Storageflex
NETWORK DATA STORAGE SOLUTIONS

Self-encrypting drives (SED): helping prevent data loss, theft, and misplacement

Version: 1.0
Updated:

Abstract:
This white paper introduces self-encrypting drive technology, or SED, an advanced data security solution based on the ability of disk drives to autonomously encrypt and add a layer of protection for valuable stored data. It covers the essentials of enabling SED global and local keys to offer flexible protective options. SED can keep your data safe even if drives are lost, stolen, or misplaced by accident across different storage enclosures.

The document also touches on different SED logical drive roaming scenarios to illustrate approaches to data protection offered by SED on Storageflex HA3969 storage systems as part of providing a highly efficient and
cost-effective solution that optimizes IT resources and provides agility in dealing with burgeoning secure data needs.

Contents

Introduction

One of the most important capabilities of a storage system is providing protective mechanisms against the high cost and other negative results of data breach or loss. Storageflex has always placed an emphasis on innovating new security measures and incorporating solutions as they emerge across the industry. Storageflex aims to enhance the security capabilities of as many storage products as possible while maintaining an attractive cost proposition, encouraging and helping organizations put comprehensive security strategies in place to better safeguard their data.

Products covered by this document

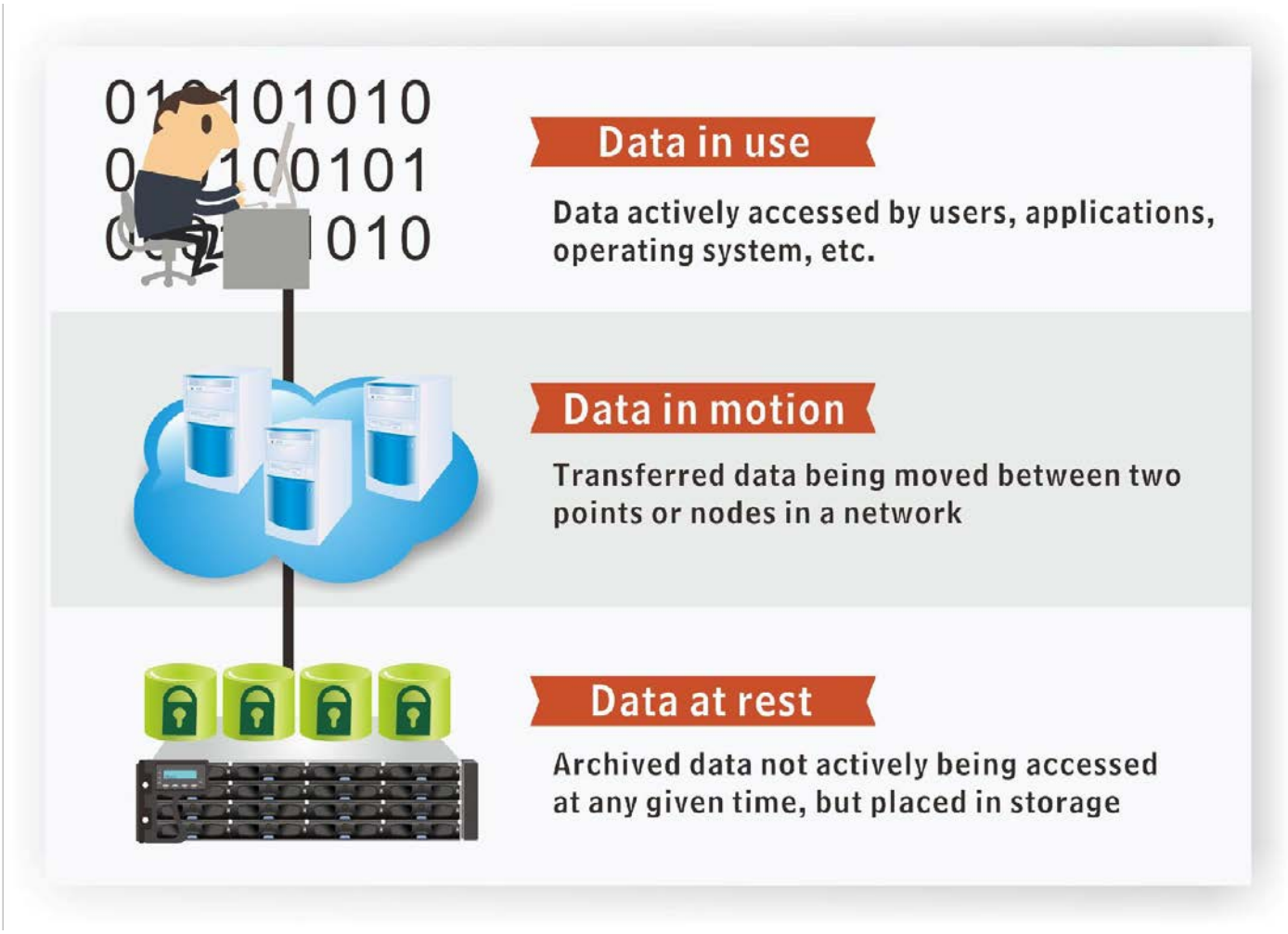
HA3969 3.5” Drive Bays family

What is an SED?

