IBM

Operator Guide
3592 Models J1A, E05, E06, EU6, J70 and C06

IBM System Storage TS1120 and TS1130 Tape Drives
and TS1120 Controller

IBM

Operator Guide
3592 Models J1A, E05, E06, EU6, J70 and C06

Fourth edition

This edition applies to the IBM System Storage TS1120 Tape Drive and to all subsequent releases and modifications until otherwise indicated in new editions. This edition replaces GA32-0556-02.

Read this first

This is the fourth edition of the IBM® System Storage™ TS1120 and TS1130 Tape Drives and TS1120 Controller Operator Guide. This document provides information for operators using the IBM System Storage TS1120 Tape Drive (3592 Model E05), the IBM System Storage TS1130 Tape Drive (3592 Models E06 and EU6), the IBM TotalStorage® Enterprise Tape Drive 3592 Model J1A, the IBM System Storage TS1120 Tape Controller Model C06, the IBM TotalStorage Enterprise Tape Controller 3592 Model J70, and the IBM TotalStorage Enterprise Tape Cartridge 3592 products.

Do you have comments or suggestions?

Your feedback is important in helping to provide the most accurate and high-quality information. If you have comments or suggestions for improving this publication, you can send us comments electronically by using these addresses:

- Internet: starpubs@us.ibm.com
- IBMLink™ from U.S.A.: STARPUBS at SJEVM5
- IBMLink from Canada: STARPUBS at TORIBM
- IBM Mail Exchange: USIB3VVD at IBMMAIL

You can also mail your comments by using the Reader Comment Form in the back of this manual or direct your mail to:

International Business Machines Corporation
Information Development
Building 9032-2, Department GZW
9032 South Rita Road
Tucson, Arizona U.S.A. 85744-0002

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

Tables

Safety and Environmental Notices

Observe the safety notices when using this product. These safety notices contain danger and caution notices. The notices are sometimes accompanied by symbols that represent the severity of the safety condition.

Most danger or caution notices contain a reference number (Dxxx or Cxxx). Use the reference number to check the translation in the *IBM Systems Safety Notices*, G229–9054 manual.

The sections that follow define each type of safety notice and give examples.

Danger Notice

A danger notice calls attention to a situation that is potentially lethal or extremely hazardous to people. A lightning bolt symbol always accompanies a danger notice to represent a dangerous electrical condition. A sample danger notice follows:

DANGER

An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the products that attach to the system. It is the customer's responsibility to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. *(D004)*

Caution Notice

A caution notice calls attention to a situation that is potentially hazardous to people because of some existing condition. A caution notice can be accompanied by one of several symbols:

If the symbol is...	It means....
	A generally hazardous condition not represented by other safety symbols.
Class II	This product contains a Class II laser. Do not stare into the beam. (*C029*) Laser symbols are always accompanied by the classification of the laser as defined by the U. S. Department of Health and Human Services (for example, Class I, Class II, and so forth)..
	A hazardous condition due to mechanical movement in or around the product.

If the symbol is...	It means....
> 18 kg (40 lb)	This part or unit is heavy but has a weight smaller than 18 kg (39.7 lb). Use care when lifting, removing, or installing this part or unit. (*C008*)

Sample caution notices follow:

Caution

> The battery is a lithium ion battery. To avoid possible explosion, do not burn. Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (*C007*)

Caution

> The system contains circuit cards, assemblies, or both that contain lead solder. To avoid the release of lead (Pb) into the environment, do not burn. Discard the circuit card as instructed by local regulations. (*C014*)

Caution

> When removing the Modular Refrigeration Unit (MRU), immediately remove any oil residue from the MRU support shelf, floor, and any other area to prevent injuries because of slips or falls. Do not use refrigerant lines or connectors to lift, move, or remove the MRU. Use handholds as instructed by service procedures. (*C016*)

Caution

> Do not connect an IBM control unit directly to a public optical network. The customer must use an additional connectivity device between an IBM control unit optical adapter (that is, fibre, ESCON®, FICON®) and an external public network . Use a device such as a patch panel, a router, or a switch. You do not need an additional connectivity device for optical fibre connectivity that does not pass through a public network.

Environmental notices

This section identifies the environmental guidelines that pertain to this product.

Product recycling and disposal

This unit contains recyclable materials.

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM product recycling offerings can be found on IBM's Internet sites at *http://www.ibm.com/ibm/ recycle/us/index.shtml* and *http://www.ibm.com/ibm/environment/products/ index.shtml*

Note: This paragraph is also translated into Spanish as follows:

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos ya no les sean útiles. IBM dispone de una serie de programas y servicios de devolución de productos en varios países, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de IBM en el sitio web de IBM *http://www.ibm.com/ibm/environment/products/index.shtml*
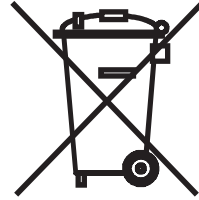
Notice: This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

Remarque : Cette marque s'applique uniquement aux pays de l'Union Européenne et à la Norvège.

L'etiquette du système respecte la Directive européenne 2002/96/EC en matière de Déchets des Equipements Electriques et Electroniques (DEEE), qui détermine les dispositions de retour et de recyclage applicables aux systèmes utilisés à travers l'Union européenne. Conformément à la directive, ladite étiquette précise que le produit sur lequel elle est apposée ne doit pas être jeté mais être récupéré en fin de vie.

注意: このマークは EU 諸国およびノルウェーにおいてのみ適用されます。

この機器には、EU 諸国に対する廃電気電子機器指令 2002/96/EC(WEEE) のラベルが貼られています。この指令は、EU 諸国に適用する使用済み機器の回収とリサイクルの骨子を定めています。このラベルは、使用済みになった時に指令に従って適正な処理をする必要があることを知らせるために種々の製品に貼られています。

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

Battery return program

This product may contain sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or a lithium ion battery. Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to *http://www.ibm.com/ibm/environment/ products/index.shtml* or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM Equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Please have the IBM part number listed on the battery available prior to your call.

For the European Union:
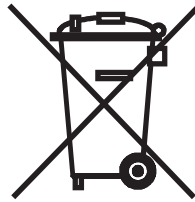
For Taiwan:

Please recycle batteries

廢電池請回收

Batteries or packaging for batteries are labeled in accordance with European Directive 2006/66/EC concerning batteries and accumulators and waste batteries and accumulators. The Directive determines the framework for the return and recycling of used batteries and accumulators as applicable throughout the European Union. This label is applied to various batteries to indicate that the battery is not to be thrown away, but rather reclaimed upon end of life per this Directive.

Les batteries ou emballages pour batteries sont étiquetés conformément aux directives européennes 2006/66/EC, norme relative aux batteries et accumulateurs en usage et aux batteries et accumulateurs usés. Les directives déterminent la marche à suivre en vigueur dans l'Union Européenne pour le retour et le recyclage des batteries et accumulateurs usés. Cette étiquette est appliquée sur diverses batteries pour indiquer que la batterie ne doit pas être mise au rebut mais plutôt récupérée en fin de cycle de vie selon cette norme.

バッテリーあるいはバッテリー用のパッケージには、EU 諸国に対する廃電気電子機器指令 2006/66/EC のラベルが貼られています。この指令は、バッテリーと蓄電池、および廃棄バッテリーと蓄電池に関するものです。この指令は、使用済みバッテリーと蓄電池の回収とリサイクルの骨子を定めているもので、EU 諸国にわたって適用されます。このラベルは、使用済みになったときに指令に従って適正な処理をする必要があることを知らせるために種々のバッテリーに貼られています。

In accordance with the European Directive 2006/66/EC, batteries and accumulators are labeled to indicate that they are to be collected separately and recycled at end of life. The label on the battery may also include a chemical symbol for the metal concerned in the battery (Pb for lead, Hg for mercury and Cd for cadmium). Users of batteries and accumulators must not dispose of batteries and accumulators as unsorted municipal waste, but use the collection framework available to customers for the return, recycling and treatment of batteries and accumulators. Customer participation is important to minimize any potential effects of batteries and accumulators on the environment and human health due to the potential presence of hazardous substances. For proper collection and treatment, contact your local IBM representative.

Spain

This notice is provided in accordance with Royal Decree 106/2008 of Spain: The retail price of batteries, accumulators and power cells includes the cost of the environmental management of their waste.

Perchlorate Material - California

Special handling may apply. See *http://www.dtsc.ca.gov/hazardouswaste/perchlorate* for more information.

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5 Chapter 33. Best Management Practices for Perchlorate Materials. This product/part may include a lithium manganese dioxide battery which contains a perchlorate substance.

About this publication

This publication provides basic instructions for operating, cleaning, and troubleshooting the IBM 3592 high performance tape subsystem.

Related publications

The following publications provide related information about the IBM tape drive, medium, changer, and library device drivers:

IBM System Storage TS1120 Tape Drive and Controller publications

- *IBM System Storage TS1120 and TS1130 Tape Drives and TS1120 Controller Introduction and Planning Guide*, GA32-0555
- *IBM System Storage TS1120 Tape Drive 3592 SCSI Reference*, GA32-0562
- *IBM TotalStorage 3952 Tape Frame Model C20 Introduction, Planning, and User's Guide*, GA32-0463

IBM TotalStorage Enterprise Tape System 3590 publications

- *IBM TotalStorage Enterprise Tape System 3590 Introduction and Planning Guide*, GA32-0329
- *IBM TotalStorage Silo Compatible Tape Frame 3590 Introduction, Planning, and User's Guide*, GA32-0366
- *IBM TotalStorage Enterprise Tape System 3590 Operator Guide*, GA32-0330
- *IBM TotalStorage 3590 Tape Subsystem Hardware Reference Guide*, GA32-0331

IBM TotalStorage Enterprise Automated Tape Library (3494) publications

- *IBM TotalStorage Automated Tape Library (3494) Introduction and Planning Guide*, GA32-0448
- *IBM TotalStorage Automated Tape Library (3494) Operator's Guide*, GA32-0449

IBM System Storage TS3400 Tape Library publications

- *IBM System Storage TS3400 Tape Library Planning and Operator Guide*, GC27-2107

IBM Encryption Key Manager publications

- *IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide*, GA76-0418
- *IBM Encryption Key Manager component for the Java platform Quick Start Guide for LTO Ultrium 4*, GA76-0420
- *IBM Encryption Key Manager component for the Java platform Quick Start Guide for TS1120 Tape Drives*, GA76-0421

zSeries—S390 publications

- *IBM eServer™ zSeries 900 Platform Reference Guide* , G326-3092
- *Introduction to IBM S/390 FICON*, SG24-5176 (IBM Redbook).
- *S/390 System Overview Parallel Enterprise Server — Generation 5*, GA22-7158
- *S/390 System Overview Parallel Enterprise Server — Generation 6*, GA22-1030

IBM Fibre Channel publications

- *IBM TotalStorage SAN Switch 2109 Model F16 Installation and Service Guide*, SY27-7623
- *IBM Fiber-Optic Channel Link Planning and Installation*, GA32-0367

IBM FICON publications

- *FICON (FCV Mode) Planning Guide*, SG24-5445-00 (IBM Redbook).
- *Planning for: Fiber Optic Links (ESCON, FICON, Coupling Links, and Open system Adapters)*, GA23-0367
- *Maintenance Information for: Fiber Optic Links (ESCON, FICON, Coupling Links, and Open System Adapters)*, SY27-2597
- *Fiber Channel Connection (FICON) I/O Interface Physical Layer*, SA24-7172
- *Introduction to IBM System/390® FICON*, SG24-5176
- *Planning for the ED-5000 Enterprise Fibre Channel Director*
- *IBM eServer zSeries Connectivity Handbook*, SG24-5444
- *IBM Tape Solutions for Storage Area Networks and FICON*, SG24-5474

Related software publications

For information regarding software related to the IBM TotalStorage Enterprise Tape System 3592, refer to:

- *IBM TotalStorage and System Storage Tape Device Drivers Installation and User's Guide*, GC35-0154
- *IBM TotalStorage and System Storage Tape Device Drivers Programing Reference*, GC35-0346
- *IBM Tape Device Drivers: Encryption Support*, GA32-0565
- *Basic Tape Library Support User's Guide and Reference*, SC26-7016
- *Environmental Record Editing and Printing (EREP) Program User's Guide and Reference*, GC35-0151
- *z/OS DFSMS: Introduction*, SC26-7397
- *z/OS DFSMS: Object Access Method Planning, Installation, and Storage Administration Guide for Tape Libraries*, SC35-0427
- *z/OS DFSMS Software Support for IBM System Storage TS1130 and TS1120 Tape Drives (3592)*, SC26-7514
- *z/OS DFSMS Migration*, GC26-7398.
- *z/VM General Information Version 4 Release 3.0*, GC24-5991

Other publications

- *American National Standard Institute Small Computer System Interface* X3T9.2/86-109 X3.180, X3B5/91-173C, X3B5/91-305, X3.131-199X Revision 10H, and X3T9.9/91-11 Revision 1

IBM online access

IBM pSeries—RS/6000, AIX information

For additional information about IBM eServer pSeries® servers, visit the info center at:

- **http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base/**

IBM iSeries—AS400 information

For additional information about iSeries® or AS/400® systems, visit the infocenter at:

* **http://publib.boulder.ibm.com/pubs/html/as400/infocenter.html**

IBM Storage media support

The following URL provides access to current regional and country-specific IBM addresses and telephone numbers.

* **http://www.storage.ibm.com/media/distributors**

IBM TotalStorage Enterprise Tape System 3592 support

For general information about the 3592 Tape System, visit the following URL:

* **http://www.ibm.com/systems/storage/tape/3592/**

For general information about the TS1120 Tape Drive, visit the following URL:

* **http://www.ibm.com/servers/storage/tape/ts1120/index.html**

For general information about the TS1130 Tape Drive, visit the following URL:

* **http://www.ibm.com/servers/storage/tape/ts1130/index.html**

For information about supported servers for the 3592 Tape System, TS1120 and TS1130 tape drives, visit the following URL:

* **http://www.ibm.com/servers/storage/tape/compatibility/pdf/3592_interop.pdf**

The following URLs provide access to additional current information related to 3592 Tape System.

Device driver support

To access the 3592 Firmware and Device Driver Matrix, visit the following URL:

* **http://www.ibm.com/servers/storage/support/tape/3592/downloading.html**

To access the TS1120 and TS1130 Firmware and Device Driver Matrix, visit the following URL:

* **http://www.ibm.com/servers/storage/support/tape/ts1120/downloading.html**

You can download device driver software and read documentation about various device drivers at the following URL:

* **ftp://ftp.software.ibm.com/storage/devdrvr/**

IBM Network Integration and Deployment Services

The following URL provides information about connectivity and the integration of cabling systems.

* **http://www.ibm.com/services/networking/integration**

IBM Tape Storage publications

Use this URL for IBM Hardware product documents in a PDF format for viewing and printing.

* **http://www.ibm.com/servers/storage/tape/resource-library.html#publications**

SAN Fabric

This link provides information on high-performance switches and gateways.

* **http://www.storage.ibm.com/ibmsan/products/sanfabric.html**

I/O connectivity

This link provides updated information regarding FICON and fibre channel connectivity.

* **http://www.ibm.com/servers/eserver/zseries/connectivity**

Redbooks

Use this URL to access the IBM Redbooks®:

* **http://www.redbooks.ibm.com/**

Vendor support

This URL provides compatibility information in PDF format for implementing software, servers, and operating systems with IBM tape drives and libraries.

* **http://www.ibm.com/servers/storage/tape/compatibility/pdf/ ts1120_isv_matrix.pdf**

Non-IBM support

Brocade information

Use this URL for information on Brocade products and support.

* **http://www.brocade.com/**

Cisco information

Use this URL for information on Cisco products and support.

* **http://www.cisco.com/**

HP information

The following publications and URL relate to HP-UX systems:

* *HP-UX Reference for HP-UX 10.20, 11.00, and 11i*, Hewlett-Packard Company
* *System Administration Tasks, HP-UX Release 10.20, 11.00, and 11i*, Hewlett-Packard Company
* Additional HP information can be found at this URL: **http://docs.hp.com**

Linux information

Red Hat information

The following URL relates to Red Hat Linux systems:

* **http://www.redhat.com**

SuSE information

The following URL relates to SuSE Linux systems:

* **http://www.suse.com**

McData information

This URL provides access to information about McData products and support.

* **http://www.mcdata.com/**

Microsoft Windows information

The following URL provides access to information about Microsoft® Windows® systems:

* **http://www.microsoft.com**

SGI information

The following URL provides access to information about SGI systems:

- **http://techpubs.sgi.com/library**

SUN information

The following URL provides access to information about Solaris (Sun) systems:

- **http://docs.sun.com/**

Chapter 1. Introduction

The IBM System Storage TS1130 (3592 Model E06 and EU6) Tape Drive, the TS1120 (3592 Model E05) Tape Drive and Controller (3592 Model C06), and the 3592 Model J1A Tape Drive and Model J70 Controller offer a dramatic improvement in performance and cartridge capacity for Enterprise Class tape customers that currently use the IBM TotalStorage Enterprise Tape System 3590. The 3592 tape drives and controllers can be used for the following:

- Creating tapes for file archival
- Backing up and restoring systems
- Storing and accessing sequential application data sets
- Creating and accessing temporary data sets
- Satisfying off-site data storage requirements for disaster recovery
- Providing data interchange with other systems that use 3592 tape drives
- Meeting data acquisition needs
- Creating data tapes that cannot be altered, but can be read many times

Summary of Changes

This summary of changes includes specific release updates to this document. Paragraphs with content changes for the most recent revision are indicated by revision bars, visible to the left of any added or revised text.

Fourth Edition

In the fourth edition, information was added on the following topics:

- New TS1130 Tape Drives (3592 Model E06 and 3592 Model EU6). See "Drive and Media Information" on page 2.
- Support for IPv6 on the 3592 Model C06 Tape Controller. See "Controller Information" on page 3.
- This publication has also been updated for compliance with International System of Units (SI) measurements.

Third Edition

In the third edition, information was added on the following topics:

- Support for new 700 GB (651.93 GiB) IBM TotalStorage Enterprise Tape Cartridge 3592 Extended and IBM TotalStorage Enterprise Tape Cartridge 3592 Extended WORM, media types JB and JX.

Second Edition

In the second edition, information was added on the following topics:

- Encryption support on the IBM System Storage TS1120 Tape Drive (TS1120 Tape Drive). See "Tape Encryption Overview" on page 3 for more information.
- Power on and power off procedures for the 3592 tape controllers. See Chapter 5, "3592 Tape Controller Power Procedures," on page 33.
- Error codes related to the IBM Encryption Key Manager component for the Java™ platform (EKM). See "Encryption Key Manager-Reported Errors" on page 40.
- Encryption-related FID codes. See Appendix B.

Drive and Media Information

The 3592 drive is a single cartridge unit designed for automation. Two models are available: the TS1130 (3592 Model E06) and TS1120 (3592 Model E05). The 3592 Model J1A Tape Drive is withdrawn. A 3592 Model E05 canister may be upgraded through the Miscellaneous Equipment Specification (MES) process to contain a 3592 Model E06 drive. The result is a 3592 Model EU6 Tape Drive, which is the functional equivalent of the Model E06. Table 4 on page 20 shows tape capacities by drive. Enhancements to the 3592 tape drives include:

- AES 256-bit data encryption capability increases security with minimal performance impact.
- Up to 160 Mb/s[1]. native data rate for the Models E06 and EU6, four times faster than the Model J1A at 40 Mb/s. (Up to 100 Mb/s. for the Model E05.)
- Up to 1000 GB (931.32 GiB[2]) native cartridge capacity for the Models E06 and EU6 using the IBM TotalStorage Enterprise Tape Cartridge 3592 Extended (3000 GB [2793.96 GiB] at 3:1 compression), more than a threefold increase over the maximum 300 GB (279.39 GiB) native tape cartridge capacity (900 GB [838.19 GiB] at 3:1 compression) of Model J1A.
- Up to 640 GB (596.04 GiB) native cartridge capacity for the Models E06 and EU6 using the standard IBM TotalStorage Enterprise Tape Cartridge 3592 (1920 GB [1788.14 GiB] at 3:1 compression), more than a twofold increase over the maximum 300 GB (279.39 GiB) native tape cartridge capacity (900 GB [838.19 GiB] at 3:1 compression) of Model J1A.
- 128 GB (119.21 GiB) for Models E06 and EU6, 1000 GB (93.13 GiB) for Model E05, and 60 GB (55.88 GiB) for Model J1A on the Economy tape cartridge with very fast read/write access
- 1000 GB (931.32 GiB), 640 GB (596.04 GB), and 128 GB (119.21 GiB) WORM (Write Once, Read Many) capacities on Models E06 and EU6) for increased security of data (279.39 GiB) and 60 GB (55.88 GiB) for Model J1A)
- Scaling capability to optimize fast access, storage capacity, or a combination of both
- Dual ported switched fabric 4-Gb/s Fibre Channel attachments
- High reliability and availability design
- Additional performance and access improvements
- Smaller form factor that allows double the number of drives in a single 3494 frame or standalone rack

A note on terminology and model names

Throughout the remainder of this publication, the 3592 Models E06, EU6, E05, and J1A Tape Drives are all referred to collectively as the 3592 Tape Drive unless a specific model is being discussed. When software is discussed, the TS1120 and TS1130 names may be used. Where necessary the different models of the IBM TotalStorage Enterprise Tape Drive 3590 will be referred to as the 3590 drives or the specific 3590 models B, E, or H.

