

# Intel® vPro Technology Reference Guide

---

Revision 1.0  
March 6, 2009



# Revision History

Revision	Revision History	Date
1.0	First release.	March 6, 2009

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 Intel® Active Management Technology may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

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

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

Intel® Active Management Technology requires the computer system to have an Intel(R) 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/](http://www.intel.com/technology/platform-technology/intel-amt/)

Throughout this document Intel ME refers to Intel® Management Engine and Intel® AMT refers to Intel® Active Management Technology.

Intel, the Intel logo, Intel® AMT, Intel vPro, Centrino, Centrino Inside, and vPro Inside are trademarks or registered trademarks of Intel Corporation in the United States and other countries.

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

Copyright © 2009 Intel Corporation. All rights reserved.

# Contents

---

<b>Preface</b> .....	<b>5</b>
Intended Audience .....	5
What This Document Contains .....	5
Feature Version Matrix .....	6
<b>Client Initiated Remote Access (CIRA) and Client Initiated Local Access (CILA)</b> .....	<b>7</b>
Client Initiated Remote Access (CIRA) Overview .....	7
CIRA System and Infrastructure Requirements .....	7
Management Presence Server (MPS) Overview .....	8
Configuring the Intel® AMT Platform for Remote Access .....	10
Loading Certificates .....	10
MPS Parameters .....	10
Enabling Remote Access .....	11
Implementing a User-Initiated Trigger .....	11
Client Initiated Local Access (CILA) Overview .....	12
CILA Deployment and Use Overview .....	13
CILA Components .....	13
Setup and Configuration Process .....	13
What you need .....	13
Intel AMT Configuration .....	14
SMB Mode .....	14
Enterprise Mode .....	16
Alert Subscription – Both SMB and Enterprise Modes .....	18
OS Configuration .....	18
<b>Intel® Anti-Theft Technology – PC Protection (Intel® AT-p)</b> .....	<b>19</b>
Detection Mechanisms .....	21
Poison-pill Responses .....	21
Excessive login attempts can trigger poison pill for PC disable .....	21
Server login timeout can trigger poison pill for PC disable .....	22
Reactivation and Full System Recovery .....	22
<b>Audit Log (also known as Access Monitor)</b> .....	<b>23</b>
Requirements .....	23
Things to note .....	23
More Information .....	24
<b>Microsoft* Network Access Protection (NAP)</b> .....	<b>25</b>
Requirements .....	25
Things to note .....	26
More Information .....	26
<b>Intel® Management and Security Status Tool</b> .....	<b>27</b>
System Requirements .....	27
Usage Overview .....	28
General Tab .....	28
Intel® AMT Tab .....	30

Intel AMT State.....	31
Advanced Information.....	31
Remote Connectivity / Request Assistance .....	33
Intel® TPM Tab.....	34
Intel® AT tab .....	36
Exiting the Application.....	37
<b>Setup and Configuration Server version 5 (SCS 5) .....</b>	<b>38</b>
Overview .....	38
New Features Since Beta Release .....	38
New Features in SCS 5.0.....	38
NAP support .....	38
Usability improvements .....	38
Support for change hostname/UUID .....	39
Support for automatic configuring and extracting PID from hello packet .....	39
Extended AMTList APIs to support recovering configuration parameters.....	39
Attempt connection with AMT using FQDN .....	39
Support for Active Directory forest configurations.....	39
New SCS console.....	39
WSDL improvements.....	40
Other features added in the Beta release .....	41
<b>Intel® Trusted Platform Module .....</b>	<b>42</b>
Requirements .....	42
Things to note .....	42
Provisioning the Intel TPM .....	43
Take TPM ownership .....	43
To Verify .....	44
Recover from a changed or missing TPM token .....	44
<b>WS-MAN and DASH 1.0 Compliance .....</b>	<b>46</b>
<b>Figures</b>	
Figure 1: CIRA Topology. ....	9
Figure 2: CIRA Connection Between Intel AMT Client and Management Console. ....	9
Figure 3: Example of In Band CIRA & CILA User Initiated Connection tool. ....	12
Figure 4: Intel® AT-p Usage Model.....	20

## Preface

---

This Technical Reference Guide highlights significant and noteworthy features and functionality of the Intel® vPro Technology platform. This guide is not intended to be all inclusive. Rather, it is intended to provide an overview of the highlighted technologies and, where appropriate, provide links to more detailed documentation on a given technology. Procedures included in this guide are for example only, to help the reader better understand the technology being described, and are not intended for use in actual implementations.

## Intended Audience

This document is intended for Information Technology (IT) professionals who need to be aware of new features of the Intel vPro Technology platform. Readers should already have a basic familiarity with Intel vPro Technology, including configuration and use of the Intel® AMT platform for out-of-band management. Readers should also be familiar with the basics of IT infrastructure, especially networked environments and their component technologies.

## What This Document Contains

This document contains the following sections:

Section	Description
CIRA and CILA	Provides a conceptual overview of CIRA and CILA functionality.
Intel® Anti-Theft Technology – PC Protection (Intel® AT-p)	Provides a conceptual overview of Intel® AT-p functionality.
Access Monitor	Describes the Access Monitor feature, also known as “AuditLog.”
Microsoft NAP Integration	Describes the basics of Intel vPro Technology’s support of Microsoft NAP.
Intel Management Security and Status (IMSS) Tool	Provides a conceptual overview of the IMSS tool.
SCS version 5	Highlights the notable new features of SCS version 5.0.
WSMAN and DASH	Asserts Intel vPro compliance to these standards and provides links to more information on the standards themselves.

## Feature Version Matrix

The chart below indicates the Intel® AMT versions with which the features described in this guide are associated.

**Table 1: Feature Version Matrix**

	Intel AMT 3.x	Intel AMT 4.0	Intel AMT 4.1	Intel AMT 5.0	Intel AMT 5.1
<b>CIRA/CILA (Fast Call for Help)</b>		X	X	X	?
<b>Intel® AT-p</b>			X		?
<b>Audit Log</b>				X	?
<b>Microsoft NAP support</b>				X	?
<b>Intel® Management and Security Status Tool</b>				X	?
<b>Setup and Configuration Server version 5.0</b>				X	?
<b>Intel® Trusted Platform Module</b>				X	?
<b>WS-MAN and DASH Compliance</b>				X	?

# Client Initiated Remote Access (CIRA) and Client Initiated Local Access (CILA)

---

This section provides overviews of Client Initiated Remote Access (CIRA) and Client Initiated Local Access (CILA).

## Client Initiated Remote Access (CIRA) Overview

Intel® Active Management Technology (Intel® AMT) Release 4.0 introduces client initiated remote access (CIRA). In previous releases, an Intel AMT platform needed to operate within an enterprise's network to be reachable by management consoles. Any enterprise separation between the Intel AMT device and the console, such as a firewall, would make the platform unreachable. By configuring the Intel AMT platform to be able to initiate a connection to an intermediate server running in the enterprise "demilitarized zone" (DMZ), the platform can be managed remotely when it is connected to the Internet anywhere in the world.

## CIRA System and Infrastructure Requirements

This section gives an overview of the hardware, software and network components required to make use of CIRA.

Intel AMT 4.0 or greater	
Management Console	Manages Client. Must be able to receive alerts from the MPS and use MPS as a proxy for AMT commands. This comes from an ISV
OS User Initiated Agent	Provides the User Interface allowing a Knowledge Worker to "Call for Help" from within the OS. This comes from an ISV.
BIOS User Initiated Agent	Provides the User Interface allowing a Knowledge Worker to "Call for Help" without an OS, during system boot. This comes from the OEM and is optionally provided by MEBX in the form of CTRL-ALT-F1.
Manageability Presence Server (MPS)	Accepts Intel AMT connections from outside a firewall and acts as the intermediary between Intel AMT and the Management Console. This comes from an ISV.
Setup and Configuration Application	Configures AMT with policies and certificates needed to support CIRA. This comes from an ISV.

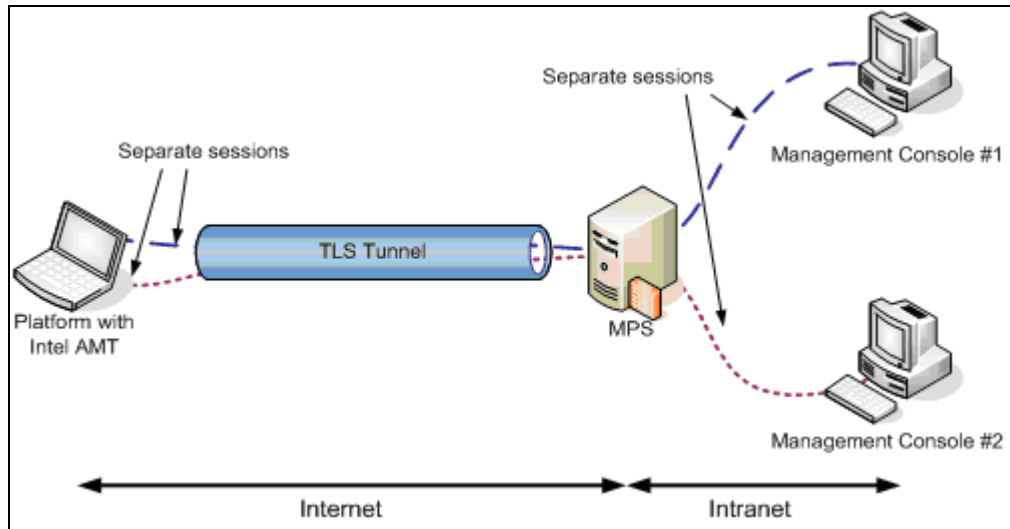
Certificate Authority	Generates certificates for CIRA use. This is provided within the target IT enterprise infrastructure.
DHCP Server	Intel AMT uses the domain suffix (option 15) from DHCP to determine if it is in or out of the corporate network. This is provided within the target IT enterprise infrastructure.
Firewall rules	These rules define permissible traffic between two locations. Although a firewall is not technically required for CIRA, it is the expected mode of operation. The firewall must have a rule that allows TLS tunnel traffic from Intel AMT on the Internet to go through to the MPS in the DMZ. This is provided within the target IT enterprise infrastructure.