SEDs have an encryption controller (ASIC) and an encryption key both embedded on the hard drive itself. SED encryption is automatic and transparent without performance degradation. A unique encryption key is generated randomly at the factory for each SED. The encryption is essentially fail-safe, and means drives are extremely secure when installed in an array or when removed – so even if the physical drive is stolen or misplaced, the data on it remains protected against intrusion.

Why implement SED protection?

To avoid the high cost and many other negative consequences of a data breach or loss, it is important for organizations to put a comprehensive security strategy in place. This requires understanding where data is at all times across the entire organization and securing it at each stage and point. These points or levels of security can be broken down into three basic categories: data-in-use, data-in-motion, and data-at-rest.



The primary focus of SED solutions is securing data at rest. Self-encrypting drives (SEDs) are well-suited to mitigating the security vulnerabilities of data at rest, and are becoming a standard technology provided by many of the world's top hard drive vendors. This allows for interoperability and ensures greater market competition and more attractive pricing. Based on the Storageflex SED solution, users can secure data efficiently and easily.

How it works

SED automatically executes full disk encryption when a write job is performed by using the embedded encryption key. Encrypted data is decrypted before leaving the drive when a read request is met. When a new SED is acquired, it already has an embedded encryption key, until the user evokes it to start the authentication check process.

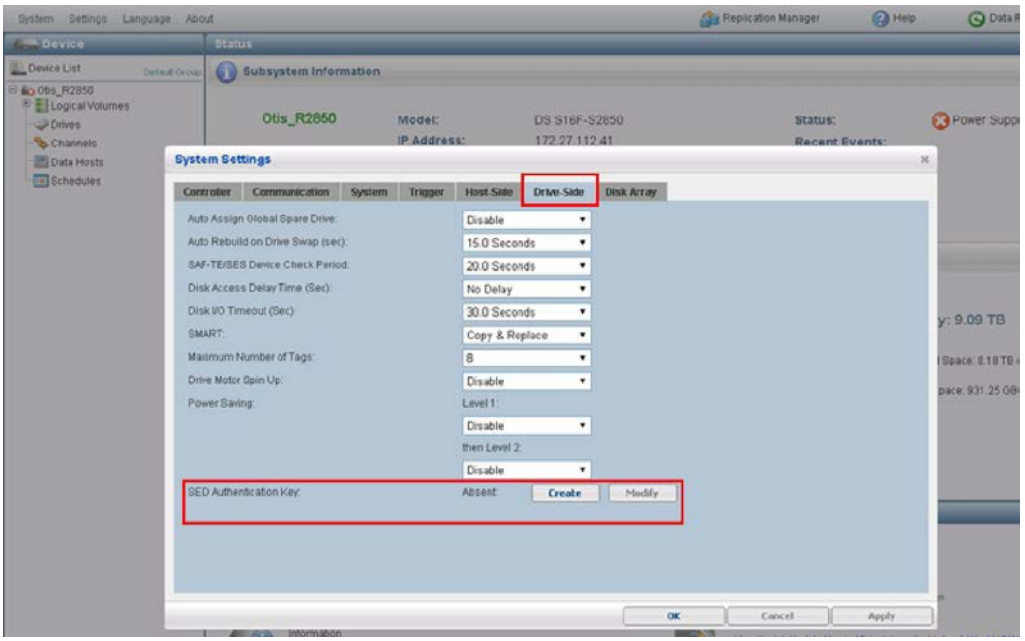
SED protection

Storageflex flexible SED key introduction

Custom settings included with the Storageflex SED solution allow users to set global and local keys separately through a few simple steps in the dedicated SED sub-section of the GUI. All SED functions are integrated into the intuitive and user friendly SANWatch interface for easy access.