---

1. One mebibit per second (Mb/s) = 2^{20} bits = 1,048,576 bits per second.

2. One gibibyte (GiB) = 2^{30} bytes = 1,073,741,824 bytes = 1024 mebibytes (MiB).

Controller Information

IBM's newest high-performance tape controller, the System Storage TS1120 (C06) Controller, offers:

- 3592-C06 1.21.5.x microcode provides limited IPv6 support for TS1120 controllers in a standalone rack or attached to one or more TS3400 libraries.
- Support for up to four 4-Gb/s. FICON attachments
- Support for up to eight ESCON attachments
- Attachment of up to 16 3592 tape drives and support for 700 GB (651.93 GiB) IBM TotalStorage Enterprise Tape Cartridge 3592 Extended and Extended WORM media types, as well as 500 GB (465.66 GiB) and 100 GB (93.13 GiB) IBM TotalStorage Enterprise Tape Cartridge 3592 media types.
- Increased hierarchical storage management (HSM) performance through use of new search CCW to speed HSM Audit functions

Tape Encryption Overview

Data is one of the most highly valued resources in a competitive business environment. Protecting that data, controlling access to it, and verifying its authenticity while maintaining its availability are priorities in our security-conscious world. Data encryption is a tool that answers many of these needs.

The IBM System Storage TS1120 (3592 Model E05) and TS1130 (3592 Model E06) tape drives are capable of encrypting data as it is written to any size IBM TotalStorage Enterprise Tape Cartridge 3592, including WORM cartridges. Encryption is performed at full line speed in the tape drive after compression. (Compression is more efficiently done before encryption.) This new capability adds a strong measure of security to stored data without the processing overhead and performance degradation associated with encryption performed on the server or the expense of a dedicated appliance.

Three major elements comprise the tape drive encryption solution:

The encryption-enabled tape drive
> All TS1130 Tape Drives are *encryption-capable*. All TS1120 Tape Drives with Feature Code 5592 or 9592 are *encryption-capable*. This means that they are functionally capable of performing hardware encryption, but this capability has not yet been activated. In order to perform hardware encryption, the tape drives must be *encryption-enabled*. In an IBM System Storage TS3500 Tape Library, TS1120 or TS1130 tape drives can be encryption-enabled through the IBM System Storage Tape Specialist.

> **Note:** When a TS1130 Tape Drive is attached to a 3592 J70 or C06 tape controller, the tape drive must be encryption-enabled for system-managed encryption. This applies even when encryption is not being used by the host.

> When TS1130 or TS1120 tape drives are attached to a control unit, this process consists of having an IBM representative set up the drive as encryption-enabled. Only encryption-enabled TS1120 and TS1130 tape drives can be used to read and write encrypted 3592 tape cartridges.

Encryption key management
> Encryption involves the use of several kinds of keys, in successive layers. How these keys are generated, maintained, controlled, and transmitted depends upon the operating environment where the encrypting tape drive is installed. Some applications, such as Tivoli Storage Manager, are capable of performing

key management. For environments without such applications or those where application agnostic encryption is desired, IBM provides the IBM Encryption Key Manager component for the Java platform to perform all necessary key management tasks. "Managing Encryption" describes these tasks in more detail.

Encryption policy
This is the method used to implement encryption. It includes the rules that govern which volumes are encrypted and the mechanism for key selection. How and where these rules are set up depends on the operating environment. See "Managing Encryption" for more information.

Note: In the Tape Storage environment, the Encryption function on tape drives (desktop, stand-alone and within libraries) is configured and managed by the customer and not the IBM System Services Representative (SSR). In some instances SSRs will be required to enable encryption at a hardware level when service access or service password controlled access is required. Customer setup support is by Field Technical Sales Specialist (FTSS), customer documentation, and software support for encryption software problems. Customer "how to" support is also provided via support line contract.

Managing Encryption

The IBM Encryption Key Manager component for the Java platform (hereafter referred to as the Encryption Key Manager) is a Java software program that assists IBM encryption-enabled tape drives in generating, protecting, storing, and maintaining encryption keys that are used to encrypt information being written to, and decrypt information being read from, tape media (tape and cartridge formats). The Encryption Key Manager operates on z/OS®, i5/OS®, AIX®, Linux®, HP-UX, Sun Solaris, and Windows, and is designed to be a shared resource deployed in several locations within an Enterprise. It is capable of serving numerous IBM encrypting tape drives, regardless of where those drives reside (for example, in tape library subsystems, connected to mainframe systems through various types of channel connections, or installed in other computing systems.)

The Encryption Key Manager uses a keystore to hold the certificates and keys (or pointers to the certificates and keys) required for all encryption tasks. It supports the following IBM keystores: JCEKS, JCE4758KS/JCECCAKS, JCE4785RACFKS/ JCECCARACFKS, JCERACFKS, PKCS11IMPLKS, and IBMi5OSKeyStore. See *IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide*, GA76-0418, for detailed information about EKM and the keystores it supports.

The Encryption Key Manager acts as a daemon process awaiting key generation or key retrieval requests sent to it through a TCP/IP communication path between the Encryption Key Manager and the tape library, tape controller, tape subsystem, device driver, or tape drive. When a tape drive writes encrypted data, it first requests an encryption key. Upon receipt of the request, the Encryption Key Manager generates an Advanced Encryption Standard (AES) key and serves it to the tape drives in two protected forms:

For TS1120 and TS1130 Tape Drives: The Encryption Key Manager generates an Advanced Encryption Standard (AES) key and serves it to the tape drives in two protected forms:

- Encrypted or *wrapped*, using Rivest-Shamir-Adleman (RSA) key pairs. The tape drive writes this copy of the key to the cartridge memory and three additional places on the tape media in the cartridge for redundancy.
- Separately wrapped for secure transfer to the tape drive where it is unwrapped upon arrival and the key inside is used to encrypt the data being written to tape.

When an encrypted tape cartridge is read by a TS1120 or TS1130 Tape Drive, the protected AES key on the tape is sent to the Encryption Key Manager where the wrapped AES key is unwrapped. The AES key is then wrapped with a different key for secure transfer back to the tape drive, where it is unwrapped and used to decrypt the data stored on the tape. The Encryption Key Manager also allows protected AES keys to be rewrapped, or rekeyed, using different RSA keys from the original ones used when the tape was written. Rekeying is useful when an unexpected need arises to export volumes to business partners whose public keys were not included; it eliminates the need to rewrite the entire tape and enables a tape cartridge's data key to be reencrypted with a business partner's public key.

There are three methods of encryption management to choose from. These methods differ in where the encryption policy engine resides and where key management is performed for your encryption solution, and how the Encryption Key Manager is connected to the drive. Your operating environment determines which is the best for you. Key management and the encryption policy engine may be located in any one of the following three environmental layers.
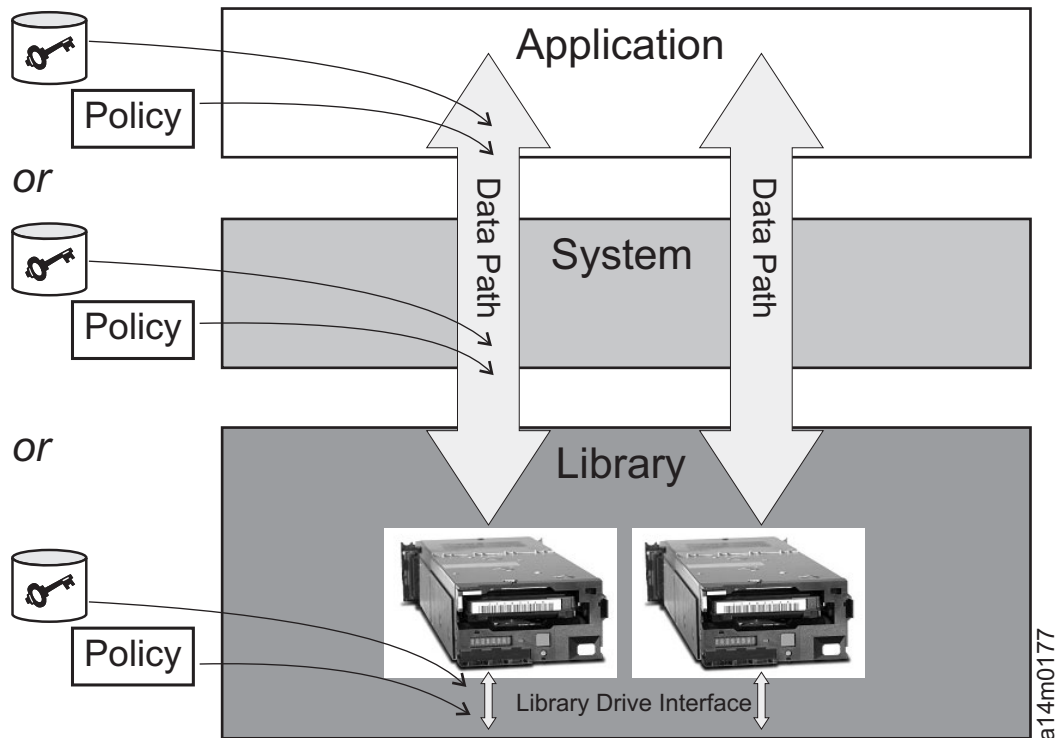
Figure 1. Three possible locations for encryption policy engine and key management.

Application Layer
Initiates data transfer for tape storage, for example TSM.

System Layer
Everything between the application and the tape drives, for example the operating system, z/OS DFSMS™, device drivers, and FICON/ESCON controllers.

Library Layer
The enclosure for tape storage, such as the IBM System Storage TS3500 Tape Library. A modern tape library contains an internal interface to each tape drive within it.

Application-Managed Tape Encryption

This method is best where operating environments run an application already capable of generating and managing encryption policies and keys, such as Tivoli Storage Manager. Policies specifying when encryption is to be used are defined through the application interface. The policies and keys pass through the data path between the application layer and the encrypting tape drives. Encryption is the result of interaction between the application and the encryption-enabled tape drive, and does not require any changes to the system and library layers. Because the application manages the encryption keys, data volumes written and encrypted using the application-managed encryption method can only be read by the same software application that wrote them.

The Encryption Key Manager is not required by, or used by, application-managed tape encryption.

Application-managed tape encryption on IBM TS1120 and TS1130 tape drives may use either of two encryption command sets:
* The IBM encryption command set developed for the Encryption Key Manager
* The T10 command set defined by the InterNational Committee for Information Technology Standards (INCITS)

Application-managed tape encryption using the TS1120 and TS1130 Tape Drive is supported in the following IBM libraries:
* IBM System Storage TS3400 Tape Library
* IBM System Storage TS3500 Tape Library
* IBM TotalStorage 3494 Tape Library

For details about setting up Application-Managed tape encryption, see your Tivoli Storage Manager documentation or visit http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/index.jsp for more information.

System-Managed Tape Encryption

This method is best for encryption on TS1120, TS1130 tape drives in Open Systems and System z™ operating environments where the applications that write or read from tape are not capable of performing the key management required for application-managed encryption.

Open Systems

Encryption policies specifying when to use encryption are set up in the IBM tape device driver. System-managed tape encryption and library-managed tape encryption interoperate with one another. In other words, a tape encrypted using system-managed encryption may be decrypted using library-managed encryption, and vice versa, provided they both have access to the same keys and certificates. Otherwise, this may not be feasible.

For details on setting up system-managed encryption on tape drives in an AIX, Linux, Windows, or Solaris environment, see *IBM Tape Device Drivers Installation and User's Guide*, and the *Planning and Operator Guide* for your tape library.

System z

Encryption policies specifying when to use encryption are set up in z/OS DFSMS (Data Facility Storage Management Subsystem) or implicitly through each instance of IBM device driver. Additional software products such as IBM Integrated Cryptographic Service Facility (ICSF) and IBM Resource Access Control Facility (RACF®) may also be used. Key generation and management is performed by the Encryption Key Manager, a Java application running on the host or externally on another host. Policy controls and keys pass through the data path between the system layer and the encrypting tape drives. Encryption is transparent to the applications.

For TS1120 and TS1130 tape drives connected to an IBM Virtualization Engine TS7700, encryption key labels are assigned on a per-storage pool basis using the TS7700 Maintenance Interface. DFSMS storage constructs are used by z/OS to control the use of storage pools for logical volumes, resulting in an indirect form of encryption policy management. For more information, see the white paper, *IBM Virtualization Engine TS7700 Series Encryption Overview,* available at http://www.ibm.com/support/docview.wss?&uid=ssg1S4000504.

With system-managed encryption, System z hosts can rekey an encrypted tape on the TS1120 and TS1130 tape drives. Refer to the appropriate operating system documentation for the mechanism that is used to initiate a rekey operation. For example, with z/OS, the existing IEHINITT utility is enhanced to support rekeying. Rekeying is useful for customers who export volumes to multiple business partners because it eliminates the need to rewrite the entire tape and enables a tape cartridge's data key to be reencrypted with a business partner's public key.

For details on setting up system-managed encryption on TS1120 and TS1130 tape drives in a System z platform environment, see *z/OS DFSMS Software Support for IBM System Storage TS1130 and TS1120 Tape Drives (3592)*.

Library-Managed Tape Encryption

This method is best for TS1120 and TS1130 tape drives in an open-attached IBM System Storage TS3400 or TS3500 tape library, or IBM TotalStorage 3494 Tape Library. For TS3500, barcode encryption policies may be used to specify when to use encryption, and are set up through the IBM System Storage Tape Library Specialist Web interface. In such cases, policies are based on cartridge volume serial numbers. Library-managed encryption also allows other options, such as encryption of all volumes in a library, independent of bar codes. Key generation and management is performed by the Encryption Key Manager, a Java application running on a library network-attached host. Policy control and keys pass through the library-to-drive interface, therefore encryption is transparent to the applications.

Library-managed encryption, when used with certain applications such as Symantec Netbackup™ or the EMC Legato NetWorker, includes support for an *internal label option*. When the internal label option is configured, the TS1120 or TS1130 Tape Drive automatically derives the encryption policy and key information from the metadata written on the tape volume by the application. Refer to your *Tape Library Operator's Guide* for more information.

Note: If you use library-managed encryption and IBM tape and changer drivers
running on Open Systems platforms (AIX, HP-UX, Linux, Solaris, Windows),
information for bulk rekey is available in the *IBM Tape Device Drivers
Installation and User's Guide*, available at ftp://ftp.software.ibm.com/storage/
devdrvr/Doc/IBM_Tape_Driver_IUG.pdf.

System-managed tape encryption and library-managed tape encryption interoperate
with one another. In other words, a tape encrypted using system-managed
encryption may be decrypted using library-managed encryption, and vice versa,
provided they both have access to the same keys and certificates. Otherwise, this
may not be feasible.

About Encryption Keys

An encryption key is typically a random string of bits generated specifically to
scramble and unscramble data. Encryption keys are created using algorithms
designed to ensure that each key is unique and unpredictable. The longer the key
constructed this way, the harder it is to break the encryption code. Both the IBM
and T10 methods of encryption use 256-bit AES algorithm keys to encrypt data.
256-bit AES is the encryption standard currently recognized and recommended by
the U.S. government, which allows three different key lengths. 256-bit keys are the
longest allowed by AES.

Two types of encryption algorithms may be used by the Encryption Key Manager:
symmetric algorithms and asymmetric algorithms. Symmetric, or secret key
encryption, uses a single key for both encryption and decryption. Symmetric key
encryption is generally used for encrypting large amounts of data in an efficient
manner. 256-bit AES keys are symmetric keys. Asymmetric, or public/private
encryption, uses a pair of keys. Data encrypted using one key can only be
decrypted using the other key in the public/private key pair. When an asymmetric
key pair is generated, the public key is typically used to encrypt, and the private key
is typically used to decrypt.

The Encryption Key Manager uses both symmetric and asymmetric keys; symmetric
encryption for high-speed encryption of user or host data, and asymmetric
encryption (which is necessarily slower) for protecting the symmetric key.

Encryption keys may be generated by the Encryption Key Manager, by applications
such as Tivoli Storage Manager, or by a utility such as keytool. The responsibility
for generating AES keys and the manner in which they are transferred to the tape
drive depends on the tape drive type and the method of encryption management.
However, it may be helpful to understand the difference between how the
Encryption Key Manager uses encryption keys and how other applications use
them.

How the Encryption Key Manager Processes Encryption Keys

On TS1120 and TS1130 tape drives

In system-managed and library-managed tape encryption, unencrypted data (clear
text) is sent to the tape drive and converted to ciphertext using a symmetric 256-bit
AES Data Key (DK) generated by the Encryption Key Manager. The cyphertext is
then written to tape. The Encryption Key Manager uses a single, unique Data Key
for each Enterprise Tape Cartridge. This Data Key is also encrypted, or wrapped, by
the Encryption Key Manager using the public key from an asymmetric Key
Encrypting Key (KEK) pair. This process creates an Externally Encrypted Data Key
(EEDK). The EEDK is written to the cartridge memory and to three additional places

on the tape media in the cartridge. The tape cartridge now holds both the encrypted data and the means to decrypt it for anyone holding the private part of the KEK pair. Figure 2 illustrates this process.

The DK is also wrapped a second time, possibly using the public key of another party, to create an additional EEDK. Both EEDKs can be stored on the tape cartridge. In this way, the tape cartridge can be shipped to a business partner holding the corresponding private key that would allow the DK to be unwrapped and the tape decrypted by the business partner.

Clear Data → $E_{sym}\{data,DK\}$ → Cipher Text → Encrypted Tape

DK

KEK → $E_{asy}\{DK,KEK\}$ → EEDK → Encrypted Tape

a14m0176
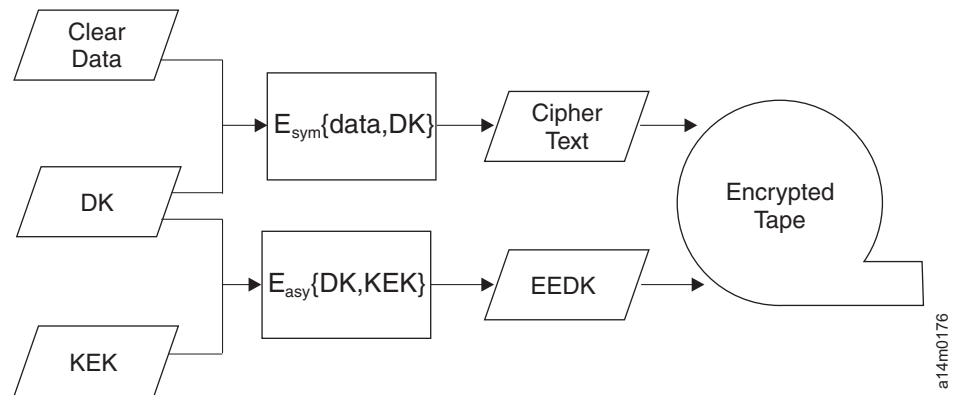
Figure 2. Encryption Using both Symmetric and Asymmetric Encryption Keys. System-Managed and Library-Managed Encryption on TS1120 and TS1130 tape drives

Encryption Key Processing by Other Applications (Encryption Key Manager not Used)

In application-managed tape encryption, unencrypted data (clear text) is sent to the tape drive and converted to ciphertext using a symmetric Data Key (DK) provided by the application, and is then written to tape. The Data Key is not stored anywhere on the tape cartridge. Once the encrypted volume is written, the Data Key must be in a location available to the application, a server database, for example, in order for the volume to be read.