## Management Presence Server (MPS) Overview

A Management Presence Server (MPS) enables enterprise management consoles located behind the enterprise firewall to connect to Intel AMT platforms located outside the enterprise. The MPS mediates between the Intel AMT platform and Intel AMT management console, using a tunneling protocol to secure the communications with the Intel AMT platform.

The MPS appears as a proxy server to management consoles.

The Intel AMT platform connects to the MPS to establish a secure connection to the enterprise network. Once a TLS tunnel is established between the Intel AMT platform and the MPS, multiple management consoles can connect with the platform. The MPS uses the Intel AMT port forwarding protocol (APF) built into the Intel AMT platform to differentiate between different management console sessions. The MPS creates and tears down sessions and allocates/de-allocates ports as management consoles initiate and complete actions. The Intel AMT platform will drop the tunnel connection after a defined period of inactivity. See Figure 1 below.

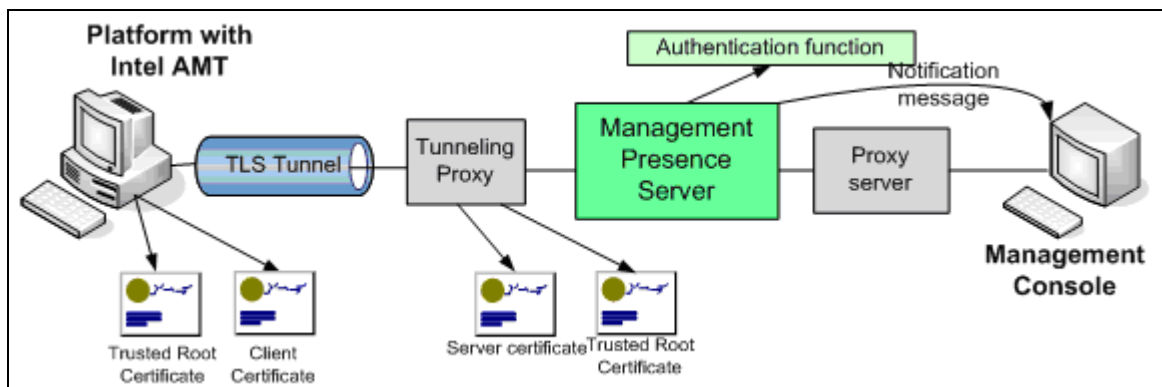


**Figure 1: CIRA Topology.**

The MPS depends on third-party software to implement some of the required functionality.

- A Tunneling Proxy establishes the TLS tunnel with the Intel AMT platform and passes the traffic through to the MPS.
- A Proxy server handles proxy HTTP connections between management consoles and the MPS. The HTTP proxy socksifies the connections and forwards the connections by proxy chaining to the MPS.

See Figure 2 below.



**Figure 2: CIRA Connection Between Intel AMT Client and Management Console.**

See Appendix A: Setting Up the Management Presence Server (MPS) on page 27 for information on setting up a Management Presence Server.

## Configuring the Intel® AMT Platform for Remote Access

A setup and configuration application is required to prepare an Intel AMT platform for remote access. Since the setup and configuration activity will include the installation of corporate IT generated certificates and settings, the setup and configuration activity must be performed while the setup and configuration application and the Intel AMT platform are on the same intranet.

See the Network Interface Guide for the SOAP interface commands that perform the following functionality. See the WS-Management Flows document and the WS-Management Class Reference for WS-Management support to this process. The setup and configuration sample demonstrates configuring for remote access using the SOAP interface. Note that you can also use the Setup and Configuration Service version 5 (SCS 5) to configure for remote access.

The setup and configuration application adds necessary certificates, adds MPS information and remote access policies, and then enables remote access:

### Loading Certificates

The Intel AMT device requires a trusted root certificate at a minimum and a client certificate if TLS with mutual authentication will be used.

Trusted root certificate: Used to authenticate the server certificate sent by the tunneling proxy when setting up the TLS tunnel.

Client Certificate: Sent by the Intel AMT device when mutual authentication is used. The tunneling proxy must have a trusted root certificate corresponding to this certificate.

### MPS Parameters

These parameters define how to connect to the MPS and the conditions that initiate a remote access connection.

#### MPS information

These parameters tell the Intel AMT device how to connect to an MPS. The parameters include:

- Address and port where the tunneling proxy listens for Intel AMT connection requests.
  - The address is either an IP address or FQDN
  - If an IP address is provided, then a Common Name (CN) for the MPS must be provided.
  - Intel AMT uses either the CN provided with an IP address or the FQDN to validate the server certificate sent by the MPS.
- A pointer to a trusted root certificate used for TLS authentication of the MPS.
- Either a pointer to a client certificate used for TLS mutual authentication or a user name/password pair used by the MPS for authentication.

## Remote access policies

A policy defines what can trigger a remote connection, which MPS is contacted, and how long the TLS tunnel is maintained. Policy parameters include:

- Trigger type — the trigger can be user-initiated, triggered by an alert, or triggered periodically.
  - User initiated trigger — A user can initiate an MPS connection either In Band from a host OS application or Out of Band via a BIOS/MEBx request. This trigger type is used when performing a Fast Call for Help.
  - Alert trigger — Whenever an event occurs that sends an alert to a network address, the Intel AMT device initiates an MPS connection, if there is no connection currently active. This trigger type is used when performing Remote Alerts.
  - Periodic trigger — The Intel AMT device connects to an MPS periodically. The policy includes a time interval that determines when a new connection should be attempted. This trigger type is used when performing Scheduled Maintenance.
  - Trigger type priorities – When multiple policies have been defined and a tunnel is already active with an MPS and another trigger occurs, then, if the new trigger is of higher priority and requires a connection to a different MPS, then the current connection will be dropped and the device will connect to the other MPS. A User-initiated trigger has the highest priority, while a periodic trigger has the lowest priority.
- Tunnel lifetime — defines how long the TLS tunnel should stay open, in seconds.
- MPS to connect to — When the trigger occurs Intel AMT attempts to connect to the MPS designated in the policy. A policy can point to two MPS definitions. Intel AMT attempts to connect to the first MPS. If the attempt fails, it tries to connect to the second MPS. The sequence is repeated one more time. Another trigger is required for an additional connection attempt.

## Enabling Remote Access

The setup and configuration application must do two things to enable remote access.

- Enable environment detection, including with it a list of domain suffixes that define the locations that are “inside the enterprise”. When a trigger occurs, if the Intel AMT device detects that it is outside the enterprise, it will connect to the MPS. Otherwise, alerts are sent directly to their destination and periodic and user-initiated triggers are ignored.
- There are two flags that correspond to a user initiated trigger. These specify whether AMT will allow In Band and/or Out of Band user-initiated triggers. For a user-initiated trigger to function, at least one of these must be enabled.

## Implementing a User-Initiated Trigger

When there is a defined “user-initiated” trigger, and In Band user initiation is enabled, a local agent can initiate a remote access session by sending a command via the Intel® Management Engine Interface (Intel® ME interface, or MEI).

## Client Initiated Local Access (CILA) Overview

CILA or Client Initiated Local Access is a combination of hardware and software that allows the Knowledge Worker to request support from IT by choosing options in the OS (In Band) or during the boot process (out of band). This could augment or even replace the need to pick up the phone to call for help. This is called a User Initiated Connection and usually consists of a single mouse click or key stroke. The name is taken from CIRA.

The same API call is used to trigger a User Initiated Connection for CIRA and CILA. As such, it is possible for an ISV to create a single CIRA & CILA initiation tool for Knowledge Worker use (as shown in Figure 3).



**Figure 3: Example of In Band CIRA & CILA User Initiated Connection tool.**

In fact, the same BIOS initiation methods used for CIRA, also work for CILA. CTRL-ALT-F1 during Intel MEBx load is one example. It is also possible for an ISV to design an initiation tool to support only one; CILA or CIRA. An example of that is the Intel Management and Security Status tool. It only allows the knowledge worker to click “connect” if the platform is outside the corporate environment (CIRA).

Although CIRA & CILA use the same API call to make the healing request, there are key differences in these technologies. First, CILA only functions inside the corporate firewall; hence the word “Local” in the name. Second, unlike CIRA, CILA does not establish any tunnel or connection. Rather, it sends a unique CILA PET alert to the console. It is then up to the console to connect to AMT to take action. As such, there is no reliance on a Managed Presence Server (MPS), and no need to set AMT settings such as Environment Detection or CIRA policies. Finally, because of these differences, ISV implementation of CILA is different than for that of CIRA. Basically, an ISV must subscribe to the CILA PET alert, and then act upon it once received. This action may be anything from an email, a pop-up message, or a complex support ticket queue.

## CILA Deployment and Use Overview

### CILA Components

This section gives an overview of the hardware, software and network components required to make use of CILA.

Intel AMT 4.0 or greater	
Management Console	Subscribes to the CILA PET event. This comes from an ISV
OS User Initiated Agent	Provides the User Interface allowing a Knowledge Worker to “Call for Help” from within the OS. This comes from an ISV
BIOS User Initiated Agent	Provides the User Interface allowing a Knowledge Worker to “Call for Help” without an OS, during system boot. This comes from the OEM and is optionally provided by MEBx in the form of CTRL-ALT-F1.
SNMP Trap listener	Receives CILA PET events from AMT and then takes some action such as presenting a user pop-up message to an IT Professional. This can be provided by an ISV or be an off-the-shelf SNMP trap listener.