How to enable SED key?

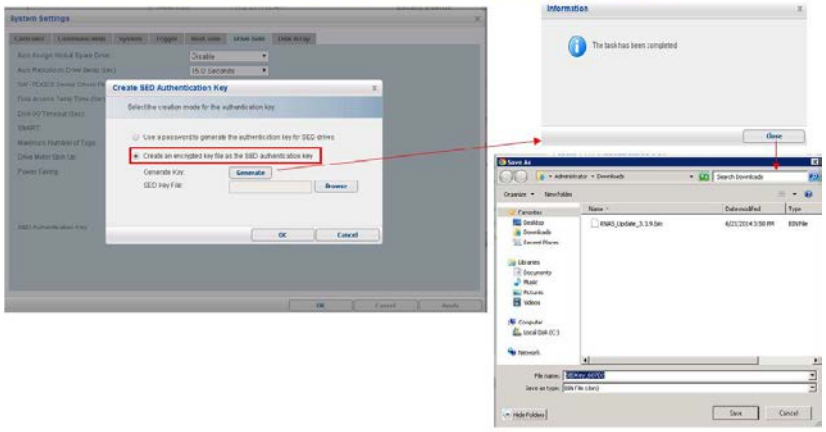
- Global key settings are for a subsystem rather than a logical disk, and users can enable and apply an SED key directly



➢ Use a password to generate the key for an SED

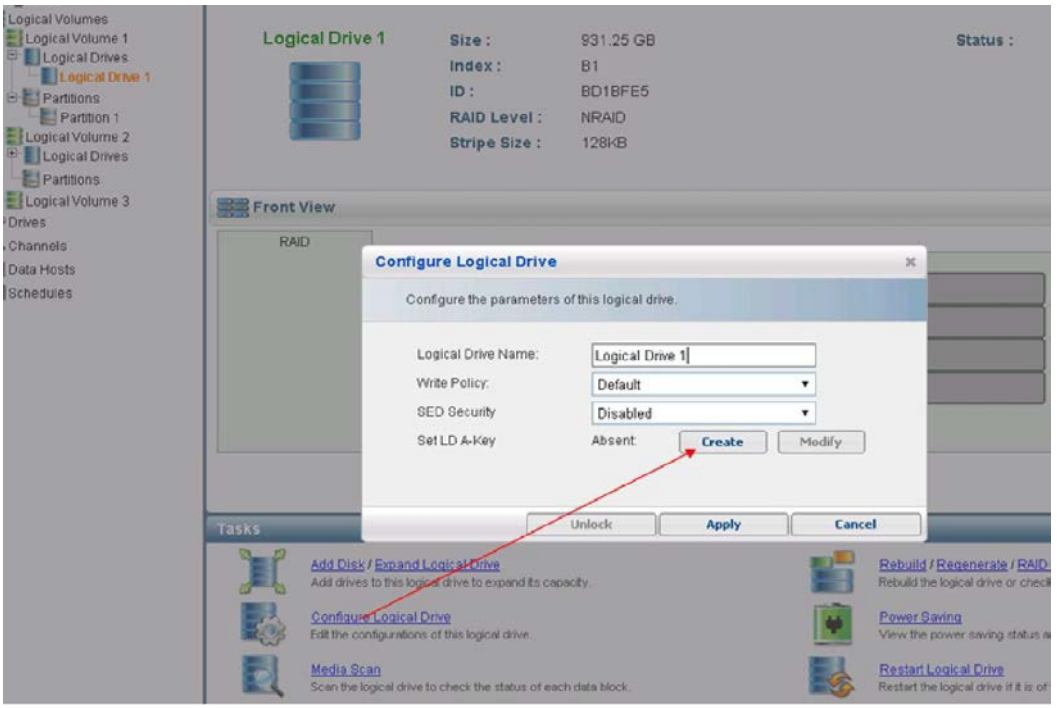
- Create an encrypted key file for an SED

