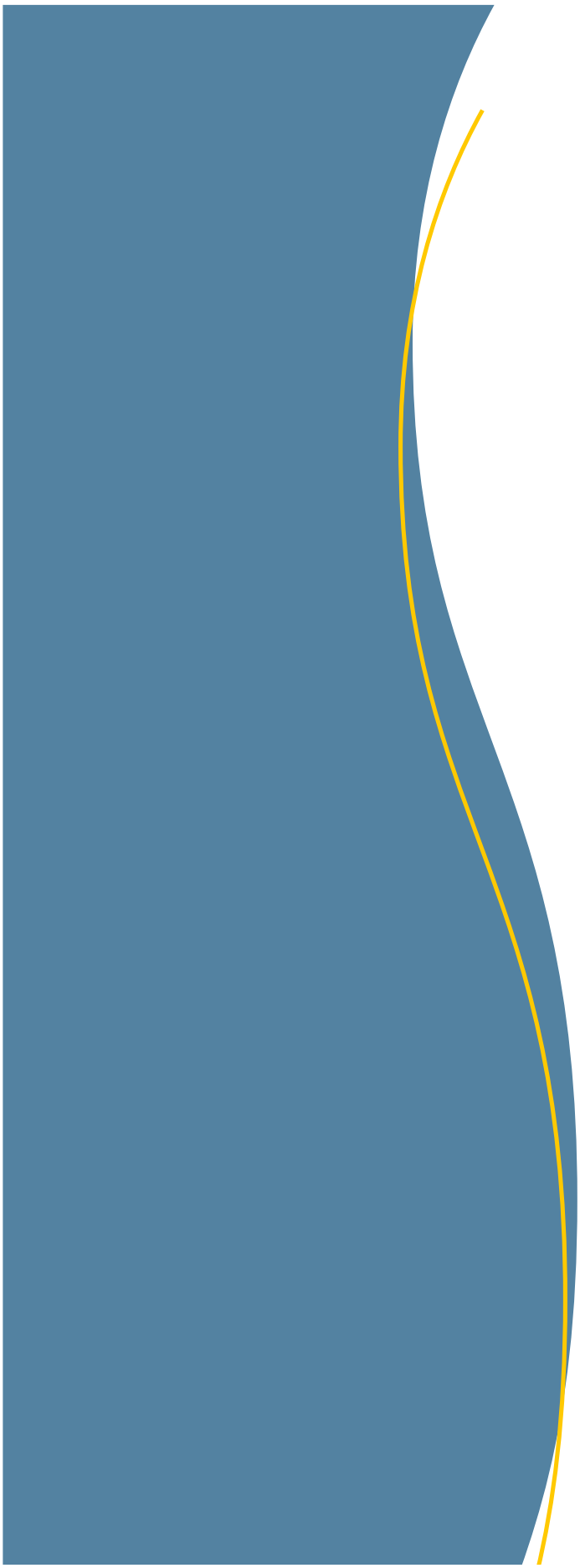


# StorageTek Tape Drive Encryption Solutions

## Best Practices
## June 2008

Revision: 3.1

---

We welcome your feedback. Please contact STK Test Engineering at:

rick.schworm@sun.com; mikal.green@sun.com; richard.birkelo@sun.com

# Contents

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web sun.com

# Change History

| Document Description | |
|---|---|
| Document owner | Rick Schworm and Mikal Green—-Systems Integration Engineers |
| Organization | Sun StorageTek Test Engineering—Mainframe Customer Emulation & Test |

| Revision | Date | Description |
|---|---|---|
| V1.0 | 02/06/2007 | RAS/MWG - Initial Draft Completed |
| V1.1 | 04/06/2007 | RAS/MWG – Incorporate comments from initial review and add VSM attach section. |
| V1.2 | 05/09/2007 | Initial Release |
| V2.0 | 04/10/2008 | MWG/RAS – Draft rewrite for KMS 2.0 |
| V2.01 | 04/16/2008 | Updates |
| V2.02 | 04/28/2008 | Updates |
| V3.0 | 05/14/2008 | Add 9840D support |
| V3.1 | 06/13/2008 | Updates |



Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web sun.com

# Introduction

The purpose of this document is to present solutions which allow for mixed encryption environment implementations using Sun's Key Management System (KMS) 2.0.

Mixed encryption environments are defined as a library configuration that contains both encrypted and non-encrypted drives. Currently, both T10000 and 9840D drives offer encryption cabability. Mixtures of drive families along with the mixture of encrypted and non-encrypted drives are supported.

This document is not intended to be a step-by-step guide, but rather serves to highlight the issues and obstacles involved in a typical mixed drive configuration and present recommended best practices for overcoming them. It describes an encryption solution using the enterprise encryption system known as KMS 2.0. There are substantial differences between Ultra1.x and KMS 2.0 and the best practices discussed in this paper reflect those changes in detail. To summarize:the Ultra 1.x solution delivered keys on a drive basis via a Token while KMS 2.0 delivers keys on a volume basis via a KMA appliance.

The information presented in this document is supported by testing initiatives that were conducted in Sun's Mainframe Customer Emulation Test Lab.

## Audience

This documentation is intended for Sun employees, field personnel, partners, and customers who are interested in learning more about the Sun StorageTek encryption solution. Intended audience are those who are already familiar with the information contained within the systems assurance and installation guide.

## Related Publications

- Key Management System (KMS) 2.0 Installation and Service Manual
- Key Management System (KMS) 2.0 Administration Guide
- Key Management System (KMS) 2.0 Systems Assurance Guide
- StorageTek Cypto Key Management Solution Version 2.0 Management Practices Whitepaper
- Key Management System(KMS) 2.0 Open Systems Implementation Whitepaper
- NearLine Control Solution T10000 Support Documentation Update
- NearLine Control Solution 9840D Support Documentation Update
- Storage Management Component (SMC) MVS software Config and Admin Guide
- Sun Storagetek Virtual Tape Control System (VTCS) Admin Guide, Command & Utility Guide

# Chapter 1: Encryption System Overview

Encryption serves to limit access to data by making information unreadable without special knowledge. This is typically accomplished by applying a cryptographic algorithm called a cipher to the data. The result is an encrypted ciphertext that is unreadable until an inverse algorithm is again applied to decrypt the data. This requires access to the key value used to encrypt the data. Data is transported and stored in this unreadable state, thus achieving data security when information is most vulnerable.

Due to heightened data security requirements and industry compliance standards, there is an increasing need for encryption in today's datacenters. This need can be met by one of the following options: host-based, in-band appliance-based or device-based encryption.

## Host-Based Encryption:


Host-based encryption is also referred to as encryption at creation. In this scenario, data is encrypted on the host at the time of data creation. The encrypted data is then transferred to the storage devices on which it will reside. Host-based encryption is typically accomplished by enabling special encryption features through the operating system, database or backup application.

***Pros:***

- ◊ Secure: Data is encrypted at creation and remains encrypted through the lifecycle of the data.
- ◊ Difficult to bypass: Central point of encryption at data creation ensures security regardless of what storage device the data rests on.

***Cons:***

- ◊ Performance Hit: Data is encrypted before it is transferred to a storage device and unable to be compressed. This can reduce performance by up to 60% and will result in a significant increase in the storage capacity required (typically by 2x or more).
- ◊ Resource Intensive: Encrypting the data on the host requires significant server resources that would normally be used to serve other functions.
- ◊ Infrastructure Refresh: This often requires an upgrade to existing legacy operating infrastructure.

## In-Band Encryption:

In-Band encryption occurs while data is in transit. In this scenario, data is encrypted by a dedicated encryption appliance that sits in the data path between the host and the storage device. Encryption occurs as data is transferred to storage devices. Data leaves the host as plaintext and is converted to encrypted ciphertext before coming to rest on the storage devices. Data is retrieved in the same fashion by leaving the storage device as encrypted ciphertext and then decrypted to plaintext before being presented to the host.

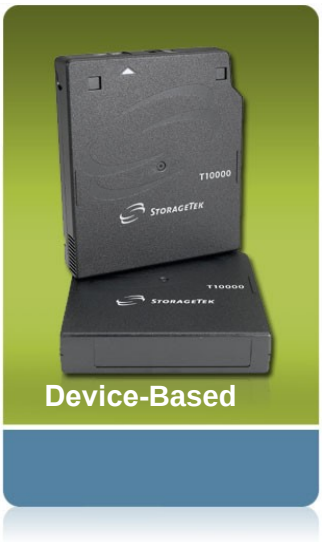
***Pros:***

- ◊ Utilize Legacy Infrastructure: Ability to fit seamlessly into both legacy operating and storage infrastructure makes for a quick encryption implementation.
- ◊ Transparent to Storage and Hosts: Encryption process occurs transparent to hosts and storage devices.

***Cons:***

- ◊ Less Secure: Because this is an in-band solution it is easier to bypass than other encryption scenarios.
- ◊ Not Scaleable: As the number and speed of storage devices grow, an increasing amount of individual in-band appliances will be required to maintain the encryption solution.
- ◊ Commitment: After an in-band appliance-based encryption scenario is implemented, the customer is committed to maintaining that in-band appliance for the lifecycle of their data even if it negatively impacts performance or cost in the future.

## Device-Based Encryption:




Device-based encryption is also referred to as data at rest encryption. In this scenario, data is encrypted on the storage device as it is written. The encrypted data remains on the storage device while at rest and can be physically transported in a secure state. Device-based encryption removes the load of encryption from the hosts and the network. Encryption is handled by the storage device after compression is performed.

***Pros:***

- ◊ High Performance: Device-based encryption is the most efficient encryption scenario from a performance perspective. This is accomplished by removing the load of encryption from the host or the network. Since the storage device is handling the encryption process, full data compression can be realized.
- ◊ Highly Secure: Encryption occurs and is validated at a device level.
- ◊ Difficult to Bypass: Storage devices sit at the end of the data path and cannot be bypassed. Devices are only capable of writing encrypted data.
- ◊ Legacy Configuration Support: No change required to existing hardware and software environment.

***Cons:***

- ◊ Storage Refresh: May require a tape drive upgrade depending on current hardware in place.

## Sun Encryption

Sun's encryption solution utilizes an AES(Advanced Encryption Standard)-256 substitution-permutation network cipher algorithm that is applied by the storage peripheral device, in the example below, the T10000 tape drive. CCM-AES is the mode employed by this solution. This is a FIPS (Federal Information Processing Standard) compliant encryption standard. Key management occurs outside of the data path and the encryption of sensitive data is completely transparent to the application. A cluster of KMAs manage these encrypting devices by authenticating enrollment processes, securing the distribution of encryption keys and providing a policy-based lifecycle key management solution. The cluster serves to provide failover, load-balancing and data protection by replicating changes across the cluster in real time. KMA to drive communications occur over an isolated secured network in recommended configurations. Encryption keys are never in the clear, even during delivery over a secured network.

Administration of the encryption solution is performed via the KMS manager GUI that can be installed on workstations or management servers. Separation of roles and responsibilities are customized to meet the needs of the organization and a quorum is created to govern critical operations such as adding a new KMA to the cluster. Key policies, key groups and agent assignments are defined through the manager GUI and enable the automated management of encryption keys throughout the lifecycle of the data being encrypted.

When a tape cartridge is mounted, the encryption agent requests the appropriate encryption keys from the KMS cluster. Any KMA in the cluster is capable of providing all necessary functions to any drive enrolled in the cluster. Keys are transferred to the encryption agent and are used for writing and reading the data. A different write key is issued for each tape. The KMA database keeps track of all keys used on a tape and supplies the keys automatically when the tape is mounted. The expiration period of an encryption key depends on policy-based settings that were defined through the KMS manager GUI. When a tape is loaded in an encrypted drive after the key's encryption period has expired, a new encryption key is generated and issued.

The illustration below depicts a logical sample environment that consists of a two KMA cluster servicing multiple automated tape libraries.

## The Sun Encryption Solution

The Sun Tape Encryption Solution is a device-based encryption implementation. Data remains encrypted at rest. Initial offerings will support the enrollment of several tape drive models capable of acting as an encryption agents in this solution. Key management is performed outside the data path.


**Figure 1: Sun's Encryption Solution**

### Encryption Components

**Key Management Appliance (KMA)** – A secure, dedicated appliance for creating, managing and storing encryption keys. It delivers policy-based lifecycle key management and ensures the security and authenticity of the encryption solution. The KMA is a Sun x2100M2 server hardware with a Sun SCA6000 security card.

**KMS Cluster** – A Key Management System is comprised of multiple KMAs clustered together. Key management appliances are clustered to provide failover, load balancing and data protection. KMAs in a cluster act in an active/active manner. All KMAs can provide full functionality to any encryption agent and changes made on any one KMA are quickly replicated to all KMAs within the cluster.

**KMA Manager Software** – The key management appliance is a locked down, security hardened device. There are only very limited options available to a privileged security officer through the console or ELOM (enhanced lights out manager) of the appliance. Other than specific operations, administration of the StorageTek Crypto Key Management Solution occurs through a GUI management program that is executed from a customer provided workstation or server.

**Encryption Agent** – The encryption agent is a generic term for the peripheral device that is used with the KMS to manage encrypted data and obtain keyed material. At the time of release, the Crypto Key

Management 2.0 System supports only the StorageTek T10000A and 9840D tape drives. In subsequent releases, T10000B and LTO4 encryption agents will be enhanced to operate with KMS 2.0. The T10000A tape drive has a native transfer rate of 120 MB/s and has demonstrated speeds up to 330 MB/s using compression. The drive utilizes a 4GB FC interface. Standard T10000 media have a 500GB uncompressed capacity with a shorter "Sport" cartridge at 120GB. WORM VolSafe media is available in both 500GB and 120GB uncompressed capacity format.

## Benefits of the Sun Encryption Solution

**Performance:** Data is encrypted after tape compression occurs which allows for maximum performance and the most efficient possible usage of tape media. Sun utilizes a very powerful encryption algorithm (CCM-AES-256) that is also highly efficient. Only a 100 byte overhead is required for each block of encrypted data that is recorded. Many backup / restore or archiving applications realize maximum performance when utilizing an average blocksize between 256KB and 1MB. The T10000 tape drive supports blocksizes up to 2MB. Given this, the impact of encryption on performance is negligible. This gives Sun a significant advantage over competitor products where encryption overhead, processing strain and inability to realize maximum compression by encrypting before the data reaches the storage device all contribute to drastic performance degradation.

**Ease of Management:** The KMS software manager GUI provides a central point of administration for a scalable encryption solution that can grow to manage multiple libraries of encrypted drives in multiple locations. Powerful policy-based lifecycle management options allow for intuitive and automated administration of encryption keys.

**Security:** AES-256, which Sun utilizes as a block cipher algorithm, is the most powerful commercially available security algorithm and Sun's implementation has been validated by NIST – the US Government National Institute of Standards and Technology. The key management appliance is a locked down, security hardened device. Separation of roles and responsibilities allows for a system of checks and balances to be implemented. Quorum operations are required for changes to the configuration that could pose a security risk.

# Chapter 2: Planning Encrypted Installations

## Things to Consider

Several things to consider when planning a data encryption implementation are laid out below.

### KMS Deployment

One KMS cluster is capable of administering an encryption solution for an entire organization even if that organization contains datacenters in multiple locations. Using one cluster introduces a single point of administration and serves to increase ease of management and simplicity of the solution. To achieve maximum failover, load balancing and redundancy, it is required that a minimum of two KMAs be deployed per location. For instance, if an organization employs an encryption solution across datacenters in Dallas and Atlanta, they would include 2 KMAs at each location. All four KMAs would be clustered together and would continually replicate any changes across the cluster. The KMA's at each location connect to the drives at that location using the private network within the library. If the Sun Service Delivery Platform(SDP) is deployed, it also attaches to that private network. An encrypting tape drive in the Dallas site would request encryption keys from either of the two KMAs at that location over the isolated services network.

