the Configuration\ConfigScripts subdirectory in the Setup and Configuration Application folder.

6.2 Usage

Setup and Configuration User's Guide contains detailed usage of the tool. The following is only a brief summary of the tool.

The SCA will check for certain signed certificates when executed. If these signed certificates are not present, the application can create signed demo certificates with which the application can function correctly. To create the demo certificates, simply agree when prompted by the application.

This tool does not support the use of multiple client certificates installed on the local host. The certificates used to install the program should not be used on any other systems. If the user already has the appropriate certificates, it is unnecessary to install the demo certificates.

```
ConfigurationServer.exe [-port <Port Number>]
```

-port <Port Number>—the port is the IP listening port number for which the Intel® AMT system is configured. The sample SCA can be started without any parameters in which case the default port will be used for listening. The listening port should match the one configured on the Intel® AMT device during setup. By default, port 9971 is used to establish a connection to the SCA.

6.3 PSK/PID File Format

The sample PSK/PID file PSK.Repository.xml is located in the Configuration\ConfigScripts subdirectory in the Setup and Configuration Application folder, along with PskGenerator.exe.

PskGenerator.exe will output a single PID/PPS pair directly to the screen. This pair should then be placed in the PSK.Repository.xml file in format described in Table 2. Each Intel® AMT device must have a unique pair in order to establish a secure connection so that it can be set up by the SCA.



Platform OEMs may preload Intel® AMT devices with PID/PPS pairs. The repository will be based on a file delivered by the OEM.

Table 2. PSKRepository.xml format

Variable name	Allowed settings	Usage
<pairs>	<pair> <pid>xxxx-xxxx</pid> <pps>xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx</pps> </pair>	Used to define a PID-PPS key pair. This same PID-PPS should be used during the Factory Mode setup of each Intel® AMT device

6.4 Sample TLS Certificates

The SCA is bundled with sample TLS certificates. These are only samples and should not be re-distributed.

The sample certificates are not distributed in the build, but can be installed by running the command checkcs.bat located in the iamtconfiguration\CertGenerator\ClientSecScripts\ folder. To enable TLS, the user should modify default.config.xml or <UUID>.config.xml. These files contain the parameters used by the SCA.

6.4.1 Configuring an Intel® AMT System in Enterprise Mode

An Intel® AMT device can be configured in one of two modes, Small Business or Enterprise. Small business mode can be configured through the MEBx, however, enterprise mode requires an SCA which may be provided by an ISV. The SCA provided as part of the Intel® AMT validation tools, verifies that an Intel® AMT device can be set up and configured by an application. The device in question should be tested with ISV software in addition to the SCA. The following steps need to be performed in order to set up and configure a device in enterprise mode:

1. Modify the PSK repository
2. Configure the setup parameters file default.conf.xml
3. Prepare the Intel® AMT device
4. Install the sample certificates for the SCA and run the application.

Enterprise mode requires the SCA to be running on a dedicated system on the same network as the Intel® AMT device.

6.4.2 Modifying the PSK Repository

The PSK repository file PSK.repository.XML contains the PID/PPS pairs for each Intel® AMT system the needs to be configured by the Setup and Configuration Application. The format should be maintained for all entries that are added (see Table 2).

The PSK Generator PSKGenerator.exe will generate different PID/PPS pairs that can be inserted into the PSK repository file PSK.repository.XML. USBFile.exe will also create an XML file with PID/PPS pairs (see Section 6.4.3). The XML file generated by this tool can be copied and pasted into the PSK.repository.xml.

6.4.3 USBfile.exe

USBfile.exe creates a bin file and an XML file for USB key setup and configuration. The binary file created can also be used by the FAUPD tool and the XML file can be used for the PSK Repository. The usage is as follows:

```
USBfile.exe –Create <Bin File> <XML file> <user name> <Password> <Num>
USBFile.exe –View <Bin File>
```

- -Create—will create a new bin file and a new XML file to be used for USB key setup and configuration or for the PSK file for FAUPD.

  <Bin File>—name of the bin file to be created.

  <XML File>—name of the XML file to be created.

  <user name>—admin user name that is used for USB key setup and configuration.

  <Password>—password that is used during the USB key setup and configuration.

  <Num>—a number in decimal format that determines the number of PID/PPS pairs to create in the XML and bin file.

- -View—will output the contents of a bin file to the screen.

  <Bin File>—name of the bin file to display.

6.4.4 Configure Setup Parameters

The setup parameters file needs to be modified for each device. The format is <UUID>.conf.xml, where <UUID> is the Intel® AMT device's UUID.

If the UUID of the system does not find a unique configuration file, the default configuration file will be used default.conf.xml.