  - Create an encrypted key file as Controller-id.bin



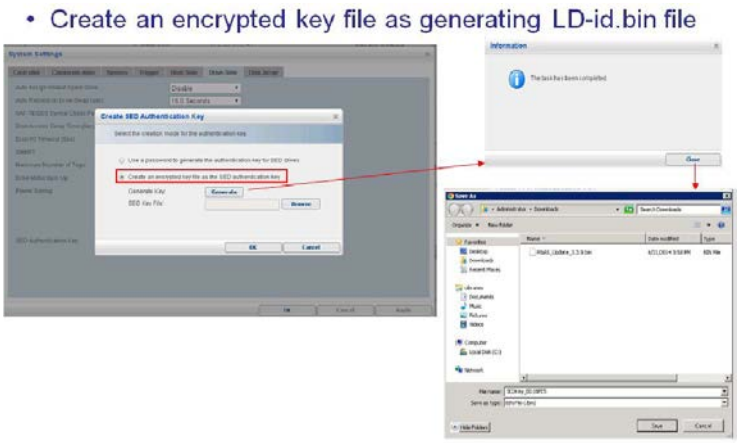
    - The authentication key then saves onto the backplane

- Local key settings apply to logical disks on Storageflex HA3969 3.5” Drive Bays system, which offer the flexibility of creating different local keys for each logical disk, as needed by users



    - Use a password to generate the key for an SED

- Create an encrypted key file for an SED



- Authentication key then saves onto the hard drive

Introduction to enabling SED functionality and its scope

Things to consider when mixing SED and non-SED in the same logical disk

- All SEDs of a specific LD/element must be at the same security status (all secured or all unsecured)
- During LD creation, SED and non-SED intermix is not supported
- LD rebuilding supports the use of SED-only spares

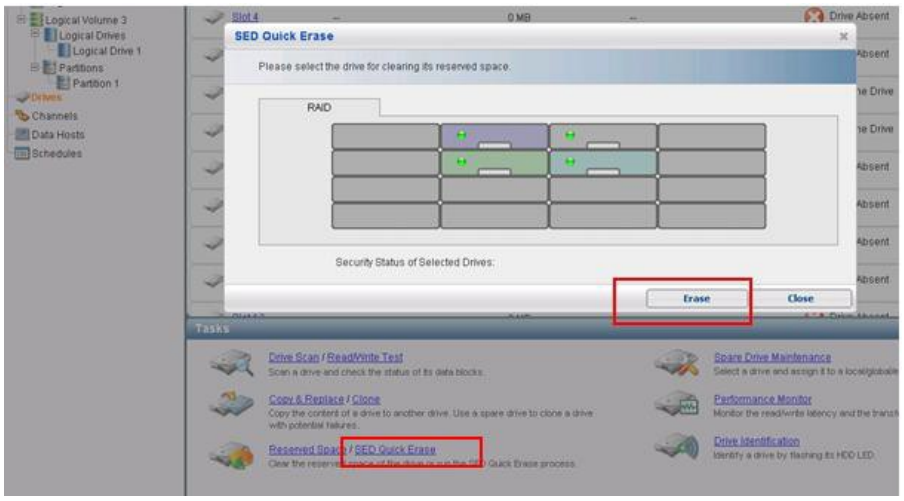
SED function operation

Auto lock

This feature is supported. Users are prompted to unlock an auto locked LD when the system is reset or rebooted. Authentication/unlocking require password or encryption key for access.