TS1120 and TS1130 tape drives can use applications such as Tivoli Storage Manager for application-managed encryption. Tivoli Storage Manager uses a single, unique Data Key for each tape cartridge.

Alternatively, the tape drives can be used by applications that use the T10 command set to perform encryption. The T10 command set uses symmetric 256-bit AES keys provided by the application. T10 can use multiple, unique Data Keys per tape cartridge, and even write encrypted data and clear data to the same tape cartridge. When the application encrypts a tape cartridge, it selects or generates a Data Key using a method determined by the application and sends it to the tape drive. The key is **not** wrapped with an asymmetric public key and it is **not** stored on the tape cartridge. Once the encrypted data is written to tape, the Data Key must be in a location available to the application in order for the data to be read.

The process for application-managed tape encryption is shown in Figure 3 on page 10.
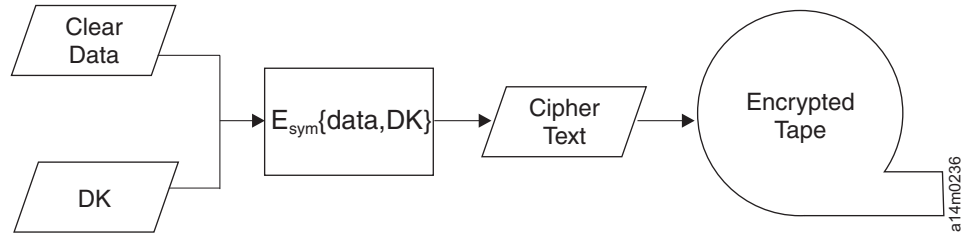
| *Figure 3. Encryption Using only Symmetric Encryption Keys. Application-Managed Encryption on TS1120 and TS1130 tape drives.*

Supported Installations

The 3592 Tape Drives and the TS1120 (C06) Controller are supported in the following environments:

| • IBM System Storage TS3400 Tape Library (see the *IBM System Storage TS3400*
| *Tape Library Planning and Operator Guide*, GC27-2107)

• IBM System Storage TS3500 Tape Library (see the *IBM System Storage TS3500 Tape Library Introduction and Planning Guide*, GA32-0559)

• IBM TotalStorage Enterprise Tape Library 3494 (see the *IBM TotalStorage Enterprise Automated Tape Library (3494) Introduction and Planning Guide*, GA32-0448)

• standalone racks

The TS1120 (C06) Controller does not support 3590 tape drives. When installed in the 3494 tape libraries, the TS1120 (C06) Controller is located in the IBM System Storage 3952 Tape Frame F05 (3952 Tape Frame). When installed in the 3584 tape libraries, the TS1120 (C06) Controller is located in the IBM TotalStorage 3953 Tape Frame F05 (3953 F05 Tape Frame).

The 3592 Tape Drives and/or the 3592 J70 Controller are supported in the following environments:

• IBM System Storage TS3500 Tape Library – 3592 Tape Drives only. The 3592 Model J70 Controller is not supported (see the *IBM System Storage TS3500 Tape Library Introduction and Planning Guide*, GA32-0559)

• IBM TotalStorage Enterprise Tape Library 3494 (see the *IBM TotalStorage Enterprise Automated Tape Library (3494) Introduction and Planning Guide*, GA32-0448)

• IBM TotalStorage Enterprise Tape Drive Frame 3590 Model A14 (see the *IBM TotalStorage Enterprise Tape System 3590 Introduction and Planning Guide*, GA32-0329)

• standalone racks

| The 3592 Tape Drives use a tape cartridge with a form factor similar to the 3590 tape cartridges, which allows them to be used in automated environments, such as the ones listed above and also in StorageTek Automated Cartridge System (ACS) solutions (see the *IBM System Storage 3952 Tape Drive Frame Introduction, Planning, and User's Guide*, GA32-0463 or the *IBM TotalStorage Silo Compatible Tape Frame 3590 Introduction, Planning, and User's Guide*, GA32-0366).
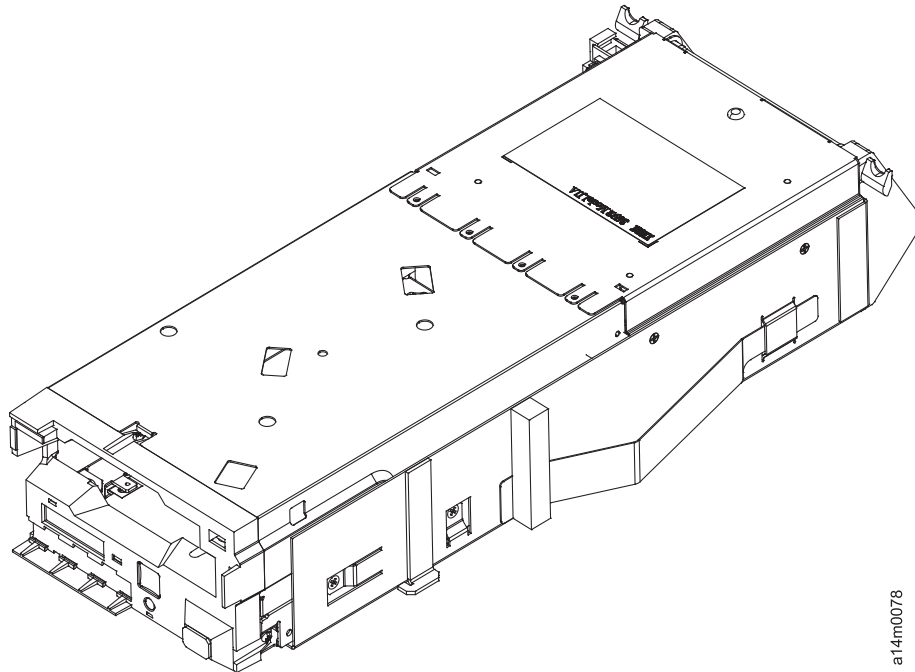
Figure 4. 3592 Tape Drive in Canister

The 3592 drive can connect to IBM tape controllers, including the TS1120 (C06) Controller, the 3592 Model J70, and the 3590 Model A60, for FIbre CONnections (FICON) and Enterprise Systems CONnection (ESCON). The 3592 Model J1A Tape Drive can connect to the TS1120 (C06) Controller, the 3592 Model J70, or the 3590 Model A60, but the 3592 Model E05/E06/EU6 Tape Drive only connects to the TS1120 (C06) Controller and the 3592 Model J70 Controller. For consistency of drive capability, all 3592 Model E06 and EU6 tape drives connected to IBM tape controllers must be configured as encryption-enabled. The 3592 tape cartridge has external dimensions (form factor) that allow it to be used within existing storage cells of libraries containing 3590 tapes. However, the 3592 tape drives must be installed in frames separate from any 3590 drives. Model 3592 tape cartridges are not compatible with 3590 tape drives, and, likewise, 3590 tapes cannot be used in the 3592 drives.

The 3592 drive is enclosed in a canister, and is a hot-swappable/quick disconnect field-replaceable unit (FRU). Installations and replacements are to be completed by qualified IBM service representatives only. The tape drive canister unit does not have its own power supply, but is powered on when the canister is plugged into the drive cradle, or frame installation. Each drive cradle has dual redundant power supplies, which provide power to the two canister slots. Once power is supplied to the unit, the drive will perform several self-tests. Fibre Channel connectors should not be connected to the canister until configuration has been completed through the service panel by the service technician.

In certain installations, the 3592 tape drives can be attached through Fibre Channel switches to the TS1120 (C06) Controller, the 3592 Model J70, or the 3590 Model A60 (3592 Model J1A only) control unit. The 3592 model J70 also supports the attachment of 3590 models B, E, and H Fibre Channel attached tape drives. For more information on these control units and switches, see the *IBM System Storage TS1120 Tape Drive and Controller Introduction and Planning Guide*, GA32-0464 or the *IBM TotalStorage Enterprise Tape System 3590 Introduction and Planning*

Guide, GA32-0329. Once the tape controller is installed, there are no accessible operator controls or displays. All tape controller displays and controls are for use by qualified IBM service representatives only.

This document will cover the operations of the 3592 drive. For more detailed technical planning information for the 3592, see the *IBM System Storage TS1120 Tape Drive and Controller Introduction and Planning Guide*, GA32-0464.

Drive environmental conditions

The following table summarizes the recommended environmental conditions when operating, storing, and shipping the 3592 drive.

Table 1. Tape Drive 3592 environmental operating, storage, and shipping conditions

Condition	Air Temperature	Relative Humidity (non-condensing)	Maximum Wet Bulb
Operating	16 to 32°C (60.8 to 89.6°F)	20 to 80%	26°C (78.8°F)
Recommended Operating Range	20 to 25°C (68 to 77°F)	40 to 50%	23°C (73.4°F)
Storage*	1 to 60°C (33.8 to 140°F)	10 to 90%	26°C (78.8°F)
Shipping*	-40 to 60°C (-40 to 140°F)	10 to 90%	26°C (78.8°F)
*Excluding tape cartridges. See "Environmental and shipping specifications for tape cartridges" on page 30 for more information on the environmental conditions recommended for the tape cartridges.			

Substantial deviations in either direction from the recommended operating range, if sustained for extended periods of time, will expose the unit to greater risk of failure. Limited deviations from the recommended operating range will minimize the risk of thermal and hygroscopic expansion effects.

When the drive is installed, acclimation time is required before using the drive if the temperature of the drive is different from the temperature of the environment it will be operated in. The drive must be acclimated to the operating environment for a minimum of 4 hours after the drive has been unpacked. If any condensation is observable on the exterior surfaces, acclimate the drive for at least 4 hours, plus 1 additional hour after all condensation has evaporated.

Chapter 2. Drive controls, displays, and messages

The 3592 drive is a highly automated device, and is typically managed through a Library Manager or host and its associated software. Additional displays and operations are available for the individual drives, primarily when the library has been set to manual mode. The following sections describe components, operations, and messages that operators may need to become familiar with, in the event of library automation failures.

> ⚠ **CAUTION:**
> **The operator should remember the importance of safe operation when performing any of the tasks in this book. The operator should know the location of, and how to use the switches and controls on the particular tape library where this drive is installed. The front doors on the library should not be opened during normal operation because of the moving components within the library. (72XXC356)**

> ⚠ **Attention:** Take care in handling the front of the drive. Keep the entire bezel, and particularly the white reflective fiducials and the black surfaces surrounding the fiducials clean (see 1 in Figure 5 on page 14). Oil or dirt on the black surfaces adjacent to the reflective fiducials can cause reflectance problems, interfering with the library cartridge handling device's ability to locate the drive.

The Unload button (see 4 in Figure 5 on page 14) is used to manually unload a tape from the drive. If you press this button while a tape is loaded, the drive will complete any operation in progress, then rewind and unload the cartridge. The Reset button 5 will generate a drive reset. The microcode will terminate any current tape motion and come to a complete stop before honoring the reset. The button is recessed to prevent accidental activation. Use a pencil or small screwdriver to press the reset button. The green LED power indicator 6 shows whether or not power is provided to the drive. As part of the power-up process, the LED will automatically come on, and the drive will perform a number of power-on self tests. During reset, the LED may display in a blinking mode. This indicates that the drive is attempting to unload the cartridge prior to the actual reset process.

Drive front panel components

Figure 5 on page 14 shows the front bezel of the 3592 drive and its main components. Since these components are on the front side of the drive, they will generally only be accessible from the interior of the library.

1 Reflective fiducials	5 Reset button
2 Tape cartridge slot	6 LED power indicator
3 Non-reflective fiducial	7 8-character message display
4 Unload button	8 3494 Fiducial
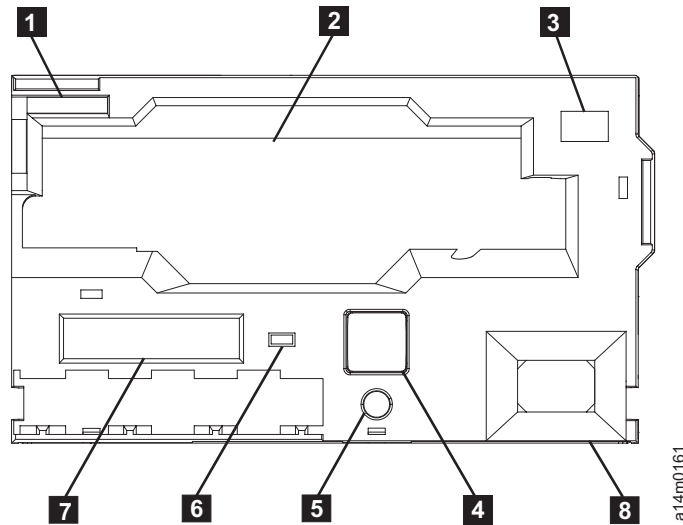
Figure 5. Front view, 3592 Tape drive

Fiducials

Reference keys **1** and **3** in Figure 5 identify the fiducials on the front bezel of the 3592 drive. These fiducials are used by cartridge-handling devices to locate where the tape system device is installed. The reflective fiducials **1** are white, and their light-reflective properties are used by the cartridge handling devices to locate the drive. The non-reflective fiducial **3** is a hole, which is used by a different type of locating mechanism. Any debris on these fiducials or shiny contamination on other areas of the bezel can interfere with this device locating function. Do not cover or change any of the fiducials. **8** identifies the 3494 Fiducial.

Display panels

When the 3592 drive is managed through a host and its associated software, refer to the appropriate library operator guide and software manuals for information about retrieving drive information. There are also times, such as in manual mode, when information about an individual drive may need to be viewed directly from the drive itself. Two different displays provide messages and action options; one is a message display for the operator on the front of the drive, and the other is a separate service panel for a qualified service representative.

On the front of the drive, an 8–character display panel (see **7** in Figure 5) displays drive status codes and also offers a limited actions menu. These display messages are described in more detail in "Drive messages."

Drive messages

In the event of library automation failures, the Library Manager operator panel or other host operator panel may indicate that manual operations are required for specific drives and tape cartridges. In addition to the messages on the library display panel, individual drives can also display messages on the 8–character drive message display.

These messages can be of four types:

- mount messages (which are governed by the host control or library)
- attention messages
- FID (failure ID) messages
- drive status messages

Some of these messages will require intervention by a service representative.

Mount messages

These messages are governed by the host or library and its associated software. The messages displayed will vary, depending upon the installed host software. As an example, it may indicate to manually mount a specific tape cartridge into the drive.

Attention messages

When the drive message displays ATTN DRV, the drive has experienced either a load error (indicated by the LOAD ERR alternating message) or an unload error (indicated by the UNLOAD E alternating message). If you receive either of these messages, call your service representative.

FID messages

Failure ID (FID) messages are short codes that can be used by service technicians to isolate problems with the device. If a FID message appears, you must note the message before contacting your service representative. This message is commonly a two-part, alternating message on the display. A FID error condition message has priority over all other types of messages, and persists until corrected. Technicians use the FID code to identify the failing FRU within the drive subsystem, therefore it is necessary for the operator to make note of the FID message to provide this information to the service representative. An example of the format of these messages is 'FID1 FF', alternating with an engineering error code, such as 931C9999. In this example, 'FID' indicates to the operator that a hardware failure occurred, and 1 indicates the severity code. 'FF' is the FID number that the service representative uses to enter the Maintenance Package. The alternating display of the engineering error code provides specific support information to the service organization. See Appendix B, ″FID messages,″ for more information on FID messages.

Drive status messages

A variety of messages can be displayed on the 8–character panel which indicate the current status of the drive. Typically, drive-generated status messages are right-justified and have an * (asterisk) as the final character, and usually indicate the process the drive is currently going through. If the first character is @ (*at* symbol), the drive is at the specified state, and the process has been completed.

Table 2. Drive status messages

Message	Message Meaning
<blank>	If the message panel is blank, there are several possibilities: • The drive is not powered on • The drive is ready • There is no status • No cartridge is mounted
<all 8 elements fully lit>	During the reset/power-on process, the diagnostic test is verifying that all elements are working.

Table 2. Drive status messages (continued)

AJAR*	A cartridge is in the throat of the drive and is not in a loadable position. Alternatively, if no cartridge or other obstruction is in the drive, the sensor may not be functioning correctly, and the hardware may be defective. If no cartridge or other obstruction is in the drive, contact your service representative.
CLEAN*	Drive cleaning is in process
CODELOAD	Microcode is being loaded. This process takes a few minutes. The drive should not be powered off or reset in this condition.
DIAGS*	Diagnostics are running
EMPTY*	There is no cartridge in the throat of the drive. Alternatively, if a cartridge is in the drive, the sensor may not be functioning correctly, and the hardware may be defective. If a cartridge is present in the drive, contact your service representative **Note:** Microcode levels prior to release level 464 (October 2003) will not display ″EMPTY*″ when no cartridge is present in the drive (the display will be blank). This is not an error condition. If this behavior is desired, the drive code should be updated to the latest version.
ERASE*	Data erase is in process
LOAD*	Load is in progress
@LOAD*	Load is complete, cartridge is at load point
LOCATE*	Locate is in progress
MIDTAPE*	Drive was reset or powered on with a tape loaded, and is in the process of bringing drive and tape to cleanly recovered state. Exercise patience, process may take up to 15 minutes.
NEW CODE	Codeload has completed, drive in process of resetting to apply that code
READ*	Data read is in progress
READY*	Drive is in ready state. (Panel can also be blank in ready state)
RESET* and RESET!!!	Drive is in the process of resetting
REWIND*	Rewind operation is in progress
UNLOAD*	Unload has been requested, or is in progress
@UNLOAD*	Unload is complete, the cartridge is in the unloaded position. (Note that the display will go blank if the cartridge is removed)
WRITE*	Data write is in progress

In addition to the drive status messages listed in Table 2 on page 15, the icons displayed in Figure 6 on page 17 may also be displayed as the first or last character in the message display. These icons provide information about the drive or the tape cartridge currently in the drive. All icons, except the ″clean required″ icon appear as the leftmost character. The ″clean required″ icon replaces the ″*″ symbol in the status messages, as the rightmost character.

Icon	Meaning
▲	Physical write protect
⌂	Logical write protect
▯	Dump present
⣏	Clean required
⣇	WORM tape

a14m0144

Figure 6. Drive message display icons

- Physical write protect means that the cartridge write-protect switch is positioned to prevent writing data to the tape.
- Logical write protect means that either the host has sent a command to prevent writing to the tape, or the drive has disallowed writing due to some internally detected condition.
- Dump present indicates that there is performance-related data stored within the drive dynamic random access memory. This dump data can be retrieved by a service representative for troubleshooting purposes.
- Clean required means that the drive needs to be cleaned by means of a cleaning cartridge.
- WORM tape indicates that the cartridge currently in the drive is a WORM cartridge.

Chapter 3. IBM TotalStorage Enterprise Tape Cartridge 3592

The 3592 Tape Drive has a bidirectional read/write head capable of operating at three different recording densities, depending on the tape drive model. The 3592 Model E06 reads data in EFMT1 (512 tracks on 8 channels), EFMT2 (896 tracks on 16 channels), and EFMT3 (1152 tracks on 16 channels), but only writes EFMT2 and EFMT3. The 3592 Model E05 drive writes and reads EFMT1 and EFMT2. The 3592 Model J1A writes and reads only EFMT1.

Table 3. Supported 3592 R/W Formats

3592 Tape Drive	EFMT1 512 Tracks/ 8 Channels	EFMT2 896 Tracks/ 16 Channels	EFMT3 1152 Tracks/ 16 Channels
Model J1A	R/W		
Model E05	R/W[1]	R/W	
Model E06[2]	R	R/W	R/W
[1] Model E05 can read and write EFMT1 operating in native or J1A emulation mode. [2] Model E06 does not support emulation but reads all three formats in native mode.			

The standard TotalStorage Enterprise Tape Cartridge 3592 Data has a native capacity of 640 GB (596.04 GiB) when formatted for EFMT3, 500 GB (465.66 GiB) when formatted for EFMT2, and 300 GB (279.39 GiB) when formatted for EFMT1.