## Setup and Configuration Process

This section is intended to provide the fundamental process for setting up and configuring a demonstrable implementation of CIRA or CILA. Some of the steps and values for parameters may vary depending on your specific implementation circumstances.

### What you need

This section provides a step-by-step guide to set up CIRA or CILA in the iLab network environment. The iLab environment is meant to be representative of common IT shop network environment, although it does not cover all cases. Still, these steps should provide a method to easily set up and experiment with CIRA/CILA, and the steps can be adapted to fit most IT environments.

CIRA and CILA can be used in Small Business Mode (SMB) and Enterprise Mode (ENT). For SMB mode, this section uses the Intel Manageability DTK. For ENT, this section uses SCS to provision and then use the Manageability DTK to subscribe to, trigger, and receive alerts.

You will need the following:

- Base Interop iLab deployment; PTE or full iLab access.

- SCS 5 VM (SCS5).
- Intel AMT 4 system (Client) joined to the vprodemo.com domain.
- System to use as a console. This can be a VM. The AMT Tools VM in iLab works nicely. (Console).
- Intel Manageability DTK .54i or equivalent. Note – this guide is written with version .54i. Other versions may change the User Interface.

Where applicable, the steps specify the machine in the topology on which each step is performed. For example, “MPS: do this.” means that you are to perform that step on the MPS machine.

## Intel AMT Configuration

Intel AMT can be configuring in either of two modes: SMB and Enterprise. The configuration method for each mode is described below.

### SMB Mode

1. Pre Configuration.
  - a. Console: Install Manageability DTK.
2. Provision the Client



#### NOTE

*The following substeps may differ from system to system:*

- a. Client: Boot Client and press ctrl+P when prompted.
  - b. Client: log in as admin (admin).
  - c. Client: navigate to the Intel AMT Configuration menu and press Enter.
  - d. Client: Choose Host Name and enter the Client's OS host name. Be sure the host name matches the OS. Also, do NOT enter the FQDN, just the host name.
  - e. Client: Choose TCP/IP.
  - f. Client: When prompted set DHCP to enabled.
  - g. Client: When prompted set the domain name to vprodemo.com.
  - h. Client: Choose Provision Model.
  - i. Client: Set it to Small Business.
  - j. Client: press Esc until prompted to exit or save changes. Press Y.
3. Add Client to Manageability Commander
    - a. Console: On Console launch Manageability Commander
    - b. Console: Under Network discovery enter the start and end IP as the Client's IP and click Start
    - c. Console: Under Discovered computers the Client will appear.
    - d. Console: Select the Client and click Add computer
    - e. Console: Set username & password as P@ssw0rd.
    - f. Console: Click OK
  4. Add MPS to Manageability Commander
    - a. Console: Open Manageability Commander
    - b. Console: Right click on the Network node and Click Add MPS Server

- c. Console: Name the Server hostname as the MPS FQDN (mps.vprodemo.com)
  - d. Console: Use the defaults for the rest and press OK
  - e. Console: Right click mps.vprodemo.com and choose Add Intel AMT Computer...
  - f. Console: Fill in the FQDN of the UUT. For ENT use vprodemo\itproadmin (P@ssw0rd). For SMB use admin (P@ssw0rd).
  - g. Console: Do NOT check Use TLS security. Click OK.
5. Set flags for CILA
- a. Console: Select the Client in the tree node and click Connect
  - b. Console: Select The Management Engine tab
  - c. Console: Click the \* button next to Remote Access
  - d. Console: Enable BIOS and OS initiated connections by clicking the \* button next to them.
  - e. Console: Click OK

### Configure Environment Detection

1. Select the Client in the tree node and click Connect.
2. Select the Networking tab and click Advanced Settings.
3. Select the General Settings tab.
4. Under Environment Detection click Edit and set the following:
  - a. Environment Detection: Enabled
  - b. Circuit Breaker Policy: (None)
  - c. Local domain suffix list:
    - vprodemo.com
5. Click OK.
6. Click Close.

### Configure CIRA Policies

1. Console: Add Root Certificate by:
  - a. Console: Select The Management Engine tab
  - b. Console: Click the \* button next to Certificate & CRL store
  - c. Console: Choose the Trusted Roots tab
  - d. Console: In the dropdown list choose DC1.vprodemo.com and click Add
  - e. Console: Choose the Certificates tab and click New...
  - f. Console: Leave settings as default and click OK
  - g. Console: Click Close
2. Console: Setup Remote Access Policy by:
  - a. Console: Click the \* button next to Remote Access
  - b. Console: Enable BIOS and OS initiated connections by clicking the \* button next to them.
  - c. Console: Under Remote Access Servers click Add
  - d. Console: For Server DNS Name use the FQDN for the MPS.
  - e. Console: Set port to 2002
  - f. Console: For Server Authentication choose TLS Certificate authentication and leave the certificate on the default setting
  - g. Console: Click OK
  - h. Console: Under Remote Access Policy Click Add and set the following:

- i. Console: Trigger Type: User Initiated Tunnel
- j. Console: Tunnel Lifetime: 0 Note: 0 means don't close the tunnel
  - Console: Remote Servers: check the box for the server just created
  - Console: Click OK
- k. Console: Click Close

CIRA is now configured.

## Enterprise Mode

### Pre Configuration

1. Console: Install Manageability DTK.
2. Console: Install any required certs for mutual TLS. Note, iLab's SCS profile configure mutual TLS. A console cert can be generated as follows:
3. Console: Open Internet Explorer
4. Console: Navigate to <http://dc1.vprodemo.com/certsrv>
5. Use itproadmin and P@ssw0rd for credentials
6. Console: Click Request a Certificate
7. Console: Click Advanced Certificate Request
8. Console: Click Create and Submit a request to this CA
9. Console: For Certificate Template choose ACS
10. Console: For Name and Friendly Name enter <FQDN of Console>

### Setup a SCS profile

A CIRA profile is already configured in iLab's SCS 5 VM. Rather than giving a step-by-step this section outlines the minimum required settings in SCS. If in iLab or PTE skip this step.

1. In SCS Console
  - a. Profile -> Profile Components -> Trusted Root Certificates
    - Add the Root CA for the Enterprise.
  - b. Profile -> Profile Components -> CIRA Policies -> Management Presence Servers
    - Add all MPSs here.
  - c. Profile -> Profile Components -> CIRA Policies ->
    - Add all desired policy settings here such as a User Initiated Connection
  - d. Profile -> All Profiles -> Edit Profiles
    - Set a domain and check the box for "This is the Computer's Home Domain".
    - User Remote Access choose the desired CIRA policies for this profile.

### Provision the Client – including setting the CILA flags

This method uses an Activator script that is pre-configured on ilab's SCS5 VM. Any provisioning method is valid. Read the SCS 5 VM config document for details on configuring the activator script.

1. Console: Right Click My Computer and choose Map Network Drive

2. Console: Enter \\scs5.vprodemo.com\public for the folder. Choose x: as the drive. Click Finish
3. Console: Run x:\AMTConsole.exe
4. Console: Install with Defaults.
5. Console: Go Start -> Programs -> Intel -> Intel AMT SCS Console -> Intel AMT SCS Console
6. Console: If the Auto Login screen pops up fill in <https://scs5.vprodemo.com/amtscs> and click Login
7. Console: uncheck Display the window every time I start and then click Close
8. Console: Leave Intel AMT Setup and Configuration Console open.
9. Client: Boot to windows.
10. Client: Right Click My Computer and choose Map Network Drive
11. Client: Enter \\scs5.vprodemo.com\public for the folder. Choose x: as the drive. Click Finish
12. Client: Open the vPro IMSS (Start -> Programs -> Intel Management and Security -> Intel Management and Security status) Note this comes with the AMT (MEI & SOL) drivers.
13. Client: If the Intel Management and Security Status window does not open this is because it started in the system tray. It looks like a blue square, filled with white, with a blue key. Double click it.
14. Client: Verify that the general tab lists Intel AMT as awaiting configuration.
15. Client: run x:\provision.bat. In less than 5 minutes the batchfile will stop and Intel Management and Security Status will list AMT as Configured
16. Console: Check in AMT Setup and Configuration Console and verify that the Client is provisioned it will show up under Platforms -> All Platforms. Right-click All Platforms and choose Refresh if needed.

#### **Add Client to Manageability Commander**

1. Console: On Console launch Manageability Commander
2. Console: Under Network discovery enter the start and end IP as the Client's IP and click Start
3. Console: Under Discovered computers the Client will appear.
4. Console: Select the Client and click Add computer
5. Console: Set username & password as P@ssw0rd.
6. Console: Click ok

#### **Add MPS to Manageability Commander**

1. Console: Open Manageability Commander
2. Console: Right click on the Network node and Click Add MPS Server
3. Console: Name the Server hostname as the MPS FQDN (mps.vprodemo.com)
4. Console: Use the defaults for the rest and press OK
5. Console: Right click mps.vprodemo.com and choose Add Intel AMT Computer...
6. Console: Fill in the FQDN of the UUT. For ENT use vprodemo\itproadmin (P@ssw0rd). For SMB use admin (P@ssw0rd).
7. Console: Do NOT check Use TLS security. Click OK.

## Alert Subscription – Both SMB and Enterprise Modes

1. Console: Open Manageability Commander if needed.
2. Console: Right click the Client and choose Connect.
3. Console: Select the Client and expand tree.
  - a. Click the Event Log tree node under the Client.
4. Console: Click Event Filter.
5. Console: Choose Policy ID 1 and click Edit Filter....
6. Console: Set Event Sensor Type to Match All Event Types.
7. Console: Click OK and then Close.
8. Console: Click Alert Subscriptions.
9. Console: Set the IP Address to the IP of the Console.
10. Console: Set Event Filter to 1 - Any Entity, Any Type, Any Sensor.
11. Console: Click Add.
12. Console: Click Close.



