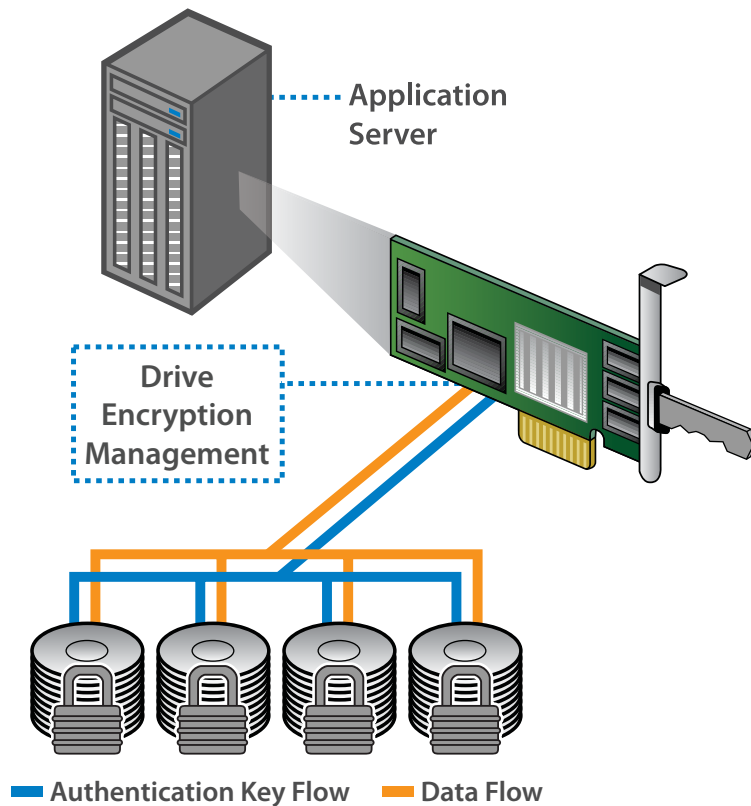


Intel® RAID: Drive Encryption Management

Significantly reduce risk of data being compromised when drives leave the server



Intel® Drive Encryption Management enables SEDs to encrypt data on drives.

KEY BENEFITS:

- Locks drives and secures data the moment a drive is removed from a system.
- Helps secure a drive's data from unauthorized access or modification.
- Instantly and securely renders data on SED drives unreadable.
- Significantly reduces cost and time of re-purposing and retiring drives.

A company's data may be its most valuable asset, and if misplaced or stolen, organizations run the risk of lost revenue, legal and compliance implications, and a tarnished reputation. And since data spends most of its life at rest on drives within the data center, as these drives leave for repair, retirement, relocation or maintenance, data is vulnerable to being lost or stolen.

The emergence of self-encrypting drives (SEDs) mitigates the security vulnerabilities of data-at-rest. Intel Drive Encryption Management, an Intel Premium feature,

when paired up with SEDs, provides you with the data encryption and services you need for hard disk drives. Self encrypting drives help protect your data, reduce your costs, and minimize the impact and liability of theft. And this is all done behind the scenes with transparency to your end users.

Simple, Secure and Cost-Effective Self-Encrypting Drive Management

While the encryption capabilities of the drives are the primary level of security, management of the self-encrypting drives is critical to its execution. In fact, the security capabilities offered with drive-level encryption are only as good as the management tool used to implement and manage them.

Intel Drive Encryption Management, offered with select models of Intel's SAS 2.0 family of RAID products, maintains, and controls the key linkage and communications with the self-encrypting drives, secures user-selected volume groups, and authorizes the drives to encrypt and decrypt data with pass phrase and security key management.

Auto Lock

Auto Lock with Local Key Management locks the SED using an authentication key. When secured in this manner, the drive's data encryption key is locked whenever the drive is powered down. In other words, the moment the SED is switched off or unplugged, it automatically locks down the drive's data.

When the drive is powered back on, it requires authentication before being able to unlock its encryption key and read any data on the drive. This protects against any type of insider or external theft of drives or systems.

Instant Secure Erase

Instant Secure Erase provides instant data protection via cryptographic erase. Whether the drive is 73GB or 1TB, this feature will delete the existing data encryption key and regenerate a new data encryption key in seconds, enabling drives to be returned, retired, sold or reused securely. If you decide to use Instant Secure Erase only (without Auto Lock), you will not be required to maintain authentication keys or passwords in order to access the drive's data. The SED will automatically encrypt the data being written to the drive and decrypt data being read from it. When it is time to repurpose or retire the drive, the owner simply sends a command to the drive to perform the cryptographic erase. This command replaces the encryption key inside the encrypted drive, making it impossible to ever decrypt the data. Using Instant Secure Erase, businesses can save time and money by simplifying decommissioning of drives and preserving hardware value for returns and repurposing.

Ordering Information:

Physical Key Order Code	AXXRPFKDE
Supported RAID Controllers and Modules	<ul style="list-style-type: none">▪ Intel RAID Controller RS2BL040▪ Intel RAID Controller RS2BL080▪ Intel RAID Controller RS2PI008 (August '10)▪ Intel RAID Controller RS2MB044▪ Intel RAID Controller RS2WG160 (August '10)▪ Intel RAID Controller RS2SG244 (August '10)
Supported Self-Encrypting Drives	See http://support.intel.com for a list of Self-Encrypting Drives tested with Intel RAID controllers.



Unlock advance features by adding upgrade keys to Intel® RAID Controllers.

For more information on the Intel® RAID Premium Features, visit:

www.intel.com/go/RAID

Locate how to make Intel® RAID part of your server environment. Contact an Intel® Channel Partner Program participant.



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.

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

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

Copyright © 2010 Intel Corporation. All rights reserved.

Printed in USA

0510/SJ/ExactMarket/PDF

♻️ Please Recycle

323917-001US

