



# Intel® Active Management Technology ISV Coexistence Guidelines

Version 3.0.1, December 2006

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppels 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, or life sustaining applications.

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

The API and software 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.

This document and the software described in it are furnished under license and may only be used or copied in accordance with the terms of the license. The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document. Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

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 ordering number and are referenced in this document or other Intel literature may be obtained by calling 1-800-548-4725 or by visiting Intel's website at <http://www.intel.com>.

Copyright © 2006, 2007 Intel Corporation.

\* Third party other names and brands may be claimed as the property of others.

## 1 Overview

The Intel® Active Management Technology (Intel® AMT) Software Development Kit (SDK) provides the necessary documentation, API's and libraries to utilize Intel AMT. This SDK is distributed as a part of Intel® Early Access Program (EAP) to Independent Software Vendors (ISVs) under a Non-Disclosure Agreement (NDA) with Intel Corporation.

When multiple ISVs are interacting with the same client platforms, it is possible for the ISVs to interfere with the operation of applications from another company. This document provides a set of coexistence guidelines for each ISV to follow to help prevent the exploitation of certain features of Intel AMT to the exclusion of other ISV applications.

## 2 Terms and Acronyms

Acronym or Term	Definition
ACL	Access Control List - Credentials used to limit access to resources.
Agent	Software that runs on a client PC with OS running.
Host or Host CPU	The processor that is running the operating system. This is different than the Intel AMT processor running the Intel AMT FW
Host Service/Application	An application that is running on the Intel AMT-enabled system platform
Intel AMT Configuration	Any changes that can be made after Intel AMT Setup.
Intel AMT Setup	The phase between the factory default state and the issue of the first CommitChanges() command.
ISV	Independent Software Vendor
IT User	Information Technology user. Typically very technical and uses console to ensure multiple PCs on a network function correctly.
MC (Management Console)	Centralized software responsible for communicating with the Intel AMT device.
NVM	Non-Volatile Memory. A memory that will not have content erased even if there is no power applied to it. In Intel AMT, this is achieved using a FLASH device
OEM	Original Equipment Manufacturer - Those companies manufacturing and selling systems that might include Intel AMT.
OOB interface	Out Of Band interface. This is the SOAP over HTTP or SOAP over HTTPS protocol.
PET	Platform event trap is a specification (see the Intel AMT Network Interface Guide) defining the format for managed systems to alert a remote console.
Remote Management application	An application that sends commands and configurations to the FW via the OOB interface. examples: firewall, ISV NVM application
SDK	Software Development Kit
SOAP	Simple Object Access Protocol - An XML based protocol for information exchange in decentralized and distributed environments.
System States	Operating System power states such as S0, S3, S5.

Acronym or Term	Definition
TLS	Transport Layer Security - A protocol intended to secure and authenticate communications across a public networks by using data encryption. TLS is designed as a successor to Secure Sockets Layer (SSL) and uses the same cryptographic methods but supports more cryptographic algorithms.
WSDL	Web Service Definition Language

### 3 Guidelines

The coexistence guidelines are provided in five general categories:

1. Configuration and Setup
2. Warning Messages
3. Application Dependencies
4. Security
5. Resource Usage

The table format indicates the guideline description, rationale, and whether the guideline is covered in the compliance tool.

#### 3.1 Configuration and Setup

ID	Guideline	Rationale	Compliance Tool
CS.DHCP_Hostnames	When Intel AMT and the host processor on the platform are configured using DHCP, make sure that Intel AMT and the host have the same hostname and that the name is not changed without IT involvement.	Changing hostnames could prevent other applications from connecting by invalidating certificates used when TLS authentication is enabled, because the certificates were defined using a different hostname. Independent of the authentication scheme used, if the hostname is changed, then DNS entries for the Intel AMT device will be updated with the new name and applications that do a DNS lookup for the device using the old hostname will not be able to find it.	
CS.Accounts	ISVs should allow IT administrators to configure user name(s) and password(s) used by the ISV application.	Account information should not be created if the Administrator is unaware of it.	
CS.Changing_Admin_Password	If the console allows the changing of the Admin password through the console interface, the console must have the	To prevent errors	

ID	Guideline	Rationale	Compliance Tool
	user type in the password twice. (Specifically denying paste operations)		
CS.Limited_User_Accounts	ISVs should limit user accounts created for their application to 1. Restrictions should be implemented at the remote console.	There are only 8 slots available for ISV applications. There is no need for a definition of more than one account.	Supported
CS.Certificate_Availability	ISV should provide access to the physical certificates used to generate the certificates loaded into the Intel AMT FW so that appropriate clients may obtain the necessary certificates to create a TLS connection. At a minimum, the root certificate of the authority chain must be provided in PEM and DER formats. This assumes the ISV created a configuration server that is either passing certificate requests to a CA or acting as a CA.	While only one application will setup the Intel AMT system, many others will need the certificate to communicate with it.	
CS.FPACL_Exist	Before storage operations, ISV applications should test that the FPACL defining them as partners still exists, and if not they should recover gracefully.	ISV FPACL entry may have been removed by another ISV application.	
CS.FPACL_Modifications	Whenever the FPACL is to be modified, ISVs must expose the entire FPACL to the IT admin and depict the proposed changes (add, delete, etc.) and allow the IT admin to ratify or modify the request to suit their enterprise needs. This would have to be done during configuration and any application maintenance.	IT administrators must maintain control over the applications that require access to protected storage.	

### 3.2 Warning Messages

Warning messages should be displayed when an action that an ISV application initiates could possibly harm the functionality of another ISV application.