### NOTE

*You are now subscribed to all events coming from the client, not just CILA.*

## OS Configuration

The Intel Management & Security Status Tool (IMSS) can be used for In Band CIRA initiation. However, it currently does not support CILA. As such, another tool is needed. In this case, the Manageability DTK is used.

1. Client: Install Open Manageability DTK. (only required for OS initiated connections – in band)

# Intel® Anti-Theft Technology – PC Protection (Intel® AT-p)

With Intel® Anti-Theft Technology – PC Protection (Intel® AT-p), businesses now have built-in client-side intelligence to help secure sensitive data regardless of the state of the operating system (OS) and network connectivity. This hardware-based technology provides compelling tamper-resistance and increased protection to extend your security capabilities anywhere, anytime, on or off the network, and minimize business risk.

Intel AT-p offers the option of activating hardware-based client-side intelligence to secure the PC and its data if a notebook is lost or stolen. Because the technology is built into PC hardware, it provides local, tamper-resistant defense that works even if the OS is re-imaged, a new hard-drive is installed, or the notebook is not connected to the network.

The following table provides an overview of Intel AT-p's features.

**Table 2: Intel® Anti-Theft Technology PC Protection (Intel® AT-p) Features**

Intel AT-P Feature	How it works	Benefit
<b>Detection (Triggers)</b>	<ul style="list-style-type: none"> <li>• <b>Excessive login attempts</b> - The system keeps track of an IT-determined number of login failures in a pre-boot authentication (PBA) module.</li> <li>• <b>Timeframe login requirement</b> – If the ISV agent does not log in to central server by a specific time/date (per IT policy), the Intel AT-p firmware can trigger a response.</li> <li>• <b>Notification from the central server</b> – Upon notification from the end-user (loss/theft), IT flags the notebook in a central server database (hosted in the Internet). The next time the flagged notebook connects on the internet, it synchronizes with the central server and receives the “poison pill” (PC Disable and/or Data Disable) per IT policy.</li> </ul>	<ul style="list-style-type: none"> <li>• Local detection mechanisms (login failures and timeframe login requirement) work even if no network connection is available.</li> <li>• Ability to integrate with existing encryption solutions' pre-boot authorization (PBA).</li> <li>• Flexible policy engine allows IT to determine which detection mechanism should be used and what action to take.</li> </ul>

<p><b>PC disable</b></p>	<p>Poison pill message renders the PC inoperable by blocking the OS from booting.</p>	<ul style="list-style-type: none"> <li>Minimizes the potential of a stolen notebook being used and sensitive data being accessed.</li> <li>PC Disable can be triggered locally or remotely Tamper-resistant.</li> <li>Over time, it becomes a theft deterrent.</li> </ul>
<p><b>Reactivation</b></p>	<p>Return notebook to full functionality via:</p> <ul style="list-style-type: none"> <li>Local passphrase that was set by user.</li> <li>Recovery token (one-time use) provided by IT.</li> </ul>	<p>Simple way to restore notebook to full functionality without compromising local security features for data access disable or PC disable.</p>

The Intel AT-p usage model is shown in Figure 4.

## Intel® Anti-Theft Service Usage Model

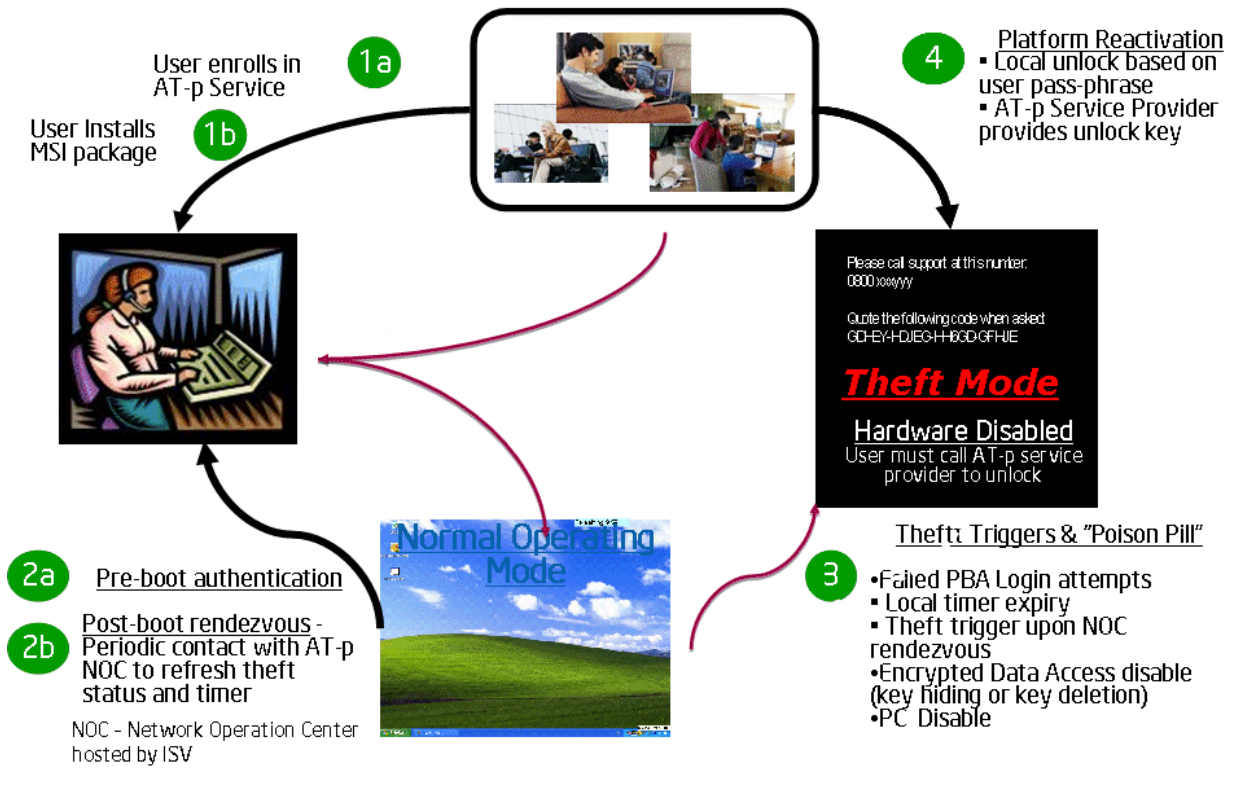


Figure 4: Intel® AT-p Usage Model

## Detection Mechanisms

Intel AT-p includes two programmable, interdependent hardware-based timers to help identify unauthorized access to the system: a disable timer and an unlock timer. Using these programmable timers, Intel AT-p can detect potential loss or theft situations, shift into “theft mode,” and then respond according to configured IT policy.

Local, hardware-based detection and trigger mechanisms include:

- **Excessive login attempts** - The system is disabled after an IT-determined number of login failures in the pre-OS screen.
- **Timeframe login requirement** - The system is disabled if the ISV agent does not log in to central server by a specific time/date.
- **Notification from the central server** - If IT flags the notebook in the central server database, the next time that notebook’s ISV agent logs into the network, the notebook synchronizes with the central server and, after receiving the server’s notification, performs IT defined policy based actions.



### NOTE

*Vendors have the option to host this service on the Internet in order to allow communication with notebooks outside the corporate firewall.*

## Poison-pill Responses

There are several poison-pill responses to theft mode. The responses are flexible, and can be programmed to do the following:

- Disable access to data, by deleting software-based encryption keys or other cryptographic credentials required to access encrypted data on the hard drive.
- Disable the PC by blocking the boot process, even if the hard drive is replaced or reformatted.
- Disable both the PC and access to the AT-p data storage area. Also, an encryption ISV can enable this action to erase encryption keys and disable the PC.

### Excessive login attempts can trigger poison pill for PC disable

Disabling a PC after excessive login attempts can be an effective way to prevent loss of encrypted data. For example, an engineer’s notebook and wallet might be stolen in an airport. The thief might try to log in using information from the engineer’s wallet but - based on IT policy - after three login attempts, the Intel Anti-Theft trigger is tripped, and the system locks down.

If an encryption ISV has provided this feature, encryption keys for encrypted data can be erased from the hard drive and the PC disabled. In this case, even if the thief removes the hard drive and installs it in another device, the security credentials that provide access to encrypted data on the hard drive have been erased and cannot be stolen. Until reactivated by the authorized user or IT, the PC will not boot and the encrypted data cannot be accessed.

## Server login timeout can trigger poison pill for PC disable

In another example, a research scientist's notebook might contain highly sensitive data about a new invention. In this case, IT has defined the triggers on the scientist's notebook to require the notebook to log in daily. During a family event, the scientist takes time off and does not log in for two days. Based on locally stored policy for the login timeframe, the notebook enters "theft mode," disables itself (and erases the encryption keys for encrypted data on the hard drive, if an encryption ISV has provided this feature). Even if the notebook is removed from the lab while the user is away, the notebook has secured itself until the scientist returns and reactivates the system.

## Reactivation and Full System Recovery

To recover when a notebook is being returned to service, Intel AT-p also includes two reactivation mechanisms:

- Local passphrase, which is a strong password preprovisioned in the notebook by the user. To reactivate the system, the user simply enters this passphrase in a special BIOS login screen.
- Recovery token, which is generated by IT or by the user's service provider via the theft management console, upon request by the user. For reactivation, a one-time recovery token is provided to the user via phone or other means, and the user enters the token in a special BIOS login screen.

Both passphrase and recovery token return the PC to full functionality. Both methods offer a simple way to recover the notebook without compromising sensitive data or the system's security features.

# Audit Log (also known as Access Monitor)

---

Audit Log, also known as Access Monitor, supports detection of security policy violations, based on the principle of accountability. The “Audit” Log tracks Intel AMT actions based on policies set by the IT Professional in the Auditor role. The Auditor is the only person allowed to access the audit log. By checking the Audit Log activity, suspicious or non-complaint activities may be detected.

