

WINCHESTERSYSTEMS®

Purpose-Built Storage

Self Encrypting Disks (SED)

and

Secure Erase

Ensuring Your Data is Safe.....

Table of Contents

Introduction	3
Products covered by this document	3
What is a SED?.....	3
Why implement SED protection?	3
How it works.....	4
SED Protection	4
Winchester Systems flexible SED key introduction.....	4
How to enable SED key?	4
Introduction to enabling SED functionality and its scope	7
SED Functional Operation	7
Isolated logical drive support.....	7
Secure Erase	7
Drive-based operation view	8
SED Logical Drive Roaming Operation	9
What is SED Logical Drive roaming?	9
SED Logical Drive roaming scenarios.....	9
Conclusions	10

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. Winchester Systems has always placed an emphasis on innovating new security measures and incorporating solutions as they emerge across the industry. Winchester Systems 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

All FlashDisk FX and RF Series Arrays

What is a SED?

SEDs have an encryption controller (ASIC) and an encryption key both embedded on the hard disk 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 disks are extremely secure when installed in an array or when removed . 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 Winchester Systems SED solution, users can secure data efficiently and easily

How it works

SED automatically executes full disk encryption when a write operation 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 waiting until the user evokes it to start the authentication check process.

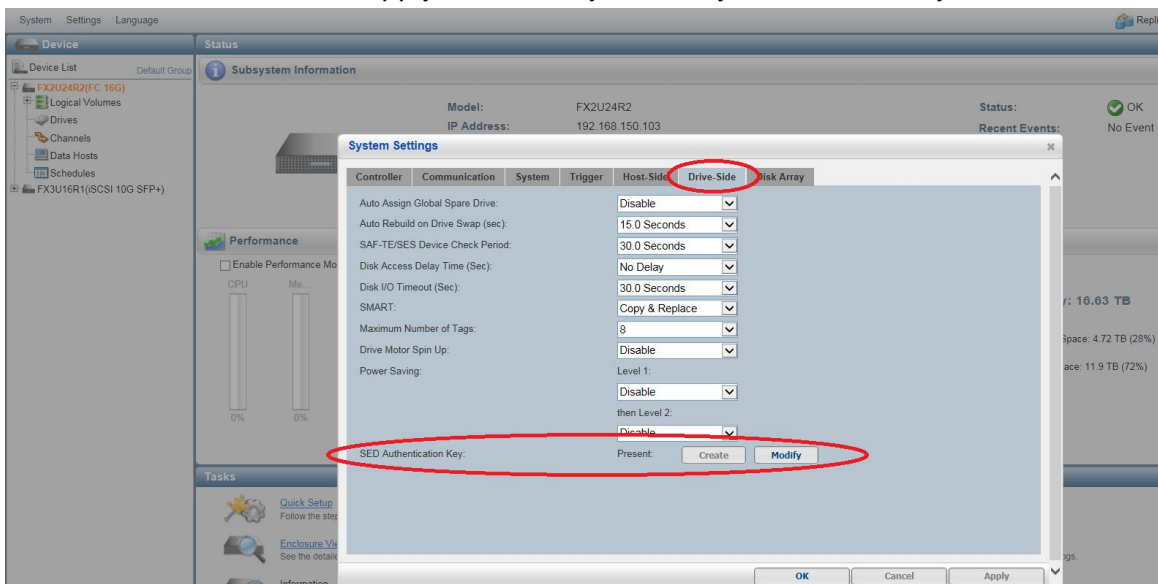
SED Protection

Winchester Systems Flexible SED Key Introduction

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

How to Enable a SED Key?

- **Global key** settings are for a complete subsystem rather than a logical drive, and users can enable and apply an SED key manually or automatically:



- Manually by entering a password of choice to generate the key for an SED:



- Automatically by creating an encrypted key file and saving it as a .bin file somewhere safe:



- The SED authentication key created manually or automatically is then saved onto the subsystem backplane.
- **Local key** settings apply to logical drives created on the Winchester System FlashDisk systems, which offer the flexibility of creating different local keys for each logical drive as needed by users. These keys can also be created manually, or, automatically:



- Manually by entering a password of choice to generate the key for an SED:

Self Encrypting Disks (SED) and Secure Erase



- Automatically by creating an encrypted key file and saving it as a .bin file somewhere safe:



- Authentication key then saves onto all of the hard disks.

Introduction to Enabling SED Functionality and its Scope

Things to Consider when Mixing SED and non-SED in the same

Logical Drive

- All SEDs of a specific logical drive must be at the same security status (all secured or all unsecured).
- During logical drive creation, mixing of SED and non-SED disks is not supported.
- Rebuilding of a secured logical drive supports the use of only SED spare drives.