This file contains certificate information, the old username/password, and new username/password. It also contains a number of options for each generation of Intel® AMT. Please read the notes inside the XML file carefully to determine which parameters are used. For example, if the user would like to access the Web UI in enterprise mode the Web UI interface option should be entered in the set_enabled_interfaces section.

The default.conf.xml file and the PSK Repository file are both located in the \iAMTConfiguration\ConfigScripts\ folder.



6.4.5 Preparing Intel® AMT Devices

An Intel® AMT device must be prepared so that it can be configured in enterprise mode. The PID/PPS pairs entered in the PSK Repository file must match the Intel® AMT device. Both the PID and the PPS must match the Intel® AMT device or the setup and configuration process cannot be completed.

Entering the PID/PPS can be done by manually through the MEBx, preloaded through AMTNVM, or with a USB key. For more information on USB key provisioning, see the Setup and Configuration User's Guide

The Intel® AMT device must also contain the IP address of the Setup and Configuration computer along with a port number. The SCA default port number is 9971. This may be changed.

6.4.6 Install Sample Certificates

If the SCA does not have the proper certificates, the application will prompt the user to install the sample certificates which allows the user to configure Intel® AMT devices without purchasing certificates. Answering yes to all the prompts will install the sample certificates in their default locations.

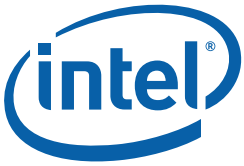
After the certificates are installed, the application will listen for incoming connections. If no port number has been specified, the application will use port 9971. This port number must be specified on the Intel® AMT device.

After the Intel® AMT device has been prepared and is ready to be configured, it will send out "hello" packets to the specified port and server IP address. Once this "hello" packet is received, the SCA will acknowledge the request and complete the process.

After the configuration process is complete, a message will be displayed on the screen and the SCA will listen for the next "hello" packet. The MEInfo tool can be used to verify that the process is complete.

§





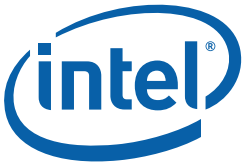
Appendix A Error Codes

A.1 Common Tool Errors – Applies to all Tools

A.1.1 Host and Network Interface Errors

Error Number	Error String	Possible Corrective Actions
0	The request succeeded	Refer to SDK documentation
1	An internal error in the Intel® AMT device has occurred	
2	Intel® AMT device has not progressed far enough in its initialization to process the command.	
3	Command is not permitted in current operating mode.	
4	Length field of header is invalid.	
5	The requested hardware asset inventory table checksum is not available.	
6	The Integrity Check Value field of the request message sent by Intel® AMT enabled device is invalid.	Refer to SDK documentation
7	The specified ISV version is not supported	
8	The specified queried application is not registered.	
9	Either an invalid name or a not previously registered Enterprise name was specified	
10	The application handle provided in the request message has never been allocated.	
11	The requested number of bytes cannot be allocated in ISV storage.	
12	The specified name is invalid.	Refer to SDK documentation
13	The specified block does not exist.	
14	The specified byte offset is invalid.	
15	The specified byte count is invalid.	
16	The requesting application is not permitted to request execution of the specified operation.	

Error Number	Error String	Possible Corrective Actions
17	The requesting application is not the owner of the block as required for the requested operation.	
18	The specified block is locked by another application.	
19	The specified block is not locked.	
20	The specified group permission bits are invalid.	
21	The specified group does not exist.	
22	The specified member count is invalid.	
23	The request cannot be satisfied because a maximum limit associated with the request has been reached.	
24	The specified key algorithm is invalid	
25	Authentication failed	
26	The specified DHCP mode is invalid.	Refer to SDK documentation
27	The specified IP address is not a valid IP unicast address.	
28	The specified domain name is not a valid domain name.	
29	Unsupported version	
30	The requested operation cannot be performed because a prerequisite request message has not been received.	
31	Invalid Table type	Refer to SDK documentation
32	The specified provisioning mode code is undefined.	
33	Unsupported object	
34	The specified time was not accepted by the Intel® AMT device since it is earlier than the baseline time set for the device.	
35	Starting Index is invalid.	
36	Specified parameter is invalid.	
37	An invalid netmask was supplied a valid netmask is an IP address in which all ‘1’s are before the ‘0’ – e.g. FFFC0000h is valid FF0C0000h is invalid).	
38	The operation failed because the Flash wear-out protection mechanism prevented a write to an NVRAM sector.	