Access Monitor provides oversight into Intel AMT actions to support security requirements.

By default, the Audit Log logs nothing when first enabled. The Auditor must choose what is logged and to what severity. Once this policy is set Audit Log behaves as follows:

- Events can be set to “Enabled” or “Critical”
- When the log is ~ 75% full events marked “Enabled” are no longer logged. However, the action that triggers the event still succeeds.
- When the log is 100% full events marked critical are no longer logged and are blocked from operation. For example, if SOL is being logged as critical and the log is full, AMT returns “PT\_STATUS\_AUDIT\_FAIL” the next time SOL is attempted. This will continue until the Auditor clears the log.

## Requirements

- Intel AMT version 4 or greater. Standard Manageability does not support Audit Log.
- A management console (ISV) capable of creating a user with Audit Log permission. This can be done during provisioning or afterwards.
- A management console (ISV) capable of enabling the log. This includes setting a certificate used for log signing. This can be done during provisioning or afterwards.
- A management console (ISV) capable of setting audit log policies, reading, locking, and clearing the log.

## Things to note

- The Auditor role is separate from the Administrator role. Only a user marked as an ‘Auditor’ can access the Audit log; even the Administrator cannot access it.
- To be an Auditor the user must be assigned the permission aka ‘realm’ for Audit Log.
- Only one ACL entry can be designated auditor.
- If Audit log is activated, then clients can’t be unprovisioned without authorization from the user designated as “Auditor”. The Auditor must “unlock” the audit log for unprovision to happen
- An AMT Administrator can not manage the auditor account.
- Given 3, 4, and 5, it is highly recommended to grant the Auditor permission to a Kerberos user or group rather than a single digest user. This will allow active directory to control which user’s have access to the Audit Log. If a digest user has

Auditor permission and they forget their password, there is no way to recover once the Audit Log fills or to unprovision AMT.

- At the time of this writing, no consoles are known to have plans to implement Audit Log. The Manageability DTK and the Intel AMT 5 SDK do have tools and examples for Audit Log. Also, SCS 5 is able to create an ACL entry for the Auditor user.

## More Information

For more information on Audit Log, see the Intel AMT 5 SDK (available at <http://softwarecommunity.intel.com/articles/eng/1181.htm>) under .\DOCs\Intel AMT Audit Log.pdf.

# Microsoft\* Network Access Protection (NAP)

---

Microsoft's new Network Access Protection (NAP) controls network access on a computer by computer basis, granting or denying access based on identity information on each computer and on configured corporate policies. An individual computer's identity information is referred to as its "posture" in Microsoft NAP.

NAP lets network administrators categorize groups of users and grant or deny network access based on the groups to which a user or computer belongs. They can also grant or deny access based on an individual computer's compliance level with corporate policies. NAP can even repair a given client's non-compliance and then upgrade its network access level once the repairs are complete.

For more information on Microsoft NAP, follow the link below:

<http://technet.microsoft.com/en-us/network/bb545879.aspx>

Intel AMT can be incorporated into a NAP environment. This provides two main benefits:

- When the operating system is unavailable (non H0 or S0 states), Intel AMT can authenticate to NAP, thereby gaining access to the network and enabling down the wire OOB access.
- Intel AMT posture can be sent in H0/S0 states as part of authentication, ensuring that only properly provisioned Intel AMT systems are granted access.

## Requirements

The following are required for Microsoft NAP integration:

- Intel AMT version 4.0 or greater
- Full NAP infrastructure
- Windows 2008 Server with NAP services installed and configured
- An 802.1x capable switch
- An OS Agent to perform In Band authentication – Microsoft Vista\* has one included, but it requires configuration
- A management console capable of setting NAP policies and certificates in Intel AMT
- An Intel State of Health Validator (a fully functional sample is included in the Intel AMT 5 SDK) installed on the NAP server
- An LMS-SOL driver for In Band Intel AMT authentication data

## Things to note

- For in-band NAP, the OS driver must be loaded and the trust agent running. If the driver is loaded but the NAP trust agent is not running, Intel AMT will not try to connect.
- NAP is only available in wired modes.
- If the OS is off, Intel AMT posture data returns an OS version of 0.0. In this way, conditional parameters can be defined to identify Intel AMT posture data only, if this is desired. For example:
  - If the OS is up (OS version  $<>$  0.0), use only OS posture data (i.e., is firewall on)
  - If OS is down (OS version = 0.0), use Intel AMT posture data (i.e., Intel AMT  $\geq$  version 4.0)
  - Remediate all other conditions

## More Information

See the following links for more information on Microsoft NAP integration:

- AMT 5 SDK (<http://softwarecommunity.intel.com/articles/eng/1181.htm>):  
. \DOCS\Intel AMT System Health Validator Sample.pdf
- NAP How-to: <https://dpgsites.intel.com/sites/bd-cv/Strategic%20Initiatives/AMT/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fbd%2Dcv%2FStrategic%20Initiatives%2FAMT%2FShared%20Documents%2Fhowtos&View=%7BDF776723%2D917D%2D45B0%2D9519%2DD0CD68846BAB%7D>

# Intel® Management and Security Status Tool

---

The Intel® Management and Security Status application displays information about a platform's Intel Active Management Technology (Intel AMT), Intel® Trusted Platform Module (Intel® TPM) and Intel® Anti-Theft Technology (Intel® AT) services.

The Intel Management and Security Status icon indicates whether Intel AMT, Intel TPM and Intel AT are running on the platform. The icon is located in the notification area. By default, the notification icon is displayed every time Windows\* starts.



## NOTES

*The Intel Management and Security Status icon will be loaded to the notification area only if Intel AMT, Intel TPM or Intel AT is enabled in the platform.*

*The information displayed in the Intel Management and Security Status is not shown in real time. The data is refreshed at different intervals.*

## System Requirements

To enable installation and use of the Intel Management and Security Status Application, the following are required on the platform:

- Intel AMT versions 4.x or 5.x.
- Microsoft\* Windows\* XP or Windows Vista\* 32/64
- Microsoft .NET Framework 2.0 or 3.5
- The Intel MEI driver. Instructions on installing Intel MEI can be found in the Bring Up Guide document.
- The LMS/SOL or Intel TPM drivers. The Intel Management and Security Status Application is bundled with these drivers. Installing either of these drivers also installs the application.

## Usage Overview



### NOTE

*This section only provides an overview of the tool's usage. For detailed usage instructions and advanced configuration options, see the "Intel Management and Security Status Tool User's Guide."*

Whenever either Intel AMT, Intel TPM or Intel AT is enabled, Intel Management and Security Status icon is loaded into the notification area when Windows\* starts. It can also be started using the shortcut located in **All Programs\ Intel Management and Security Status** in the Windows\* start menu.


While the Intel Management and Security Status is running, the Intel Management and Security Status icon is visible in the notification area. This icon will appear blue if any one of the aforementioned technologies is enabled on the computer. In any other case, the icon will appear gray.

#### **To view the Intel Management and Security Status Application:**

- Double-click the Intel Management and Security Status icon, or
- Right-click the icon and choose **Open**, or
- Use the shortcut located in **All Programs\ Intel Management and Security Status** in the Windows\* start menu.

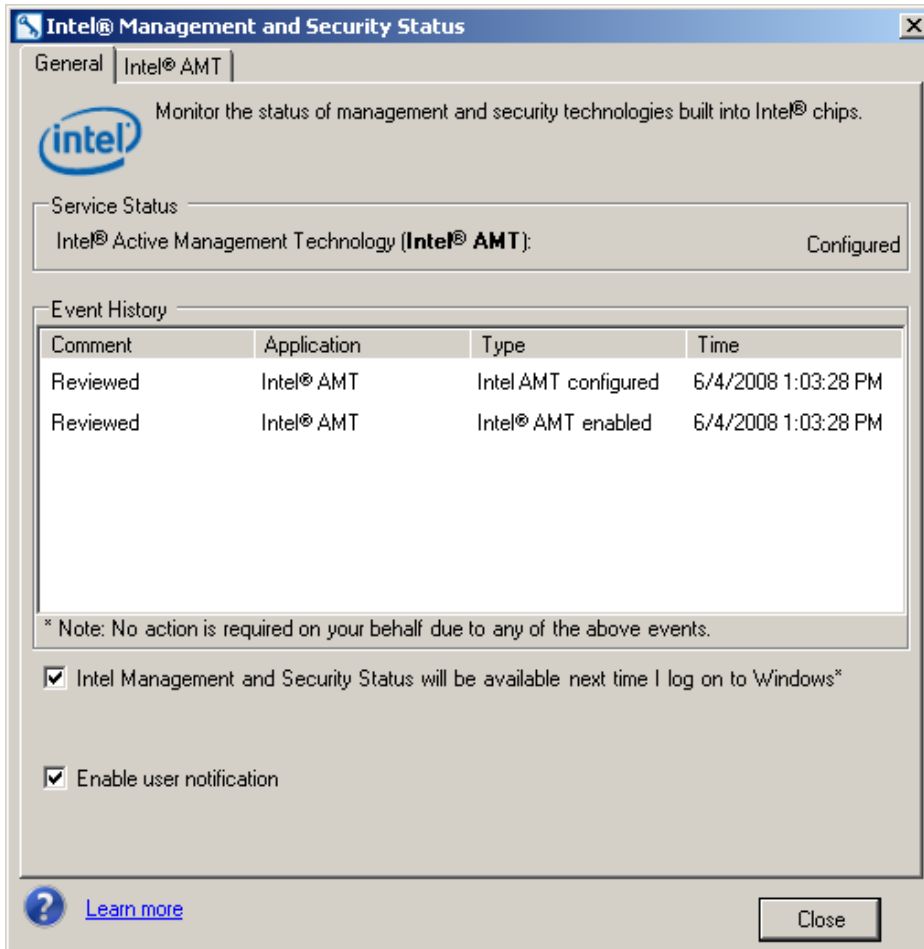
#### **To close the Intel Management and Security Status icon and application:**

Right-click the icon and choose **Exit**.