### Mixing Drives

Unlike the Fiber Channel implementation, the T10000 and 9840D FICON drive returns a different device type to the library when encryption is enabled versus disabled. This information is communicated to NCS enabling the management of encrypted and non-encrypted drives

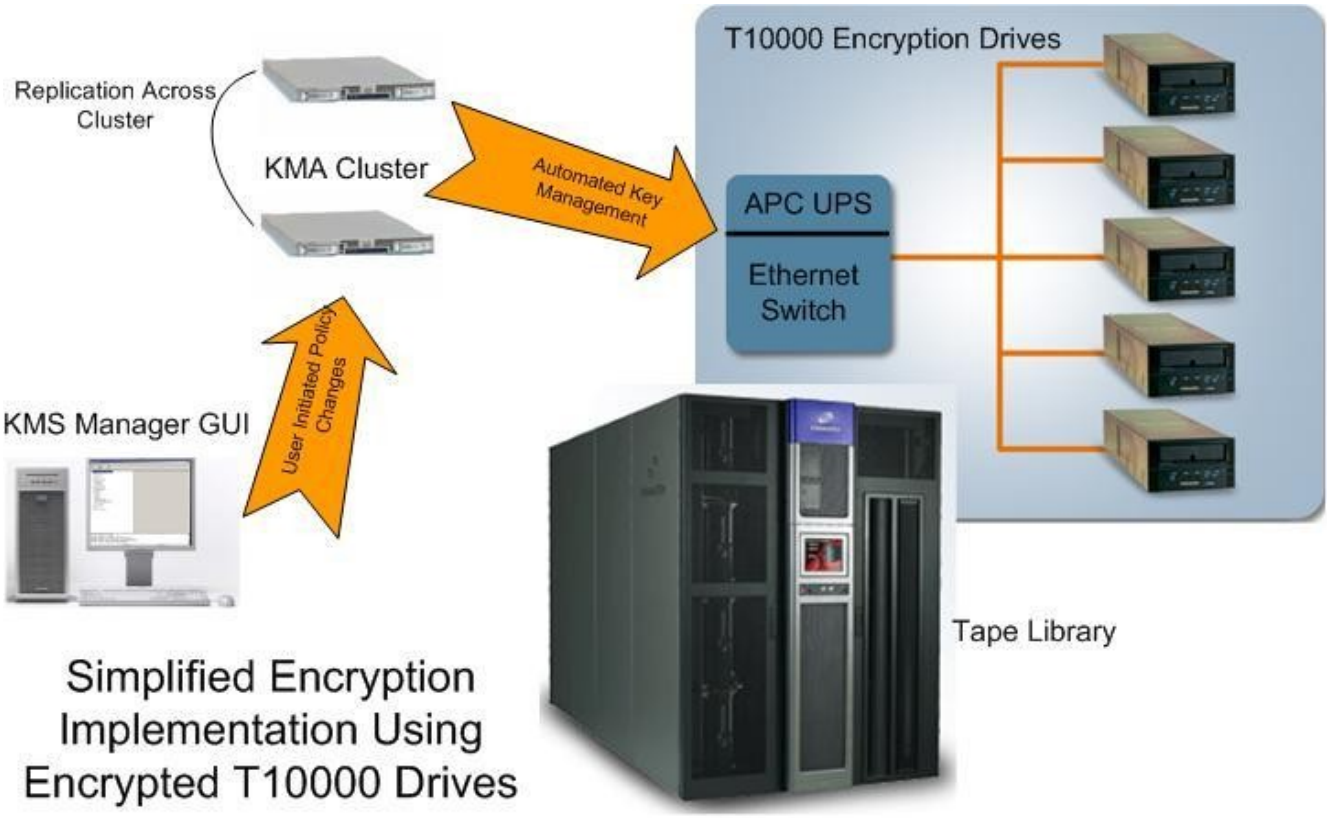
Encryption management occurs outside of the data path. The solution is application transparent and because of this, applications are unaware that encryption is taking place.

The following are important things to consider when planning an encryption implementation. Encrypted drives can read cartridges that contain non-encrypted data but they cannot append to them and no drive can read encrypted data or append to an encrypted cartridge without the proper key.

### Software Requirements

As stated previously, the encryption solution is transparent to customer applications. However, support for encrypted devices is only available in NCS 6.1 and later via the application of PTFs. Library microcode updates are required along with the microcode update of any non-encrypting drive. Specifics are located in Prerequisites.

## Sample Configuration




## Sample Configuration Overview

- **Administer all Sun Tape Encryption for an entire organization with a KMS cluster:** This provides a redundant management system that is capable of spanning across multiple site locations and enables encrypted data to be more readily shared within the organization. An active KMS cluster is kept current with live updates between all KMA's within the customer organization.
- **All drives in an organization should have access to the same encryption key groups:** All T10000A tape drives (agents) in an organization should have access to all key group encryption keys.
- **All drives in the same library should share default access to the same key group**: All T10000A Encryption tape drives that reside in the same library have the same default key group. This is important so that allocation of encrypted drives within the library is simply determined by encryption or non-encryption status.

## Benefits of the Configuration

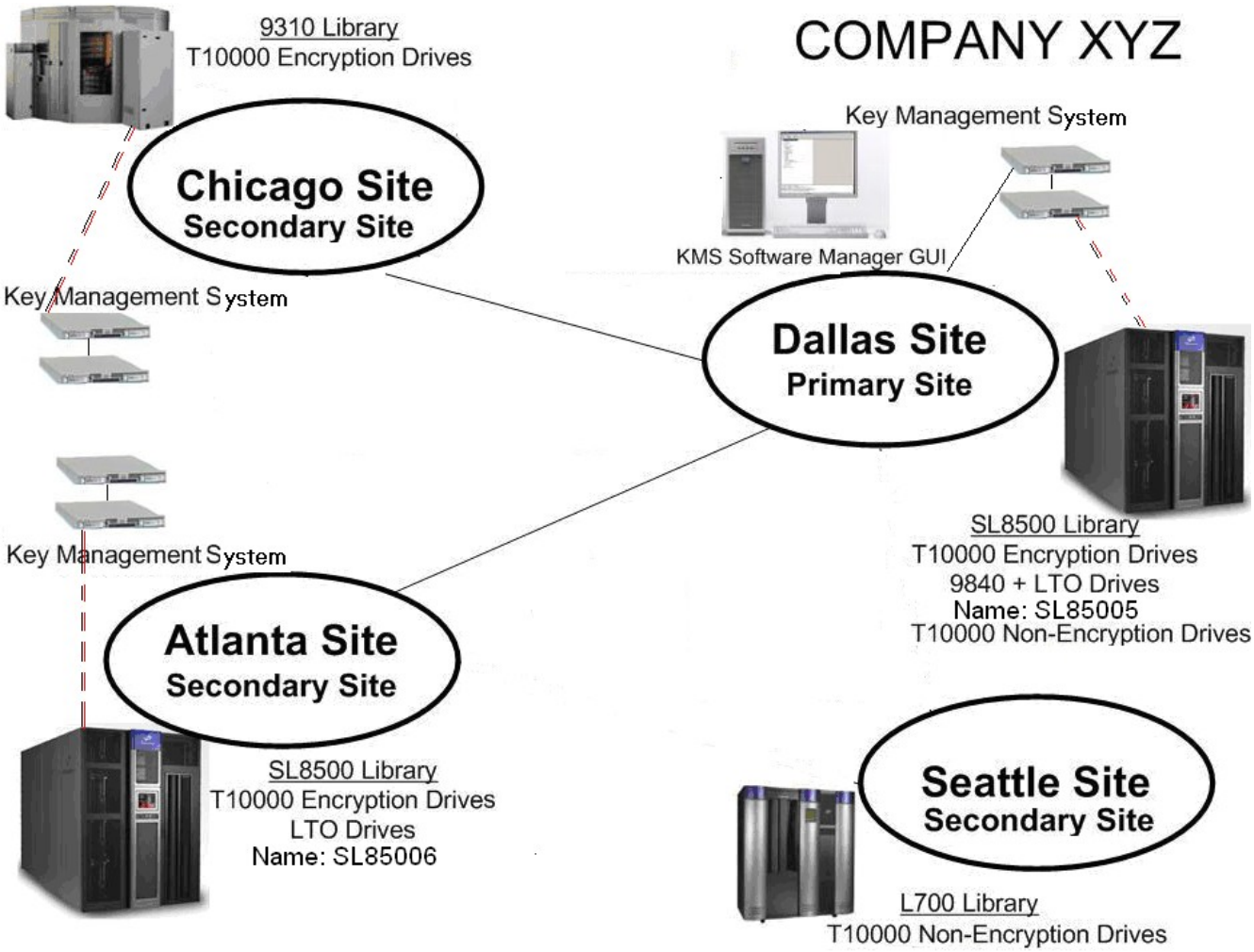
- **Key protection:** Key protection is an important consideration. Losing keys is equivalent to losing data and not having the correct keys available at the right time results in losing access to data. Effective key protection is the greatest benefit of the recommended configuration. This configuration will serve to limit the number of unnecessary encryption keys and ensure that all T10000A drives will always have access to the proper key.



Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web sun.com

◊ **Ease of management:** By using a KMS cluster administration and implementing a key management strategy where all drives share encryption key groups, the management burden is taken off the customer. This enables a datacenter to manage an encrypted solution transparently with no impact to day to day operations.

## Sample Configuration




In the above example, Company XYZ manages data storage sites in 4 locations. Their primary site is located in Dallas and this is where two of the six total KMA's reside. Another set of two KMA's are installed in Atlanta which is used as a disaster recovery site for Dallas, final set of KMA's are in Chicago. The KMS cluster consists of 6 total KMA's, drives from each respective site will pull keys from the KMA's at the site on the service network (dashed lines in red from KMS to Drives).The KMS Software Manager GUI session administers the cluster on the management network (solid lines in grey between sites), the updates are propogated to all KMA's. The GUI can reside on any selected customer workstation or server anywhere in the management network. It is recommended that Company XYZ store a backup of the KMS database at a remote site or in a vault.

Encrypted T10000 drives are located at three Company XYZ sites. In the Dallas site, there are also non-encrypted T10000 drives which are located in a separate library. Of the libraries that contain encrypted T10000 drives, some also contain a mix of other drive types.

Per the recommended configuration, all T10000 encryption drives that share a library may also share a key group. Following this recommendation, Company XYZ would begin their encrypted solution with the following 3 key groups: Dallas1, Atlanta1, Chicago1. In this example each drive at a site will obtain keys in one group for each data unit at the respective site. The other 2 key groups will be available to each respective site for read keys only. This key management solution allows for encrypted cartridges from any site to be exchanged with any other site if needed.

Here is an example of what an initial key allocation looks like for three different T10000 encryption drives, one drive grouplocated in Dallas one drive group in Atlanta and the other in Chicago.

| Location of Drive | Dallas | Atlanta | Chicago |
|---|---|---|---|
| Default Write Key Group | Dallas1 | Atlanta1 | Chicago1 |
| Read Key Group | Atlanta1 | Chicago1 | Dallas1 |
| Read Key Group | Chicago1 | Dallas1 | Atlanta1 |

The length of proctect time a key offers is based on the policy assigned via the KMS Software Manager GUI. For more information on key management practices see StorageTek Cypto Key Management Solution Version 2.0 Management Practices Whitepaper

.

# Chapter 3: Implementation Details

## Overview

When implementing a mixed drive solution, the selection of the proper drive for a particular tape is crucial. This selection is actually implemented by removing the undesired drives from the candidate list of available drives supplied by the operating system.

NCS/VTCS management of a mixed encryption solution is analogous to the management of a mixed 9940B and 9940A environment; with 9940B equivalent to encrypted and 9940A equivalent to non-encrypted.

The HSC and SMC software handles a mixed encrypted and non-encrypted environment using the following assumptions and rules:

- When a new volume is entered into an ACS that contains encrypting drives compatible with the volume media, the volume is assumed to be encrypted, unless overridden with a VOLATTR statement.
- A volume's encrypted status is reset only when the volume is mounted as scratch.
- If a volume is known (or assumed to be) encrypted, SMC allocation will automatically exclude non-encrypting drives.
- If a volume is known to be non-encrypted, SMC allocation will allocate either encrypting or non-encrypting drives, unless a VOLATTR statement limits the allocation to either encrypting or non-encrypting recording techniques.
- Encrypted data cannot be appended to non-encrypted data, or vice versa. If non-encrypted volumes will be appended in a mixed environment, VOLATTR statements are required to limit allocation to non-encrypting drives.

To aid this management, the segregation of non-encrypted and encrypted volumes via VOLATTR statements is recommended. That is, define a volume to be used on either an encrypted or non-encrypted device.

## Prerequisites

The following section lists the minimum prerequisites for 9840D and T10000A support. You should check for later maintenance available in the Sun System Handbook at SunSolve : http://sunsolve.sun.com/handbook_pub/validateUser.do?target=STK/STK_index.

| **NCS Software –** | **6.1** | **6.2** |
|---|---|---|
| HSC PTFs – | L1H136H<br>L1H13C4 | L1H13Q2<br>L1H13ZE |
| SMC PTF – | L1A00HK<br>L1A00JI | L1A00LQ |
| VTCS PTF - | L1H13ZO<br>L1H13Y8 | L1H13ZC |
| CSC PTF – | L1C1082 | L1C1093 |
| Library Station PTF – | L1S106F | L1S106G |

| Library Microcode | SL8500 | 9310 |
|---|---|---|
| | FRS_3.95 | 4.4.08 |

**T10000A Microcode** – 1.37.114

**9840D Microcode** – 1.42.706

**Virtual Operator Panel** – 1.0.11.17

**VTSS Microcode (VSM4 & VSM5)** - D02.02.00.E6

**VTSS Microcode (VSM3 )** - N01.00.77.00

**Key Management System** – 2.0 Build308

**Note:** The microcode is required for **both** encrypted and non-encrypted drives. This allows a non-encrypted drive to recognize an encrypted tape is mounted and present proper error information to the host.

**Note:** Encryption support is only available in NCS 6.1 and later.

.

## Installation/Maintenance

The following section attempts to summarize the installation steps noting subtleties found during test. Detailed steps are found in the associated product documentation.

The following components can be installed independently but this order is recommended:

1. Install Library Microcode

   This enables the library to report the correct device type to NCS.

2. Install VTSS Microcode

   This enables both a VSM4 or VSM5 to handle encryption related FSCs returned from the drive.

3. Install NCS/VTCS PTFs and identify drives

   These enable NCS to recognize the new device types and implement the new MODEL and RECTECH values required for the correct management of media and drives.

   Use SET Utility to add drives to the NCS Control Data Set.

4. Install Drives

   The Customer Service Engineer will install the drives in the library usingVirtual Operator Panel (VOP).

5. Install KMS Hardware

   The Customer Service Engineer will use the KMS 2.0 Installation and Service Manual to install the hardware. This hardware is a KMA Cluster consisting of 2 or more KMA units.

6. Configure KMS Software

   The Customer will use the KMS 2.0 Administration Guide to identify and manage the various encryption components.

   This includes the importing of keys, the definition of KMS Roles, establishing encryption key policies and the identification of encryption agents (drives) and dataunits (tape volumes).

7. Enable Drives for Encryption

   This is accomplished via the VOP application:

   a. The Customer Service Engineer will supply the PC Key ( License Key) and crypto serial number (CSN) for each tape drive to the customer. This information can be obtained from the Sun Licensing center. The information is supplied to the drive via the VOP application to enable encryption activity on the drive The PC Key is used in 2.0, it is referred to as encryption enablement to the drive.

   b. The customer will then define the device to the KMS as an encrypting agent.

      **Note:** To accommodate drive replacement, we suggest naming the device with a unique characteristic, e.g., drive serial number or date. This name will show up in 2 places: on the drive as the Agent ID and in the KMS database as the Agent ID

      **Note**: Use the description field for other miscellaneous information pertinent to the site.

   c. Successful enrollment of the drive is indicated by a solid AMBER Encryption LED on the drive, and in KMS database as the drive has an Enrolled=True condition.

   The drive must be given a default key group from which encryption processing keys are obtained. Other key groups can be assigned to the drive for read purposes. A more indepth discussion on key management can be found in the KMS 2.0 StorageTek Cypto Key Management Solutions Management Practices white paper.

   a. When ever the drive is actively encrypting or decrypting the Encryption LED will be RED. This can be seen physically on the drive and in the VOP application when connected to the drive.
   b. The keys are obtained from the KMS cluster when the write or read operation occurs on the data unit.

   **Note:** If a drive loses power the keys will be lost on the drive, but the keys will remain in the KMS database in the KMS cluster.

8. Cause NCS to recognize encryption is enabled

   At this point, both VOP and SL8500 show encrypted drives but the HSC does not. You need to issue an HSC VARY ACS ,MODIFY LSM, or MODIFY CONFIG command for HSC to obtain the encrypted status of a drive.

   MODIFY LSM is recommended because it will cause all HSCs in the complex to become aware of a drive's new characteristics.

   **Note:** An HSC VARY or MODIFY will also be necessary should a drive be replaced. Verify your drive model numbers via the DISPLAY DRIVE command before proceeding.

# Chapter 4: Native Attach Recommendations

## Overview

To reiterate: NCS management of a mixed encryption solution is analogous to the management of a mixed 9940B and 9940A environment; with 9940B equivalent to encrypted and 9940A equivalent to non-encrypted.

## T10000 A Documentation excerpts

This chapter contains examples which depict a T10000A encryption implementation. The same concepts can be used for 9840D.

To aid in understanding the remainder of this chapter, there are now 4 new T10000A models/rectechs available. Two for native attach and two for VSM.

| HSC Model (Displayed) | Drive Description | HSC Rectech |
|---|---|---|
| T1A35 | T10000A - 3590 emulation (MVS attach) | T1A35 |
| T1AE35 | T10000A - 3590 emulation (MVS attach), with Encryption enabled | T1AE35 |
| T1A | T10000A - 3490 emulation (VSM attach only) | T1A34 |
| T1AE | T10000A - 3490 emulation (VSM attach only), with Encryption enabled | T1AE34 |

There are combination RECTECH values (not documented here) which are hierarchical in nature, but we strongly recommend you use one of the above as applicable.

## Media Management Strategy

A good media management strategy is a key piece to a successful mixed encryption solution. The segregation of non-encrypted and encrypted volumes via VOLATTR statements is highly recommended.

Do **not** specify a combination rectech such as VOLATTR RECTECH(T1A), as this allows a tape to be become either encrypted or non-encrypted. Although NCS can manage the volume, its encryption status is not available from the Volume Report. This simply leads to confusion later on.

### VOLATTR Control Statement

A combination of MEDIA and RECTECH is used to define a volume. The following MEDIA and RECTECH parameters are recommended for T10000A :

VOLATTR SERIAL(VOL000-VOL499) MEDIA(T1) RECTECH(T1A35) non-encrypted

VOLATTR SERIAL(VOL500-VOL599) MEDIA(T1) RECTECH(T1AE35) encrypted

## SCRPOOL Control Statement

If implemented, encrypted and non-encrypted drives should not share media from the same pool. These are defined by SCRPOOL statements as follows:

```
SCRPOOL  NAME=T10000,RANGE=(VOL000-VOL499),LABEL=SL        non-encrypted
SCRPOOL  NAME=T10000E,RANGE=(VOL500-VOL599),LABEL=SL       encrypted
```

# Drive Management Strategy

Various alternatives are available to influence SMC to choose an encrypted or non-encrypted device. Care must be taken to exclude encrypted devices from the non-encrypted workloads.