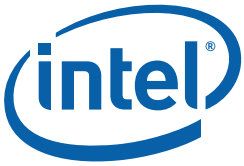


Error Number	Error String	Possible Corrective Actions
39	ME FW did not receive the entire image file.	Refer to SDK documentation
40	ME FW received an image file with an invalid signature.	
41	LME can not support the requested version.	
42	The PID must be a 64 bit quantity made up of ASCII codes of some combination of 8 characters – capital alphabets (A–Z) and numbers (0–9).	
43	The PID must be a 256 bit quantity made up of ASCII codes of some combination of 8 characters – capital alphabets (A–Z) and numbers (0–9).	
44	Full BIST test has been blocked	Refer to SDK documentation
45	A TCP/IP connection could not be opened on with the selected port.	
46	Max number of connection reached. LME can not open the requested connection.	

A.1.2 Network Interface Errors

Error Number	Error String	Possible Corrective Actions
2049	The OEM number specified in the remote control command is not supported by the Intel® AMT device	Refer to SDK documentation
2050	The boot option specified in the remote control command is not supported by the Intel® AMT device	
2051	The command specified in the remote control command is not supported by the Intel® AMT device	
2052	The special command specified in the remote control command is not supported by the Intel® AMT device	
2053	The handle specified in the command is invalid	

Error Number	Error String	Possible Corrective Actions
2054	The password specified in the User ACL is invalid	Refer to SDK documentation
2055	The realm specified in the User ACL is invalid	
2056	The FPACL or EACL entry is used by an active registration and cannot be removed or modified.	
2057	Essential data is missing on CommitChanges command.	
2058	The parameter specified is a duplicate of an existing value	
2059	Event Log operation failed due to the current freeze status of the log.	
2060	The device is missing private key material.	
2061	The device is currently generating a keypair. Caller may try repeating this operation at a later time.	
2062	An invalid Key was entered.	Refer to SDK documentation
2063	An invalid X.509 certificate was entered.	
2064	Certificate Chain and Private Key do not match.	
2065	The request cannot be satisfied because the maximum number of allowed Kerberos domains has been reached. The domain is determined by the first 24 Bytes of the SID.)	
2066	The requested configuration is unsupported	Refer to SDK documentation
2067	A profile with the requested priority already exists	
2068	Unable to find specified element	
2069	Invalid User credentials	
2070	Passphrase is invalid	
2072	Need to associate a key pair with signing Key pair handle	



A.1.3 SDK Specific Errors

Error Number	Error String	Possible Corrective Actions
4096	An internal SDK error occurred	Refer to SDK documentation
4097	An ISV operation was called while the library is not initialized	
4098	The requested library I/F is not supported by the current library implementation.	
4099	One of the parameters is invalid (usually indicates a NULL pointer or an invalid session handle is specified)	
4100	The SDK could not allocate sufficient resources to complete the operation.	
4101	The Library has identified a HW Internal error.	
4102	The application that sent the request message is not registered. Usually indicates the registration timeout has elapsed. The caller should reregister with the Intel AMT enabled device.	Refer to SDK documentation
4103	A network error has occurred while processing the call.	
4104	Specified container can not hold the requested string	
4105	ISVS_InitializeCOMinThread was not called by the current thread.	
4106	URL required	

A.2 Intel® ME Interface Errors – Applies to all Tools

Error Number	Error String	Possible Corrective Actions
8192	Intel ® ME Interface : Internal error	Tool failed due to an internal error. Please report error
8193	Intel ® ME Interface : Cannot locate ME device	
8194	Intel ® ME Interface : Memory access failure	
8195	Intel ® ME Interface : Write register failure	
8196	Intel ® ME Interface : Cannot allocate memory	Close other applications and retry

Error Number	Error String	Possible Corrective Actions
8197	Intel ® ME Interface : Circular buffer overflow	Tool failed due to an internal error. Please report error
8198	Intel ® ME Interface : Not enough memory in circular buffer	
8199	Intel ® ME Interface : ME Device not ready for data transmission	
8200	Intel ® ME Interface : Unsupported bus message protocol version	
8201	Intel ® ME Interface : Unexpected interrupt reason	
8202	Intel ® ME Interface : Intel ® AMT device unavailable	
8203	Intel ® ME Interface : Unexpected ME device response	
8204	Intel ® ME Interface : Unsupported message type	
8205	Intel ® ME Interface : Cannot find host client	
8206	Intel ® ME Interface : Cannot find ME client	
8207	Intel ® ME Interface : Client already connected	Tool failed due to an internal error. Please report error
8208	Intel ® ME Interface : No free connection available	
8209	Intel ® ME Interface : Illegal parameter	
8210	Intel ® ME Interface : Flow control error	
8211	Intel ® ME Interface : No message	
8212	Intel ® ME Interface : Buffer too large	
8213	Intel ® ME Interface : Buffer too small	
8214	Intel ® ME Interface : Circular buffer not empty	

§