The following sections describe the information available in the application's tabs. More information about the application is available by clicking either the **Learn more** button  or link.

## General Tab

The **General** tab, shown below, provides basic information about the Intel AMT, Intel TPM and Intel AT status and events.



Events and some of their details are displayed in the Event History box. These can be sorted by clicking on the relevant column header.

The status of Intel AMT, Intel TPM and Intel AT is displayed in the Service Status group box. The status may be one of the following:

- Intel AMT: Configured / Unconfigured / Not detected / Information unavailable.
- Intel TPM: Operational / Not detected.
- Intel AT: Enabled / Disabled

**Intel Management and Security Status will be available next time I log on to Windows:** Checking this box causes the Intel Management and Security Status Application to be invoked, and the icon to be displayed, whenever you log on to Windows.



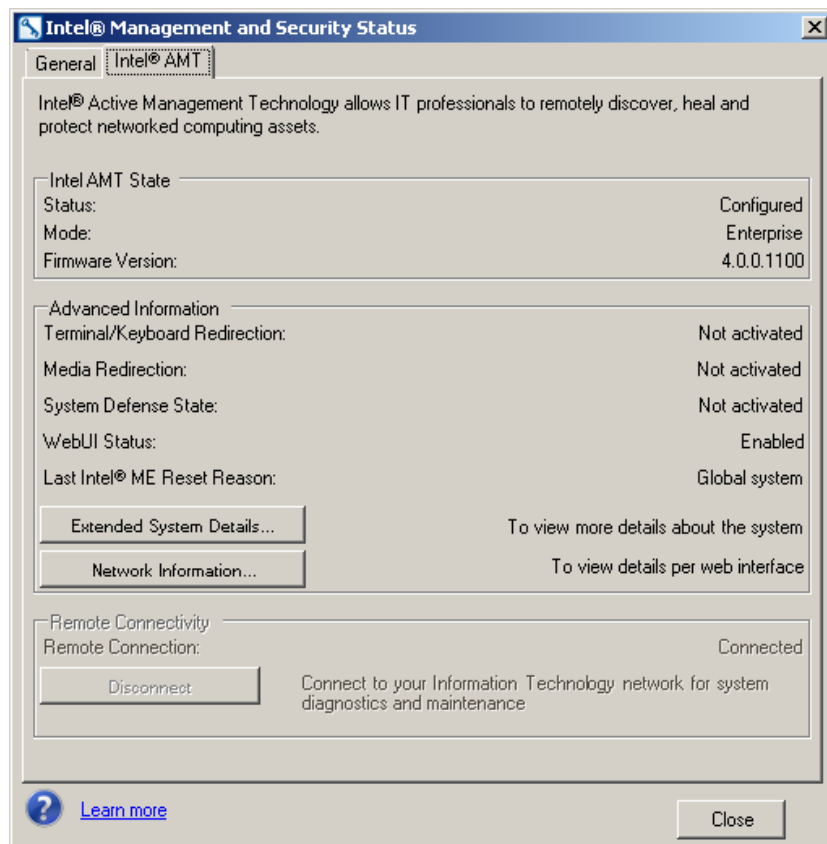
**NOTE**

*The application never loads automatically with Windows\* log on if all the technologies it displays (Intel AMT, Intel TPM or Intel AT) are disabled in the system.*

**Enable user notification:** Allow the Intel Management and Security Status icon to display notifications in the notification area when one of the technologies is enabled or disabled.

## Intel® AMT Tab

Click the **Intel® AMT tab**, shown below, to display Intel AMT information.



## Intel AMT State

The following information is provided:

- **Status**

The operational status of Intel AMT.

Possible values: Configured / Unconfigured / Not detected / Information unavailable.

- **Mode**

The operational mode of Intel AMT.

Possible values: Enterprise / Small business / Awaiting configuration / Disabled / Not detected.

- **Firmware Version**

The Intel AMT firmware version.

## Advanced Information

The following information is provided:

- **Terminal/Keyboard Redirection**

Indicates whether there are any open terminal/keyboard redirection sessions.

Possible values: SOL activated / Not activated.

- **Media Redirection**

Indicates whether there are any open IDE redirection sessions.

Possible values: IDER activated / Not activated.

- **System Defense State**

Indicates whether System Defense is currently active.

Possible values: Activated / Not activated.

- **WebUI Status**

Indicates whether a remote user can view or change Intel® AMT information via the Web UI.

Possible values: Enabled on TLS / Enabled / Disabled.

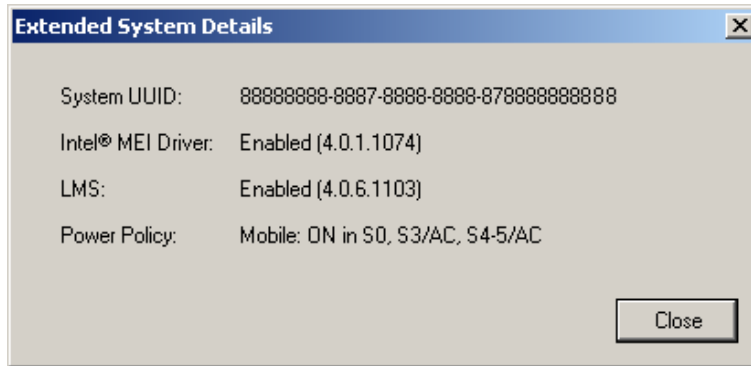
- **Last Intel® ME Reset Reason**

Displays the reason that the Intel AMT was last reset.

Possible values: Global System / FW reset / Power Up / Unknown cause / Information unavailable

- **Extended System Details button**

Click the Extended System Details button to show additional Intel AMT information:



- **System UUID**

The current System Unique Universal Identification. Standard System UUID presentation, such as, 03000200-0400-05AA-0006-000700080009

- **Intel MEI Driver**

The version of the Intel Manageability Engine Interface driver.

States are: Enabled(x.x.x.x) / Disabled(x.x.x.x) / Uninstalled

- **LMS Driver**

The version of the LMS service.

States are: Enabled(x.x.x.x) / Disabled(x.x.x.x) / Uninstalled

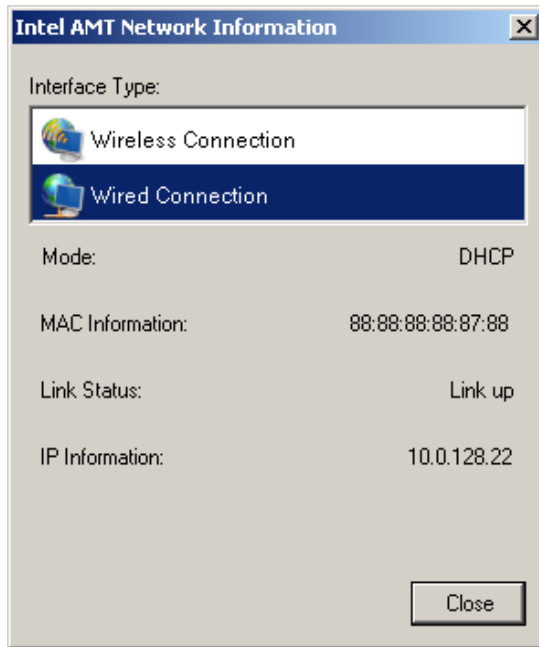
- **Power Policy**

The power policy which is currently in effect.

States are: ON in S0, or any other power policy supported by the system.

Click **Close** to return to the Intel AMT tab.

Click the **Network Information** button to display network details regarding Intel AMT wireless and wired connectivity, as shown below.



Under **Interface Type**, click either **Wireless Connection** or **Wired Connection** to display information on the following items for the selected interface (only wired information is available in Intel AMT 5.0):

- **Mode**  
Possible values: Static / DHCP
- **MAC Information**  
XX:XX:XX:XX:XX:XX – e.g. 88:88:88:0A:88:87
- **Link Status**  
Whether the link is currently active.  
Possible values: Link down / Link up
- **IP Information**  
X.X.X.X – e.g. 10.102.0.1
- **Configured for Wireless**  
Possible values: Wireless disabled / Wireless enabled

## Remote Connectivity / Request Assistance

The Remote Connectivity section provides CIRA (Client Initiated Remote Access) capabilities, which allow a user to connect the Intel AMT system to the company's Information Technology network from an external internet connection.

Click the **Connect / Request Support** button to connect to your Information Technology network for system diagnostics and maintenance. The current connection status is displayed in the Remote Connectivity section.

Starting from Intel AMT 5.1, CILA (Client Initiated Local Access) feature was added to this section. This feature allows a user connected to the internal corporate network to send a support request to the IT administrator.