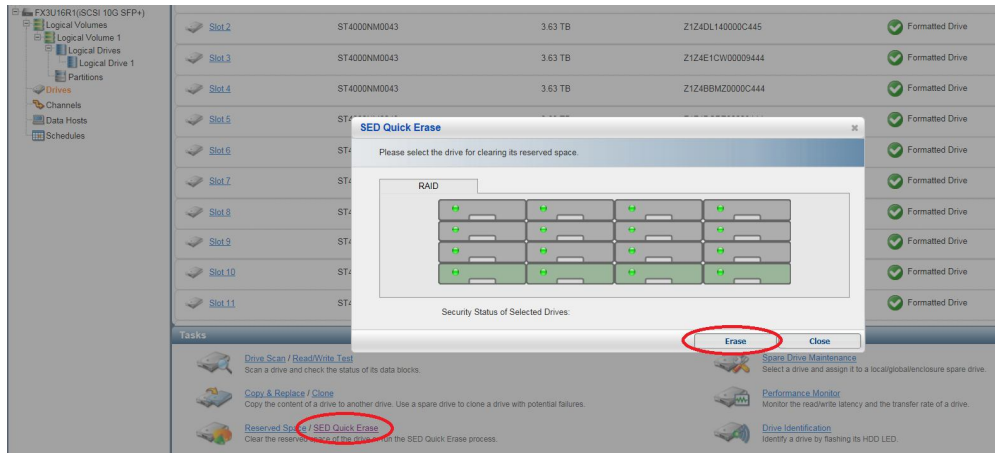
SED Functional Operation

Isolated Logical Drive

Users are prompted to unlock an isolated logical drive when the system is reset or rebooted. Authentication and unlocking require the password or saved encryption key .bin file for access.

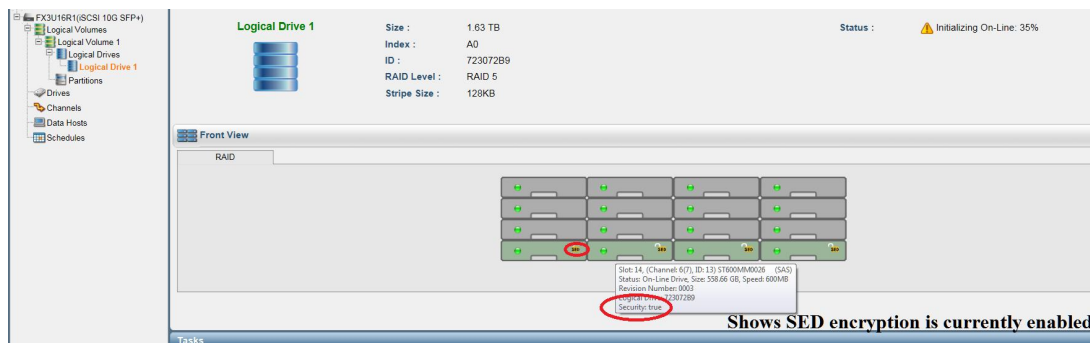
Secure Erase

- Allows users to quickly and easily erase specific SEDs through the FlashDisk Global Manager user interface. 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 and destroyed. The data remains in an inaccessible encrypted format that can no longer be used, making traditional time-consuming deletion unnecessary



Drive-Based Operational View

- Users can obtain information for every disk easily through the FlashDisk Global Manager and check the security status of selected disks as shown below:



SED Logical Drive Roaming Operation

What is SED Logical Drive Roaming?

- Moving or migrating an SED-enabled logical drive between Winchester Systems FlashDisk storage systems or enclosures.

SED LD Roaming Scenarios

- Move SED-enabled Logical Drive to a system with the same global/local SED key.
 - Enables SED security for the logical drive automatically after roaming.
- Move SED-enabled logical drive to a system with a different global/local SED key.
 - Isolates and takes the logical drive offline (sets operational state as an isolated logical drive).
 - To bring the SEDs in an isolated logical drive back online, authenticate with the old key and then forcibly modify it with a new key.
- Move SED-enabled logical drive to a system not configured with any SED key.
 - Isolates and takes the logical drive offline (sets operational state as an isolated logical drive).
 - To bring the logical drive online, authenticate with the old key and then set SED status to disabled.

Caution:

1. Older FlashDisk models may not support SED without simultaneously upgrading to the latest firmware and FlashDisk Global Manager version.

******WARNING******

If the Global SED Key is lost or forgotten, the only method to recover is destructive. All data will be lost and the subsystem must be returned to the factory to clear the key and return the subsystem to proper operation.

Conclusions

Winchester Systems offer comprehensively and thoroughly designed RAID storage products that augment data protection in numerous ways. As Winchester Systems 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.

Winchester Systems SED via the FlashDisk Global Manager 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 disks, logical drives, and subsystems. 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 more 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, Winchester Systems 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.