The TotalStorage Enterprise Tape Cartridge 3592 Economy has a native capacity of 128 GB (119.21 GiB) in EFMT3, 100 GB (93.13 GiB) in EFMT2, and 60 GB (55.88 GiB) in EFMT1.

The TotalStorage Enterprise Tape Cartridge 3592 Extended has a native capacity of 1000 GB (931.32 GiB) in EFMT3 and 700 GB (651.93 GiB) in EFMT2. The TotalStorage Enterprise Tape Cartridge 3592 Extended is not supported on the 3592 J1A Tape Drive or on a 3592 E05 Tape Drive emulating a 3592 J1A Tape Drive (EFMT1).

Capacities of data cartridges can be increased through data compression, with the actual compression and capacity depending upon the specific data. WORM cartridges are also available in all capacities. All Enterprise Tape Cartridge 3592 types can be encrypted.

The 3592 tape drive is designed to support capacity scaling of individual 3592 Data tape cartridges over a broad range of capacities. The effect of capacity scaling is to contain data in a specified fraction of the tape, yielding faster locate and read times. Alternatively, 3592 Economy tape cartridges can be used to achieve this faster performance.

The 3592 tape drive also divides the tape into longitudinal segments. Using this capability, it is possible, for example, to segment 300 GB (279.39 GiB) Data tapes into two segments, one segment of 60 GB (55.88 GiB) with very fast access, and another 200 GB (186.26 GiB) segment for additional capacity. The 3592 Data tapes can be purchased pre-formatted in these segments, or can be segmented and capacity scaled at a later time. Segmentation is only available within a specified range of capacity scaling settings. Capacity scaling is not supported for Economy or WORM (any size) tapes. For information on implementing segmentation and

capacity scaling, consult the PDF files in the Doc directory, which you can find by navigating in a web browser to either of these two URLs:

* `ftp://ftp.software.ibm.com/storage/devdrvr`
* `ftp://207.25.253.26/storage/devdrvr`

Refer also to the *IBM System Storage TS1120 Tape Drive SCSI Reference* for more technical information regarding WORM, capacity scaling, and segmentation.

Cartridge types and characteristics

Cartridges can be distinguished by the text on the label, as well as by the color of the tape cartridge case and the color of the cartridge label (see 2 in Figure 7 on page 21), write-protect switch 4, and door (see 1 in Figure 9 on page 23). The characteristics of the four different data cartridge types and the cleaning cartridge that can be used by operators with the 3592 drive are summarized in Table 4. The main external components of the IBM 3592 TotalStorage Enterprise Tape Cartridge are shown in Figure 7 on page 21.

The capacity of the IBM 3592 TotalStorage Enterprise Tape Cartridge depends on whether it is used by the 3592 Model J1A, Model E05, or Model E06. The J1A uses Enterprise Format 1 (EFMT1) recording technology. The E05 also uses EFMT1 but when operating as a native E05, it also uses Enterprise Format 2 (EFMT2) technology, which records at increased density. The E06 does not support J1A emulation but can read EFMT1 data and write to tapes formatted in EFMT2 or EFMT3 (when writing from BOT). The J1A cannot read or write using EFMT2 or EFMT3. Therefore, tapes using EFMT2 can only be used in the E05 and E06. Tapes using EFMT3 can only be used in the E06.

All Enterprise Tape Cartridge types can be used with the encryption function of the 3592 Models E05 and E06. Encrypted cartridges use a unique, Enterprise Encrypted Format 2 (EEFMT2) or Enterprise Encrypted Format 3 (EEFMT3) format.

Table 4. IBM TotalStorage Enterprise Tape Cartridge 3592 types

Name	Type (Media)[1]	Native Capacity (EFMT1)	Native Capacity (EFMT2)	Native Capacity (EFMT3)	Case Color	Label, Door, & Write-Protect Switch Color	Part Number
DATA[2]	JA (MEDIA5)	300 GB (279.39 GiB[3])	500 GB (465.66 GiB)	640 GB (596.04 GiB)	Black	Dark Blue	18P7534
EXTENDED DATA	JB (MEDIA9)	N/A	700 GB (651.93 GiB)	1000 GB (931.32 GiB)	Black	Dark Green	23R9830
ECONOMY	JJ (MEDIA7)	60 GB (55.88 GiB)	100 GB (93.13 GiB)	128 GB (119.21 GiB)	Black	Light Blue	24R0316
WORM	JW (MEDIA6)	300 GB (279.39 GiB)	500 GB (465.66 GiB)	640 GB (596.04 GiB)	Platinum (silvery gray)	Dark Blue	18P7538
EXTENDED WORM	JX (MEDIA10)	N/A	700 GB (651.93 GiB)	1000 GB (931.32 GiB)	Platinum (silvery gray)	Dark Green	23R9831

ECONOMY WORM	JR (MEDIA8)	60 GB (55.88 GiB)	100 GB (93.13 GiB)	128 GB (119.21 GiB)	Platinum (silvery gray)	Light Blue	24R0317
CLEANING	JA + CLN	—	—	—	Black	Gray	18P7535

[1]This type designation appears as the last two characters on standard barcode labels. In addition, for cleaning cartridges, the first three characters of the volume serial number (VOLSER) are CLN.

[2]The Data (EFMT1) type cartridge can also be ordered in a 279.2 GB (260 GiB) segmented, capacity scaled format providing 60 GB (55.88 GiB) of high performance random access, and an additional 200 GB (186.26 GiB) of capacity.

[3]One gibibyte (GiB) = 2^{30} bytes = 1,073,741,824 bytes = 1024 mebibytes (MiB)

Note: In addition to these cartridges, there is a ″CE″ cartridge for use by IBM Service Representatives only. The VOLSER label for this cartridge begins with ″CE″ followed by a space and three numerals, and ending with ″JA″.

Cartridge external components

The main external components, common to all types of 3592 tape cartridges are shown in Figure 7 and Figure 8 on page 22.
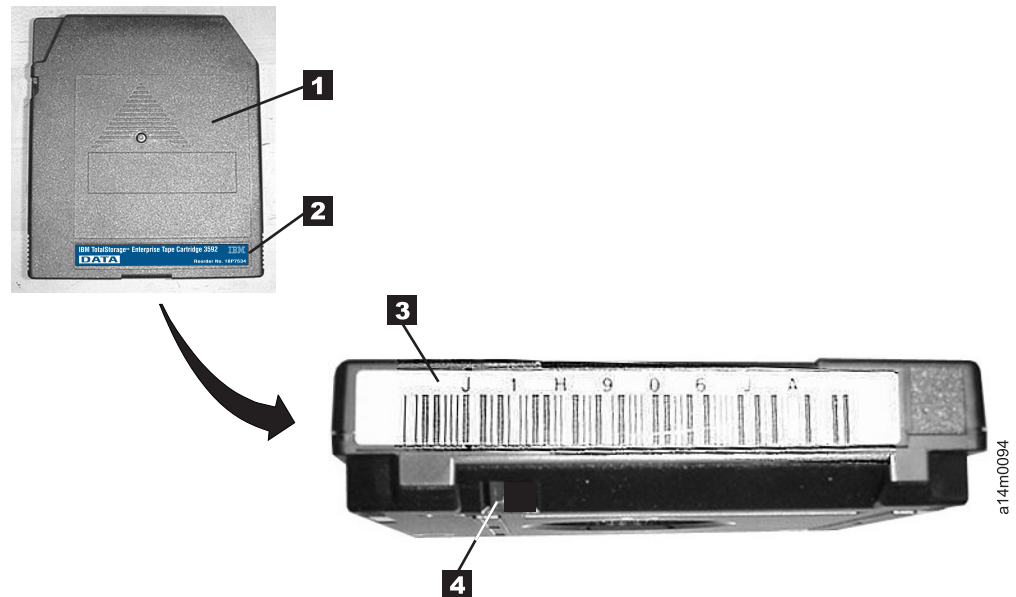
Figure 7. IBM TotalStorage Enterprise Tape 3592 Data Cartridge

1	Cartridge case	**3**	Cartridge bar code label
2	IBM product label	**4**	Write-protect selector

In tape libraries, the library vision system identifies the types of cartridges during an inventory operation. The vision system reads a volume serial number (VOLSER) **3** , which appears on the label on the edge of the cartridge. The VOLSER

contains from one to six characters, which are left-justified on the label. If fewer than six characters are used, spaces are added. The media type is indicated by seventh and eighth characters. The different cartridge type codes are shown in the ″Type″ column of Table 4 on page 20.

If you are attaching VOLSER labels to cartridges that do not have pre-attached labels, place the label entirely within the label recessed area on the cartridge. See **3** in Figure 7 on page 21 as an example of proper placement. The label must be flat to within 0.5 mm (0.02 in.) over the length of the label and have no folds, missing pieces, tears, or any extraneous markings. Failure to follow these placement requirements will result in degraded readability.

Each data cartridge includes a write-protect selector **4** which can be set to prevent data from being over-written or erased from the tape by the tape drive. To write-enable a cartridge, slide the selector to the left (see **1** in Figure 8), which exposes a square hole, to permit data to be written to and erased from the cartridge. To write-protect a cartridge, slide the selector to the right **2** , which covers the hole, preventing data to be written to or erased from the cartridge.
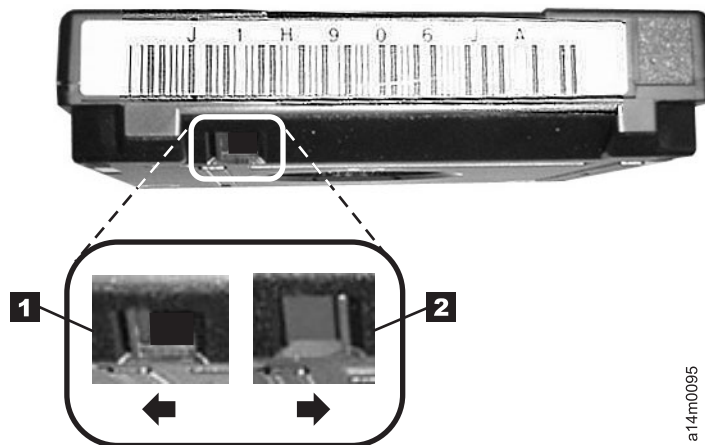
Figure 8. Write-protect selector

1 Write-enabled   **2** Write-protected

When you insert a cartridge into the drive, a threading mechanism pulls the tape leader pin and the attached tape out of the cartridge, across the drive head, and onto a non-removeable take-up reel. The cartridge door (**1** in Figure 9 on page 23) protects the tape from contamination when the cartridge is out of the drive. The only time you should manually retract this door is to check for proper tape pin position (see Figure 17 on page 36).

Figure 9. Data cartridge door

Cartridge Memory (CM)

Each 3592 data cartridge contains a passive, contactless, silicon storage device called cartridge memory (CM). This CM holds information about the cartridge and the media in the cartridge, and holds statistics about the media in the cartridge. The cartridge and media information is stored in a protected, read-only area of the CM. This information is read by the CM reader in the drive, by using a contactless, radio-frequency interface, when the cartridge is loaded into the drive. The media performance statistics are stored in an unprotected, read/write area of the CM. These statistics are updated by the CM reader just before the cartridge is unloaded. The media performance statistics are maintained by the Statistical Analysis and Reporting System (SARS) portion of the drive microcode. Each cleaning cartridge also contains a CM, which tracks the number of cleaning uses.

Write Once Read Many (WORM)

Some records retention and data security applications require the write-once, read-many (WORM) function of tape data storage. The 3592 tape drive, when used in conjunction with WORM media, could serve as a replacement to the IBM 3995 Optical Library where long term records retention is required.

WORM function is accomplished on the 3592 by a combination of a special WORM tape cartridge and microcode controls in the drive. All 3592 drives with the appropriate microcode version installed are capable of reading and writing WORM cartridges.

WORM Tape Cartridge Characteristics

The following lists characteristics of WORM cartridges:

- WORM format pervades the entirety of every WORM cartridge. The WORM tape media is formatted to give every block on a WORM cartridge write-once, read-many protection. Additionally, the cartridge memory (CM) has a WORM indicator byte in the cartridge type field. Both of these conditions must be true for the drive to work with a WORM cartridge. If one condition is true and the other is false, an ATTN DRV - Invalid Cartridge message will post.

- Each WORM cartridge is identified using a World-wide Unique Cartridge Identifier (WWCID), which is permanent and locked, providing another level of security for data that must be maintained. This permanent locked information is stored in both the cartridge CM and on the tape itself, and can also be associated with the unique barcode VOLSER. WORM cartridges can be audited using the WWCID and the write mount count.

- WORM cartridges are labeled with a 'JW,' 'JX,' or 'JR' and they are color-coded to distinguish them from re-writable cartridges (the color-coding is distinguishable by people with any of the three major varieties color blindness).
- The WORM cartridge is tamper-proof (see "WORM Microcode Controls").
- WORM cartridges can only be read (or appended) on WORM-enabled 3592 drives. Non-WORM enabled drives will not be able to take any action with a WORM cartridge other than to unload it.
- A WORM cartridge can never be made non-WORM.
- A non-WORM cartridge cannot be made WORM.
- Written user data can never be modified or erased. Destruction of the data requires destruction of the media and its usability (heat, crushing, physical shredding, or magnetic fields sufficient to destroy all formatting required to ever read or write the cartridge again)

WORM Microcode Controls

When the drive senses that a cartridge is a WORM cartridge, the microcode prohibits the changing or altering of user data already written on the tape. The microcode keeps track of the last appendable point on the tape by means of an overwrite-protection pointer stored in the cartridge memory (CM). Statistical Analysis and Reporting System (SARS) data can be written and updated on WORM tapes because the SARS data is not in the user area of the tape.

Note: When a WORM cartridge is loaded and positioned at a non–appendable point on a drive attached to a controller, the controller will give good status to a write type command if the data being written is exactly the same as what is already recorded on the media at the same location. However, the tape is not actually written. The tape position will be after the block with the apparent overwrite and all data following will still be valid on tape. When positioned at a non–appendable point on a WORM cartridge, the microcode will report overwrite errors only if attempts are made to write conflicting data. The scenario for this apparent overwrite is as follows: The host issues a write type command to the controller and the tape is at a non–appendable point. The controller will attempt to write the WORM cartridge but the drive will give an overwrite error. The controller will then read the block and compare to the block received from the host. If the block is exactly the same then the controller will give good status to the host and leave the tape positioned after the block which was apparently overwritten. If the block varies in data or size then the controller will reposition the tape in front of the block just read and report the overwrite error to the host. This process is not optimal for performance considerations.

Capacity scaling and segmentation

The 3592 tape drives are designed to support capacity scaling of individual Data tape cartridges over a broad range of capacities. The effect of capacity scaling is to contain data in a specified fraction of the tape, yielding faster locate and read times. Alternatively, economy-length tapes can be purchased to achieve this faster performance.

The 3592 tape drives also divide the tape into longitudinal segments. Using this capability, it is possible, for example, to segment standard 322.1 GB (300 GiB) Data tapes in EFMT1 format into two segments, one segment with 64.2 GB (60 GiB) with very fast access, and another 214.7 GB (200 GiB) segment for additional capacity.

The 322.1 GB (300 GiB) Data tapes can be purchased pre-formatted in these segments, or can be segmented and capacity scaled at a later time. Segmentation is only available within a specified range of capacity scaling settings. Capacity scaling is not supported for either economy or WORM (any size) tapes. For information on implementing segmentation and capacity scaling, consult the README files in the FTP directory pertaining to your device driver, which you can find by navigating in a web browser to either of these two URLs:

- `ftp://ftp.software.ibm.com/storage/devdrvr`
- `ftp://207.25.253.26/storage/devdrvr`

The 3592 tape drive allows an application to issue a command to scale individual cartridges to 20% of their full capacity. For the Model E06 Tape Drive operating in EFMT3 format, the TotalStorage Enterprise Tape Cartridge 3592 Extended (MEDIA9) can be scaled to 200 GB (186.26 GiB), and the TotalStorage Enterprise Tape Cartridge 3592 Data (MEDIA5) can be scaled to 128 GB (119.21 GiB).

For the native Model E05 Tape Drive operating in EFMT2 format, the TotalStorage Enterprise Tape Cartridge 3592 Extended (MEDIA9) can be scaled to 140 GB (130.39 GiB), and the TotalStorage Enterprise Tape Cartridge 3592 Data (MEDIA5) can be scaled to 100 GB (93.13 GiB).

For the 3592 J1A Tape Drive, or the Model E05 operating in EFMT1 format, the data cartridge (MEDIA5) can be scaled to 60 GB (55.88 GiB). Customers using z/OS can exploit the capacity scaling capability of the 3592 drive. A data class parameter determines whether a tape is to be scaled. OPEN processing will scale a tape when the associated data class requests it and the tape is being written from load point (DISP=NEW, file sequence 1). On a subsequent reading of a performance scaled MEDIA5 EFMT1 tape, the data will be entirely contained in the first 60 GB (55.88 GiB) of the tape, yielding very fast locate and read times, while MEDIA5 EFMT2 data will be contained in the first 100 GB (93.13 GiB).

DFSMShsm™ and DFSMSdfp™ OAM can exploit this new feature, as well as other applications that use standard Open/Close/EOV processing. Refer to *z/OS DFSMS Software Support for IBM System Storage TS1130 and TS1120 Tape Drives (3592)*, SC26-7514, for more information about software support for the 3592 drive.

Refer also to the *IBM TotalStorage Enterprise Tape System 3592 SCSI Reference* for more technical information regarding WORM, capacity scaling, and segmentation.

Cartridges pre-scaled for 60 GB (55.18 GiB) or 100 GB (93.13 GiB) capacity are also available for order with the 3599 Tape Media method. These pre-scaled cartridges can be ordered (and labeled) for a specific VOLSER range. This allows capacity scaling to be exploited by an application that permits media pools to be defined by VOLSER range. For information on which Independent Software Vendors (ISV) support capacity scaling by command or with the pre-scaled cartridges, please go to the following URLs:

- For TS1120: `http://www.ibm.com/servers/storage/tape/compatibility/pdf/ts1120_isv_matrix.pdf`
- For 3592: `http://www.ibm.com/servers/storage/tape/compatibility/pdf/3592_isv_matrix.pdf`

Note: VTS does not support capacity scaling or segmentation.

Chapter 4. Cartridge care and handling

This chapter describes the care and handling of the IBM TotalStorage Enterprise Tape Cartridge.

Handling the cartridges

⚠ **Attention:** Do not insert a damaged tape cartridge into your tape drive. A damaged cartridge can interfere with the reliability of a drive and may void the warranties of the drive and the cartridge. Before inserting a tape cartridge, inspect the cartridge case, cartridge door, and write-protect switch for breaks.

Incorrect handling or an incorrect environment can damage the IBM TotalStorage Enterprise Tape Cartridge or their magnetic tape. To avoid damage to your tape cartridges and to ensure the continued high reliability of your IBM TotalStorage Enterprise Tape Drives and IBM System Storage TS1120/TS1130 Tape Drives, use the following guidelines:

Provide training

- Post procedures that describe proper media handling in places where people gather.
- Ensure that anyone who handles tape has been properly trained in handling and shipping procedures. This includes operators, users, programmers, archival services, and shipping personnel.
- Ensure that any service or contract personnel who perform archiving are properly trained in media-handling procedures.
- Include media-handling procedures as part of any services contract.
- Define and make personnel aware of data recovery procedures.

Ensure proper packaging

- When you ship a cartridge, ship it in its original or better packaging.
- Use only shipping containers that securely hold the cartridges in place during transportation. This can be in a well-packaged cardboard box or other container. One such container can be procured from Perm-A-Store at the following URL: **www.turtlecase.com**.
- If you ship the cartridge in a cardboard box or a box of a sturdy material, ensure the following:
  - Place the cartridge in polyethylene plastic wrap or bags to protect it from dust, moisture, and other contaminants.
  - Pack the cartridge snugly; do not allow it to move around.
  - Double-box the cartridge (place it inside a box, then place that box inside the shipping box) and add padding between the two boxes.
- Never ship a cartridge in a commercial shipping envelope. Always place it in a box or package.