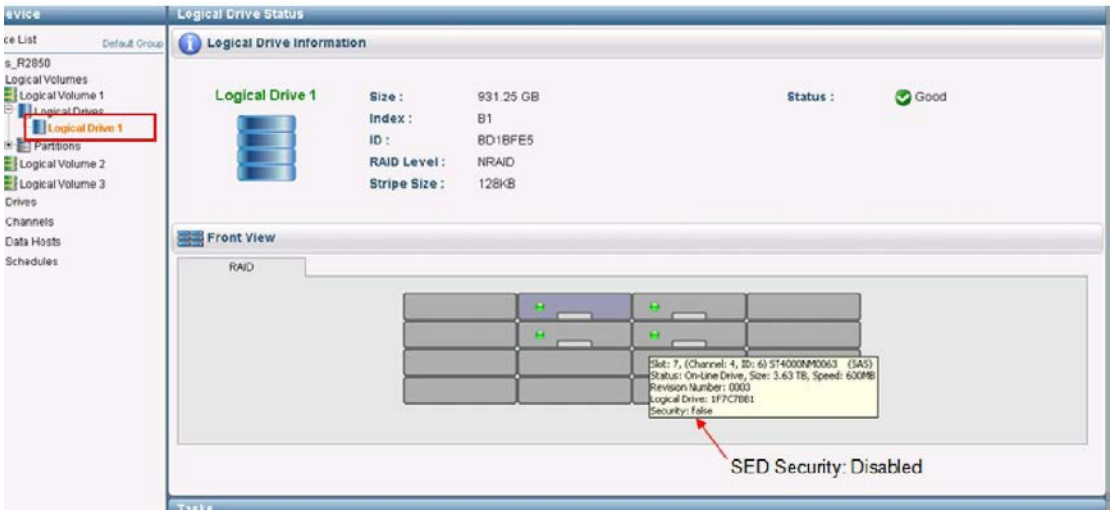
Secure/quick erase

- Allows users to quickly and easily erase specific SEDs through the GUI. This is another benefit of enabling the SED feature, as the device can be securely erased in a matter of seconds, as opposed to several hours using traditional drive wipe methods. The SED can be instructed to simply change the encrypted key, rendering all data on the drive effectively unreadable or destroyed. The data remains in an inaccessible encrypted format that can no longer be used, making traditional time-consuming deletion unnecessary
- Secure/quick erase available for specific SEDs, independent of any overall LD



Drive-based operation view

- Users can check attributes to obtain information for every drive easily through the GUI
- Indicates the security status of selected drives as shown below



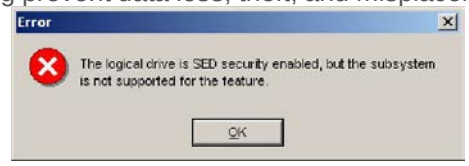
SED LD roaming operation

What is SED LD roaming?

- Moving or migrating an SED-enabled logical drive between HA3969 storage systems or enclosures

SED LD roaming scenarios

- Move SED-enabled LD to a system with the same global/local SED key
    - Enables SED security for the LD automatically after roaming
- Move SED-enabled LD to a system with a different global/local SED key
    - Locks and takes the LD offline (moving an isolated logical drive)
    - To bring the SEDs in an isolated LD back online: ask to authenticate with old key, then forcibly modify it with a current key
- Move SED-enabled LD to a system not configured with any SED key
    - Locks and takes the LD offline (moving an isolated logical drive)
    - Bring the LD online: ask to authenticate with old key unlock, then set SED status to disabled
- Roaming to a system with no SED support, but with properly licensed firmware



- Upgrade to new firmware, license and install SANWatch build with HA3969 SED feature
- Bring the LD online: ask to authenticate with old key unlock, then set SED status to disabled

Caution:

1. Older models may not support SED without upgrading to the latest firmware, license, and SANWatch version simultaneously. Models prior to the G7 series do not offer SED support (HA3969 G6 and older)
2. Important! SED and non-SED mix not allowed during LD creation. Mixing the two types may cause LD formatting failure
3. If a controller fails, in-progress scan operations resume when another controller takes over (only applies to models with redundant controllers)

Conclusions

Storageflex HA3969 systems offer comprehensively and thoughtfully-designed RAID storage products that augment data protection in numerous ways. As Storageflex is always keen on implementing new and more advanced security measures, we are taking decisive action to make self-encrypting disks (SEDs) available on a variety of recent and future systems. SED technology offers one of the most airtight data protection methods available in the storage industry, and directly addresses many widespread causes of data loss.

Storageflex HA3969 SED via the SANWatch interface is also very easy to use and has no negative impact on system performance. Users do not require extensive technical training to make the most of our SED functionality, and can quickly and conveniently tap greater flexibility with multiple settings and the ability to apply them to specific drives. Once more, it is important to remember that SED also brings major time savings when deleting data: changing encryption in mere seconds with a few mouse clicks is much preferable to traditional data deletion methods, which take exponentially more time to complete and are less secure.

As storage and security continue to converge, solutions like SED are leading the way by providing organizations with the strong, easy-to-use security needed to protect data. As always, Storageflex is leading the move towards more readily available and reliable deployment of the latest storage technologies, and is your best personal partner in meeting the needs of your organization.