Select desired drive via the TAPEREQ MODEL parameter. For example:

```
TAPEREQ DSN(*.BACKUP.**)    MODEL(T1AE35)          encrypted
TAPEREQ DSN(*)              MODEL(T1A35)           non-encrypted
```

Select desired drive via the TAPEREQ ESOTERIC parameter. For example:

```
TAPEREQ DSN(*.BACKUP.**)    ESOTERIC(SL85006E)     encrypted
TAPEREQ DSN(*)              ESOTERIC(SL85006)      non-encrypted
```

Select desired drive via the TAPEREQ SUBPOOL parameter. For example:

```
TAPEREQ DSN(*.BACKUP.**)    SUBPOOL(T10000E)       encrypted
TAPEREQ DSN(*)              SUBPOOL(T10000)        non-encrypted
```

# SMC Allocation Matrix

The following matrix illustrates the drive type which should be selected based solely on a volume's recording technique and encryption status for both specific and scratch requests.

Some background on the fields might be helpful.

- ENCRYPTED: INVISIBLE indicates the ENCRYPTED status is not displayed in response to a DISPLAY VOLUME DETAIL command, therefore, the volume is NOT encrypted
- ENCRYPTED:UNKNOWN is the initial status of newly entered volumes.

  **Note:** Unless overridden by RECTECH, the default is for a volume to be encrypted.
- ENCRYPTED:YES indicates the volume has been or is destined to be encrypted
- RECTECH(T1A) is a "combination" recording technique and indicates the volume may be used on either an encrypted or unencrypted drive. This is NOT a recommended best practice, but may be encounter by customers with existing T10000A devices.

**Specific mount request:**

| VOLATTR | ENCRYPT:INVISIBLE | ENCRYPT:UNKNOWN | ENCRYPT:YES |
|---|---|---|---|
| RECTECH(T1A) | T1A35 & T1AE35 | T1AE35 | T1AE35 |
| RECTECH(T1A35) | T1A35 | T1A35 | T1AE35 |
| RECTECH(T1AE35) | T1AE35 | T1AE35 | T1AE35 |

**Note:** The encrypted status takes precedence over the recording technique for specific mounts.

**Note:** While a RECTECH(T1A35) and ENCRYPT:YES seems illogical, this situation would only be encountered when the RECTECH of the tape has been changed after the tape was used on an encrypted device.

**Scratch mount request:**

When a volume is mounted as scratch, the existing encrypted status is ignored and only the VOLATTR is honored.

# Examples

This section supplies screen shots of the mixed encryption solution implemented in the Mainframe Customer Emulation and Test lab, together with notes identifying pertinent information.

## NCS perspective

- A **DISPLAY DRIVES** command demonstrating the difference between encrypted and non-encrypted drives.

```
|SLS4633I DISPLAY DRIVES COMMAND
DRIVE LOCATION    VOLSER STATUS    MODEL     MEDIA
01B0  00:02:01:04 TTK031 DISMOUNT  T1A35     T1ALL
01B1  00:01:01:11 TTK030 DISMOUNT  T1A35     T1ALL
01B2  00:00:01:06 T12840 ON DRIVE  T1AE35    T1ALL
01B3  00:01:01:00 T12850 ON DRIVE  T1AE35    T1ALL
01B4  00:02:01:08 T12851 ON DRIVE  T1AE35    T1ALL
01B5  00:03:01:13 T12841 ON DRIVE  T1AE35    T1ALL
```

  **Note:** Drives 1B0-1B1 are non-encrypted
  Drives 1B2-1B5 are encrypted

- A **DISPLAY VOLUME DETAIL** command demonstrating the difference between encrypted and non-encrypted tapes.

  **Note:** The ENCRYPTED field is only displayed for encryption capable volumes and only in response to a DISPLAY VOLUME DETAIL command. It is only updated when the volume is dismounted after being used for a scratch request. It can contain two values, UNKNOWN and YES.

  - UNKNOWN is the initial status upon the volumes entry into the library.
  - YES indicates the volume has been written to on an encrypted drive.

```
|SLS0601I VOLUME TTK031 - DETAIL:
    HOME CELL:      00:02:10:14:00
    SCRATCH:        NO
    SELECTED:       NO
    MOUNTED:        DRIVE   1B0
    EXTERNAL LABEL: YES
    LABEL READABLE: YES
    INSERTED:       2008-03-10  10:29:40
    LAST SELECTED:  2008-03-24  08:10:59
    SELECT COUNT:   00000309
    MEDIA TYPE:     T10000T1
    RECTECH:        T1A35
    MEDIA LABEL:    READABLE
    MEDIA MATCH:    YES
    DENSITY:        T1A000T1
```

**Note:** The ENCRYPTED field is not displayed.

```
|SLS0601I VOLUME T12858 - DETAIL: 089:
    HOME CELL:      00:01:02:03:00
    SCRATCH:        NO
    SELECTED:       NO
    EXTERNAL LABEL: YES
    LABEL READABLE: YES
    INSERTED:       2008-01-24  10:12:12
    LAST SELECTED:  2008-03-22  11:42:23
    SELECT COUNT:   00000001
    MEDIA TYPE:     T10000T1
    RECTECH:        T1AE35
    MEDIA LABEL:    READABLE
    MEDIA MATCH:    YES
    DENSITY:        T1A000T1
    ENCRYPTED:      UNKNOWN
```

**Note:** The ENCRYPTED field is UNKNOWN

```
|SLS0601I VOLUME T12840 - DETAIL:  230
    HOME CELL:      00:00:02:00:00
    SCRATCH:        NO
    SELECTED:       NO
    EXTERNAL LABEL: YES
    LABEL READABLE: YES
    INSERTED:       2007-01-10  10:28:50
    LAST SELECTED:  2007-01-24  07:38:29
    SELECT COUNT:   00000333
    MEDIA TYPE:     T10000T1
    RECTECH:        T1AE35
    MEDIA LABEL:    READABLE
    MEDIA MATCH:    YES
    DENSITY:        T1A000T1
    ENCRYPTED:      YES
```

**Note:** The ENCRYPTED field is YES

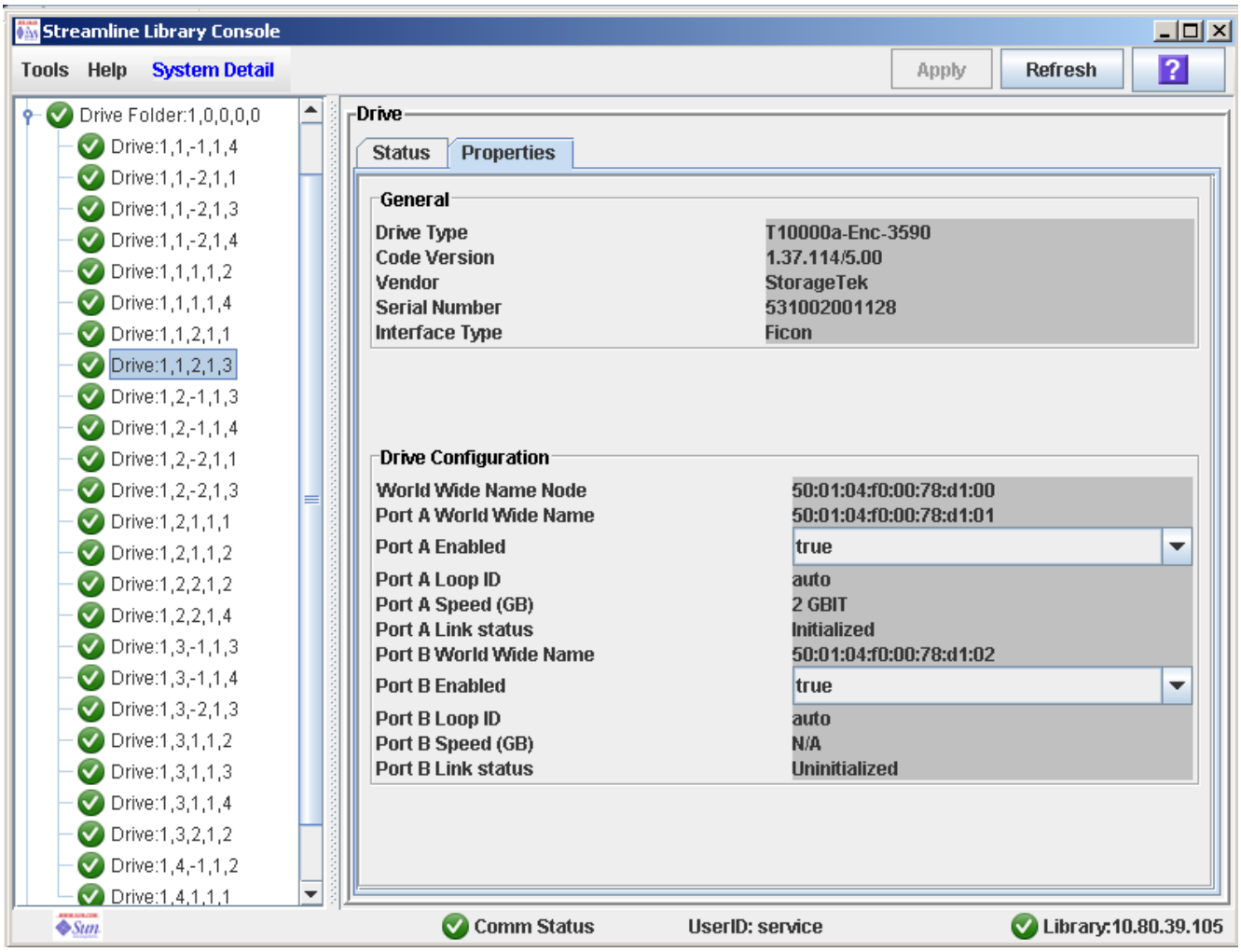
After a volume has been mounted as scratch on an encrypting drive, a specific mount for that volume will always be directed to an encrypting drive and CANNOT be overridden by a VOLATTR. If the volume's encrypted status is unknown or non-encrypted, the VOLATTR

recording technique is always honored. When a volume is mounted as scratch the VOLATTR is always honored.

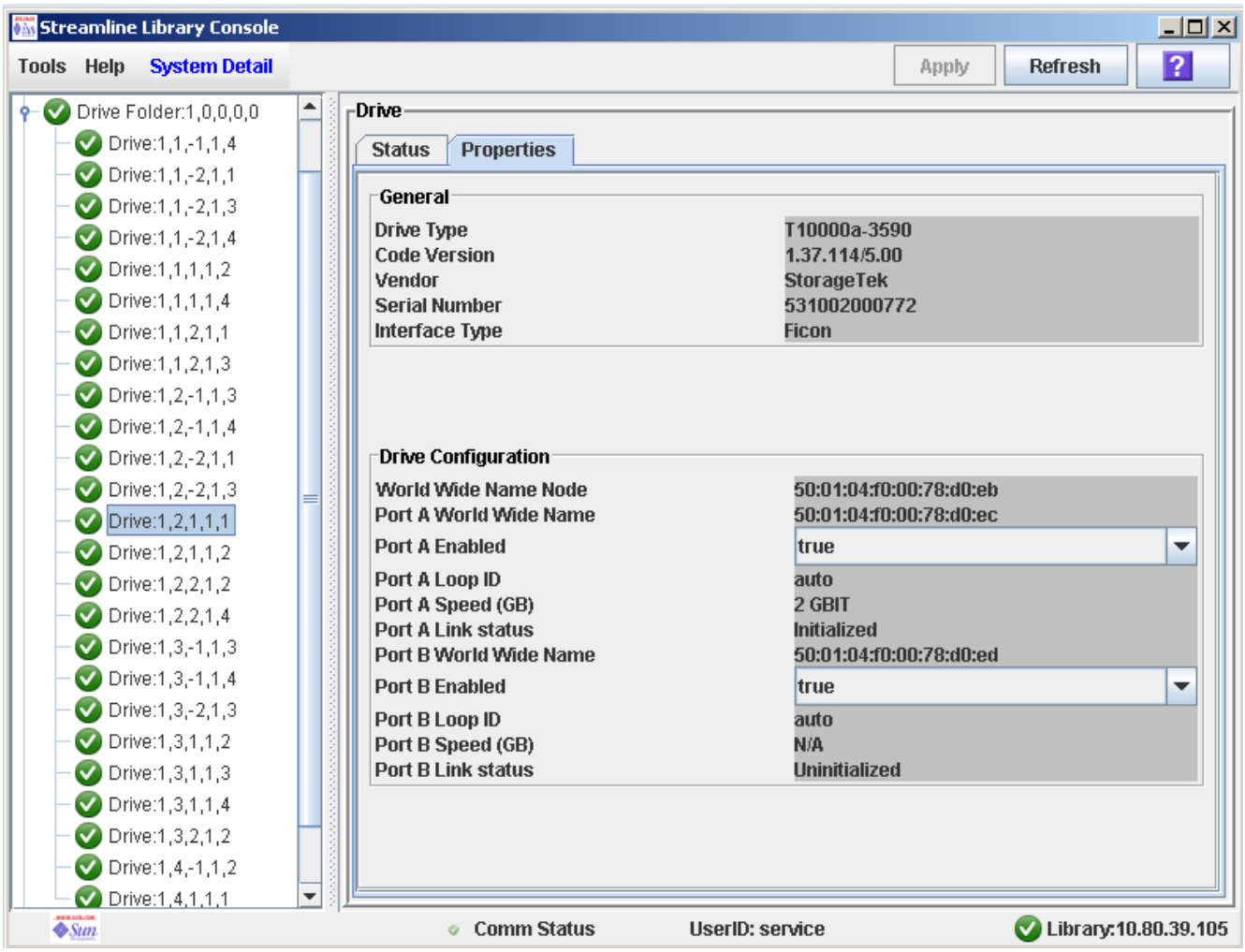
## SL8500 perspective

- Drive display demonstrating the difference between encrypted and non-encrypted drives.

**Encrypted drive – as determined from Drive Type field.**



**Non-Encrypted drive – as determined from Drive Type field.**



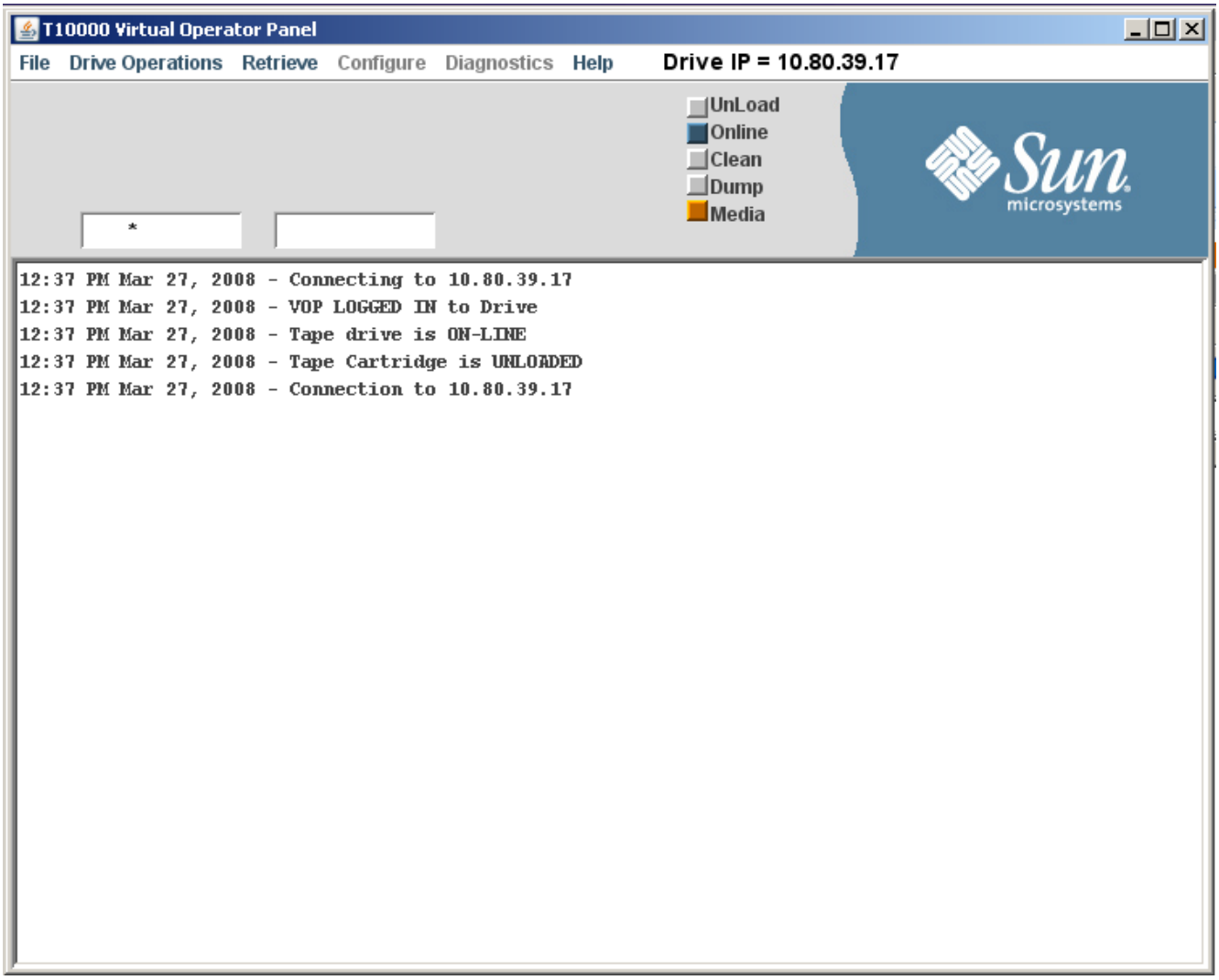

**Note:** When a drive is initially installed, it is non-encrypted by default. Only when you enable encryption via the VOP application does it identify itself as an encrypted device. Only then can the library indicate to HSC the drive is encrypted.

