Protect Laptops and Data with Intel® Anti-Theft Technology

It's not your laptop. It's your business. Lock it tight.

TECHNOLOGY BRIEF FOR IT PROFESSIONALS
3rd generation Intel® Core™ processor family
Intel® Anti-Theft Technology

Intel® Anti-Theft Technology can now lock and unlock your lost or stolen laptops.

Laptops with the 3rd generation Intel® Core™ processor family with Intel® Anti-Theft Technology (Intel® AT) provide intelligent protection of lost or stolen assets. Businesses can now prove security and privacy regulatory 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 activates 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: password created on provisioning or one-time code generated by IT.

Intel AT is activated through service subscription from Intel AT-enabled software and service providers. Intel AT is available on most laptops with 3rd gen Intel® Core™ processor, 2nd gen and 3rd gen Intel® Core™ i5 vPro™ and Core™ i7 vPro™ processors, and select previous-generation processors. You can find a list of service providers and Intel AT capable laptops at antitheft.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, over a wired or wireless LAN connection. Hardware-based detection and trigger mechanisms, all configurable by flexible IT policies, include:

- **Excessive login attempts or time spent in the pre-boot authentication (PBA) screen**. The laptop can automatically trigger a lock down and prevent access to data if someone tries to log in too many times unsuccessfully or takes too long to log in. The PBA timer provides an additional level of security to prevent automated attacks.
- **Missed check-ins with the central server**. If check-in with the central server is 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 through 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.)
- **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 laptop. This feature eliminates a traditional vulnerability in data protection of laptops and is available on laptops with the 2nd gen and 3rd gen Intel Core i5 vPro and Core i7 vPro processors.

Flexible IT-specified responses

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

- **Disable the laptop**. 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, such as a secondary hard drive, removable drive, CD, DVD, or USB key, are tried.
- **Disable access to encrypted data**. Delete essential elements of cryptographic materials that are required to access encrypted data on the hard drive.[1]
- **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 lockdown 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, through 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.

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.

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 to minimize your business risk.

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

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

 0612/JKO/MESH/PDF 325058-001US