Provide proper acclimation and environmental conditions

- Before you use a cartridge, let it acclimate to the normal operating environment for a minimum of 24 hours. If you see condensation on the cartridge, wait an additional hour.
- Ensure that all surfaces of a cartridge are dry before inserting it.
- Do not expose the cartridge to moisture or direct sunlight.
- Do not expose recorded or blank cartridges to stray magnetic fields of greater than 350 oersteds (for example, terminals, motors, video equipment, X-ray equipment, or fields that exist near high-current cables or power supplies). Such exposure can cause the loss of recorded data or make the blank cartridge unusable.
- Maintain the conditions that are described in "Environmental and shipping specifications for tape cartridges" on page 30.

Perform a thorough inspection

After purchasing a cartridge and before using it, perform the following steps:

- Inspect the cartridge's packaging to determine potential rough handling.
- When inspecting a cartridge, open only the cartridge door. Do not open any other part of the cartridge case. The upper and lower parts of the case are welded and held together with screws; separating them destroys the usefulness of the cartridge.
- Inspect the cartridge for damage before using or storing it.
- Check that the leader pin is properly seated (see Figure 17 on page 36).
- If you suspect that the cartridge has been mishandled but it appears usable, copy any data onto a good cartridge immediately for possible data recovery. Discard the mishandled cartridge.

Handle the cartridge carefully

- Do not drop the cartridge. If the cartridge drops, slide the cartridge door back and ensure that the leader pin is properly seated. If the leader pin has become dislodged, go to "Repositioning a leader pin."
- Do not handle tape that is outside the cartridge. Handling the tape can damage the tape's surface or edges, which may interfere with read or write reliability. Pulling on tape that is outside the cartridge can damage the tape and the brake mechanism in the cartridge.
- Do not stack more than six cartridges. Although 3590 tapes can be stacked with 3592 tapes, be cautious about mixing the different types of cartridges, since they are not interchangeable, and can be used only with their respective drives.
- Do not degauss a cartridge that you intend to reuse. Degaussing makes the tape unusable.

Repositioning a leader pin

If the leader pin in your cartridge becomes dislodged from its pin-retaining spring clips, you must use the IBM Leader Pin Reattachment Kit (part number 18P8887) to reposition it.

Repositioning a leader pin

A leader pin that is improperly seated inside a cartridge can interfere with the operation of the drive. Figure 10 on page 29 shows a leader pin in the incorrect **1** and correct **2** positions.

To place the leader pin in its proper position, you will need the following tools:

- Plastic or blunt-end tweezers
- Cartridge manual rewind tool (from the Leader Pin Reattachment Kit, part number 18P8887)
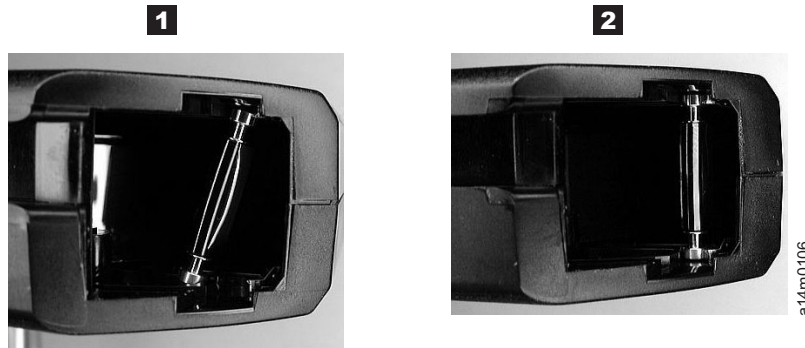
Figure 10. Leader pin in the incorrect and correct positions. The cartridge door is open and the leader pin is visible inside the cartridge.

To reposition the leader pin, perform the following steps.

1. Slide open the cartridge door (**1** in Figure 11) and locate the leader pin **2** (you may need to shake the cartridge gently to roll the pin toward the door).
2. With plastic or blunt-end tweezers, grasp the leader pin and position it in the pin-retaining spring clips **3** .
3. Press the leader pin gently into the clips until it snaps into place and is firmly seated.
4. Close the cartridge door.
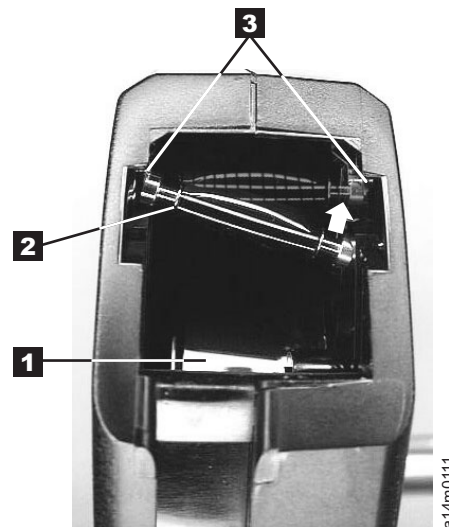
Figure 11. Placing the dislodged leader pin into the correct position. The cartridge door is open, showing the leader pin out of position

5. To rewind the tape, insert the cartridge manual rewind tool (**1** in Figure 12 on page 30) into the cartridge's hub **2** and turn it clockwise until the tape becomes taut.
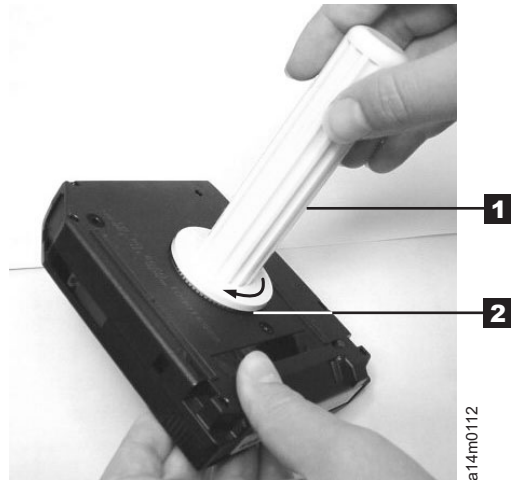
Figure 12. Rewinding the tape into the cartridge

6. Remove the rewind tool by pulling it away from the cartridge.

Environmental and shipping specifications for tape cartridges

Before you use a tape cartridge, acclimate it to the operating environment for 24 hours or the time necessary to prevent condensation in the drive (the time will vary, depending on the environmental extremes to which the cartridge was exposed).

The best storage container for the cartridges (until they are opened) is the original shipping container. The plastic wrapping prevents dirt from accumulating on the cartridges and partially protects them from humidity changes.

When you ship a cartridge, place it in a sealed, moisture-proof bag to protect it from moisture, contaminants, and physical damage. Ship the cartridge in a shipping container that has enough packing material to cushion the cartridge and prevent it from moving within the container.

Table 5 lists the environmental conditions for operating and storing IBM TotalStorage Enterprise Tape Cartridges.

Table 5. Environment for operating and storing the IBM TotalStorage Enterprise Tape Cartridge

Environmental Specifications		
Environmental Factor	Operational Storage	Archival Storage
Temperature	16 to 32°C (60 to 90°F)	16 to 25°C (61 to 77°F)
Relative humidity (non-condensing)	20 to 80%	20 to 50%
Wet bulb maximum temperature	26°C (79°F)	26°C (79°F)
Magnetic field	Stray magnetic field at any point on tape not to exceed 350 Oe.	

Table 5. Environment for operating and storing the IBM TotalStorage Enterprise Tape Cartridge (continued)

Note:
1. Operational storage is defined as media that is stored, but also used in a drive during storage at least once every six months.
2. Archival storage is defined as media that is stored, and used in a drive during storage less frequently than once every six months.

Cartridge quality and library maintenance

The IBM tape cartridge provides high performance and reliability with IBM magnetic tape cartridge drives when the cartridge is properly handled and stored. As discussed previously, repeated handling or inadvertent mishandling can damage the physical parts of the cartridge and make it unusable.

The magnetic tape inside the cartridge is made of highly durable materials. However, the tape wears after repeated cycles in the tape system. Eventually, such wear can cause an increase in tape errors.

Track the error data available by monitoring both the cartridge and cartridge library performance. By monitoring error data, you can identify and replace cartridges that are no longer acceptable for continued use.

Proper maintenance of your cartridge library helps to keep IBM magnetic tape cartridge systems operating in a reliable and efficient manner.

Attention: Do not degauss a cartridge tape. Degaussing the tape will erase the servo tracks and make the cartridge unusable. An attached host can be used to run a Data Security Erase if the data on the tape needs to be physically erased. This physically overwrites the data on the tape without damaging the servo tracks.

Ordering media supplies

See Appendix G, *"Ordering media supplies."*

Chapter 5. 3592 Tape Controller Power Procedures

3592 J70 Power On Procedure

To power on the 3592 J70 Tape Controller, perform the following steps:

1. Power on the 3952 F05 frame, or the rack, housing the tape controller.
2. The tape controller performs a self-test when power is applied to the frame or rack. When the self-test completes, the tape controller's display panel (**1** in Figure 13) displays **OK**, indicating that the tape controller is in standby mode.
3. When OK appears in the tape controller's display panel (**1** in Figure 13), press the Power ON/OFF button (**2** in Figure 13).

   Note: The power on process can take as long as eight minutes to complete after pressing the Power ON/OFF button.
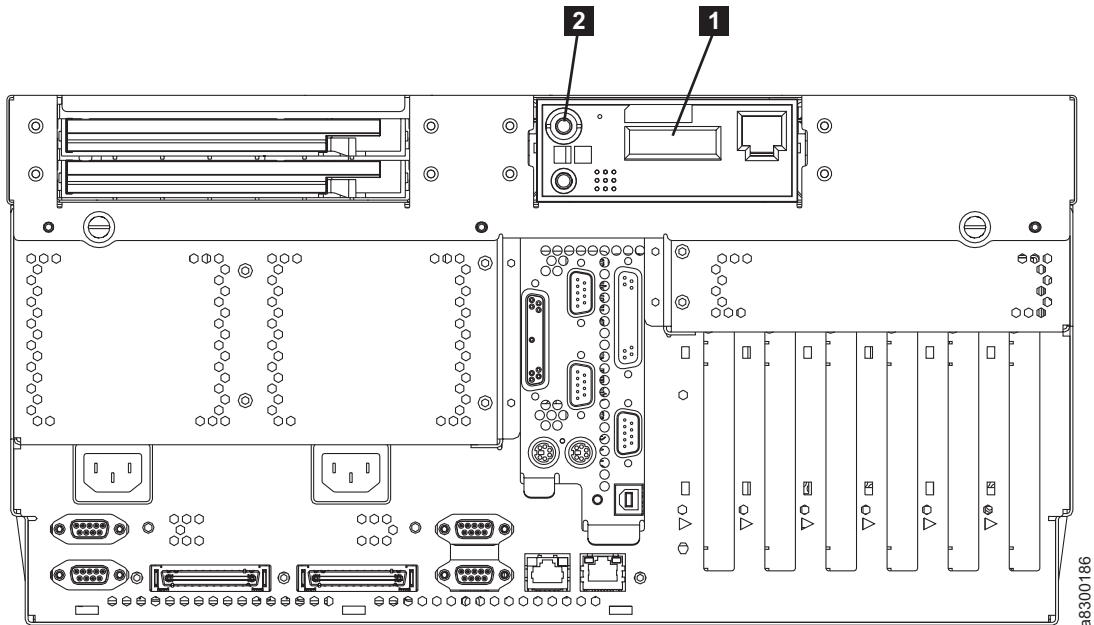
Figure 13. Rear View of 3592 J70 Tape Controller

TS1120 Tape Controller Power On Procedure

To power on the 3592 TS1120 Tape Controller, perform the following steps:

1. Power on the 3952 F05 frame, or the rack, housing the tape controller.
2. The tape controller performs a self-test when power is applied to the frame or rack. When the self-test completes, the tape controller's power LED (**1** in Figure 14 on page 34) will flash, indicating that the tape controller is in standby mode.
3. When the tape controller's power LED (**1** in Figure 14 on page 34) flashes, press the Power ON/OFF button (**2** in Figure 14 on page 34).

   Note: The power on process can take as long as nine minutes to complete after pressing the Power ON/OFF button.
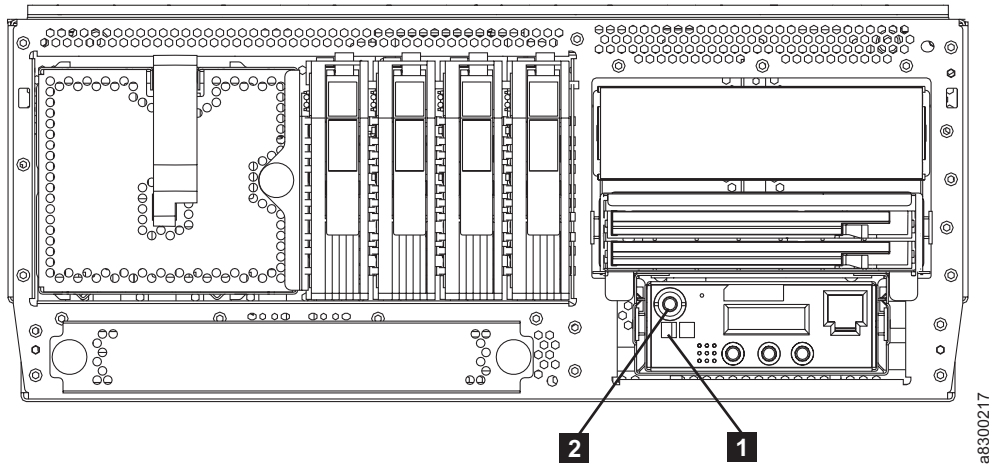
Figure 14. Rear View of TS1120 Tape Controller

3592 J70 Tape Controller Power Off Procedure

To power off the 3592 J70 Tape Controller, perform the following steps:

1. Make sure the customer is informed to vary off all operations from the 3592 J70 Tape Controller in preparation for shutdown.
2. Press and hold down the Power ON/OFF button (**2** in Figure 13 on page 33) for approximately 2 seconds.
3. Be patient. Wait for the power down process to reach standby mode.
4. The 3592 J70 Tape Controller is powered down to standby mode when **OK** appears in the tape controller's display panel (**1** in Figure 13 on page 33).
5. Power can now be removed from the 3592 F05 Frame or rack housing the tape controller, or directly from the tape controller power supplies.

TS1120 Tape Controller Power Off Procedure

To power off the 3592 TS1120 Tape Controller, perform the following steps:

1. Make sure the customer is informed to vary off all operations from the TS1120 Tape Controller in preparation for shutdown.
2. Press and hold down the Power ON/OFF button (**2** in Figure 14) for approximately 5 seconds. You will see the number in the upper right corner of the Operator Panel decrement from 4 to 1 to no number displayed. At that point, release the Power ON/OFF button.
3. Be patient. If the power down process stops before reaching standby mode, repeat step 2.
4. The TS1120 Tape Controller is powered down to standby mode when the green LED (**1** in Figure 14) on the Operator Panel blinks.
5. Power can now be removed from the 3592 F05 Frame or rack housing the tape controller, or directly from the TS1120 power supplies.

Chapter 6. Cleaning procedures

To help prevent errors caused by debris, it is important to clean the tape path, and to manually clean the outside of data cartridges, when needed. Cleaning of the tape path in each drive is an automated procedure, and will rarely require manual intervention. This will work automatically only if the appropriate cleaning cartridges (IBM part 18P7535) are installed in the library, and they still have remaining uses available. A 3592 cleaning cartridge is shipped with the first drive in each installation, and additional cleaning cartridges are available through IBM. The cleaning cartridge contains a Cartridge Memory (CM) device, which will automatically keep track of the number of times it has been used. Cleaning cartridges need to be replaced after 50 uses. The 3592 cleaning cartridges are not interchangeable with 3590 cleaning cartridges, so you must have both types of cleaning cartridges if you have both types of drives in your library.

Attention: Insert only clean and undamaged cleaning cartridges into a tape system. Do not use a china-marking (grease) pencil on the label.

The physical characteristics of the 3592 cleaning cartridge can be used to distinguish it from 3592 data cartridges. The product label on the top of the cartridge is white, with the word ″cleaning″ printed on it. In place of the write-protect switch, there is a non-moveable light gray block (see **1** in Figure 15). If you order cleaning cartridges with pre-attached labels, the first three characters of the volume serial number (VOLSER) **2** will be CLN. The cartridge door (see **1** in Figure 16 on page 36) is also light gray.

Table 6. Cleaning Times for 3592 Drives

3592 Drive	Clean Cycle Time (start of clean to end of unload)
Model J1A	3 minutes, 30 seconds
Model E05	4 minutes, 35 seconds
Model E06/EU6	

.

Figure 15. Cleaning cartridge identifying characteristics

1 Light gray non-moveable block
2 Cleaning cartridge sample label

Figure 16. Cleaning cartridge door

Cleaning the tape path

Cleaning of the tape path in the drive is an automatic procedure initiated by the drive. Changes in drive performance can generate a request for cleaning. If there are no cleaning cartridges installed in the library, or if the available cleaning cartridges have reached the maximum number of uses, cleaning will not be completed. For more information, see the *IBM TotalStorage Automated Tape Library (3494) Operator's Guide*. If the library is in manual mode, a 3592 cleaning cartridge can be manually inserted into the drive to clean the tape path. The 8–character message display will show the message, CLEAN* while the cleaning is in process.

Cleaning the tape cartridge

Before you insert a cartridge into a drive or storage cell, inspect the cartridge for damage or debris. **Damaged or dirty cartridges can reduce system reliability and cause the loss of recorded data.** If debris appears on the cartridge, wipe the outside surfaces with a lint-free cloth lightly moistened with water. No visible water residue or droplets should be observable on the cartridge during or after the wiping effort.

Attention: Do not allow any liquid to contact the tape itself. Special care should be made to never allow liquid water to enter the cartridge which can potentially wick into the layers of the tape and cause them to adhere to each other, risking pull out of the coatings during unwind.

Ensure that all cartridge surfaces are dry and that the leader pin is in place (see 1 in Figure 17) before you load the cartridge.
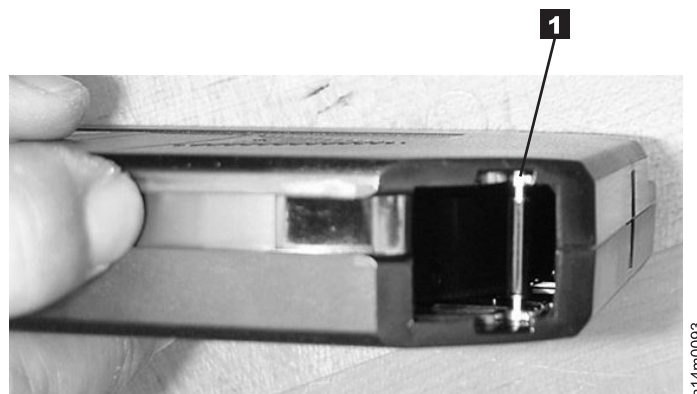
Figure 17. Tape leader pin in proper position (cartridge door manually retracted)

Chapter 7. Identifying system problems

This chapter identifies some of the problems that can occur with the system. Many problems can be resolved through the Library Manager or other host, but there may be instances when the operator will need to intervene in manual mode.

Unable to insert a tape cartridge

If you cannot insert a tape cartridge in the drive, perform the following steps:

1. Ensure that you have the proper cartridge type, and that it is oriented correctly. Cartridges for the earlier 3590 drives are not interchangeable with cartridges for the 3592 drive.

2. Inspect the tape cartridge for damage. See "Perform a thorough inspection" on page 28.

3. Ensure that there is no other cartridge already in the drive.

4. Try to load another cartridge in the tape system. Use a scratch cartridge to avoid possible damage to a data cartridge.

   If the new cartridge can be inserted in the drive, the original cartridge may be defective. Inspect the cartridge again for damage.

   If the cartridge is not damaged but it cannot be inserted, call your service representative.

FID or ATTN on the message display

If an error code appears on the message display, record all codes that are displayed for future reference. Some of these messages will require intervention by an IBM Service Representative.

FID message
> See "FID messages" on page 15, or Appendix B, ″FID Messages″, for more information.

ATTN When the drive message displays ATTN DRV, the drive has experienced either a load error (indicated by the LOAD ERR alternating message) or an unload error (indicated by the UNLOAD E alternating message). If you receive either of these messages, call your service representative.

Tape drive is not ready

If the tape drive is not ready at load point, perform the following steps:

1. If the cartridge is not inserted correctly, remove the cartridge and insert it again. If the cartridge fails to load in the tape system, remove the cartridge and inspect it for correct type or damage. See "Perform a thorough inspection" on page 28.