HSC does not poll the drive status. Rather, it is queried by four main events; HSC initialization, ACS Vary processing, LSM Vary processing, and MODIFY CONFIG processing.

## VOP perspective

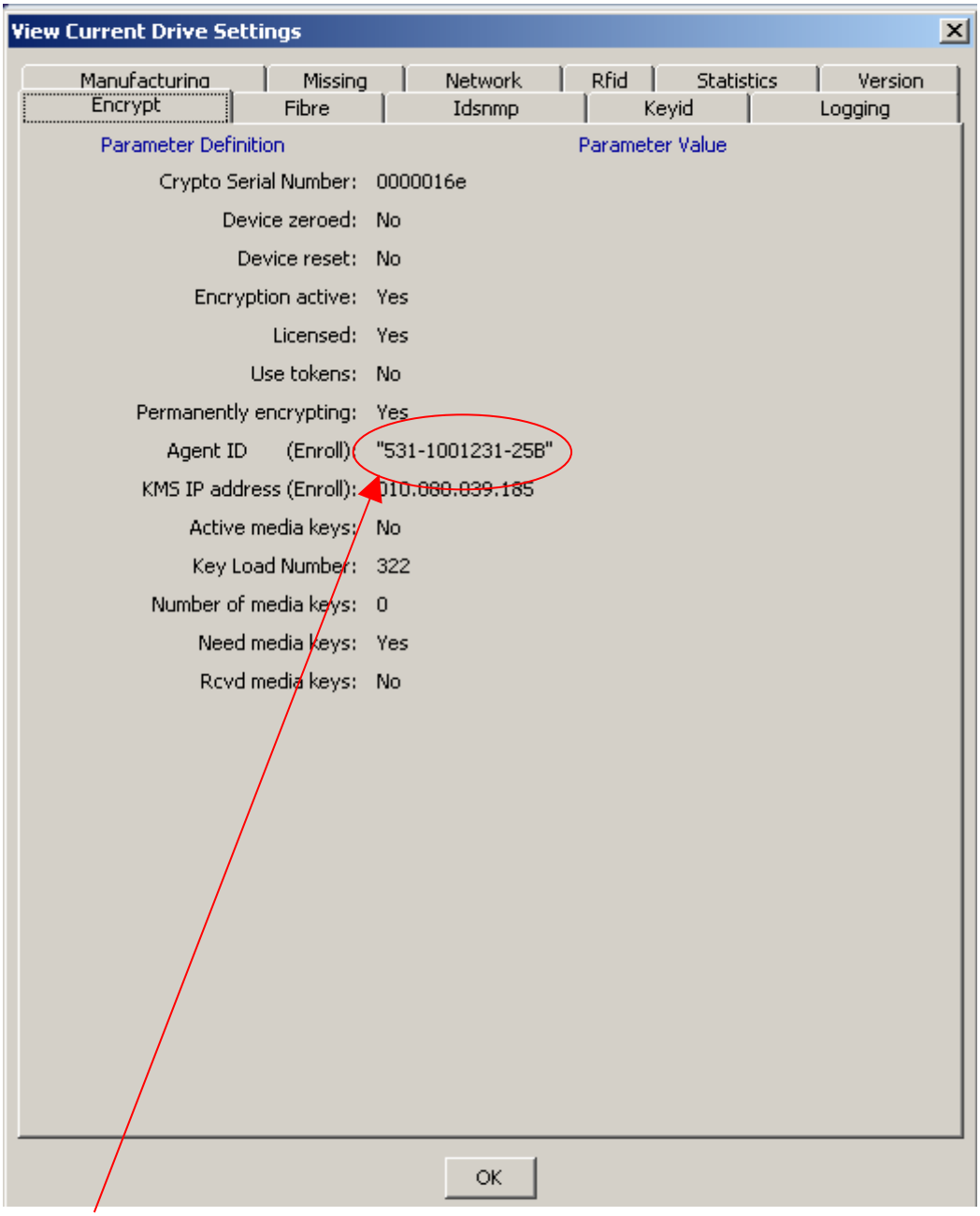
- Drive displays demonstrating an encrypted drive.

**General VOP display**

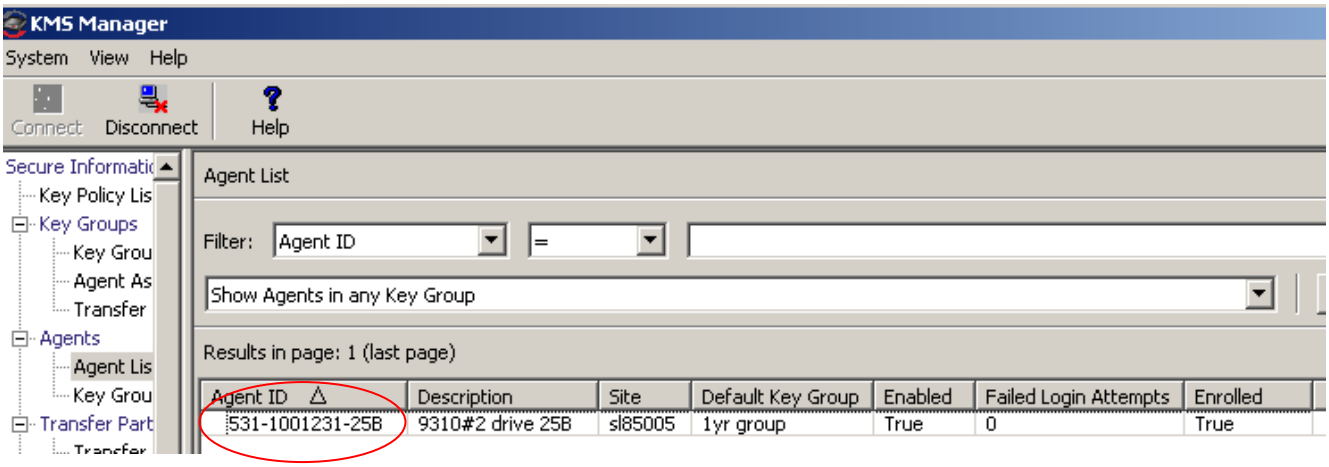



**Note:** When a drive is initially installed, it is non-encrypted by default. Only when you enable encryption via the VOP application does the Media indicator appear. It then displays identically to the Encryption LED on the drive itself.

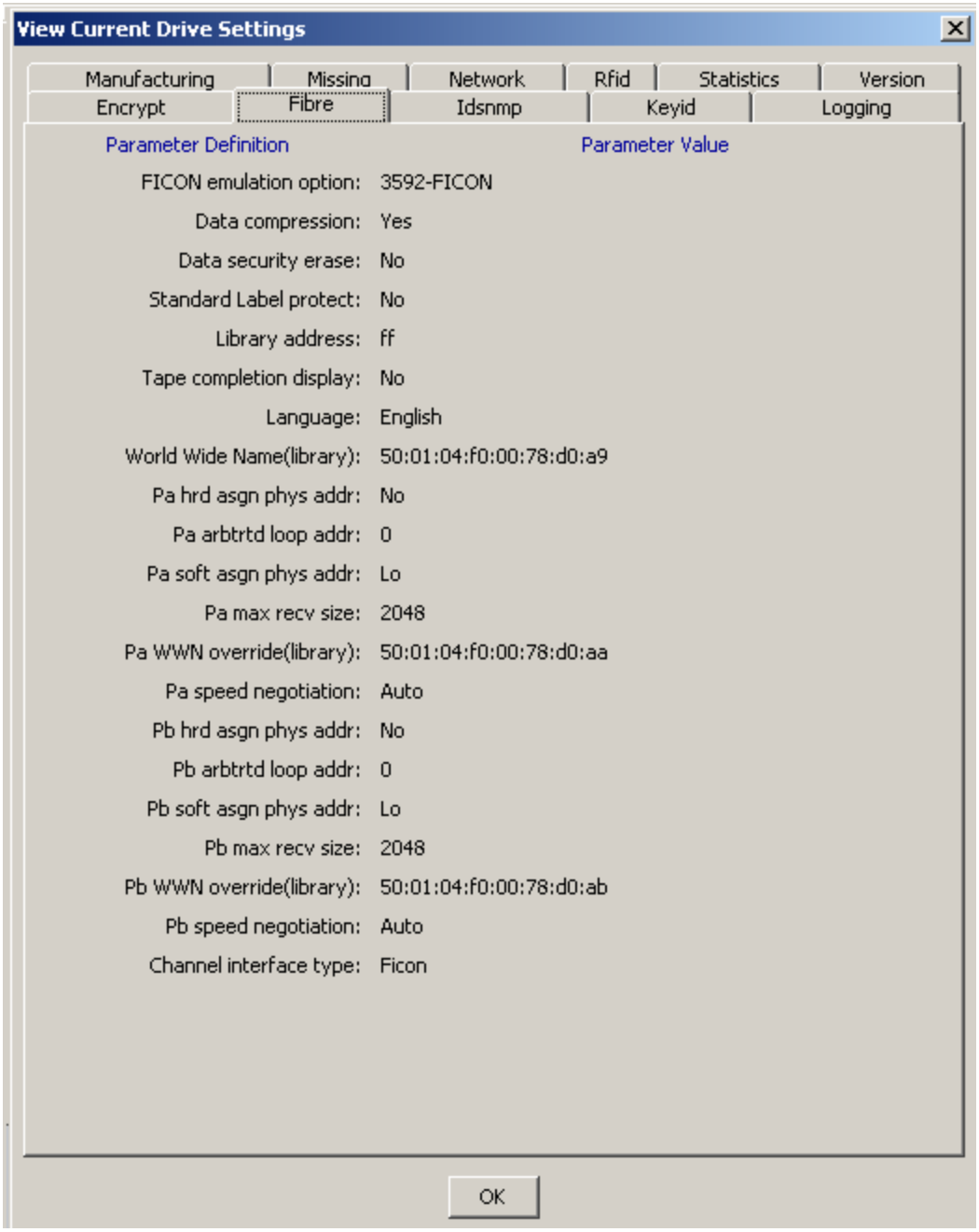
**Detail VOP in response to Review->Drive Settings->Encrypt**