ID	Guideline	Rationale	Compliance Tool
WM.Authentication	When changing authentication modes to a client or group of clients a warning message on the remote console must inform the Administrator that this could affect other ISV applications.	Changing this method could prevent other ISVs from connecting	
WM.VLAN_Update	When changing VLANs for an interface a warning message must be displayed.	Changing this method could prevent other ISVs from connecting	
WM.Ping_Response	When changing Intel AMT Ping response a warning message should be	Management apps can create actions such as	

ID	Guideline	Rationale	Compliance Tool
	displayed.	alerts which are dependent on ping response	
WM.Hostname	Changing hostname should require authorization from the IT Administrator.	See CS.DHCP_Hostnames rationale above.	
WM.IP_Address	Changing a static IP address should require authorization from the IT Administrator. Changing from static IP to DHCP or vice versa should require authorization from the IT Administrator.	All applications need a device address to access it. Changing addresses may make the device inaccessible to other applications.	
WM.User_Accounts	ISV applications should never create user accounts on clients without authorization from the IT Administrator.	To give the Administrator full knowledge of the environment	
WM.Log_Reset	A warning message must be shown before resetting the event log.	Other applications may wish to capture certain event logs	

### 3.3 Application Dependencies

ID	Guideline	Rationale	Compliance Tool
AD.Graceful_Failure	Applications should be written so that they fail gracefully when an issue arises, and so that they are not reliant on any particular function.	The Administrator might wish to provide the application with limited rights to the client	
AD.Event_Subscriptions	ISVs should never delete an event subscription that they did not create.	The event most likely will belong to another ISV	Supported per application instance
AD.Filter_Removal	ISV applications must check to see if there are existing subscriptions before allowing filter removal	To verify the filter is not being used by another ISV	Supported
AD.Agent_Registration	ISV applications should never delete Agent Presence agent registration they didn't create	The agent registration most likely will belong to another ISV	Supported per application instance

### 3.4 Security

ID	Guideline	Rationale	Compliance Tool
SE.Admin_Account_Usage	ISVs should not use the Admin account for anything but Administrative purposes.	Keeping the admin password to clients under control of the Administrator lends to better Security	Supported
SE.Admin_Password_Storage	ISV Applications should never store the admin password to clients	ISVs should use a secondary account for their application	

ID	Guideline	Rationale	Compliance Tool
SE.Admin_Account_Requirements	The application should never require the Admin account for functionality	Users may not wish to give the application total control over the clients	
SE.Hidden_Passwords	ISV applications should never display passwords to the screen in plain text	For security purposes	
SE.Password_Storage	Passwords stored within NVM or on local disk must be encrypted	For security purposes	
SE.ACL_Management	ISV application should never remove other ISV ACL info unless explicitly instructed by the IT manager	This ACL could be required by another ISV app to function.	

### 3.5 Resource Usage

ID	Guideline	Rationale	Compliance Tool
RU.Session_Length	ISV storage sessions should never be open and idle for more than 10 seconds.	Only one ISV storage session can be open at any given time. Limit session time and call ISVS_UnRegisterApplication() as soon as possible, especially when errors are encountered.	Supported
RU.Non_Partner_Space	Partner ISVs should NEVER use non-partner space	Partner ISVs have their own reserved space and should not take up space allocated for other uses.	Supported
RU.Storage_Allocation	ISVs should NEVER increase their partner space allocation without explicit configuration from the IT manager.	Changing the allotted space hedges out room for other ISVs	Supported
RU.Compression	If large blocks of data are required to be stored in the NVM, data compression should be utilized	Due to limited space within NVM	
RU.Storage_Full	ISV applications should be able to gracefully handle a full NVM space	So the application does not cause serious errors	Supported
RU.ACL_Management	ISV applications should never remove other ISV ACL info unless explicitly instructed by the IT manager	Removing an ACL will likely break another application	
RU.Frozen_Log	The event log should never be left in a frozen state	If the log is frozen other applications may not be able to write to it	Supported
RU.Total_Storage_Apps	ISVs should use only the up to the maximum default partner size for data storage (Intel AMT Release 1.0 = 24K, Intel AMT Release 2.0 = 48K).	The table can fill up, preventing other ISVs from using storage	Supported (Intel AMT Release 2.0 48K)
RU.Flash_Wear_Out	Applications should operate well below the flash wear out threshold	Multiple ISV applications working at the same time may	Supported

ID	Guideline	Rationale	Compliance Tool
RU.Lock_NVM_Before_RW	ISV application should lock NVM blocks before reading or writing data	cause each other to fail. Multiple ISV applications writing the same NVM block may cause data corruption	Supported
RU.SDF_Policy_for_A_P	When creating a System Defense Feature policy related to Agent Presence, ISVs need to use ConsoleWatchdogGetCbPolicy() to ensure that an existing System Defense Feature -Agent Presence relationship doesn't already exist. If it does, the ISV application needs to allow the IT admin to resolve the conflict and decide whether to allow or disallow the replacement.	You can only have one System Defense Feature policy in effect for all Agent Presence watchdog actions on a single device.	
RU.SOL_IDER_Persistence	ISV Applications should create the SOL and/or IDER session, and reboot the Intel AMT client one time only as the default.	Each reboot using SOL or IDER should create a new session.	
RU.SOL_IDER_Indication	ISV Applications should indicate status of SOL and/or IDER sessions (open or closed) and always provide a user interface to close the session manually.	Users execute manual remediation during open sessions and need the ability to exit the session.	