2. If a FID or ATTN message appears on the message display, record the code, press the Unload button (see **4** in Figure 5 on page 14), and try the operation again.

3. If the drive does not become ready, and no messages are displayed, call your service representative. If a FID or ATTN message appears on the message display, record the code message and see "FID or ATTN on the message display."

Unloading a tape cartridge after a power failure

If there is a power failure, the normal tape system process will unload a tape cartridge when power is restored to the device. The time required to complete the unload can vary, but may take up to 15 minutes. If the device fails to unload a tape cartridge after this period, you can attempt to unload the cartridge by pressing the Unload button on the front of the drive (see **4** in Figure 5 on page 14).

- If the drive unloads the cartridge, remove it by grasping the cartridge, and pulling it towards you.
- If, within 15 minutes, the drive does not unload the cartridge and/or a FID or ATTN message appears on the display, report the problem to your service representative. See "FID or ATTN on the message display" on page 39.

Tape fails to unload

If the tape fails to unload from the drive, perform the following steps:

1. Press the Unload button (see **4** in Figure 5 on page 14).
2. If an error code or a FID message appears on the message display, record the error code or FID message and press the Unload button again.
3. If the drive does not rewind or unload, call your service representative. If a FID or ATTN message appears on the message display, record the code and see "FID or ATTN on the message display" on page 39.

Message display is blank

If the message display on the front of the drive is blank, there are two possibilities:

- the drive has no power
- the drive is ready

Perform the following steps to resolve the problem:

1. Verify that the drive is receiving power. The power LED (see **6** in Figure 5 on page 14) should be a steady green.
2. If the drive power light is off, call your service representative.
3. If the power light is on, verify that a cartridge is in the drive. If not, insert a scratch cartridge. Verify that the message display becomes active. If the panel still does not display a message, contact your service representative.

Tape/drive read or write problems

See Appendix A, "Media/hardware problem isolation."

Encryption Key Manager-Reported Errors

This section defines error messages that are reported by the IBM Encryption Key Manager and are related to the TS1120 and TS1130 Tape Drives. The table includes the error number, a short description of the failure, and corrective actions. Refer to *IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide* for information on the EKM debug tool.

Table 7. Errors that are reported by the encryption key manager

Error Number	Description	Action
EE02	Encryption Read Message Failure: DriverErrorNotifyParameterError: ″Bad ASC & ASCQ received. ASC & ASCQ does not match with either of Key Creation/Key Translation/Key Aquisition operation.″	The tape drive asked for an unsupported action. Ensure that you are running the latest version of the Encryption Key Manager (refer to *Encryption Key Manager Introduction, Planning, and User's Guide* to determine the latest version). Check the versions of drive or proxy server firmware and update them to the latest release, if needed. Enable debug tracing on the key manager server. Try to recreate the problem and gather debug logs. If the problem persists, contact IBM for support. See "Whom Do I Contact for Encryption Key Manager Support?" on page 45.
EE0F	Encryption logic error: Internal error: ″Unexpected error. Internal programming error in EKM.″	Ensure that you are running the latest version of the Encryption Key Manager (refer to *Encryption Key Manager Introduction, Planning, and User's Guide* to determine the latest version). Check the versions of drive or proxy server firmware and update them to the latest release, if needed. Enable debug tracing on the key manager server. Try to recreate the problem and gather debug logs. If the problem persists, contact IBM for support. See "Whom Do I Contact for Encryption Key Manager Support?" on page 45.
	Error: Hardware error from call CSNDDSV returnCode 12 reasonCode 0.	If using hardware cryptography, ensure that ICSF is started.
EE23	Encryption Read Message Failure: Internal error: ″Unexpected error........″	The message received from the drive or proxy server could not be parsed because of general error. Ensure that you are running the latest version of the Encryption Key Manager (refer to *Encryption Key Manager Introduction, Planning, and User's Guide* to determine the latest version). Enable debug on the key manager server. Try to recreate the problem and gather debug logs. If the problem persists, contact IBM for support. See "Whom Do I Contact for Encryption Key Manager Support?" on page 45.

Table 7. Errors that are reported by the encryption key manager (continued)

Error Number	Description	Action
EE25	Encryption Configuration Problem: Errors that are related to the drive table occurred.	Ensure that the config.drivetable.file.url is correct in the KeyManagerConfig.properties file, if that parameter is supplied. Run the `listdrives -drivename <drivename>` command on the Encryption Key Manager server to verify whether the drive is correctly configured (for example, the drive serial number, alias, and certificates are correct). Ensure that you are running the latest version of the Encryption Key Manager (refer to *Encryption Key Manager Introduction, Planning, and User's Guide* to determine the latest version). Check the versions of drive or proxy server firmware and update them to the latest release, if needed. Enable debug tracing and retry the operation. If the problem persists, contact IBM for support. See "Whom Do I Contact for Encryption Key Manager Support?" on page 45.
EE29	Encryption Read Message Failure: Invalid signature	The message received from the drive or proxy server does not match the signature on it. Ensure that you are running the latest version of the Encryption Key Manager (refer to *Encryption Key Manager Introduction, Planning, and User's Guide* to determine the latest version). Enable debug on the key manager server. Try to recreate the problem and gather debug logs. If the problem persists, contact IBM for support. See "Whom Do I Contact for Encryption Key Manager Support?" on page 45.
EE2B	Encryption Read Message Failure: Internal error: "Either no signature in DSK or signature in DSK can not be verified."	Ensure that you are running the latest version of the Encryption Key Manager (refer to *Encryption Key Manager Introduction, Planning, and User's Guide* to determine the latest version). Check the versions of drive or proxy server firmware and update them to the latest release, if needed. Enable debug tracing on the key manager server. Try to recreate the problem and gather debug logs. If the problem persists, "Whom Do I Contact for Encryption Key Manager Support?" on page 45

Error Number	Description	Action
EE2C	Encryption Read Message Failure: QueryDSKParameterError: ″Error parsing a QueryDSKMessage from a device. Unexpected dsk count or unexpected payload.″	The tape drive asked the Encryption Key Manager to do an unsupported function. Ensure that you are running the latest version of the Encryption Key Manager (refer to *Encryption Key Manager Introduction, Planning, and User's Guide* to determine the latest version). Check the versions of drive or proxy server firmware and update them to the latest release, if needed. Enable debug tracing on the key manager server. Try to recreate the problem and gather debug logs. If the problem persists, "Whom Do I Contact for Encryption Key Manager Support?" on page 45
EE2D	Encryption Read Message Failure: Invalid Message Type	The Encryption Key Manager received a message out of sequence or received a message that it does not know how to handle. Ensure that you are running the latest version of the Encryption Key Manager (refer to *Encryption Key Manager Introduction, Planning, and User's Guide* to determine the latest version). Enable debug on the key manager server. Try to recreate the problem and gather debug logs. If the problem persists, contact IBM for support. See "Whom Do I Contact for Encryption Key Manager Support?" on page 45.
EE2E	Encryption Read Message Failure: Internal error: Invalid signature type	The message received from the drive or proxy server does not have a valid signature type. Ensure that you are running the latest version of the Encryption Key Manager (refer to *Encryption Key Manager Introduction, Planning, and User's Guide* to determine the latest version). Enable debug on the key manager server. Try to recreate the problem and gather debug logs. If the problem persists, contact IBM for support. See "Whom Do I Contact for Encryption Key Manager Support?" on page 45.
EE30	Prohibited request.	An unsupported operation has been requested for a tape drive. Enter the correct, supported command for the target tape drive.

Error Number	Description	Action
EE31	Encryption Configuration Problem: Errors that are related to the keystore occurred.	Check the key labels that you are trying to use or configured for the defaults. You can list the certificates that are available to the Encryption Key Manager by using the listcerts command. If you know that you are trying to use the defaults, then run the listdrives -drivename *drivename* command on the Encryption Key Manager server to verify whether the drive is correctly configured (for example, the drive serial number, and associated aliases/key labels are correct). If the drive in question has no aliases/key labels associated with it, then check the values of default.drive.alias1 and default.drive.alias2. If this does not help or the alias/key label exists, then collect debug logs and contact IBM for support. See "Whom Do I Contact for Encryption Key Manager Support?" on page 45.
EE32	Keystore-related problem.	Most likely cause is either that tape was encrypted using a different Encryption Key Manager with different keys or the key that was used to encrypt this tape has been renamed or deleted from the keystore. Issue `list -keysym` and ensure the request alias is in the keystore.
EEE1	Encryption logic error: Internal error: ″Unexpected error: EK/EEDK flags conflict with subpage.″	Ensure that you are running the latest version of the Encryption Key Manager (refer to *Encryption Key Manager Introduction, Planning, and User's Guide* to determine the latest version). Check the versions of drive or proxy server firmware and update them to the latest release, if needed. Enable debug on the key manager server. Try to recreate the problem and gather debug logs. If the problem persists, contact IBM for support. See "Whom Do I Contact for Encryption Key Manager Support?" on page 45.
EF01	Encryption Configuration Problem: ″Drive not configured.″	The drive that is trying to communicate with the Encryption Key Manager is not present in the drive table. Ensure that the config.drivetable.file.url is correct in the KeyManagerConfig.properties file, if that parameter is supplied. Run the `listdrives` command to check whether the drive is in the list. If not, configure the drive manually by using the `adddrive` command with the correct drive information or set the ″drive.acceptUnknownDrives″ property to true using the `modconfig` command. Enable debug tracing and retry the operation. If the problem persists, contact IBM for support. See "Whom Do I Contact for Encryption Key Manager Support?" on page 45.

Whom Do I Contact for Encryption Key Manager Support?

The entitlement for software support varies depending on the operating system on which the Encryption Key Manager is running, and depending on whether the support requirement is defect-related or implementation-related.

Table 8. IBM Encryption Key Manager Support Contacts

Type of Support	IBM Operating Systems: zOS, AIX, i5OS Linux		Non-IBM Operating Systems: Windows, Solaris, HP/UX
Defect Support	Contact IBM Service with IBM operating system's name or identifier and customer number.	Contact IBM Service with IBM Tape Library's machine type/model and serial number.	Contact IBM Service with TPC/BE name or identifier and customer number.
Implementation Support [1]	Contact SupportLine IBM Service.	Contact SupportLine IBM Service.	Contact SupportLine IBM Service.

[1] An IBM Supportline contract offers the best Encryption Key Manager implementation assistance. Some basic implementation assistance can be obtained by contacting IBM Service. Use the same machine type-model that would be used to report a defect. Should your customer require more extensive implementation assistance, billable onsite services are available from IGS and Lab Services. Contact IGS Inside Sales (888-426-4343 option 3) to obtain a Statement of Work (SOW).

If there is a defect, IBM Service is always the first point of contact. The method to engage IBM Software Service varies depending on the operating system on which Encryption Key Manager is being run.

For the following IBM operating systems: z/OS, AIX, and i5/OS, contact IBM Service (For US Customers call 800-IBM-SERV). Select the software option, then identify the operating system and the same customer number that was used to order the operating system.

For Linux, select the hardware option, and use the Machtype-Model of the tape library to report the defect.

For the non-IBM operating systems; Windows, Solaris, and HP/UX, select the software option, then identify the software as TPC/BE and supply the same customer number that was used to order TPC/BE.

Note: The relevant operating system here is the operating system on which Encryption Key Manager is running, not the operating system that is generating the encrypted IOs.

Appendix A. Media/hardware problem isolation

An error code (FID 86 or FE) will be generated when the drive experiences an error and cannot determine if the error was caused by the tape cartridge or by a problem in the drive hardware. The FID 86 or FE is not displayed on the drive, but is logged in the sense information that is returned to the host system. Follow this procedure if you receive an error when reading or writing to the drive and there is no FID displayed.

Media and drives can affect each other and the indications can be confusing. You must record the symptoms for the drive and the tape to make problem isolation possible. The failing component or tape must be isolated or you will continue to experience problems. Problems can be intermittent so careful record keeping is necessary. Keeping careful records of transient problems will enable problem isolation and resolution.

To determine the cause of the read or write errors, follow the steps below.
- Ensure that the tape drive is not overdue for cleaning. If the drive is installed in a library with automatic cleaning, ensure that the automatic clean function is enabled, and a cleaner cartridge is installed in the library. Some libraries track cleaner cartridges and *expire* them after a number of mounts. Ensure that the cleaner cartridge in the library is available.
- Determine which volume serial numbers or cartridges are potential problems.
    - Note which cartridges (VOLSER numbers) fail during the operation. (It is possible to have multiple bad cartridges.)
    - Record the MIM message code at the host and associated VOLSER numbers, if the host supports MIM messages.
    - If you receive SIM messages at the host, get the VOLSER numbers from the message and record those in your Tape Serial Log. (See Table 9 on page 48 as an example of how to establish a log and what it should include.)
- Determine if the cartridges are bad.
    - Examine the cartridge for damage. Open the door to observe if the pin is in its proper place, and examine the cartridge for cracks. If damaged, either repair or replace the cartridge.

        Note: A repaired cartridge may be used long enough to recover data on that cartridge. When the data has been recovered, the cartridge should then be taken out of service and discarded or returned to the plant of origin.
    - If the cartridges look OK, and you have access to another 3592 drive, try the operation with the suspect cartridges in the other drive. If your cartridges fail in the other drive, replace the media.
- Determine if the drive is bad.
    - Try a new tape on the suspect drive. Log all failure data on your Drive Log (see Table 10 on page 48 as an example of how to establish a log and what it should include), and try one more tape. If it also fails, call for service.
    - If only one tape fails, then log the information on both the Table 10 on page 48 and the Table 9 on page 48 for future reference.
    - If tapes show evidence of damage, do not put any more tapes on the drive until a service representative has examined the drive.

47

Table 9. Tape Log example

Failure Date	Drive	Failure Code Unknown	Failure Code FE	Failure Code 85	Failure Code 86	Failure Code 87	Failure Code (other)
10/11/2003	Drive 1	1	1	1			
10/16/2003	Drive 2	1	1			1	B3

Table 10. Drive Log example

Log Item	Drive 1	Drive 2
8A Error 4 tapes	11/9/2003 call for service	
85 Error 1 tape	11/14/2003 record tape serial	
Load failure		serial 123456 8/18/2004

Appendix B. FID messages

Table 11 describes FID messages and customer action for the FID. A FID can be displayed on the drive message display panel (an 8–character display located on the front of the drive) or obtained from host software or error logs.

Table 11. FID messages

FID	Description	Customer Action
50	Encryption Configuration 100% Drive Canister	Encryption configuration installed during manufacturing is incorrect. Drive canister must be replaced.
51	Encryption Self-Test (POST HW) 100% Drive Canister	Encryption hardware power on self test failed. Drive canister must be replaced.
52	Encryption Self-Test (POST FW)	Encryption firmware power on self test failed. See FID E6 in this table.
53	Encryption Self-Test (Invoked) 50% Drive Canister; 50% Microcode	An explicitly invoked encryption self test failed. See FID E6 in this table.
54	Encryption Self-Test (Automatic) 80% Drive Canister; 20% Microcode	An automatically invoked encryption diagnostic failed.
55	Encryption Module Failure 80% Drive Canister; 20% Microcode	An unexpected failure of hardware function occurred.
58	Encryption Error 100% Drive Canister	An error was detected during the encryption of data.
59	Decryption Error 25% Drive Canister; 25% Microcode 25% EKM; 25% Cartridge	An error was detected during the decryption of data.
5A	Encryption External Key Manager (EKM) Failure	An unexpected status was returned by the key manager. Check library/proxy interface, check EKM log. Not a drive or microcode problem. Requires investigation by customer.
5B	Encryption PROXY Failure	A failure or timeout occured on the proxy interface. Check library/proxy interface, check EKM log. Not a drive or microcode problem. Requires investigation by customer.
5F	Security Prohibited Function	A function was attempted which is prohibited due to the current security settings.
81–84, 85	Drive Problem	Call for service
86	Cartridge or Drive Problem	1. Isolate between media and hardware. See Appendix A, "Media/hardware problem isolation," on page 47. 2. Call for service if problem remains.
87	Cartridge Problem	1. Isolate between media and hardware. See Appendix A, "Media/hardware problem isolation," on page 47. 2. This failure may be caused by a damaged cartridge. Inspect the cartridge that was being used when the error occurred for physical defects. Replace the cartridge if it is damaged. 3. Call for service if problem remains.
8A	Drive Performance Problem	Call for service

Table 11. FID messages (continued)

FID	Description	Customer Action
90	Drive Problem	Call for service
9C	Hardware or configuration problem	Call for service
AA, AB, AC, AD	Configuration Problem	Call for service
AE, AF	Hardware Problem	Call for service
BF	Hardware Problem	Call for service
C1	Drive Problem	Call for service
D8	Drive Problem	Call for service
E4	Drive Problem	Call for service
E5, E6	Drive or microcode problem	Call for service
ED	Informational Message	Microcode dump exists in flash memory. The flash dump can be cleared by the service representative only.
F2, F4	Cartridge or Drive Problem	Call for service
F5	Fibre Channel error	See "Fibre Channel" on page 61. If problem persists, call for service.
F6	Cleaning needed for performance reasons.	Clean the tape drive (run cleaning tape). If this FID continues to be posted, call for service.
F7	Fibre wrap test failure.	If this FID continues to be posted, call for service.
FE	Cartridge or Drive Problem	1. Isolate between media and hardware. See Appendix A, "Media/hardware problem isolation," on page 47. 2. This failure may be caused by a damaged cartridge. Inspect the cartridge that was being used when the error occurred for physical defects. Replace the cartridge if it is damaged. 3. Call for service if problem remains.
FF	Operator Procedure or Host Problem	FID FF is always presented to the host in SCSI Request Sense Data. Some types of problems also present this FID on the message display and service panel. 1. **FID FF Displayed on Drive Message Display:** (It also went to the host.) • FID FF is automatically displayed when the service representative selects **Force Error Dump** from the Services menu. • **Action:** Remove the dump icon and the FID message by pressing the Reset pushbutton. • The service representative can remove the FID message, without removing the dump icon, by selecting **Reset Drive** on the Services menu. 2. **FID FF Displayed at Host Only - Not on Drive Panel:** (Message went to the host only.) • The host receives this FID, but it is not presented on the drive message display or service panel. If FID FF was reported in host error log via a SIM message, then perform the action indicated in SIM message codes (such as clean drive). • This FID is presented for an invalid and unsupported SCSI command or parameter, which is a SCSI application program software problem. Sense data exists at the host.

Appendix C. TapeAlert error reporting

TapeAlert error reporting is an industry standard that provides a status monitoring and problem detection capability for tape devices via the fibre interface in an Open Systems environment. The TapeAlert interface is implemented using up to 64 alert flags that are read by the host from the device using log sense page 0x2e. Some of the flags are mandatory and must be supported by the tape drive. The remainder are non-mandatory flags and can be unsupported. Tape Alerts are presented in decimal format. All flags at the drive are cleared at Power On Reset (POR).

The 3592 drive supports the TapeAlert flags in Table 12 that were developed for tape drive/autoloader devices:

Table 12. Supported TapeAlert Flags

No.	Flag	Description	Customer Action
1	Read warning	The tape drive is having problems reading data. No data has been lost, but there has been a reduction in the performance of the tape.	See Appendix A, "Media/hardware problem isolation," on page 47 to isolate fault between drive and media.
2	Write warning	The tape drive is having problems writing data. No data has been lost, but there has been a reduction in the capacity of the tape.	See Appendix A, "Media/hardware problem isolation," on page 47 to isolate fault between drive and media.
3	Hard error	This flag is set for any unrecoverable read/write/positioning error, and is cleared when the cartridge is removed from the drive (this flag is set in conjunction with flags 4, 5, or 6).	Determine if flag 4, 5, or 6 exists; follow actions for those flags.
4	Media	This flag is set for any unrecoverable read/write/positioning error that is due to faulty media, and is cleared when the cartridge is removed from the drive.	If possible, copy any data you require from the tape, then discard media. If failure persists, call for service.
5	Read failure	This flag is set for any unrecoverable read error where the isolation is uncertain and the failure could be either faulty media or faulty drive hardware. It is cleared when the cartridge is removed from the drive.	See Appendix A, "Media/hardware problem isolation," on page 47 to isolate the problem. Discard media if identified as faulty. If failure persists, call for service.