Agent ID must match the KMS Agent ID

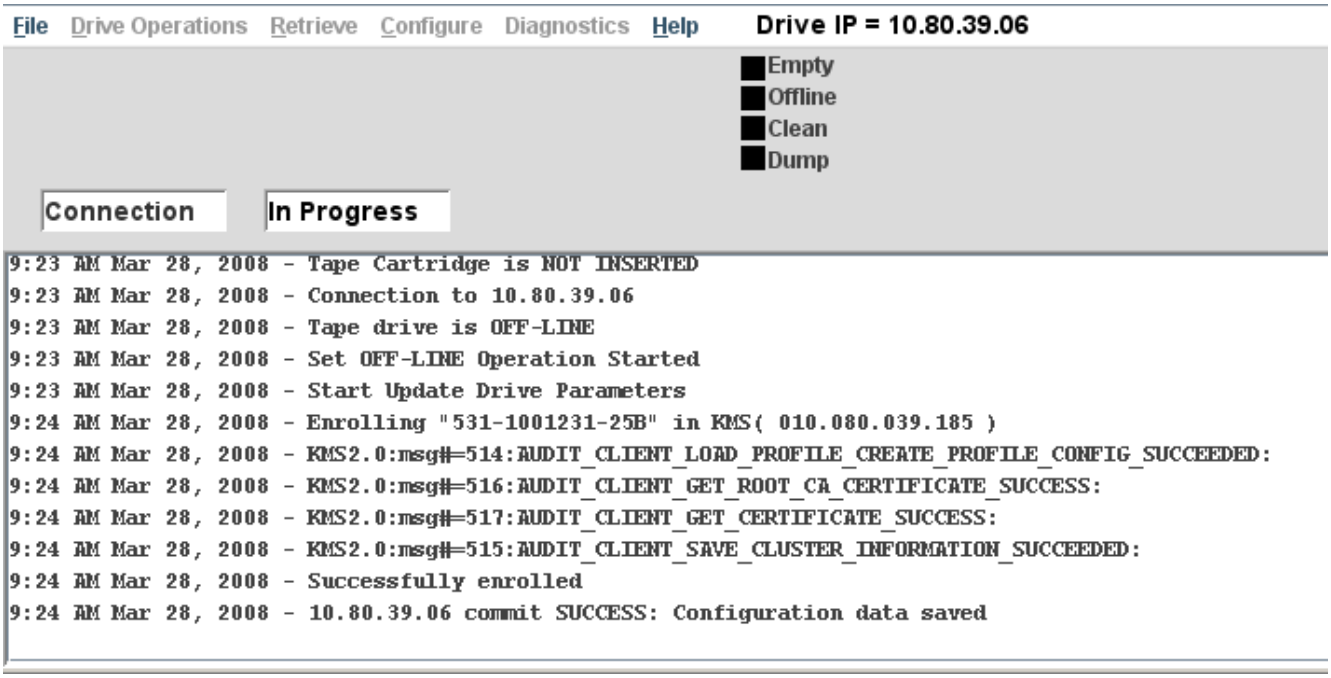


**Detail VOP in response to Review->Drive Settings->Fibre**



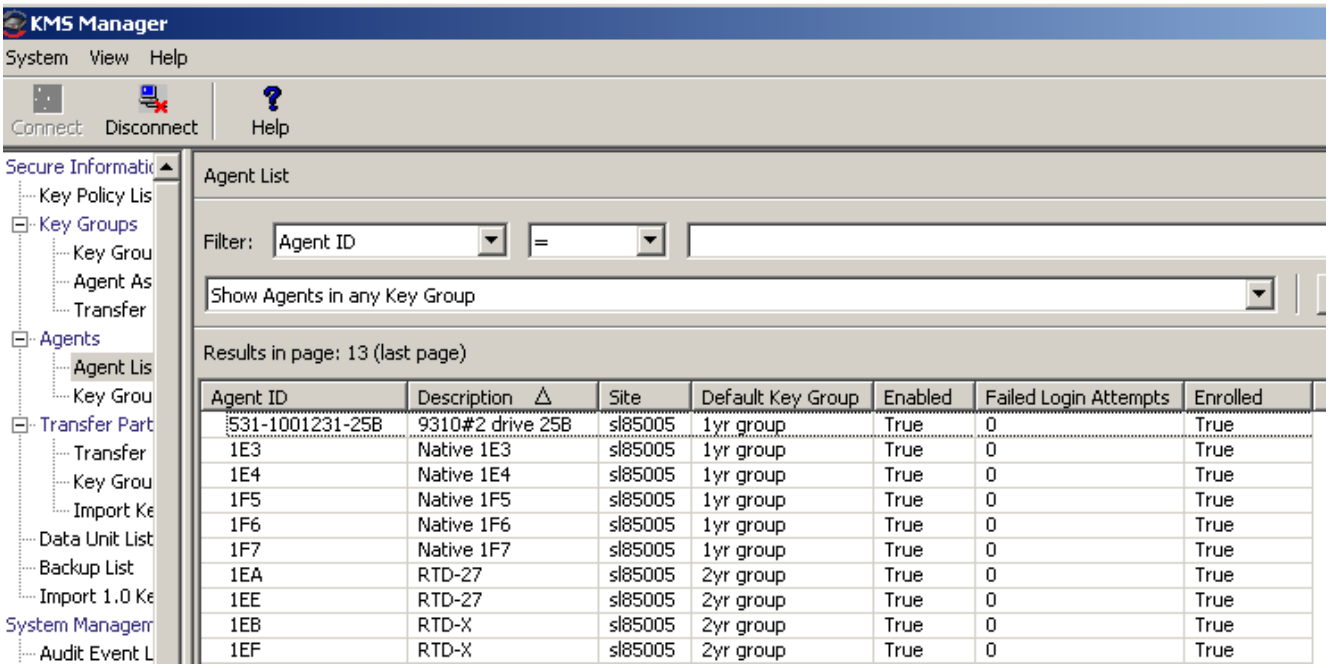

**Note:** Native attached drives can only be configured in 3592-FICON mode.

**Detail VOP in response to Commit of enrollment of drive**



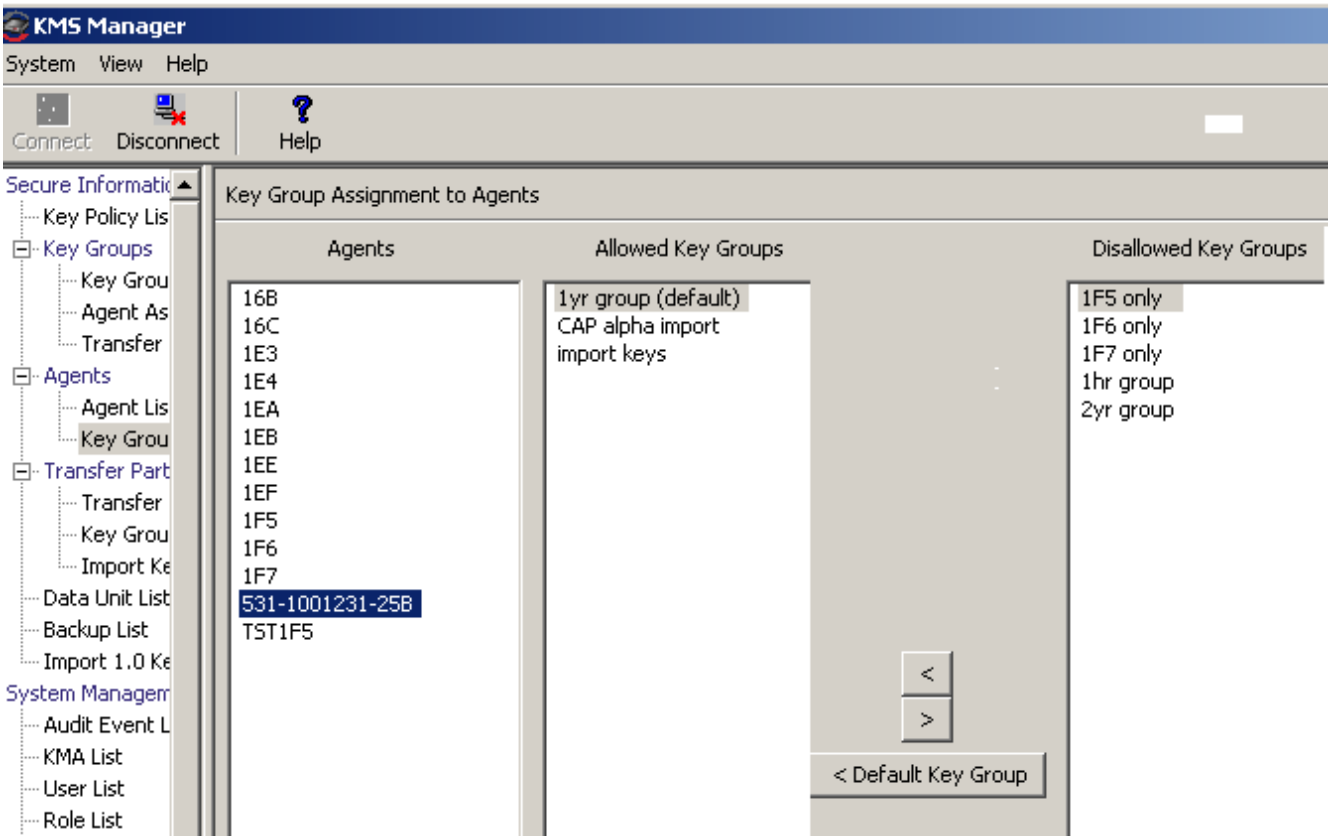

## KMS perspective

- Drives in Agent List panel



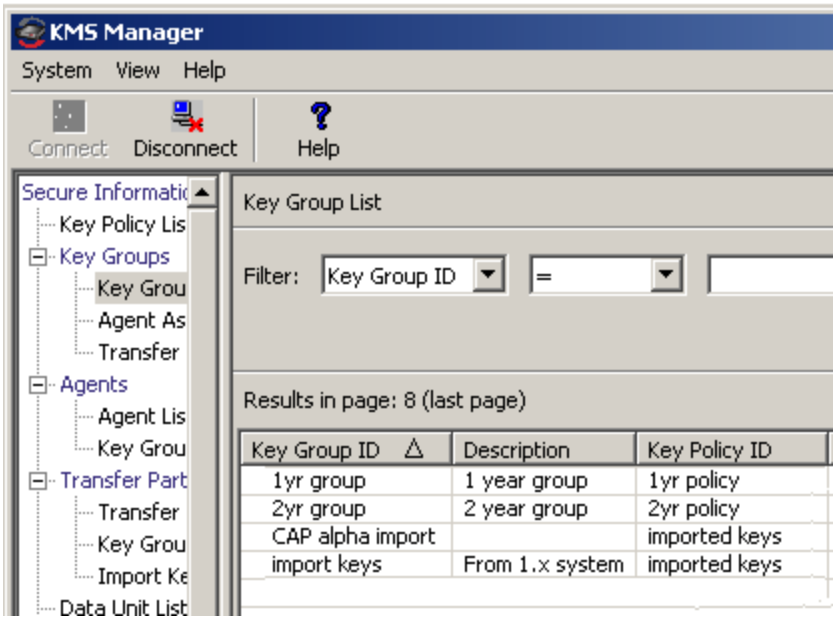

**Note**: Remember Agent ID must match what has been entered and commited on the drive.

Drives assigned to key group(s)



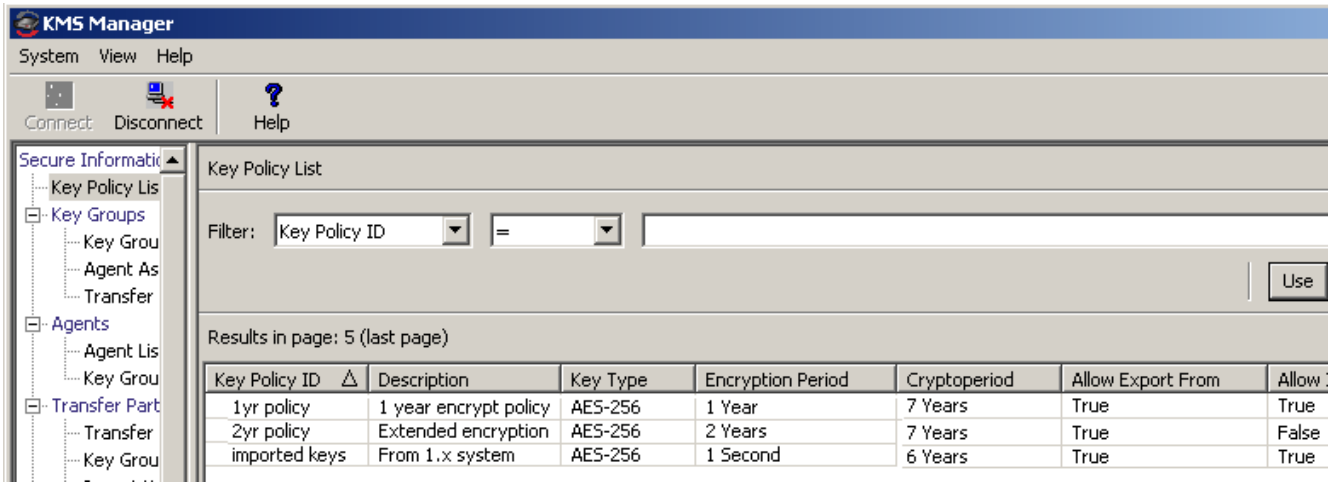

**Note**: The drive can have several key groups assigned to it. Thus, dataunits written with any keys from the allowed key groups can be read on the drive. If a new dataunit is presented the KMS will create a key from the default key group and assign the key to the dataunit.

- Key group mapped to key policy



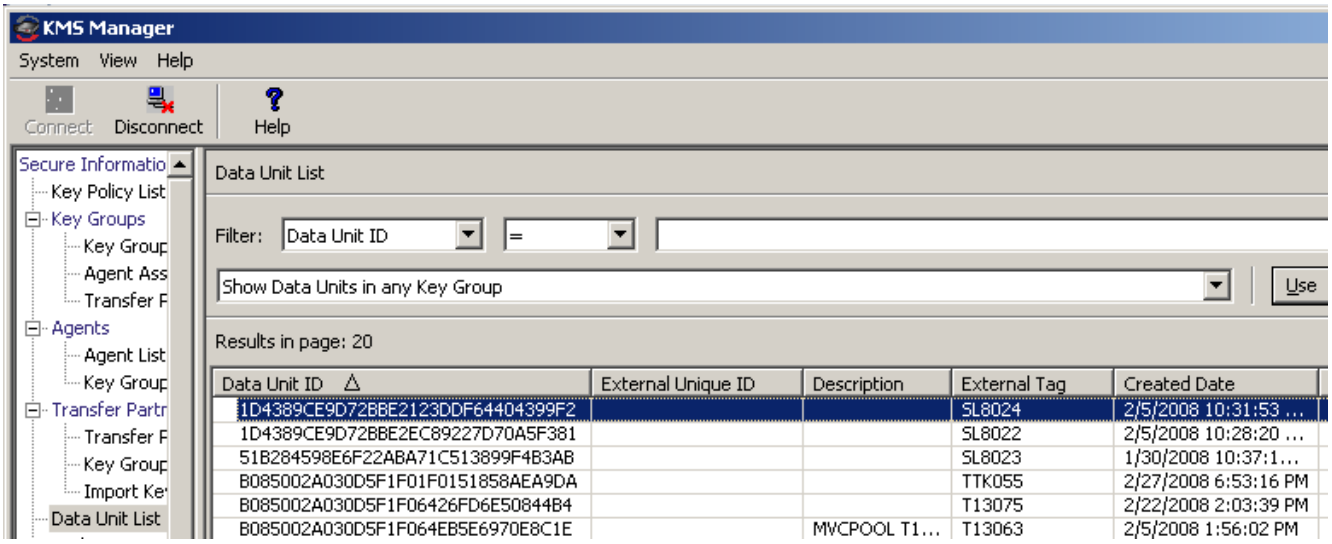

**Note**: The key group has a policy for encryption process period, cypto period, export and import status. Any particular key resides in one group only.

- Key policies, which were in turn assigned to key group(s)

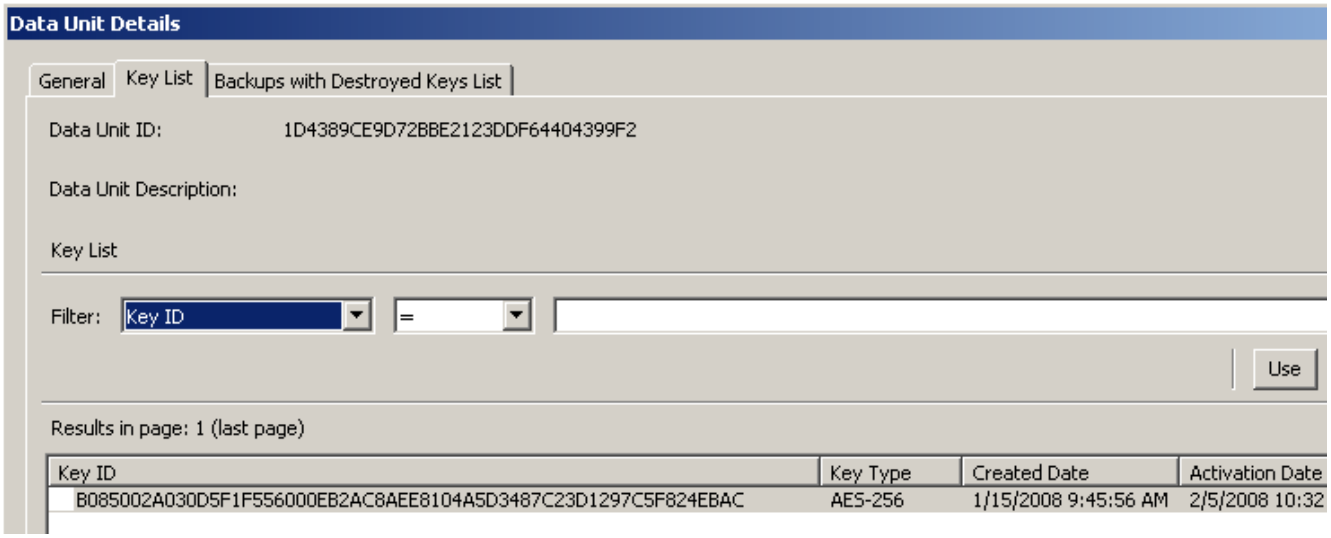


- Key for a particular data unit:

List of data units:




Details for data unit (volser):




**Note:** The actual key is never observed, however the keyid is viewable.

**Note**: The keyid cannot change because it is tied directly to the actual key. The keyid is encrypted on the tape, and no 2 data units can ever have the same keyid.

# Chapter 5: VSM Attach Recommendations

## Overview

To reiterate: VTCS management of a mixed encryption solution is analogous to the management of a mixed 9940B and 9940A environment; with 9940B equivalent to encrypted and 9940A equivalent to non-encrypted. It is strongly recommended that all volumes be defined specifically

It is possible to direct migration to encrypted drives via the MEDIA and/or MVCPOOL parameters of the STORCLAS statement.

This chapter contains examples which depict a 9840D encryption implementation. The same concepts can be used for T10000A.

## 9840D Documentation excerpts

To aid in understanding the remainder of this document, the following table identies the new Model and RECTECH values.

| HSC Model (Displayed) | Drive Description | Recommended HSC Rectech |
|---|---|---|
| T9840D | 9840D - 3490 emulation | STK1RD34 |
| T9840D35 | 9840D - 3590 emulation | STK1RD35 |
| T9840DE | 9840D - 3490 emulation - Encrypted | STK1RDE4 |
| T9840DE35 | 9840D - 3590 emulation - Encrypted | STK1RDE5 |

For completeness, the full list of available values are identified below. There are “combination” RECTECH values, which are hierarchical in nature, but we strongly recommend you use one of the above as applicable.

| | | |
|---|---|---|
| MEDIA values: | STK1R | data cartridge |
| | STK1Y | new cleaning cartridge unique to 9840D |
| RECTECH values: | STK1R | all 9840 drives |
| | STK1RD | all 9840D drives |
| | STK1RDE | all 9840D encrypted drives |
| | STK1RDN | all 9840D non-encrypted drives |
| | STK1RD34 | 9840D non-encrypted 3490 drive |
| | STK1RD35 | 9840D non-encrypted 3590 drive |
| | STK1RDE4 | 9840D encrypted 3490 drive |
| | STK1RDE5 | 9840D encrypted 3590 drive |
| STORCLAS media: | STK1RD | 9840D non-encrypted media |
| | STK1RDE | 9840D encrypted media |

# Media Management Strategy

A good media management strategy is a key piece to a successful mixed encryption solution. The segregation of non-encrypted and encrypted volumes via VOLATTR statements is highly recommended.

## Media

The 9840D utilizes the same media as previous 9840 drives, however, a new cleaning cartridge has been introduced.

| | | |
|---|---|---|
| MEDIA values: | STK1R | data cartridge |
| | STK1Y | new cleaning cartridge unique to 9840D |

## Recording Technique

Although the media is physically identical, they are logically differentiated because of the recording technique used when writing to the media.

The following recording techniques apply to a VSM attached 9840D:

- Non-encrypted - STK1RDN or STK1RD34
- Encrypted - STK1RDE or STK1RDE4

Where a recording technique is not specified, a default of non-encrypted applies. It follows that the recording technique must be specified for encrypted media.

## VOLATTR Control Statement

A combination of MEDIA and RECTECH is used to define a volume. The following MEDIA and RECTECH parameters are recommended for 9840D so there is no doubt about your intentions for the volume. It will also be your only indication regarding encryption when displaying volume information via a Volume Report.

9840D Non-encrypted:

VOLATTR SERIAL(vvvvvv-vvvvvv) MEDIA(STK1R) RECTECH(STK1RD34)

9840D Encrypted:

VOLATTR SERIAL(vvvvvv-vvvvvv) MEDIA(STK1R) RECTECH(STK1RDE4)

## Special VTCS Considerations for 9840D Media

T9840D and T9840DE transports use the **same physical form factor** but **different recording techniques** as follows:

- T9840DEs can read from media written to by T9840Ds, but cannot write to T9840DE media **unless** the entire volume is rewritten from beginning of tape.
- T9840Ds cannot read from or write to media written to by T9840DEs.

To ensure media and transport compatibility, you **must use** separate VOLATTR statements to segregate non-encrypted and encrypted media as follows:

- Define the T9840D (non-encrypted) media with VOLATTR statements that specify MEDIA(STK1R) **and** RECTECH(STK1RD34).
- Define the T9840DE (encrypted) media with VOLATTR statements that specify MEDIA(STK1R) **and** RECTECH(STK1RDE4).

For example, to define MVCs MVC000-MVC499 as non-encrypted volumes and MVCs MVC500-MVC999 as encrypted volumes, create the following VOLATTR statements:

VOLATTR SERIAL(MVC000-MVC499) MEDIA(STK1R) RECTECH(STK1RD34)

VOLATTR SERIAL(MVC500-MVC999) MEDIA(STK1R) RECTECH(STK1RDE4)

### MVCPOOL Control Statement

If implemented, encrypted and non-encrypted drives should not share media from the same pool. These are defined by SCRPOOL statements as follows:

```
MVCPOOL  NAME=T9840D,RANGE=(VOL000-VOL499)      non-encrypted only
MVCPOOL  NAME=T9840DE,RANGE=(VOL500-VOL599)     encrypted only
```

## Drive Management Strategy

The MEDIA parameter of the STORCLAS control statement can be used to direct migration to classes of drives.