**NOTE**

*The information displayed in the Intel® Management and Security Status, including in the remote connectivity section, is not shown in real time. The data is refreshed every 10 seconds.*

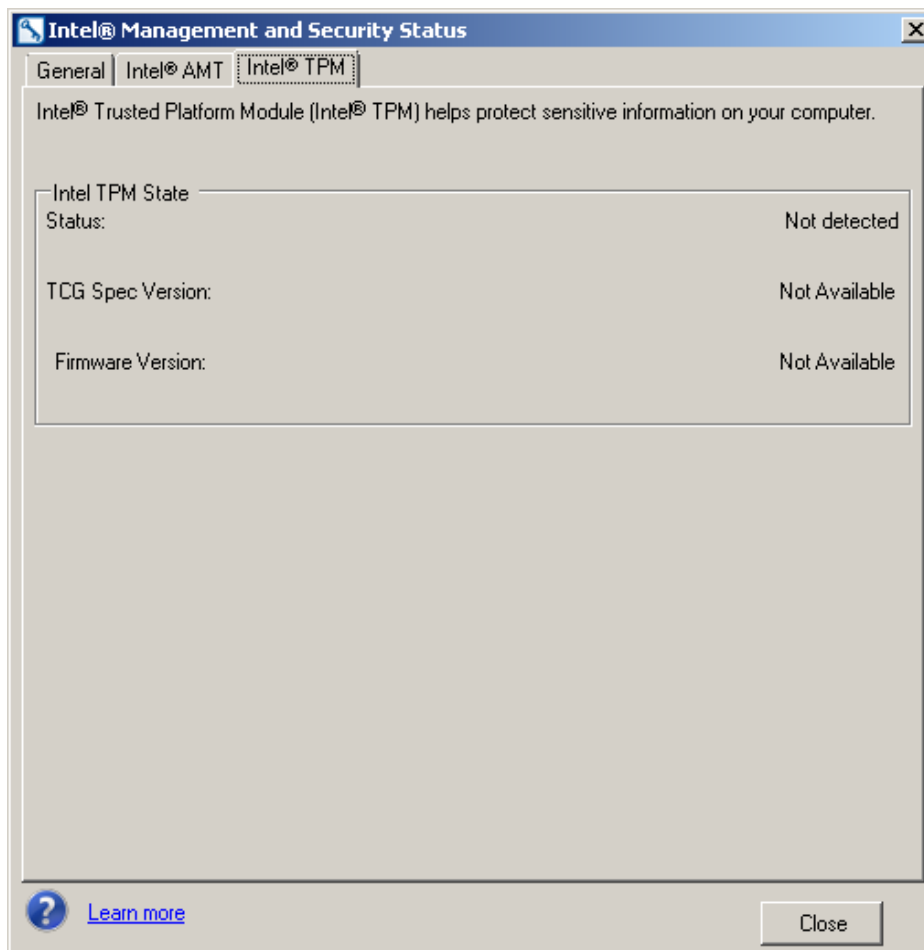
## Intel® TPM Tab



**NOTE**

*The Intel® TPM tab is visible only if Intel TPM is supported by the platform.*

Click the **Intel® TPM** tab to view Intel TPM information, as shown below.



In the Intel TPM State section, the following information is displayed:

- **Status** – The operational status of the Intel® TPM, comprising up to 3 parameters.  
The displayed status is one of the following combinations:
  - Operational - Active ; Owned ; Enabled
  - Operational - Active ; Unowned ; Enabled
  - Operational - Active ; Owned ; Disabled
  - Operational - Active ; Unowned ; Disabled
  - Operational - Inactive ; Owned ; Enabled
  - Operational - Inactive ; Unowned ; Enabled
  - Operational - Inactive ; Owned ; Disabled
  - Operational - Inactive ; Unowned ; Disabled
  - Failed - Flash corrupted
  - Failed - HW failure
  - Failed - ME reset
  - Failed - Unknown
  - Not detected
- **TCG Spec Version**  
The Trusted Computing Group version with which this Intel® TPM is compliant.
- **Firmware Version**  
The firmware version of the Intel TPM.

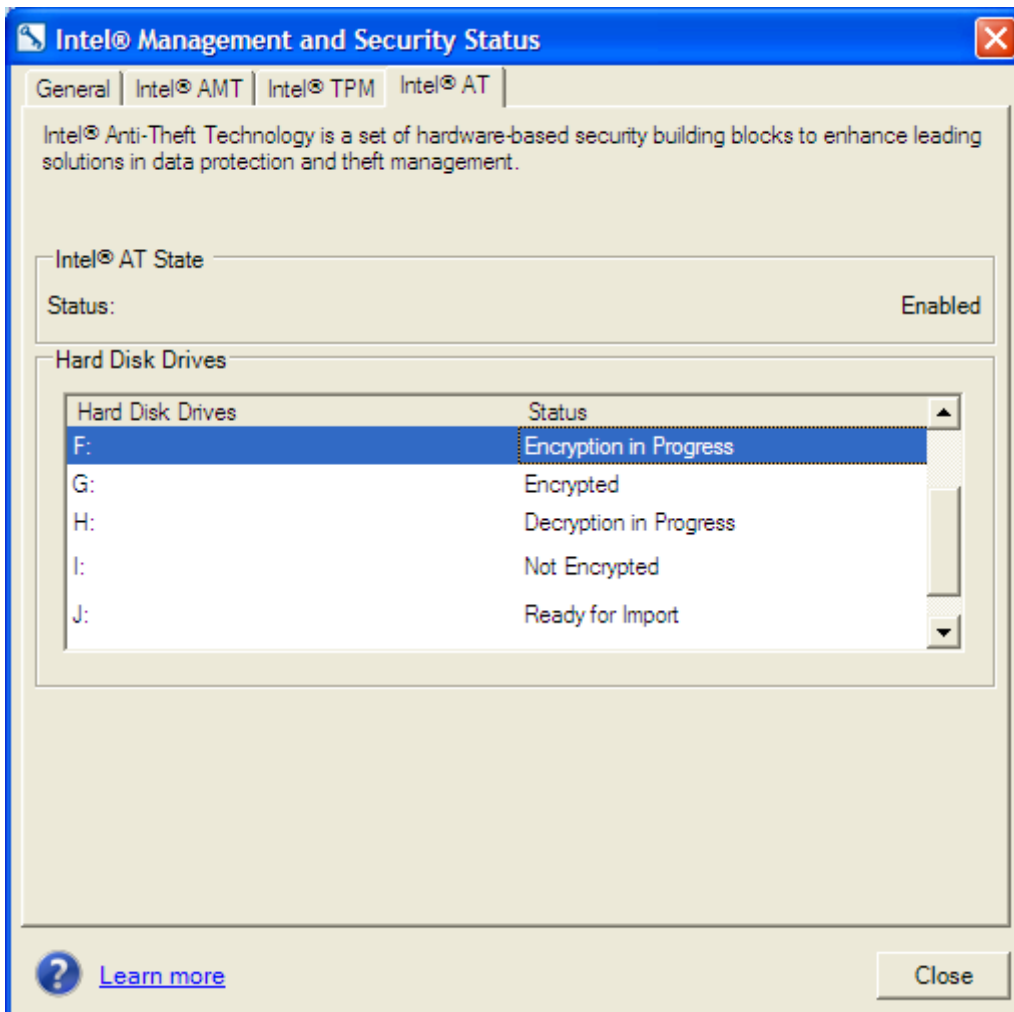
## Intel® AT tab



### NOTE

The Intel® AT tab is visible only if Intel AT is supported by the platform.

Click the **Intel® AT tab**, shown below, to view Intel Anti-Theft Technology information.



In the Intel AT State section, the following information is displayed:

- **Status**  
The operational status of Intel AT.  
Possible values: Enabled / Disabled.
- **Hard Disk Drives Status**  
The status of each Hard Disk, according to the encrypted mode of each.

Possible values: Not Encrypted / Encryption in Progress / Migration in Progress / Ready for Import / Encrypted.

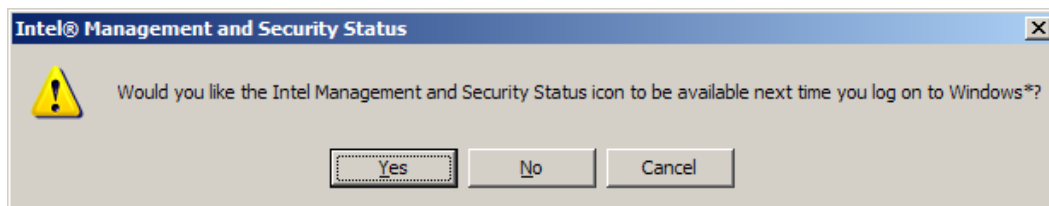
**NOTE**

*The status of the Hard Disks on the Intel AT tab is disabled (and empty) while Intel AT is not enabled in the BIOS.*

## Exiting the Application

To exit the application, right click on the Intel Management and Security Status application icon in the notification area and select **Exit**.

The following window is displayed.



Click **Yes** to automatically start the Intel Management and Security Status application the next time you log on.

**NOTE**

*The application never loads with Windows log on if all the technologies it displays (Intel AMT, Intel TPM or Intel AT) are disabled in the system.*

# Setup and Configuration Server version 5 (SCS 5)

---

## Overview

Release 5.0 of the Intel® AMT Setup and Configuration Server and Console (Intel® AMT SCS) includes a number of new features and resolves several problems.

## New Features Since Beta Release

The following features were added to SCS 5.0 since the Beta Release.

- Support for creation of the SCS database independent of the SCS service installation—This feature gives the DBA more control of access to the database.
- The SCS service can now connect to the database using Windows authentication. The SCS can now conform to a “Windows authentication only” SQL server policy.

### NOTE

*See Changes in the SCS Installation Flow for documentation of the above two features.*

- Context-sensitive help—The SCS console has help information associated with each screen. Simply press the F1 function key or click the ? at the top of the screen to see an explanation of the current display.

## New Features in SCS 5.0

This section provides basic information about all of the other new features of SCS 5.0.

### NAP support

The SCS supports NAP configuration. It is possible to configure NAC, NAP or NAC-NAP hybrid.

### Usability improvements

- New and improved SCS console.
- AD integration can be done without a schema extension.
- The SCS attempts to connect with an Intel AMT device using both the FQDN in addition to the IP (from the hello packet). Configuration succeeds even if the Intel AMT IP address has changed.
- Support for changing the Intel AMT hostname, and for changing the Intel AMT platform of a user PC.
- Multiple RCFG certificate support.

The LoadCert tool is no longer required to identify remote configuration certificates. The service now uses an algorithm for iterating through the RCFG configuration certificates that are installed in the local SCS user certificate store.