51

Table 12. Supported TapeAlert Flags (continued)

6	Write failure	This flag is set for any unrecoverable write/positioning error where the isolation is uncertain and the failure could be either faulty media or faulty drive hardware. It is cleared when the cartridge is removed from the drive.	See Appendix A, "Media/hardware problem isolation," on page 47 to isolate the problem. Discard media if identified as faulty. If failure persists, call for service.
7	Media life	The tape cartridge has reached the end of its calculated, useful life (EOL).	1. Copy data to another tape cartridge 2. Discard old (EOL) tape.
8	Not data grade	The tape cartridge is not data-grade. Any data you back up to the tape is at risk. The flag is set when severe servo problems are detected while loading a cartridge.	Discard media. If failure persists, call for service.
9	Write protect	This flag is set when the tape drive detects that the tape cartridge is physically write-protected and device driver sees a write command. It is cleared when the cartridge is removed from the drive.	Set write-protect selector on cartridge to write-enable. Ensure cartridge is not logically protected. If problem persists, call for service.
10	No removal	This flag is set when an unload is attempted and SCSI Prevent Media Removal is set to ON. This flag is cleared when the cartridge is removed from the drive.	Operator procedure error or customer software error.
11	Cleaning media	This flag is set when a cleaning tape is loaded into the drive. It is cleared when the cleaning cartridge is removed from the drive.	None. Status message only.
12	Unsupported format	This flag is set when a non-supported cartridge type is loaded into the drive. It is cleared when the cartridge is removed from the drive. Can also be caused by FMR tape loaded for read/write.	Remove invalid cartridge. If problem persists call for service.
14	Unrecoverable snapped tape	The operation has failed because the tape in the drive has snapped. The operator cannot remove the tape and must call for service.	Call for service.
15	Memory chip in cartridge	The memory in the tape cartridge has failed.	Do not use the cartridge for further backup operation.
16	Forced eject	This flag is set when a tape cartridge was manually removed.	None. Status message only.
17	Read-only format	This flag is set when a read-only formatted tape is loaded into the drive. It is cleared when the cartridge is removed from the drive.	None. Status message only.

Table 12. Supported TapeAlert Flags (continued)

18	Tape directory corrupted on load	This flag is set when the tape drive detects that the directory has been corrupted. It is cleared when the cartridge is removed from the drive.	Operator action required. Directory may be rebuilt by reading all the data on the cartridge. The tape drive must access some or all of the data on the tape media to rebuild the tape directory. To allow the tape drive to quickly rebuild, issue a Space or Locate to EOD (End of Data) request. The cartridge contains redundant versions of the tape directory. This operation completes in a few minutes. But if the Cartridge Memory (CM) directory is invalid and the tape is full, this operation can take as long as 2 hours to allow for the linear processing of all records on tapes.
19	Nearing media life	Tape cartridge is nearing its specified end-of-life.	1. Copy data to another cartridge. 2. Replace the tape cartridge.
20	Clean now	This flag is set when the tape drive detects it needs cleaning (performance problem) and is cleared when the drive is successfully cleaned.	Clean the drive at the earliest convenience if not done automatically (done automatically with library manager).
21	Clean periodic	This flag is set when the tape drive detects it needs routine cleaning (based on usage) and is cleared when the drive is successfully cleaned.	Clean the drive between jobs if not done automatically (done automatically with library manager).
22	Expired cleaning media	Replace the cleaning cartridge with a new one. This condition is set after an unsuccessful clean cycle. It is cleared when the next cleaning is attempted.	Replace the cleaning cartridge.
23	Invalid cleaning cartridge	The drive expects a cleaning cartridge to be loaded, and the loaded cartridge is not a valid cleaning cartridge.	Use a valid cleaning cartridge.
25	Dual-port interface error	A redundant Fibre interface port on the tape drive has failed.	Call for service.
26	Cooling fan failure	A tape drive or power supply cooling fan has failed.	Call for service.
27	Power supply	Power supply failed	Call for service.

Table 12. Supported TapeAlert Flags (continued)

30	Hardware A	Hardware fault when reading or writing. Reset drive and retry job.	Call for service.
31	Hardware B	This flag is set when the tape drive fails its internal Power-On-Self-Tests (POST), and is not cleared until the drive is powered OFF.	Call for service.
32	Interface	This flag is set when the tape drive detects a problem with the Fibre interface. It is cleared when the drive is powered OFF.	Call for service.
33	Eject media	This flag is set when a failure occurs that requires the tape cartridge to be ejected from the drive and retried. The flag is cleared when the cartridge is removed from the drive.	Try different media. If problem persists, call for service.
34	Download fail	This flag is set when an FMR image is unsuccessfully downloaded to the tape drive via the SCSI, Fibre, or RS-422 interface. It is cleared when the drive is powered off or a successful microcode update is performed.	Call for service.
36	Drive temperature	Drive temperature sensor indicates that the drive is too hot.	Call for service.
37	Drive voltage	This flag is set when the drive detects power supply voltages outside of the specified voltage limits. It is cleared when the drive is powered off.	Call for service.
38	Predictive failure	A hardware failure of the tape drive is predicted.	When it is convenient, call for service.
39	Diagnostics required	This flag is set when a tape cartridge or drive FID or ATTN DRV message is posted and some further isolation for media or hardware is needed. It is cleared when the drive is powered off.	Call for service.
50	Lost statistics	Media statistics have been lost at some time in the past.	None. Status message only.
51	Tape directory invalid at unload	The tape directory on the tape cartridge just unloaded has been corrupted. File search performance will be degraded.	Operator action required. Directory may be rebuilt by reading all the data on the cartridge.
52	Tape system area write failure	The tape just unloaded could not write its volume control region (VCR) successfully.	Try another tape.
53	Tape system area read failure	The tape VCR could not be read successfully at load time.	Try another tape.
54	No start of data	The start of data could not be found on the tape.	Try another tape.
55	Load failure	Operation failed because the media cannot be loaded and threaded.	Remove tape, try another tape. If problem persists, call for service.

Table 12. Supported TapeAlert Flags (continued)

57	Interface	This flag is set when the tape drive detects a problem with the RS-422 (LDI) interface. It is cleared when the drive is powered OFF, or a successful microcode update is performed.	Call for service.
58	Firmware failure	Operation failed due to microcode problem.	Call for service.

Appendix D. Problem determination

Host environment connections

iSeries / AS400 environment attachment check

Verify a 3592 is properly attached to an AS/400 with the following procedure:

1. Type **WRKCFGSTS *DEV *TAP ASTLVL(*BASIC)** at the prompt.
2. Type **VFYTAP** on the AS/400 command line.
3. Type the device associated with the 3592, such as TAP13.
4. Select the **Basic read/write test** option on the Tape Device Test Menu and follow the instructions provided.
5. When the Tape Device Test menu is displayed, select **Exit test menu**.

Other Open Systems

Verify the drive power is ON. Then refer to the *IBM TotalStorage Tape Device Drivers Installation and User's Guide* (GC35-0154) for information on open system attachments. To access the most current device driver installation and user guides online, go to: `ftp://ftp.software.ibm.com/storage/devdrvr/Doc/`

Appendix E. Rack-mount problem determination

This section is for drives installed in rack-mounts only, and does not apply for drives installed in automated environments. In addition to the front panel components described in ″Drive front panel components,″ rear panel components may also be visible and accessible in a rack-mount installation. Some of these components can be used alone, or in combination with the front panel displays to retrieve basic drive status information. This information can, in turn, be used by service technicians in isolating and correcting drive problems.

Note: The components described in this section are not accessible or visible to an operator in a IBM TotalStorage Enterprise Automated Tape Library (3494) installation. Access to the rear panel of a 3592 drive in a 3494 library installation is for qualified IBM service technicians only.

Drive rear panel components

The rear panel of the 3592 drive is the same on Model E06, EU6, E05 and J1A drives except for the model marking **2** on the right, the RS-232 Serial Port **5** on the Model E05, EU6, and J1A (see Figure 18), and the Ethernet port **7** on the Model E06 (Figure 19 on page 60). An Encryption Capable label **3** appears on some Model E05 drives.

The rear panel on all models has five LEDs **1** to display different statuses. The first two LEDs on the left, labeled Port 0 and Port 1, indicate Fibre Channel activity. The middle (third from the left) LED, labeled Library, indicates communications from the library. The fourth LED from the left, labeled Status, displays drive status. The LED on the far right, labeled Power, indicates the status of power to the drive. If the drive status LED (fourth from the left) is blinking, a status message can be viewed on the 8–character front panel message display. A service representative can also plug the service panel (see "Additional LED status indicators" on page 62) into the connector **4** to view the message. The Dual Port FC-2 (Fibre Channel) connectors **6** are also located on the rear of the drive canister. The shaded area labeled **8** is a handle for use when installing cables.
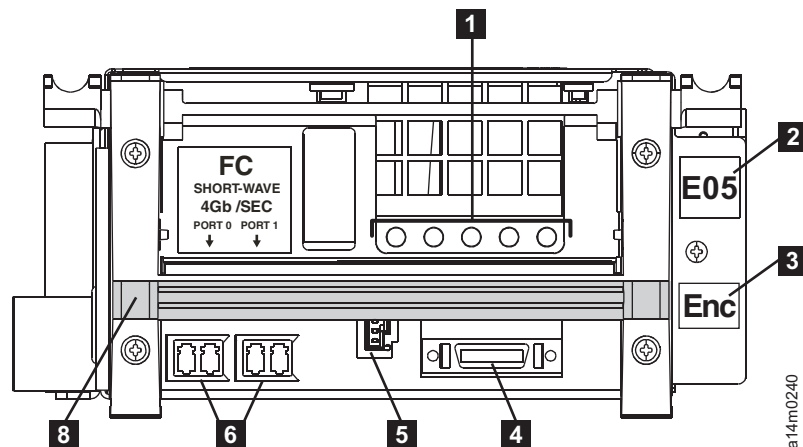

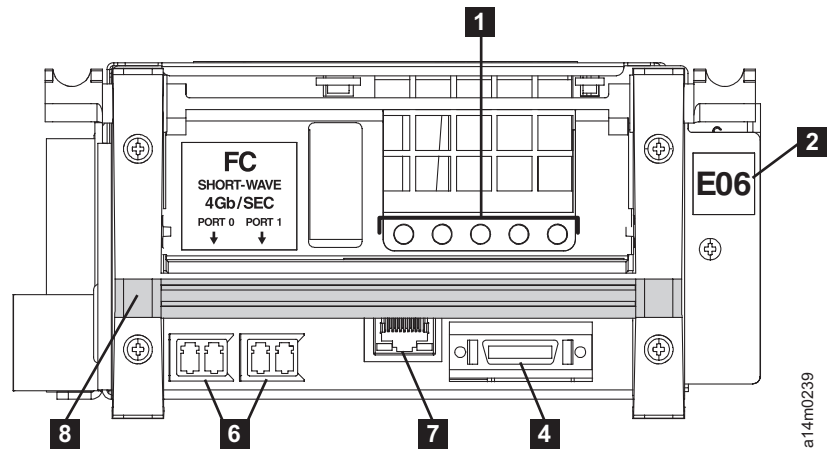*Figure 18. 3592 models E05 and J1A drive rear panel components*

Figure 19. 3592 model E06 drive rear panel components

Fibre Channel

Fibre Channel problem determination

1. Verify that the drive is receiving power. The LED on the front of the drive and the Power LED (see **5** in Figure 20) on the rear of the drive should be a steady green.

2. Check the Fibre Channel connections. Verify that the fibre cables are properly connected to the two pairs of ports at the rear of the drive canister (see **4** in Figure 18 on page 59 and Figure 19 on page 60).

3. Use the first two LEDs on the rear of the drive labeled Port 0 and Port 1 (see **1** and **2** in Figure 20) to determine if a problem exists between the drive, the cable, and the device to which it is attached. See Table 13 on page 62 for the meaning of the LED activity. Use switch, hub, or other fibre product tools and documentation as appropriate to further diagnose the problem.
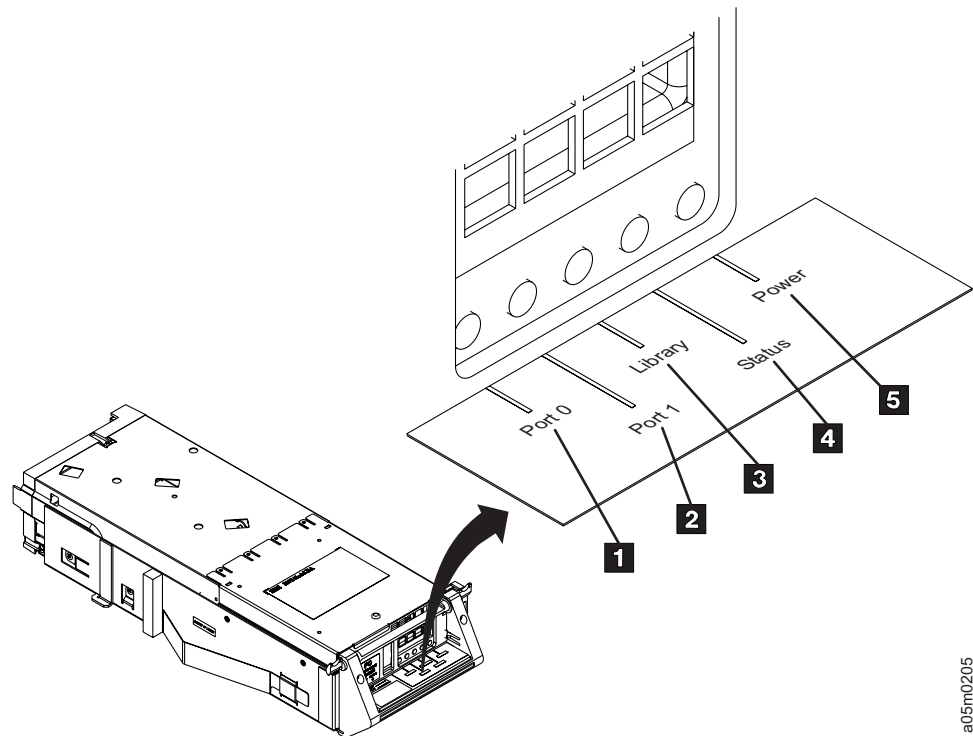

Figure 20. Drive rear panel LEDs

Table 13. Fibre Channel LED diagnostics

LED color	LED activity	Meaning
green	steady	Fibre Channel connection is good, no data being transmitted. Drive may be offline to the control unit or host.
green	blinking, .5 s intervals	Fibre Channel connection is good, data being transmitted.
yellow	blinking, 1.0 s intervals	Fibre Channel connection is detected but is not fully initialized and not ready to process commands.
<none>	<none>	No light detected through Fibre Channel.

If the problems are due to the drive or the fibre cable connected to the drive:

1. Check the Fibre Channel Attachment in its environments. For additional tape device attachment test information, refer to the *IBM TotalStorage Tape Device Drivers Installation and User's Guide* (GC35-0154) and the appendix that describes how to verify the proper attachment of your device. To access the guide online, go to:

   `ftp://ftp.software.ibm.com/storage/devdrvr/Doc/IBM_TotalStorage_tape_IUG.pdf`

2. Verify software levels and topology. Use the links in "IBM online access" on page xx to view the latest supported software and hardware. Verify that the desired topology is supported.

3. If the problem remains, call your IBM Service Representative.

Additional LED status indicators

The five LEDs on the rear of the drive can provide basic information about the status of the drive and its communication connections. In addition to the two Fibre Channel LEDs described in "Fibre Channel" on page 61, there are three additional LEDs. The Library (**3** in Figure 20 on page 61), Status **4** , and Power **5** LEDs can provide basic drive status information. Once you have identified a problem, record this information to report to your service representative. The LEDs can display steady on, blinking, or off in either yellow or green. See Table 14 for the meaning of the LED activity. If a color or mode is not listed, it is not used as a status indicator.

Table 14. Drive rear panel LED indications.

LED Number	Name/Purpose	Color	Light-on indicates:	Blinking light indicates:	No light indicates:
3	**Library** – Library communi-cations	Green	At least one message received since POST	Library communication activity	No communications since last POST of drive
4	**Status** – Drive status	Yellow	Power-on started or microcode soft reset begun	Status message is available at service panel	Drive completed POST
5	**Power** – Drive power status	Green	+5 DC or +12 V DC is present at drive	—	+5 V DC or +12 V DC is missing

Service panel

In addition, qualified IBM service representatives can attach the cable of a service panel (see Figure 21) to a connector on the rear of the drive (see **2** in Figure 18 on page 59 and Figure 19 on page 60) to perform additional functions.

- **This service panel is not intended for use by operators.**
- **This service panel is not to be used to support the 3592 installed in a IBM System Storage TS3500 Tape Library and is not shipped with the TS3500 Tape library. Functional problems can be encountered if this panel is used on drives installed in a TS3500 Tape library. See the** *IBM System Storage TS3500 Tape Library Introduction and Planning Guide, GA32-0559* **for more details on the 3592 installed in a TS3500 Tape library.**
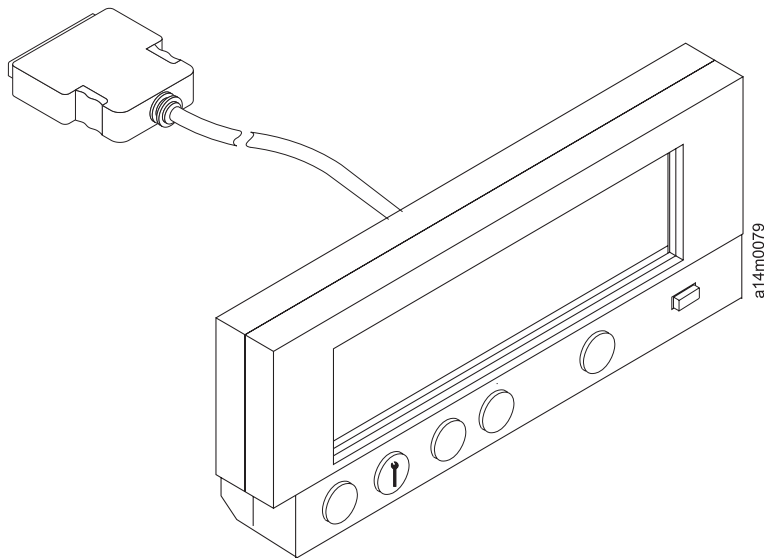

Figure 21. Service panel (To be used by qualified IBM service personnel only.)

Appendix F. Host reporting

Statistical Analysis and Reporting System

The Statistical Analysis and Reporting System (SARS) assists in determining whether read and write errors are caused by the media (tape) or the hardware in the drive. The 3592 microcode contains a Volume SARS (VSARS) algorithm and a Hardware SARS (HSARS) algorithm to analyze errors. SARS algorithms report messages through SIMs and MIMs.

Algorithms are executed in the 3592 just before a tape is unloaded. To distinguish error patterns and trends, the SARS *volume* algorithms require the tape to be mounted on different drives while the SARS *hardware* algorithms require different volumes to be mounted on one drive. As degraded hardware passes through predefined error thresholds, cleaning and service repair messages or error codes are presented. Similarly, if tape volumes continue to perform poorly on different drives, re-write or discard-media messages are presented.

The SARS reporting of Service Information Message (SIM) and Media Information Message (MIM) functions can be disabled if host software does not support SIMs and MIMs.

Service and Media Information Messages (SIMs and MIMs)

SIM and MIM functions are primary factors for improved product availability.

- A SIM alerts you when an abnormal operational condition in the 3592 requires service attention. Information in the SIM identifies the affected drive, the failing component and severity of its fault condition, and the expected operational impact of the pending service action. This information helps the user to initiate and expedite appropriate recovery and service procedures so normal operation is restored with maximum efficiency and minimal disruption.

  A SIM contains the machine type, machine serial number, and Field Replaceable Unit (FRU) which allows the dispatch of the appropriate service personnel and the replacement parts required to correct the machine fault. This procedure helps improve service response time and helps reduce the time required for machine repair.

- A MIM identifies problems with the media (tape) and the volume number of the *bad* cartridge. This allows the customer to do maintenance within the tape library and to prevent unnecessary service calls when the fault is media.