### STORCLAS Control Statement

The following MEDIA values defined within the MGMT class are required to utilize 9840media :

STOR NAME(nnnn..) MEDIA(STK1RD, …)  - 9840D non-encrypted

STOR NAME(nnnn..) MEDIA(STK1RDE, …)  - 9840D encrypted

### Control Statement Interaction

This example demonstrates the flow of TAPEREQ, MGMTCLAS and STORCLAS control statements which direct migration to encrypted drives:

TAPEREQ JOB(jobname) MGMTCLAS(ENCRYPT)

MGMTCLAS NAME(ENCRYPT) STORCLAS(S1)

STORCLAS NAME(S1) MEDIA(STK1RDE)

# Examples

## NCS perspective

- An HSC **Display VOLume DETAIL** command of an encrypted MVC.

```
SLS0601I VOLUME M04150 - DETAIL:  321
   HOME CELL:      00:02:07:00:01
   SCRATCH:        NO
   SELECTED:       NO
   EXTERNAL LABEL: YES
   LABEL READABLE: YES
   INSERTED:       2007-05-03  10:43:53
   LAST SELECTED:  2008-05-20  05:37:21
   SELECT COUNT:   00000488
   MEDIA TYPE:     STK1R
   RECTECH:        STK1RDE4
   MEDIA LABEL:    READABLE
   MEDIA MATCH:    YES
   NOT ELIGIBLE FOR SCRATCH
   DENSITY:        UNKNOWN
```

**Note:** RECTECH is the only indication the volume is encrypted and this is because of the VOLATTR specification.

- An HSC **Display DRives ALL DETail** command

```
|SLS4633I DISPLAY DRIVES COMMAND  604
DRIVE LOCATION    VOLSER STATUS    MODEL     MEDIA
0120  00:00:01:15        ONLINE    T9840C    STK1
0121  00:03:01:12        ONLINE    T9840C    STK1
0122  00:02:01:15        ONLINE    T9840B    STK1
0123  00:01:01:15        ONLINE    T9840B35  STK1
0124  00:02:01:12        ONLINE    T9840C35  STK1
0125  00:01:01:03        ONLINE    T9840C35  STK1
0126  00:01:01:01        OFFLINE   T9940B    STK2
0127  00:02:01:03        OFFLINE   T9940B    STK2
0128  00:01:01:13        OFFLINE   T9840DE   STK1
0129  00:02:01:00 M04153 ON DRIVE  T9840DE   STK1
012A  00:03:01:00        ONLINE    T9940B35  STK2
012B  00:00:01:03        ONLINE    T9940B35  STK2
012C  00:00:01:12 M04111 ON DRIVE  T9840D    STK1
012D  00:00:01:00 M04109 ON DRIVE  T9840D    STK1
012E  00:03:01:15        OFFLINE   T9840D35  STK1
012F  00:03:01:03        OFFLINE   T9840D35  STK1
```

**Note**: Drives 128-129 are encrypted RTDs and 12C-12D are non-encrypted.

## VTCS perspective

A VTCS **Display MVC** command

```
SLS6603I MVC M04150 INFORMATION:  756
 VOLSER:                M04150
 MEDIA:                 STK1RDE
 ACSID:                 00
 SIZE(MB):              75000
 MIGRATED COUNT:        207
 VTV COUNT:             207
 %USED:                 98.06
 %FRAGMENTED:           0.00
 %AVAILABLE:            1.94
 %USABLE:               0.00
 TIMES MOUNTED:         443
 LAST MOUNTED:          2008MAY20 05:37:43
 LAST MIGRATION:        2008MAY20 04:41:42
 LAST DRAIN/RECLAIM:    2008MAY19 15:45:16
 OWNER:                 VTSSU
 MVCPOOL:               DEFAULTPOOL
 SECURITY ACCESS:       NO PROFILE
 STATUS:                INITIALIZED

                        MARKED FULL
```

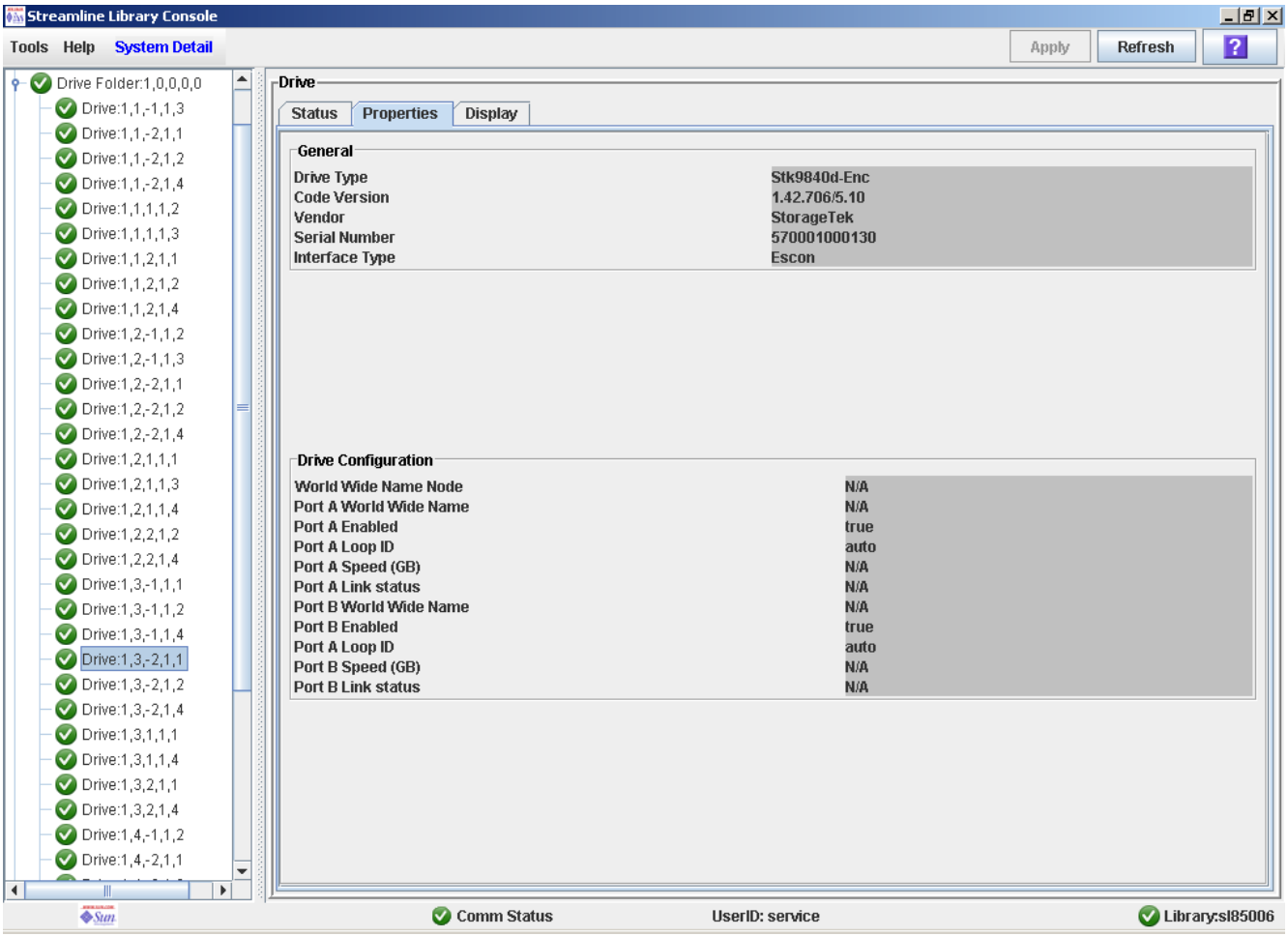
**Note:** MEDIA:STK1RDE indicates volume is intended for use on an encrypted drive.

- A VTCS **Display CONFIG** command demonstrating the difference between encrypted and non-encrypted drives.

```
SLS6603I CONFIGURATION INFORMATION  448
MAXVTV  MVCFREE  VTVATTR  RECALWER  REPLICAT  VTVPAGE  SYNCHREP
 32000      1    ALLMOUNT YES       ALWAYS    STANDARD NO

 MAXRTDS  FASTMIGR
 16       NO

CDS LEVEL SUPPORT:  V5/5.1  V6  V6.1 V6.2
                                  *    *

RECLAIM : THRESHOLD  MAX MVC  START  CONMVC
            40         40      35       3

         AUTO MIGR THR  MIGR TASKS  DEFAULT  VSM   2GB/  PAGE
VTSSNAME  LOW  HIGH     MIN   MAX     ACS   MODEL  4GB   SIZE
VTSSS      70    80       6     6      FF     3    YES   LARGE
VTSSU      70    80       6     6      FF     4    YES   LARGE

DEVNO  RTD TYPE  ACS  RETAIN  VTSSNAME  RTD NAME  CHANIF
0120   STK1RC34   00    1     VTSSS     0120840C  00  0A
0121   STK1RC34   00    1     VTSSS     0121840C  01  0E
0126   STK2PB34   00    1     VTSSS     0126940B  04  1A
0127   STK2PB34   00    1     VTSSS     0127940B  05  1E
0128   STK1RDE4   00    1     VTSSS     0128840D  02  0I
                             VTSSU     0128840D  05  0L
0129   STK1RDE4   00    1     VTSSS     0129840D  03  0M
                             VTSSU     0129840D  09  1L
012C   STK1RD34   00    1     VTSSS     012C840D  06  1I
                             VTSSU     012C840D  04  0K
012D   STK1RD34   00    1     VTSSS     012D840D  07  1M
                             VTSSU     012D840D  08  1K
01BC   T1AE34     00    1     VTSSU     01B0T10K  00  0E
01BD   T1AE34     00    1     VTSSU     01B1T10K  02  0G
01BE   T1A34      00    1     VTSSU     01B6T10K  06  1E
01BF   T1A34      00    1     VTSSU     01B7T10K  07  1G
0228   STK1RD34   00    1     VTSSU     0228840D  01  0F
0229   STK1RD34   00    1     VTSSU     0229840D  03  0H
```

## SL8500 perspective

- Drive display demonstrating an encrypted VSM attached drive. Note the Drive Type field.

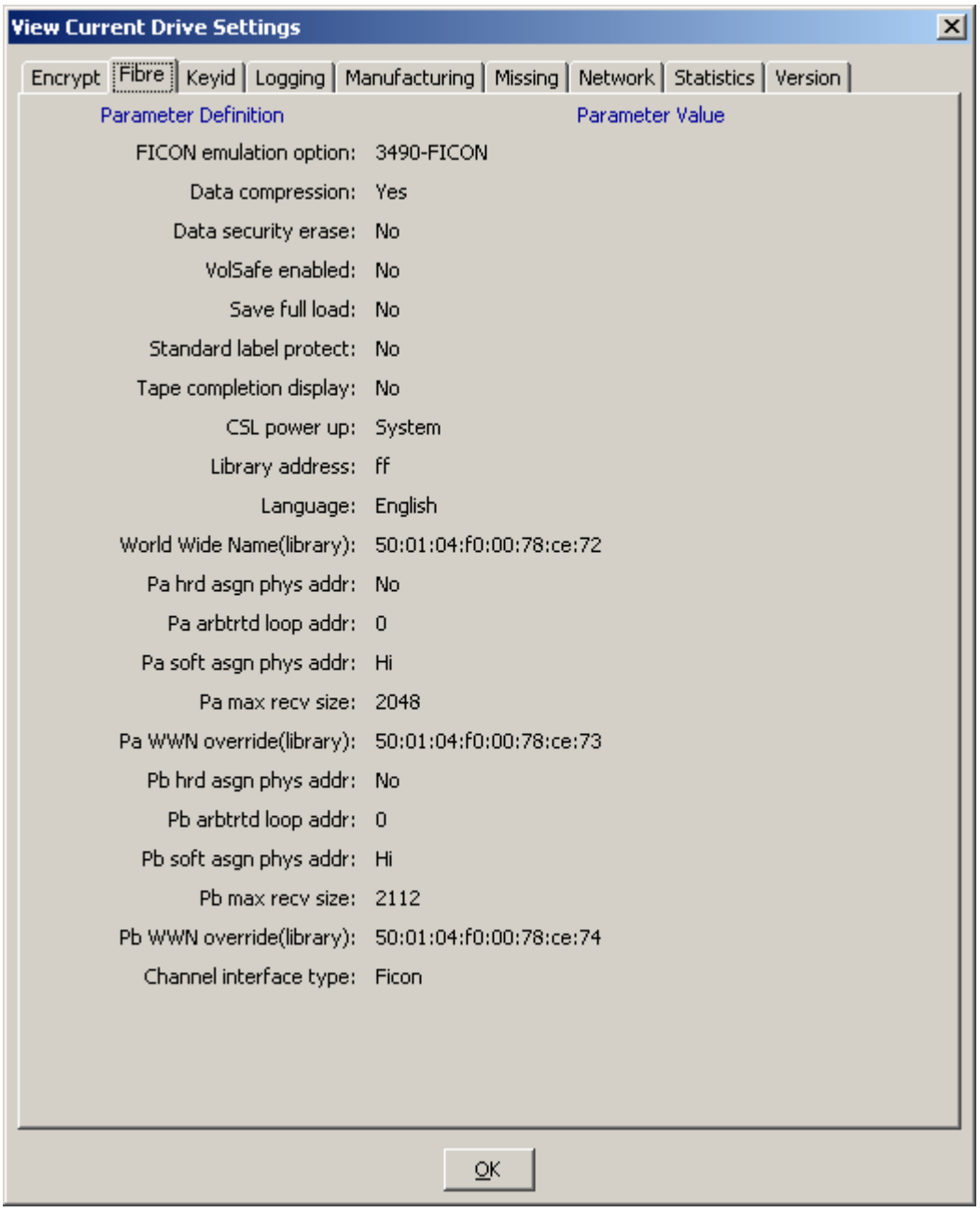



**Note:** When a drive is initially installed, it is non-encrypted by default. Only when you enable encryption does it identify itself as an encrypted device. Only then can the library indicate to HSC the drive is encrypted.

HSC does not poll the drive status. Rather, it is queried by four main events; HSC initialization, ACS Vary processing, LSM Vary processing, and MODIFY CONFIG processing.

## VOP perspective

- **Detail VOP in response to Review->Drive Settings->Fibre**




**Note:** VSM attached drives can only be configured in 3490 mode. Also, be aware that a Pa Max Recv Size of 2048 is required.

# Chapter 6: Miscellaneous Items

## Encryption Error Scenarios and Recovery

The following scenarios document the external manifestations of poor key management. To recover, it is important to understand how not having the required key when recalling data is presented at the host. This is done by examining the Fault Symptom Code (FSC) in the sense information presented by the drive. The FSC definitions can be obtained via the VOP.

Once the error has been determined, recovery steps are suggested.

### Scenario 1 – Drive does not contain necessary key to read an encrypted tape.

This scenario might be encountered if a key is assigned to a key group that the drive being used was not allowed to access.Disaster recovery situations will encounter this when the proper key groups are not assigned to the drive.

- Host Symptom:

  Bypass Label Processing:

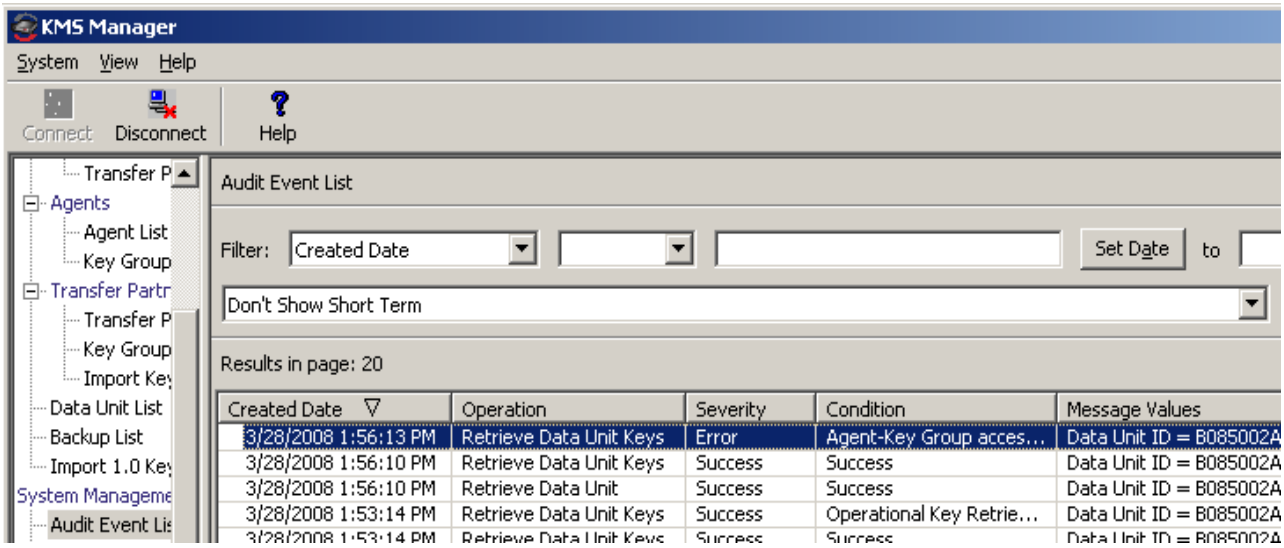
```
IEC501A M 01F6,T13103,BLP,COMP,HSC6GENR,STEP1, SYS08088.T135456.R
A000.HSC6GENR.R06
IOS000I 01F6,B6,IOE,06,0600,,**,T13103,HSC6GENR  963
 004910D050205451 2506FF30C00032D0 E3F1F3F1F0F30290 4104230012422011
 UNSUPPORT FORMAT
IGF500I  SWAP 01F6 TO 0124 - I/O ERROR
IEF196I IGF500I  SWAP 01F6 TO 0124 - I/O ERROR
3580 IGF500D  REPLY 'YES', DEVICE, OR 'NO'
```