- Intel AMT configuration can be triggered by a host agent such as the Activator (formerly known as the RCT).
- Support for automatic configuring and extracting PID from hello packet.
- Installer improvements.
  - Modify and Repair options were added to the installer.
  - Additional flow changes were inserted in order to improve usability.
  - The installer will install IIS if there is no instance on the system.
- The AMTList APIs were extended to include Intel AMT configuration parameters.
- The Activator was improved to send a hello packet and to use extended SetAMTIdentity function.
- SCS verifies that the certificate templates match their intended usage.
- Upon installation, the SCS creates a default profile.

## Support for change hostname/UUID

The API “UpdateAMTProperties” that was created for Release 3.3 was expanded to support the option of updating the FQDN or the UUID of an existing AMT record.

## Support for automatic configuring and extracting PID from hello packet

The ability to perform automatic configuring was added (i.e. SCS does not wait for a hello packet). This can either be triggered by the user via an extension to the SetAMTIdentity API that enables the user to provide all of the data needed for configuration, or triggered by the service when it attempts to extract the needed connection parameters while establishing a TLS connection.

## Extended AMTList APIs to support recovering configuration parameters

An option was added to page through the merged list of AMTs and AMTConfigurationParameters.

## Attempt connection with AMT using FQDN

The SCS attempts to connect with an Intel AMT device using both the FQDN (from the AMTConfiguration parameters) in addition to the IP (from the hello packet).

## Support for Active Directory forest configurations

SCS 5 was tested in various Active Directory forest configurations.

## New SCS console

The SCS console has been completely redesigned and re-implemented. The new console features include:

- Enhanced look and feel: icons, colors, shapes, menu bar, tool bar, and visual effects
- Usability improvements
  - User-defined collection for Intel AMT platforms and the log tables
  - One click operation on a collections of systems
  - Auto login, graphic notification for data validation, dependencies, and auto refresh
- New tools
  - CIRA support
  - USB key creation wizard
  - New profile wizard
  - A single table for showing Intel AMT configuration and Intel AMT platform tables and their connectivity status
  - Intuitive operations – when a user updates an Intel AMT device setting, the console automatically applies the change to the device and displays the success status of the operation.
  - Getting Started page
  - Automatic discovery of SCS service
  - Find Intel AMT platform
  - Platform history and zoom in to log entries
  - Automatic alert for SCS service down
  - SCS services status table

## WSDL improvements

In order to enable future functionality improvements without compromising backward compatibility, several changes were made to the SCS 5.0 WSDLs:

1. All new enumeration definitions are defined as integer enumerations and not string enumerations.
2. The WSDL definitions of the integer enumerations include reserved values for future use.
3. Selected string enumerations were redefined in the WSDLs as strings. This enables the option of adding additional strings in the future without creating backward compatibility problems. The lists of valid string values appear in the WSDLs as “enumeration value” nodes, but they are commented out. The WSDL string enumeration definitions that were changed are: UserAcIRealmType, PowerStateType, EnabledInterfacesType, AMTStatusType, RealmType and ProtocolType.
4. Many of the Complex Data Type definitions as well as some of the function output structures were expanded and now include (in the WSDLs) a wildcard element:  

```
<xsd:any namespace='##other' processContents='lax' minOccurs='0' maxOccurs='unbounded' />
```

This element allows for extending the data structures without breaking backward compatibility.

These WSDL modifications do not break backward compatibility; therefore, an old SOAP API client should work with the new SCS. Updating the WSDLs in your SOAP API client project may require several code changes (depending on the WSDL compiler in use):

- As a consequence of item 3, the valid string values that were previously defined in the files generated by a WSDL compiler may need to be inserted manually.
- As a consequence of item 4, function prototypes and/or type definitions may be modified to include a new parameter for holding the wildcard data returned in responses. This parameter should be added to the relevant places in the code, but its value should be ignored. When used in requests, wildcards in these types may have to be initialized to NULL.

## Other features added in the Beta release

- The capability was added to perform wireless configuration over WS-MAN.
- A number of improvements were made to the Console GUI.
- The installer now registers the SCS in Active Directory.
- The distribution includes a sample script for creating a certificate template that can be used for both 8021x and TLS.
- The distribution includes new documents for Activator and for troubleshooting.
- The SCS no longer supports the option of using wildcards when sorting/filtering by UUID.

# Intel® Trusted Platform Module

---

The Intel® Trusted Platform module (Intel® TPM) 1.2 component is specifically designed to enhance platform security above-and-beyond the capabilities of today's software by providing a protected space for key operations and other security critical tasks. Using both hardware and software, the Intel TPM protects encryption and signature keys at their most vulnerable stages—operations when the keys are being used unencrypted in plain-text form. The Intel TPM is specifically designed to shield unencrypted keys and platform authentication information from software-based attacks.

The firmware for the Intel TPM is part of the Intel ME firmware. This allows OEMs, should they choose, to save costs by using the Intel TPM rather than adding a discrete TPM.



## NOTE

*While using Intel TPM is optional, all Intel vPro systems must have a TPM.*

## Requirements

The Intel TPM requires one of the following Intel chipsets:

- Mobile Intel® GL40/GM45/GS45 Express Chiptset
- ICH10DO

## Things to note

If Intel AMT is unprovisioned remotely, the Intel TPM is unavailable until the system is rebooted.

The Intel TPM gets cleared if the CMOS battery is removed/changed when using Intel TPM. In that case, the Intel TPM needs to be provisioned and configured again. See the following section for instructions on recovering Bit Locker from a TPM reset.

## Provisioning the Intel TPM

TPM provisioning should not usually be required, since it is expected that TPM is provisioned in the factory. Also, TPM provisioning is only required if TXT is turned on in the BIOS. Hint: don't turn it on if it will not be used. These steps are only needed if TPM is not provisioned for some reason. This could happen if the OEMs forget to provision, if the system is preproduction, or if the TPM gets cleared (for instance the CMOS battery is flipped when using iTPM) for any reason.

To provision the TPM for TXT:

- Obtain the TPM BDK v 1.11 or greater (BIOS Developer's Kit) from IBL:
- <http://cdiapp.sym.cps.intel.com/edesign-search/SearchResults.aspx?docIds=377155>
- Extract the ebin folder to a DOS bootable thumb
- Set all required BIOS settings except leave TXT disabled – Note the names and locations of these setting vary by OEM & BIOS vendor.
- 3.5 Ensure TPM ownership has NOT been established.
- Boot the DOS thumb
- from ebin run the following:
  - def\_aux.bat
  - def\_pd.bat
  - any\_pd\_d.bat
  - rp4\_7\_5.bat LOCK
- Turn on TXT in the BIOS

TPM is now provisioned.

## Take TPM ownership

When provisioning TPM, we have to ensure that TPM ownership is not taken. To do that, Microsoft Vista provides a utility called tpm.msc which gives the status of TPM ownership. In Windows XP, no such utility exists. To check TPM ownership on Windows XP, we need to get a third party tool that can provide this data. Depending on whether it is iTPM or eTPM the tools may differ.

For Windows Vista do the following:

- Right Click the desktop and choose new -> shortcut
- Enter tpm.msc and click next.
- Name the shortcut TPM and click finish.
- Double Click the TPM icon
- Click Initialize TPM
- Manually create the password as P@ssw0rd and click Initialize
- Close TPM app.

## To Verify

1. Go Start -> Programs -> Intel Management & Security -> Privacy Client
2. Verify under the Intel TPM tab that the status is Operational - Active; Owned; Enabled

## Recover from a changed or missing TPM token

If TPM is used for BitLocker authentication there are a few circumstances where the token may no longer match. For instance, if the BIOS settings are adjusted, if the CMOS is cleared, if the coin battery is removed, or if the TPM is reset. Note that with the iTPM a coin battery flip may cause TPM to reset. To recover the TPM token:

1. Preparation before recover
  - a. Reconfigure BIOS to desired settings if needed.
  - b. Find the USB recovery key or recovery password for the platform. Note, it is possible to store this in Active Directory. The Active Directory method is not covered by this how-to.
2. Boot the CLIENT – System should halt, looking for the BitLocker Encryption Key
  - a. Insert the USB flash drive with the BitLocker Encryption Key on it. (should be on the root) note: remember the key is unique to the system.  
Press the ESC button to reboot the system  
OR
  - b. Press enter for recovery and supply the recovery password. (System will then boot to OS)
3. Take Ownership of TPM (initialize) – only required after a TPM reset
  - a. Log onto system with administrative rights
  - b. Click start > Run
  - c. Type “TPM.msc” and hit enter (Trusted Platform module Management Window should open)
  - d. Click Initialize TPM (upper right, under TPM Management on local computer)
  - e. Click on your preferred method to create the TPM owner password
    - i. Manually create the Password
      1. Input the desired password and then confirm it
      2. Click Initialize
      3. Click close when Initialization is complete
      4. Close the TPM Management ConsoleOR
    - ii. Automatically create the password
      1. Follow the steps
      2. Close the TPM Management Console
4. Re-associate BitLocker and TPM
  - a. Open Control Panel
  - b. Double click the BitLocker Drive Encryption icon.

- c. Click "Turn off BitLocker"
- d. Select / click "Disable BitLocker Drive Encryption". Wait for BitLocker to be disabled
- e. Select "Turn on BitLocker"
- f. Close the BitLocker Drive Encryption window
5. Verify Re-association of BitLocker and TPM
  - a. Remove the Thumb drive
  - b. Restart the system – system should boot to windows without requiring the Thumb drive.

## WS-MAN and DASH 1.0 Compliance

---

Intel AMT 5.0 is compliant with the WS-MAN standard and the DASH 1.0 standard. Please refer to the following website for more information on WS-MAN and DASH.

<http://www.dmtf.org/home>