TECHNOLOGY BRIEF
2nd generation Intel® Core™ processor family
Intel® Anti-Theft Technology

Protect Laptops and Data with Intel® Anti-Theft Technology

It's not your PC. It's your business. Lock it tight. Intel® Anti-Theft Technology can now lock, unlock, and locate remotely—even when the operating system is not running.

Laptops with the 2nd generation Intel® Core™ processor with Intel® Anti-Theft Technology[1] (Intel® AT) provide IT administrators with intelligent protection of lost or stolen assets. Businesses can now prove compliance even after a laptop goes missing, and can minimize legal or financial exposure, as well as the risk of a data breach.

Intel AT's flexible policy engine lets you specify the detection mechanism that asserts theft mode, the thresholds for timer intervals, and the action(s) to take. Because the technology is built into laptop hardware, Intel AT provides local, tamper-resistant, policy-based protection that works even if the OS is reimaged, the boot order is changed, a new hard drive is installed, or the laptop is disconnected from the network. When the laptop is recovered, you can reactivate it quickly and easily using your choice of methods: passwords created on provisioning, one-time codes generated by IT, or a remote reactivation message (via SMS).

Intel AT is activated through service subscriptions from Intel AT-enabled software and service providers. Find a list of service providers and Intel-AT capable laptops at **anti-theft.intel.com**.

Local and remote detection mechanisms

Intel AT includes several hardware-based detection mechanisms that can trigger a lock down. Detection mechanisms can be local (based on IT policy) or remote (via LAN, WLAN, or 3G connectivity).[2] Hardware-based detection and trigger mechanisms (all configurable by flexible IT policies) include:

- **Excessive login attempts in the pre-boot authentication (PBA) screen.** The PC can automatically trigger a lock down and prevent access to data if someone tries to log in too many times unsuccessfully.
- **Missed check-ins with the central server.** If multiple check-ins are missed, a local hardware-based timer expires, and the laptop immediately goes into theft mode, even if the system is not connected to the Internet.
- **Notification via a message sent over an IP-based wired or wireless LAN.** The next time the laptop connects to the central server, it can receive an encrypted message (the poison pill) to go into theft mode. (Note: the central server can be hosted on the Internet to allow communication with laptops outside the corporate firewall.)
- **Notification via an encrypted SMS text message over a 3G network.** For this option, the laptop does not need to be connected to the Internet, but it must be within range of a 3G network. This feature works even if the OS is not running or has been re-installed, thanks to a hardware-to-hardware link between the 3G card and the Intel AT system.[2]
- **Resume from standby.** IT administrators can now tighten the security of a laptop upon resume from standby (S3 sleep) state: If the Windows* login is not completed in a short period of time (as defined by IT), the user must re-enter the encryption login credentials before being allowed access to the PC. This feature closes a traditional vulnerability in data protection of PCs and is available on PCs with the 2nd generation Intel® Core™ i5 vPro™ and Core™ i7 vPro™ processors.

Flexible IT-specified responses

Intel AT provides flexible options for automated loss/theft responses. Depending on the mechanism, the response can be activated locally and automatically, or remotely by IT.

- **Disable access to encrypted data.** Delete essential elements of cryptographic materials that are required to access encrypted data on the hard drive.[3]

- **Disable the laptop (poison pill).** Block the boot process through the laptop's hardware. This response works even if the boot order is changed, the hard drive is replaced or reformatted, or other boot devices (for example, a secondary hard drive, removable drive, CD, DVD, or USB key) are tried.
- **Location beaconing over a 3Gnetwork.** This is possible after the PC has been disabled, thanks to a direct hardware link between the 3G module and Intel AT (no OS dependency.)
- **Customizable "lost-and-found" message.** This message is displayed after the laptop enters theft mode. For example, a lost-and-found message could say, "This laptop has been reported missing. Please call 1-555.666.777 to return the system."

IT can combine responses to provide different levels of lock down for different users.

Easy and rapid reactivation, and full system recovery

Intel AT includes several mechanisms for easy, rapid reactivation of a recovered laptop, including integration with existing software vendors' pre-boot login modules.

- **Local passphrase** entered by the user or by IT in a special pre-OS reactivation screen (via BIOS or a PBA module).
- **One-time reactivation code** generated by IT or by the user's service provider, and entered in a special pre-OS reactivation screen or PBA.
- **3G encrypted SMS message** sent from IT to the laptop makes it easy to reactivate the laptop; the user does not have to enter anything once confirmed as the rightful owner.

Whichever method is chosen, reactivation returns the laptop to full functionality in a simple and quick manner, without compromising sensitive data or the system's security features.

New Intel AT features take advantage of 3G networks

With Intel® Anti-Theft Technology (Intel® AT), IT administrators can now use encrypted SMS messages over a 3G network to send a poison pill, remotely unlock a recovered laptop quickly, or direct the system to send location information (GPS coordinates) back to the central server:

- **Poison pill delivery via an encrypted SMS message over a 3G network.** 3G connections can occur regardless of the state of the OS, via a direct hardware link between Intel AT and the 3G module.
- **Remote unlock via an encrypted SMS message over a 3G network.** This lets IT reactivate the laptop within minutes of recovering the PC.
- **Location beaconing.** Intel AT can now transmit latitude and longitude (using GPS coordinates) to the central server if the system is equipped with a supported 3G module.[2] IT administrators can specify automated beaconing at regular intervals or location information on request when the laptop is marked as lost or stolen.

To take advantage of 3G-based communication, the laptop does not need to be connected to the Internet, but it must be within range of a 3G network.[2]

Intel® Anti-Theft Technology: Intelligent protection and simple, rapid reactivation

Intel AT delivers built-in client-side intelligence to help businesses secure sensitive data regardless of the state of the OS, hard drive, boot order, or 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 your business risk.

Get powerful, built-in theft protection with Intel® Anti-Theft Technology.
Learn more at: **anti-theft.intel.com**

[1] No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT) requires the computer system to have an Intel® AT-enabled chipset, BIOS, firmware release, software and an Intel AT-capable service provider/ISV application and service subscription. The detection (triggers), response (actions), and recovery mechanisms work only after the Intel® AT functionality has been activated and configured. Certain functionality may not be offered by some ISVs or service providers and may not be available in all countries. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof.

[2] This feature requires a laptop with Intel® Anti-Theft Technology (Intel® AT) 3.0, a 3G laptop modem that supports Intel AT 3.0 functionality (for example, the Ericsson F5521gw), and OEM-enabled communication between the 3G modem and laptop.

[3] Essential cryptographic material includes anything that is essential to access the encrypted drive, including part of the encryption key, user credentials, biometric information, or other cryptographic material.

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.

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 go to: **http://www.intel.com/design/literature.htm**

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

0211/JKO/MESH/PDF 325058-001US