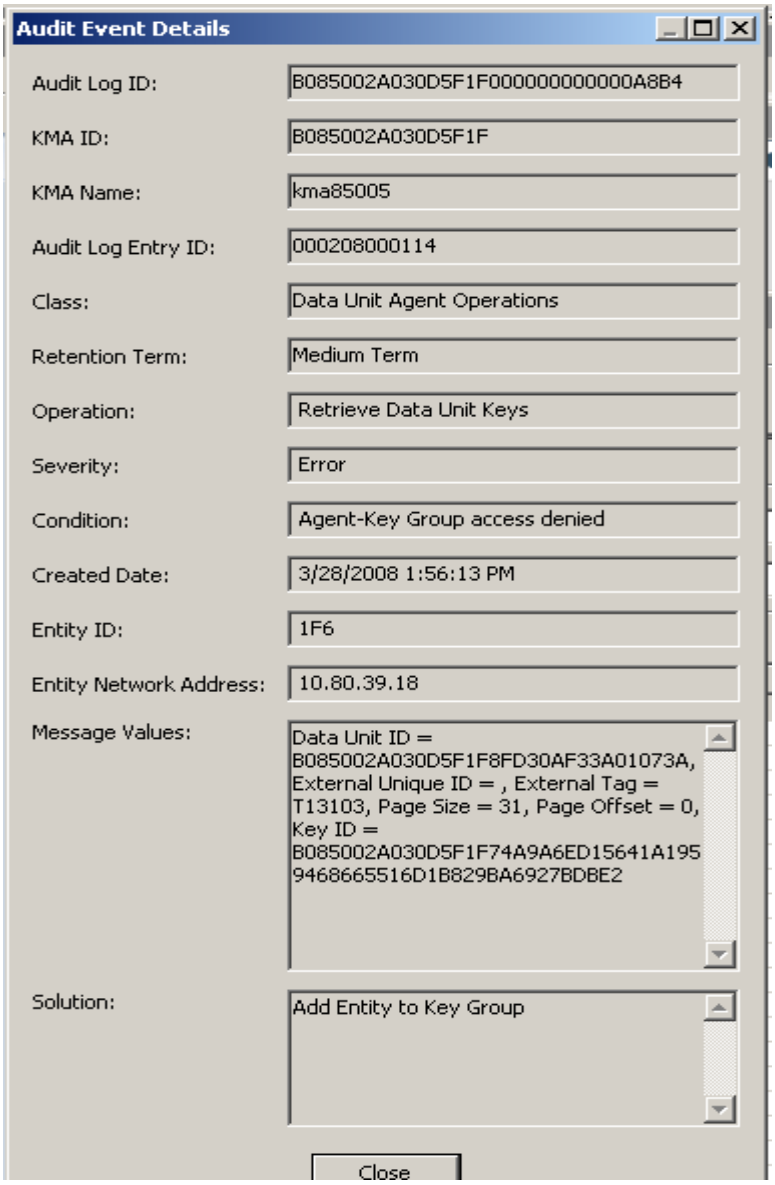
  Standard Label Processing:

```
IEC501A M
01F6,T13103,SL,,HSC6TST6,K1READ,IOP.SR7196MG.AL.FILE76.TAPE.MULT.ZIP0
IOS000I 01F6,B6,IOE,02,0600,,**,,HSC6TST6  443
 004910D050205451 2502FF30C00032D0 E3F1F3F1F0F30290 4104230012422011
 UNSUPPORTED FORMAT
IEC512I I/O ERR 01F6,
,NL,HSC6TST6,K1READ,IOP.SR7196MG.AL.FILE76.TAPE.MULT.Z
IEC502E R 01F6,,     ,NL,HSC6TST6,K1READ
IEC501A M
01F6,T13103,SL,,HSC6TST6,K1READ,IOP.SR7196MG.AL.FILE76.TAPE.MULT.ZIP0
SLS1075D DISMOUNT OF T13103 FROM DRIVE 01F6 - ERROR ON TAPE; IGNORE OR
EJECT (I/E)
SLS0088D MOUNT OF T13103 ON DRIVE 01F6 - INTERVENTION REQUIRED; MOUNT OR
IGNORE (M/I)
```

**Note:** FSC **32D0** indicates the key is missing in order to read the encrypted tape. Only reply YES to IGF500I message if you know that the TO device has access to keys on tape during the BLP tape processing.

- KMS Symptom:




**Note:** Each time the drive attempts to read the tape and the key is not available another audit event will be generated.

- Recovery Steps for BL processing:
  - ✓ Reply NO to message IFG500I to dismount tape and end application job.
  - ✓ Assign drive to correct key group. Research must be done in the KMS using the GUI to assertain what tape volume (data unit) was mounted, which key is being requested, which key group that key resides in.
  - ✓ Resubmit application job.
- Recovery Steps for SL processing:
  - ✓ R (I)gnore to message SLS1075D to dismount tape.
  - ✓ Assign drive to correct key group. Research must be done in the KMS using the GUI to assertain what tape volume (data unit) was mounted, which key is being requested, which key group that key resides in.
  - ✓ Reply to (M)ount to message SLS0088D.

## Scenario 2 – Key has been destroyed, thus label is not read

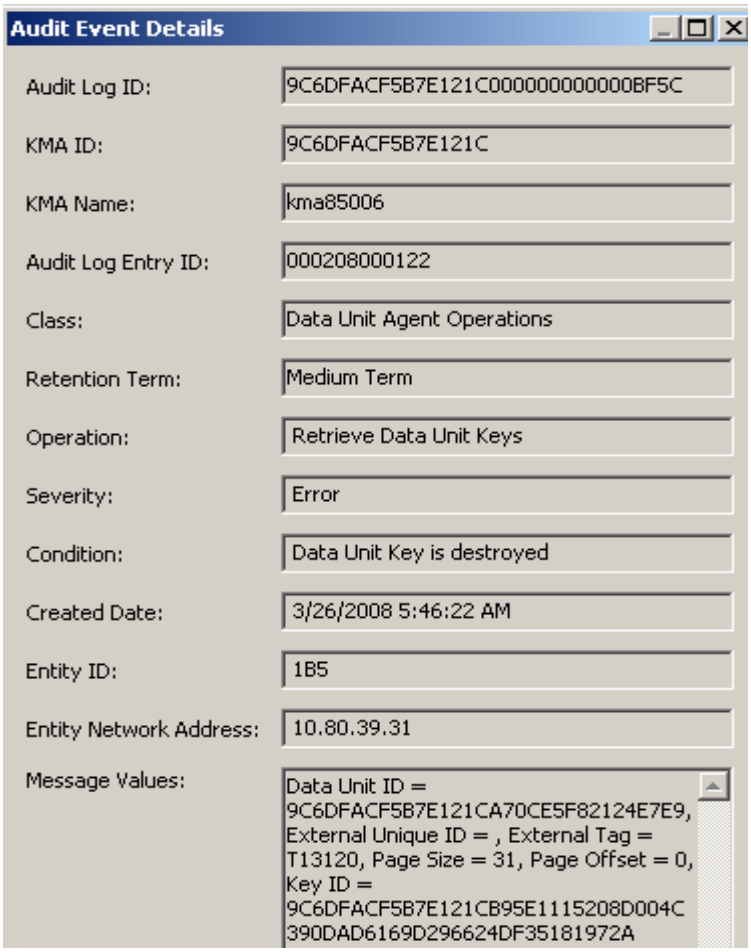
This scenario might be encountered after a key management work has been done.

- Host Symptom:

```
IEC501A M 01B5,T13120,SL,COMP,HSC0TA14,K1TAPE,IOP.SR7390RS.PD.K1
IOS000I 01B5,0B,IOE,02,0600,,**,,HSC0TA14  265
 004910D050205451 2502FF30C00032D5 E3F1F3F1F2F00290 4104230003772011
 UNSUPPORTED FORMAT
IEC512I LBL ERR 01B5,
,NL,T13120,SL,HSC0TA14,K1TAPE,IOP.SR7390RS.PD.K1
IEC704A L 01B5,T13120,SL,COMP,HSC0TA14,K1TAPE,IOP.SR7390RS.PD.K1
1501 IEC704A REPLY 'VOLSER,OWNER INFORMATION','M'OR'U'
R 1501,U
IEC705I TAPE ON
01B5,T13120,SL,COMP,HSC0TA14,K1TAPE,IOP.SR7390RS.PD.K1,MEDIA5
```

**Note:** FSC **32D5** indicates the key has been destroyed.

- KMS Symptom:




- Recovery Steps:
  - ✓ Allow rewrite of label to occur.

## Scenario 3 – Encrypted tape is mounted on a non-encrypted drive for file append or read

This scenario might be encountered if a specific unit is requested for an encrypted tape.

- Host Symptom:

```
IEC501A M 01DA,T13103,SL,,HSC6TAM9,G1AL,IOP.SR7196MG.AL.FILE84.TAPE.MULT
TMS008  IEC501A M 01DA,T13103,SL,,HSC6TAM9,G1AL,IOP.SR7196MG.AL.FILE84
IOS000I 01DA,A7,IOE,02,0600,,**,,HSC6TAM9  340
 004910D050205451 2502FF30C00032B9 E3F1F3F1F0F30290 4104230007722011
 UNSUPPORTED FORMAT
IEC512I I/O ERR 01DA,      ,NL,HSC6TAM9,G1AL,IOP.SR7196MG.AL.FILE84.TAPE
IEC502E R 01DA,,     ,NL,HSC6TAM9,G1AL
TMS014  IEC502E R 01DA,,     ,NL,HSC6TAM9,G1AL
IEC501A M 01DA,T13103,SL,,HSC6TAM9,G1AL,IOP.SR7196MG.AL.FILE84.TAPE.MULT
6066 /SLS1075D DISMOUNT OF T13103 FROM DRIVE 01DA - ERROR ON TAPE; IGNORE
OR EJECT (I/E
/SLS0099I DISMOUNT OF T13103 FROM DRIVE 01DA - VOLUME AT 00:01:02:17:00
/SLS0091I DISMOUNT OF ? FROM DRIVE 01DA - COMPLETE
6067 /SLS0088D MOUNT OF T13103 ON DRIVE 01DA - INTERVENTION REQUIRED;
 MOUNT OR IGNORE (M/I)
IOS000I 01DA,A7,IOE,02,0600,,**,,HSC6TAM9 562
004910D050205451 2502FF30C00032B9 E3F1F3F1F0F30290 4104230007722011
 UNSUPPORTED FORMAT
IEC514D DCK OR LBL ERR 01DA,T13103,HSC6TAM9,G1AL,IOP.SR7196MG.AL.FILE84
6068 IEC514D REPLY 'M'-UNLOAD OR 'A'-ABEND
```

**Note:** FSC **32B9** indicates incompatible format, in other words, encrypted data can not be read on a non-encrypted drive

- KMS Symptom:

  None, this is not an encrypted drive

- Recovery Steps:
  - ✓ Reply (I)gnore or (E)ject to message SLS1075D. Either will dismount tape.
  - ✓ Reply (M)ount or (I)gnore to message SLS0088D. Mount will only repeat error, Ignore waits for intervention by the operator.
  - ✓ Cancel job.
  - ✓ Correct allocation of tape to tape drive so that tape is mounted on an encrypted drive.
  - ✓ Resubmit failing job

## Scenario 4 – Encrypted tape is mounted on a non-encrypted drive for write from Block 0.

This scenario might be encountered if the VOLATTR RECECH is changed from T1AE35 to T1A35, thus requiring re-initialization of the tape.

- Host Symptom:

```
IOS000I 01DA,A7,IOE,02,0600,,**,,HSC6TAM9 968
 004910D050205451 2502FF30C00032B9 E2D3F8F0F2F00290 4104230007722011
 UNSUPPORTED FORMAT
IEC512I LBL ERR 01DA,      ,NL,SL8020,SL,HSC6TAM9,G1AL,IOP.SR7196MG.AL
IEC704A L 01DA,SL8020,SL,COMP,HSC6TAM9,G1AL,IOP.SR7196MG.AL
6070 IEC704A REPLY 'VOLSER,OWNER INFORMATION','M'OR'U'
```

**Note:** FSC **32B9** indicates unsupported format, in other words, encrypted data can not be read on a non-encrypted drive

- Recovery Steps:
  - ✓ Determine the appropriate response for your installation.
  - ✓ A reply of 'U' would create an un-encrypted label on the tape.
  - ✓ Job continues. Volser will be left on drive

## Scenario 5 – Non-Encrypted tape is mounted on a encrypted drive for file append

This scenario might be encountered if a specific unit is requested for a non-encrypted tape.

- Host Symptom:

```
IOS000I 01E3,B7,IOE,01,0600,,**,SL8020,HSC6TSTW  357
 804400C022212341 0101FF0000000000 00000032BA000092 2004230021742011
 WRITE PROTECTED
IEC147I 613-10,IFG0196T,HSC6TSTW,G1AL,CREATE,01E3,SL8020,IOP.SR7196MG.AL2
IEA995I SYMPTOM DUMP OUTPUT  359
SYSTEM COMPLETION CODE=613  REASON CODE=00000010
```

**Note:** FSC **32BA** indicates command is rejected, encrypted data cannot be written on non-encrypted tape except if at block 0 (see scenario 6)

- Recovery Steps:
  - ✓ Correct allocation of tape to tape drive so that tape is mounted on an encrypted drive.
  - ✓ Resubmit failing job

## Scenario 6 – Non-encrypted tape is mounted on an encrypted drive for write from Block 0.

This scenario might be encountered if the VOLATTR RECECH is changed from T1A35 to T1AE35. It is not an error scenario but is presented here to contrast it from Scenario 4.

- Host Symptom:

```
IEC501A M 01E3,SL8020,SL,COMP,HSC6TSTW,G1AL,IOP.SR7196MG.AL.FILE1.ENC
IEC705I TAPE ON
01E3,SL8020,SL,COMP,HSC6TSTW,G1AL,IOP.SR7196MG.AL.FILE1.ENC,MEDIA5
IEC205I CREATE,HSC6TSTW,G1AL,FILESEQ=1, COMPLETE VOLUME LIST,  220
DSN=IOP.SR7196MG.AL.FILE1.TAPETST.ZIPD,VOLS=SL8020,TOTALBLOCKS=36572
IEF234E K 01E3,SL8020,PVT,HSC6TSTW,G1AL
```

- Recovery Steps:
  - ✓ None, the volser is seamlessly re-labeled and the label is now encrypted.

## Scenario 7 – Drive replacement.

In the event a drive needs replacement, additional coordination is required between the Customer Service Engineer and the customer to enable encryption. The steps are a subset of those described in the Installation/Maintenance section of this document.

1. The Customer Service Engineer will install the drives in the library and must configure to 3592 emulation using a FICON interface via the T10000 Virtual Operator Panel (VOP). An IP address might also be assigned at this time.
2. The Customer Service Engineer will supply the crypto serial number (CSN) for each tape drive to the customer. This information can be obtained from the Sun Licensing Center.
3. The customer will first enter the new drive as an agent in the KMS system assigning agent ID, passphrase, key groups and default key group as appropriate.
4. The customer or CSE will then enroll the new drive as an encrypting drive via VOP providing the new agent ID, passphrase and KMA IP address.
5. Success is indicated by a solid AMBER Encryption LED on the drive, and successful enrollment of agent in the KMS.
6. The customer will verify NCS still identifies drive as T1AE35 via a DISPLAY DRIVES ALL DETAIL command.

## Scenario 8 – VSM RTD does not have key to read an encrypted MVC.

In the event a MVC is mounted on a RTD that either has missing keys or invalid keys, it can not read the encrypted data on the media. This is the VSM attached version of scenario 2 above.

