READ ME FIRST

HITACHI
Inspire the Next

REQUIREMENTS BEFORE USING SELF-ENCRYPTING DRIVES

Before you use self-encrypting drives (SEDs) with your Hitachi AMS storage system, refer to the usage guidelines and instructions in Chapter 12, "Data at Rest Encryption," in the *Hitachi Storage Navigator Modular 2 Storage Features Reference Guide for AMS* (MK-97DF8148-13). You can find this document on the documentation CD *CD-00HL220-00, Hitachi AMS 2000 Product Documentation Library CD*.

The Data at Rest encryption license key that corresponds to the serial number of your AMS storage system can be found on the Hitachi Data Systems AMS 2000 License Keys CD. You will need to install this key to enable your SED(s). For usage guidelines and instructions, refer to Chapter 12, "Data at Rest Encryption," in the *Hitachi Storage Navigator Modular 2 Storage Features Reference Guide for AMS* (MK-97DF8148-13).

Before you use self-encrypting drives (SEDs) with your AMS storage system, HDS strongly recommends that you back up the master authentication key using the procedure under the section "Back Up the Master Key" in the *Hitachi Storage Navigator Modular 2 Storage Features Reference Guide for AMS* **(MK-97DF8148-13). Then store the master authentication key in a safe place (for example, at your disaster-recovery site).**

☞ **If you lose the master authentication key, you run the risk of being unable to recover the data from your SED(s).**

READ ME FIRST

HITACHI
Inspire the Next

HDS Statement
on
AMS 2000 Data-at-Rest Encryption Feature
and
Key Management

The AMS 2000 has the ability to encrypt data stored in the hard disk drives of the disk subsystem by using the Data At Rest Encryption feature. The Hitachi data-at-rest encryption feature has two components: the Data At Rest Encryption License Key and Self Encrypting Disk (SED) Drives. Hitachi data-at-rest encryption utilizing SED technology provides AES-128 encryption. Encryption can be applied to some or all of the internal storage drives within the disk subsystem. Hitachi data-at-rest encryption utilizing SEDs also includes integrated key management functionality as well.

As part of the implementation of Data At Rest Encryption on the AMS 2000, a Master Authentication Key ("**MAK**") is created during the installation process of the feature, which is used to generate authentication keys for each SED in the array. **HDS STRONGLY RECOMMENDS THAT CUSTOMERS DO A BACKUP OF THE MAK IMMEDIATELY AFTER INSTALLATION OF THE DATA AT REST ENCRYPTION FEATURE, BEFORE LOCKING OR DISABLING DATA AT REST ENCRYPTION AND/OR SYSTEM/MICROCODE UPGRADES, AFTER REFRESHES OF THE MAK, AND AT PERIODIC INTERVALS PURSUANT TO THE CUSTOMER ORGANIZATION'S KEY MANAGEMENT POLICY. *FAILURE TO BACKUP THE MAK CAN RESULT IN PERMANENT LOSS OF DATA.***

If the SED cannot be authenticated in case of the array failures or the array model upgrade, this backup file is used to restore the MAK.

Hitachi Data Systems believes that if the data-at-rest encryption feature of the AMS 2000 is implemented properly that information leakage can be prevented when disks are lost or stolen or during the return of failed disks and/or complete subsystems to HDS. While encryption of data-at-rest is a good prevention mechanism for information leakage in the aforementioned cases, the customer is advised to implement any and all relevant controls to further limit the chance of exposure.

For further information on data-at-rest encryption, please contact your Hitachi Data Systems account team.