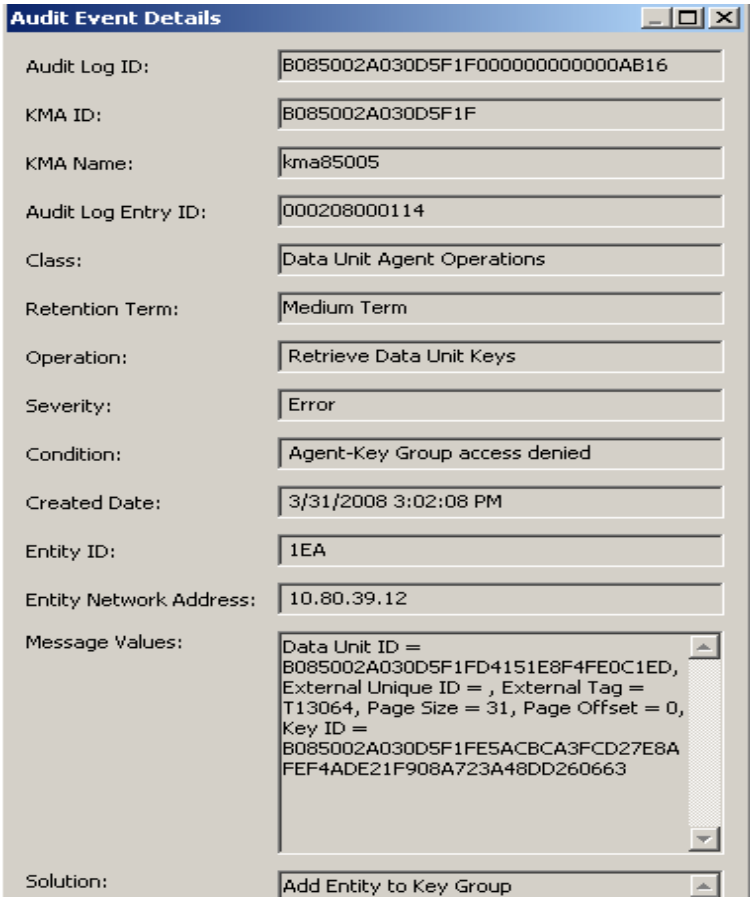
- Host Symptom:

```
IEC501A M 2F16,vtvid,BLP,COMP,jobname,stepname   <=mount request from job
IEC501A M 01EA,T13064,SL,,VTSS27  ,SWSRDRC       <=mount request, VTCS RECALL
SLS6643I MVC mvcid MOUNTED ON DRIVE 01E2TK0E
SLS6684I RTD 01EATK0E ON VTSS VTSS27 RETURNED ECAM ERROR CC=5 RC=108
SLS6625E RTD 01EATK0E REPORTED 3480XF2 INCOMPAT:
0041205C0000132400E0E3F1F3F0F6F4404000 32D0 000000CE0E372002180000
SLS6605I INITIATING SWAP OF MVC T13064 FROM RTD 01EATK0E
```

**Note:** FSC **32D0** indicates the media key is missing in order to read the encrypted tape

**Note:** A swap request will be honored for each valid online RTD for the specified VTSS. This swap will occur only once for each RTD. In the event that a RTD has the necessary key, the RECALL process will complete. In the event that no RTD has the necessary key, the MVC mount request will timeout after the last swap request is attempted.

- KMS Symptom:




- Recovery Steps:
  - ✓ If the new RTD has the proper key group, allow swap processing to find it, else continue.
  - ✓ Assign drive to correct key group, vary RTD back online to VTSS.

# Chapter 7: Alternate Key Management Scenarios

## Key Management System Disaster Recovery

Key protection is an important consideration as losing keys is equivalent to losing data and not having the correct keys available at the right time results in losing access to data. Because of this, it is necessary to plan for disaster recovery situations when implementing a key management strategy.

**An enterprise KMS installation should have five levels of key protection.**

- ◊ Once created, keys are encrypted and stored on the KMS server within the KMS database.
- ◊ A clustered KMS must be implemented which should include KMA's located in another facility. For steps on configuring a clustered KMS, please reference the KMS 2.0 Administration Guide. A minimum of two KMAs are required at each site.
- ◊ Backup of KMS database initiated using the KMS GUI, saved to local disk on the server where GUI executes.
- ◊ For additional disaster recovery protection, it is recommended that the KMS database backup be periodically sent to an off-site vault.
- ◊ Additional KMA should be placed at the DR site and connected into the production KMAs. This allows keys and other KMS information to be automatically replicated to the KMAs at the DR site.

**What happens in the event of a disaster recovery?**

- ◊ If the disaster that caused KMS database corruption or loss is local to the KMS server itself, then the first step would be to execute a restore of the latest KMS database backup if the KMS resides in a single KMA configuration. For steps on how to restore a KMS, reference the KMS 2.0 Administration Guide, and StorageTek Crypto Key Management Solution Management Practices V2.0 white paper
- ◊ If the disaster occurred in a configuration that includes clustered KMA's, the working KMA will service all requests for keys, therefore contact Sun service for a replacement KMA.
- ◊ In the rare event that all sources have been rendered inoperable in a disaster or are otherwise unavailable for recovery, redundant off-site KMA's would service requests (only from drives at the off-site location). If the drives are shared, it will be necessary to enroll the drives with the remaining KMAs. If no redundancy has been configured, then restore a KMS database backup from a vault or offsite location onto recovery KMAs.

**For a more comprehensive discussion on disaster recovery of the KMS see StorageTek Crypto Key Management Solution Version 2.0 Management Practices white paper, Chapter 8.**

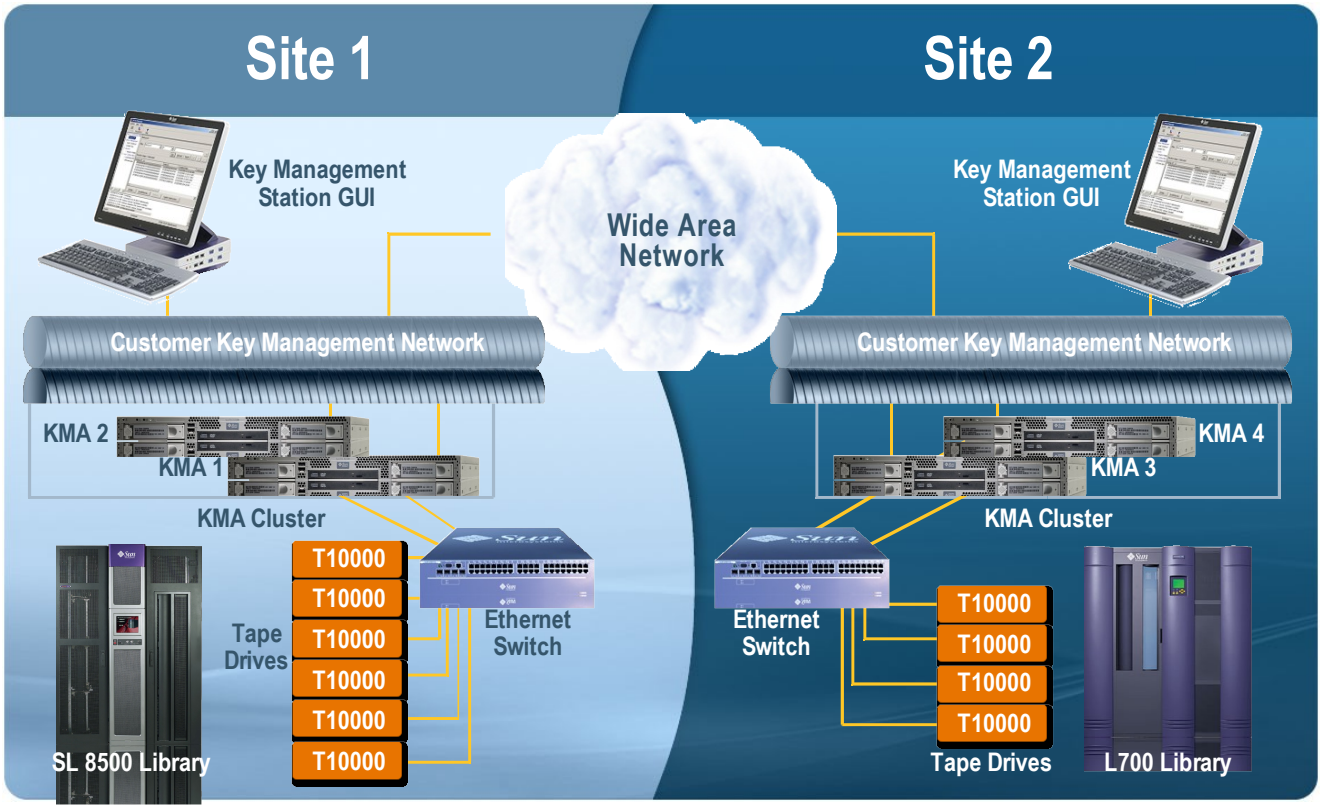
# Chapter 8: Optimizing Encryption Solution for Redundancy

## Redundant Network

Unlike version 1.0, version 2.0 of the Sun StorageTek Crypto Key Management Solution does not retain encryption keys locally on the drive after unloading a tape. All requests for keys are serviced by a KMA in the KMS cluster and provided to the drive. Protecting against component failure is a primary concern in maintaining uninterrupted operation of the encryption solution.

Each Key Management Appliance is configured with three network ports. One port is dedicated to the Enhanced Lights Out Manager (ELOM) that is used to provide remote access to the console. The ELOM is used during initial setup and configuration of the KMA. The KMA is a locked down appliance so very few functions are available through the ELOM but the security officer can utilize the ELOM to perform certain operations such as resetting the KMA. The second configured Ethernet port is dedicated to KMA management. This connects to the customer's secured network and is utilized for the KMS software manager to administer the cluster as well as for replicating changes across the cluster to other KMAs. The final configured Ethernet port is dedicated to the service network on which the encrypting tape drives should reside. It is recommended that the encrypting tape drives be installed on the services network to reduce network traffic and limit external access. To protect against component failure, it is recommended to install redundant switches on the services network.

# KMS 2.0 Sample Configuration



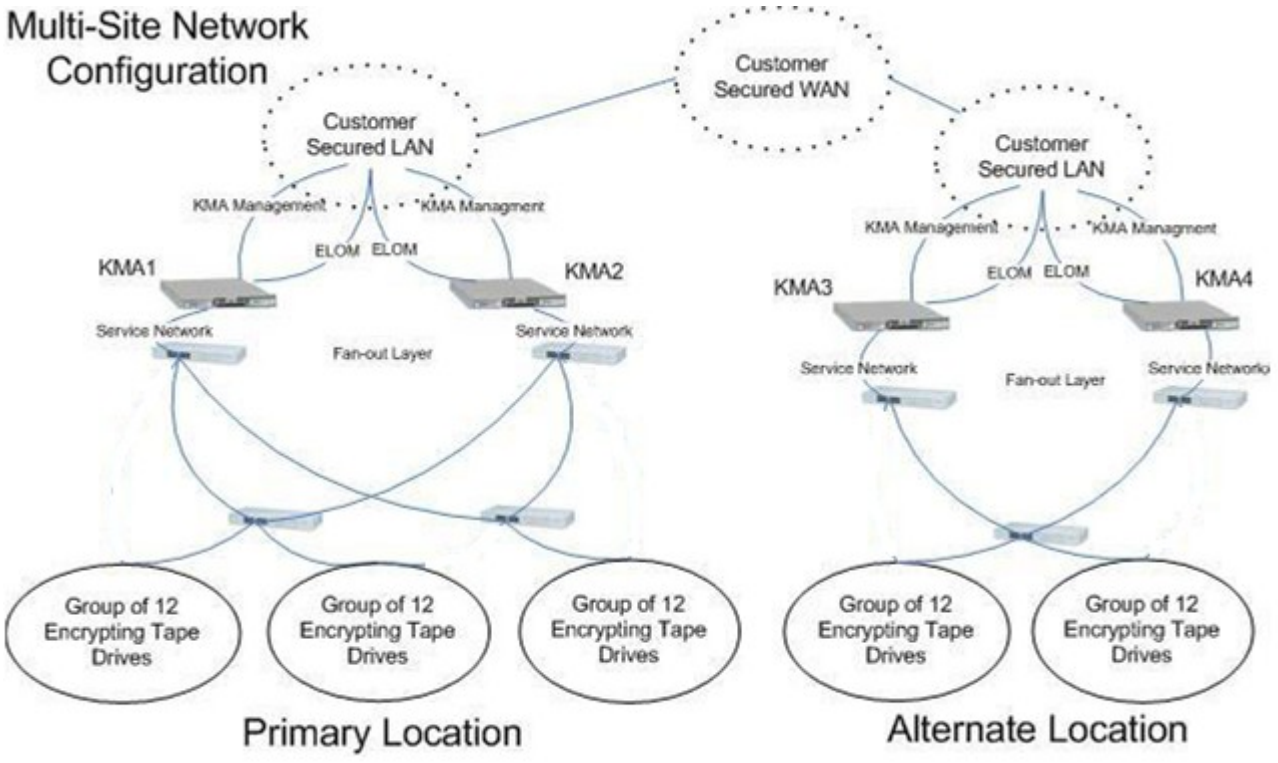

The example illustrated above right shows a simple recommended network for an environment. The first step in protecting the network is to connect the KMAs to separate switches on the services network. Any KMA can provide full functionality for any drive enrolled in the cluster. If a component failure is experienced on a KMA or on the switch to which a KMA is connected, the second KMA in the cluster will service available drives and encrypted operations will continue unaffected. Ethernet switches that are directly connected to KMAs are referred to as fan-out switches. The next step in protecting the network is to distribute encrypting tape drives evenly across all available switches, including available ports on fan-out switches. This serves to reduce the impact of a component failure

at the switch level by rendering only the drives directly connected to the failed switch temporarily inoperable. The final step is to utilize redundant cabling methods. A good rule of thumb is that any switch that is not directly connected to a KMA should have connections to two switches that are. This ensures that a single failure of a KMA or a switch will not impact the ability of the encryption solution to continue processing data. Additionally, uninterrupted power supplies can be used to protect switches and KMA components from loss of power interruptions.

For customers who place a top priority on redundancy, there are some additional configuration changes that will help further mitigate the potential for interrupted operations due to component failure. These include the addition of a third KMA to the local KMS cluster and extra switches on the services network to reduce the number of drives that would be impacted by a switch component failure. An additional KMA in the local cluster adds security in the event that a component failure forces one KMA to be unavailable for an extended period of time. The remaining KMAs can continue to function as a cluster while managing the encryption solutions. Load balancing, replication and protection of new keys are achieved.

## Multi-Site Network

A single KMS cluster can administer key management functions for encrypting tape drives spread across many site locations. The diagram below provides an example of a configuration that includes encrypting tape drives at two separate locations. It is important to note that while all four KMAs in this example are clustered together and replicate changes across the cluster, it is still highly recommended to have a local cluster of at least two KMAs at each site. This provides path redundancy and load balancing abilities for the drives at that site.




## Shared Tape Resource Centers

One challenge of implementing an encryption solution is managing shared tape resource centers. Shared tape resource centers generally consist of third party sites that manage archived information

for multiple customers.  Customers send archived information to shared tape resource centers for data protection and disaster recovery purposes..

The recommended scenario for a customer to implement a Sun Tape Encryption environment in conjunction with a third party shared tape resource center is to maintain at least 1 KMA, at the third party site. This KMA would participate in the customer KMS cluster via the management network such that all updates to the KMS cluster are reflected in the KMA at the third party site. Drives at the third party site would have to be configured to use the appropriate key groups according to the data in the KMA. The drive(s) needed would only access 1 KMS cluster at any given time frame. Essentially at the Shared Resource Center the KMA would be dedicated to 1 customer, but the drive(s) necessary to read tape volumes would be shared. Usage of the drive(s) would not be concurrent amoung customers; the drive(s) would only be dedicated to a single customer for as long as needed. The drive(s) would then be reconfigured to access a different KMA for a different customer.

Drives and tapes as the shared resource center may be used on a continuous or intermittent basis.  If drives and tapes are used on a continuous basis, the customer will need full time, or at least, frequent access to drives and KMAs.  Ideally, this will be done using drives and KMAs dedicated to the customer.  In this case, the customer can manage the drives and KMAs just as they do their prodution site drives and KMAs.

If tapes are to be moved between the shared resource location and the other customer sites, there are two approaches for transfering keys.  The preferred approach is to include the shared resource location KMAs in the prodution KMA cluster.  This will keep the shared site KMAs and the production KMAs in synch.  This allows tapes to be freely moved between sites.

Where this is not possible, “key transfer partners” can be configured.  When tapes are moved, a “key transfer file” must be generated containing the proper set of keys for the tapes.  See the StorageTek Crypto Key Management Solution Management Practice, Chapter 5  for details of setting up and using transfer partners.

If drives and KMAs are shared amoung multiple companies in a shared resource center, key management is more challenging.  The tape drives are unaware of which customer is currently using them.  So, it is impossible to configure the drives and KMS to restrict access to key based on the usage of the drives.  Other functionality, such as RACF or Top Secret should be used to control access to tapes.

Because the KMAs in this secnario are shared among multiple customers, it is not possible to configure the shared site KMAs into a production cluster.  A KMA can only belong to one cluster at a time.

## Disaster Recovery Sites

Another common use of shared resource sites is for Disaster Recovery.  In this usage, a customer will only use the drives, libraries, and other resources of the shared resource site for short periods of time, either to do a DR test or to actually recovery from a disaster.

It is assumed that tape drives, libraries, and servers will be assigned to a specific user of the shared resouce site only during a DR test or disaster recovery.  The specific equipment that will be made available is not known prior to starting the DR test or recovery.

There are two approaches for key management.  The preferred appraoch is for the customer to place KMAs at the DR site, and configure these into their production cluster using a WAN connection. These KMAs are dedicated to the specific customer.  This allows the customer's key to always be at the DR site and ready for use.  A second appraoch is to restore a backup of the customer's production

KMS onto KMAs provided by the shared resource center management. This avoids the need for a WAN link and the on-site, dedicated KMAs, but requires additional time to restore the database.

In the preferred approach, a recovery is begun by enrolling the tape drives provided by the shared resource center management into the customer's KMS cluster. This can be done by connecting the KMS Manger GUI to the KMAs at the DR site. Drive enrollment can be completed in a matter of minutes. In a true disaster recovery, these may be the only remaining KMAs from the customer's cluster. Once the enrollment is complete, and the drives have been configured on the provided servers or LPARs, tape IO can begin.

In the alternative approach, KMAs must be provided by the shared resource center management at the beginning of the test or recovery. The customer's KMS backup must be restored. The restore operation requires both the normal KMS backup (two files) and a core security backup. The restore requires a quorum of the key split credential members in effect when the core security backup (not the normal backup) was performed. Restore operations take about 20 minutes per 100,000 keys. Once the restore is completed, the drive must be enrolled and configured on the provided servers or LPARs. Now tape IO can begin.



Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web sun.com