You can select, depending on your software, the severities you wish to see. For example, you may only want to see the *acute* SIM/MIM, or prefer to see all SIMs and MIMs sent to the host. SIM/MIM filtering by severity can be done through configuration options. The four severity codes are listed below:

- Severity 0 (FID4) code means the device requires service, but normal drive function is not affected.
- Severity 1 (FID3) code indicates moderate severity.
- Severity 2 (FID2) code indicates serious severity.
- Severity 3 (FID1) code indicates acute severity.

A MIM specifies what is wrong with the cartridge that is indicated. The three MIM severity codes are listed below:

- Severity 1 indicates moderate severity.

- Severity 2 indicates serious severity.
- Severity 3 indicates acute severity.

SIMs and MIMs can be reported multiple times. A configuration option allows reporting the same SIM/MIM more than once. The time between repeat SIMs/MIMs is eight hours. For example, if the configuration option is set to two, a SIM will be reported when an error occurs, it will be repeated again eight hours later, and, then again, eight hours after that message. The default is to not repeat SIMs/MIMs.

SIM/MIM presentation

SIMs and MIMs reporting varies for different systems. Refer to the *Statistical Analysis and Reporting System User Guide* which can be accessed on the IBM URL, `http://www.ibm.com/systems/storage/tape/library.html`. This book is only available on line, and cannot be ordered as a printed version.

There are specific SIM and MIM presentations for the following systems:

System   **Presentation**

System z (zSeries®, S/390®)
    IEA480E and IEA486E messages, as well as EREP reports

z/VM® (VM/ESA®)
    HCP6359I and HCP6357I messages, as well as EREP reports

z/VSE™ (VSE/ESA™)
    OP64I, OP65I, and OP20 messages, as well as EREP reports

TPF   CEFR0354I, CEFR0355W, CEFR0356W, CEFR0357E, CEFR0347W, CDFR0348W, and CDFR0349E messages, as well as EREP reports

TSM (formerly ADSM)
    ANR8972E, ANR8830E, and ANR8831W messages

AIX   SIM/MIM messages are logged to EREP reports

HP   When enabled, SIM/MIM messages are logged to /var/adm/atdd/atdd_d.log

SUN   When enabled, SIM/MIM messages are logged to /var/adm/messages

Linux   Via taped DAEMON, SIM/MIM messages are logged to /var/log with file names of the form <drive serial #>.<time stamp>.simmim

Appendix G. Ordering media supplies

This appendix provides information on different ways of ordering media supplies, including feature codes and part numbers for ordering media supplies for 3592 tape drives. Selected media supplies can be ordered using feature codes when purchasing a 3592 drive. This is so-called ″pack-in″ method of ordering, and the media will be shipped with the hardware order. Not all media types are available with this method. The 3599 Tape Media method is available for ordering all types of data and cleaning cartridges. This method is typically used for ordering larger quantities, and for ordering initialized and/or pre-labeled cartridges. Media supplies can also be ordered using part numbers, through IBM-authorized distributors.

Feature Code descriptions (″pack-in″)

Table 15 lists the media features, which can be used to order media when ordering a 3592 drive. Only the 3592 Data cartridges and the Cleaning cartridges can be ordered using this method. For all other media types, you must use the 3599 Tape Media method, or order by part number through an IBM-authorized distributor.

Table 15. Media features (″pack-in″)

Feature Code	Description
8802	One IBM TotalStorage Enterprise Tape 3592 Cleaning cartridge
8820	Twenty IBM TotalStorage Enterprise Tape 3592 Data cartridges
9590	No data cartridges

Feature Code definitions

Cleaner Cartridge (FC8802)

This feature provides a 3592 cleaning cartridge for 3592 tape drives. Maximum: five. Plant or field installation.

Twenty 3592 Data Cartridges (FC8820)

This feature provides twenty 3592 Data cartridges for 3592 tape drives. Maximum: five. Plant installation only.

Note: In addition to these cartridges, there is a ″CE″ cartridge for use by IBM service representatives only. The VOLSER label for this cartridge begins with ″CE″, followed by a space and three numerals, and ending with ″JA.″

3599 media supplies

For customers who order media using the 3599 Tape Media method, IBM TotalStorage Enterprise Tape Media 3599 provides the ability to order unlabeled, pre-labeled, initialized, and bulk-packaged tape data cartridges in a wide variety of combinations and cleaning cartridges for the 3592 tape drive. In addition to the 3592 Data cartridge, 3592 Economy and 3592 Extended cartridges are available. (The 3592 Extended cartridge is supported only on the TS1120 and TS1130 tape drives (3592 Model E05, E06, and EU6 and not on the 3592 Model J1A.) WORM cartridges are available in all three sizes. Segmentation/capacity scaling options are also available on the 3592 Data cartridge for a 60 GB (55.88 GiB) Fast Access

capability, and a 260 GB (242.14 GiB) segmented tape with 60 GB (55.88 GiB) of fast access, and 200 GB (186.26 GiB) of additional capacity.

With the 3599 Tape Media method of ordering, model numbers are used to identify the cartridge types, and feature code combinations are used to specify the quantities, labeling, and initialization options. Table 16 shows a few examples of ordering options for each cartridge type. Note that additional feature codes are required to completely specify all desired characteristics of the cartridges. Orders may be placed by calling IBM.COM, Americas at 1-800-IBM-CALL (1-800-426-2255).

3599 media feature descriptions

Table 16. 3599 media feature codes

3599 Model	Media ID/ Feature Code	Feature Code for labeling, initialization and quantity	Individual Cartridge Capacity	Description
011	JA/9030	1020	300 GB (279.4 GiB)	20–pack 3592 Data cartridges, labeled and initialized in E1 format
011	JA/9081	1020	500 GB (465.66 GiB)	20–pack 3592 Data cartridges, labeled and initialized in E2 format
011	JA/9082	1020	640 GB (596.05 GiB)	20–pack 3592 Data cartridges, labeled and initialized in E3 format
012	JA/9030	2020	300 GB (279.4 GiB)	20–pack 3592 Data cartridges, labeled, not initialized
013	JA/9030	3020	300 GB (279.4 GiB)	20–pack 3592 Data cartridges, not labeled or initialized
014	JB/4020	1020	700 GB (651.93 GiB)	20–pack 3592 Extended cartridges, labeled and initialized in E2 format
014	JB/9082	1020	1000 GB (931.32 GiB)	20–pack 3592 Extended cartridges, labeled and initialized in E3 format
015	JB/5020	2020	700 GB (651.93 GiB)	20–pack 3592 Extended cartridges, labeled, not initialized
016	JB/6020	3020	700 GB (651.93 GiB)	20–pack 3592 Extended cartridges, not labeled or initialized
E11	JJ/9050	1020	60 GB (55.88 GiB)	20–pack 3592 Economy cartridges, labeled and initialized in E1 format

Table 16. 3599 media feature codes (continued)

3599 Model	Media ID/ Feature Code	Feature Code for labeling, initialization and quantity	Individual Cartridge Capacity	Description
E11	JJ/9081	1020	100 GB (93.13 GiB)	20–pack 3592 Economy cartridges, labeled and initialized in E2 format
E11	JJ/9082	1020	128 GB (119.21 GiB)	20–pack 3592 Economy cartridges, labeled and initialized in E3 format
E12	JJ/9050	2020	60 GB (55.88 GiB)	20–pack 3592 Economy cartridges, labeled, not initialized
E13	JJ/9050	3020	60 GB (55.88 GiB)	20–pack 3592 Economy cartridges, not labeled or initialized
021	JW/9040	1020	300 GB (279.4 GiB)	20–pack 3592 WORM cartridges, labeled and initialized in E1 format
021	JW/9040	1020	500 GB (465.66 GiB)	20–pack 3592 WORM cartridges, labeled and initialized in E2 format
021	JW/9082	1020	640 GB (596.05 GiB)	20–pack 3592 WORM cartridges, labeled and initialized in E3 format
022	JW/9040	2020	300 GB (279.4 GiB)	20–pack 3592 WORM cartridges, labeled, not initialized
023	JW/9040	3020	300 GB (279.4 GiB)	20–pack 3592 WORM cartridges, not labeled or initialized
024	JX/2420	1020	700 GB (651.93 GiB)	20–pack 3592 Extended WORM cartridges, labeled and initialized in E2 format
024	JX/9082	1020	1000 GB (931.32 GiB)	20–pack 3592 Extended WORM cartridges, labeled and initialized in E3 format
025	JX/2520	2020	700 GB (651.93 GiB)	20–pack 3592 Extended WORM cartridges, labeled, not initialized
026	JX/2620	3020	700 GB (651.93 GiB)	20–pack 3592 Extended WORM cartridges, not labeled or initialized

Table 16. 3599 media feature codes (continued)

3599 Model	Media ID/ Feature Code	Feature Code for labeling, initialization and quantity	Individual Cartridge Capacity	Description
E21	JR/9042	1020	60 GB (55.88 GiB)	20–pack 3592 Economy WORM cartridges, labeled and initialized in E1 format
E21	JR/9081	1020	100 GB (93.13 GiB)	20–pack 3592 Economy WORM cartridges, labeled and initialized in E2 format
E21	JR/9042	2020	60 GB (55.88 GiB)	20–pack 3592 Economy WORM cartridges, labeled, not initialized
E21	JR/9042	3020	60 GB (55.88 GiB)	20–pack 3592 Economy WORM cartridges, not labeled or initialized
E21	JR/9082	1020	128 GB (119.21 GiB)	20–pack 3592 Economy WORM cartridges, labeled and initialized in E3 format
017	JA	7005	cleaning, 50 uses	5–pack 3592 Cleaning Cartridges, labeled and initialized
017	JA	7006	cleaning, 50 uses	5–pack 3592 Cleaning Cartridges without media identification labels

Ordering media supplies by part number

Table 17 lists the data cartridges and media supplies that you can order for 3592 tape drives. The different methods for ordering are listed at the bottom of the table.

Table 17. Ordering media supplies for 3592 tape drives

Supply Item	Capacity			Part Number
	EFMT1	EFMT2	EFMT3	
IBM TotalStorage Enterprise Tape Cartridge 3592 Data	300 GB (279.39 GiB)	500 GB (465.66 GiB)	640 GB (596.04 GiB)	18P7534
IBM TotalStorage Enterprise Tape Cartridge 3592 Extended	Not Supported	700 GB (651.93 GiB)	1000 GB (931.32 GiB)	23R9830
IBM TotalStorage Enterprise Tape Cartridge 3592 Economy	60 GB (55.88 GiB)	100 GB (93.13 GiB)	128 GB (119.21 GiB)	24R0316

Table 17. Ordering media supplies for 3592 tape drives (continued)

Supply Item	Capacity			Part Number
	EFMT1	EFMT2	EFMT3	
IBM TotalStorage Enterprise Tape Cartridge 3592 WORM	300 GB (279.39 GiB)	500 GB (465.66 GiB)	640 GB (596.04 GiB)	18P7538
IBM TotalStorage Enterprise Tape Cartridge 3592 Extended WORM	Not Supported	700 GB (651.93 GiB)	1000 GB (931.32 GiB)	23R9831
IBM TotalStorage Enterprise Tape Cartridge 3592 Economy WORM	60 GB (55.88 GiB)	100 GB (93.13 GiB)	128 GB (119.21 GiB)	24R0317
IBM TotalStorage Enterprise Tape Cartridge 3592 Cleaning	Cleaning, 50 uses			18P7535

Methods of Ordering

Use any of the three methods below to order media supplies by part number.

- Order by part number through an IBM-authorized distributor (for the closest distributor, visit the web at `http://www.ibm.com/storage/media`)
- If you do not have Internet access, order the cartridges from any authorized IBM Business Partner or your IBM Sales Representative
- Call 1-888-IBM-MEDIA.

Note: Be sure to order bar code labels for all cleaning and data cartridges. Order VOLSER labels separately (see "Ordering bar code labels").

Repair supplies

We recommend that you keep the supplies listed in Table 18, to maintain your cartridges.

Table 18. Supplies for cartridge maintenance

Description	Ordering information
Leader Pin Reattachment Kit. This kit contains the necessary tools to reattach the leader pin to the tape. It includes the rewind tool, which can be used to add tension to a tape if the leader pin is displaced. (See ″Repositioning a leader pin.″)	- Call 1-888-IBM-MEDIA to order as IBM part number 18P8887.

Ordering bar code labels

Bar code labels with VOLSERS are required for cartridges used within a library. You can order these labels separately from the IBM Data Cartridges and Cleaning Cartridges.

You can order bar code labels directly from the authorized label suppliers in Table 19 on page 72.

Table 19. Authorized suppliers of custom bar code labels

In the Americas	In Europe and Asia
EDP/Colorflex 2550 West Midway Boulevard Broomfield, CO 80020-1633 U. S. A. Telephone: 800-432-1337 or 303–666-2160 http://www.colorflex.com	EDP Europe, Ltd. 43 Redhills Road South Woodham Ferrers Chelmsford, Essex CM3 5UL U. K. Telephone: 44 (0) 1245-322380 http://www.edpeurope.com/media-labels.html
Dataware 7570 Renwick Houston, TX 77081 U. S. A. Telephone: 800-426-4844 http://www.datawarelabels.com/	Dataware Labels Europe Heubergstrasse 9 D-83052 Bruckmuhl-Gotting Germany Telephone: 49 806-29455 http://www.datawarelabels.com/
NetC, L.L.C. 100 Corporate Drive Trumbull, CT 06611 U. S. A. Telephone: 203-372-6382 http://www.netcllc.com/	NetC Europe Ltd Town Farm Bungalow North Curry Taunton Somerset U. K. TA3 6LX Telephone: 44 (0) 1823 491439 http://www.netclabels.co.uk
	NetC Asia Pacific Pty Ltd Locked Bag 14 Kenthurst NSW Australia 2156 Telephone: 61 (0) 2 9654 8272 http://www.netclabels.com.au

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

- AIX
- Enterprise Storage Server
- ESCON
- FICON
- i5/OS
- iSeries
- IBM
- pSeries
- S/390
- System Storage
- TotalStorage
- z/OS
- zSeries

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol ((R) or (TM)), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Electronic emission notices

This section contains the electronic emission notices or statements for the United States and other countries

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device might not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

European Union (EU) Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC, on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Properly shielded and grounded cables and connectors must be used in order to reduce the potential for causing interference to radio and TV communications and to other electrical or electronic equipment. Such cables and connectors are available from IBM authorized dealers. IBM cannot accept responsibility for any interference caused by using other than recommended cables and connectors.

European Community contact:

```
IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Tele: 0049 (0)711 785 1176
Fax: 0049 (0)711 785 1283
e-mail: tjahn@de.ibm.com
```

Australia and New Zealand Class A Statement

Attention: This is a Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Germany Electromagnetic Compatibility Directive

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit (vom: 2007/05/25)

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: "Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

People's Republic of China Class A Electronic Emission Statement

中华人民共和国"A类"警告声明

声 明
此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A compliance statement

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

Taiwan Contact Information

IBM Taiwan Product Service Contact Information:
IBM Taiwan Corporation
3F, No 7, Song Ren Rd., Taipei Taiwan
Tel: 0800-016-888

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Japan VCCI Class A ITE Electronic Emission Statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に
基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を
引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求
されることがあります。

Korean Class A Electronic Emission Statement

이기기는 업무용으로 전자파 적합등록을 받은 기기
이오니, 판매자 또는 사용자는 이점을 주의하시기
바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에
서 비업무용으로 교환하시기 바랍니다.

Power cords

For your safety, IBM provides a power cord with a grounded attachment plug to use with this IBM product. To avoid electrical shock, always use the power cord and plug with a properly grounded outlet.

IBM power cords used in the United States and Canada are listed by Underwriter's Laboratories (UL) and certified by the Canadian Standards Association (CSA).

For units intended to be operated at 115 volts: Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a parallel blade, grounding-type attachment plug rated 15 amperes, 125 volts.

For units intended to be operated at 230 volts (U.S. use): Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a tandem blade, grounding-type attachment plug rated 15 amperes, 250 volts.

For units intended to be operated at 230 volts (outside the U.S.): Use a cord set with a grounding-type attachment plug. The cord set should have the appropriate safety approvals for the country in which the equipment will be installed.

IBM power cords for a specific country or region are usually available only in that country or region.

Glossary

This glossary defines the special terms, abbreviations, and acronyms used in this publication and other related publications. If you do not find the term you are looking for, see the IBM Glossary of Computing Terms located at the following Web site: www.ibm.com/ibm/terminology.

A

access method.   A technique for moving data between processor storage and input/output devices.

AES.   Advanced Encryption Standard. A block cipher adopted as an encryption standard by the US government.

alphanumeric.   Pertaining to a character set that contains letters, numerals, and possibly other characters, such as punctuation marks.

arbitrated loop.   see "Fibre Channel arbitrated loop (FC-AL)"

archiving.   The storage of backup files and associated journals, usually for a given period of time.

B

backhitch.   Magnetic tape that makes a slight backward motion just prior to moving forward.

backup and recovery application.   The short-term retention of records used for restoring essential business and system files when vital data has been lost because of program or system errors or malfunctions.

bar code.   A code representing characters by sets of parallel bars of varying widths and separation which are read optically by transverse scanning.

bar code label.   A specially coded label that can be affixed to a tape cartridge and which enables a device to identify the cartridge and its volume serial number. The bar code label must be affixed to a tape cartridge to enable the library to identify the cartridge and its volume serial number.

beginning of tape (BOT).   The location on a magnetic tape that indicates the beginning of the permissible recording area.

bit.   A binary digit that may have the value of either 0 or 1.

block.   A collection of contiguous records recorded as a unit. Blocks are separated by interblock gaps, and each block may contain one or more records.

browser.   A client program that initiates requests to a web server and displays the information that the server returns.

buffer.   A routine or temporary storage location used to compensate for a difference in rate of flow of data, or time of occurrence of events, when transferring data from one device to another.

byte.   A binary number containing exactly eight bits.

C

capacity.   See *media capacity*.

capacity scaling.   A logical method of reducing the overall length of media available for write and read operations, providing faster data-access times.

cartridge door.   On a tape cartridge, a spring-loaded door that is closed to protect the magnetic tape within the cartridge. The door can be opened by the tape drive to access the tape, or opened manually to visually inspect the positioning of the tape leader pin.

certificate.   A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated.

channel.   A device that connects the processing unit and main storage with the I/O control unit.

channel path.   The physical path between the channel and the control unit. Synonymous with channel.

cleaning cartridge.   A tape cartridge that is used to clean the heads of a tape drive. Contrast with *data cartridge*.

command.   A control signal that initiates an action or the beginning of a sequence of actions.

control unit (CU).   A device that controls input and output operations of one or more devices.

conversion.   The process of changing from one method of data processing to another or from one data-processing system to another.

CPU.   central-processing unit

D

data.   Any representations such as characters or analog quantities to which meaning is, or might be, assigned.

data cartridge.   A tape cartridge dedicated to storing data. Contrast with *cleaning cartridge*.

data channel. A device that connects a processor and main storage with the I/O control unit. Synonymous with input/output channel and I/O channel.

data compression. An algorithmic data-reduction technique that encodes data from the host and stores it in less space than unencoded data. The original data is recovered by an inverse process called decompression.

data-compression ratio. The number of host data bytes divided by the number of encoded bytes. It is variable depending on the characteristics of the data being processed. The more random the data stream, the lower the opportunity to achieve compression.

data transfer rate. The average number of bits, characters, or blocks per unit time passing between corresponding equipment in a data transmission system. The rate is expressed in bits, characters, or blocks per second, minute, or hour.

degauss. To make a magnetic tape nonmagnetic by means of electrical coils carrying currents that neutralize the magnetism of the tape.

device. Any hardware component or peripheral, such as a tape drive or tape library, that can receive and send data.

device driver. A file that contains the code needed to use an attached device.

DFSMS. Data Facility Storage Management Subsystem

DK. Data Key. An alphanumeric string used to encrypt data.

download. To transfer programs or data from a computer to a connected device, typically a personal computer.

drive head. The component of a drive that records an electrical signal onto magnetic tape, or reads a signal from tape into an electrical signal.

drive loaded. A condition of a tape drive in which a tape cartridge has been inserted in the drive, and the tape has been threaded to the beginning-of-tape position. Also known as a mount.

dump. To write the contents of storage, or of a part of storage, usually from an internal storage to a external medium, for a specific purpose such as to allow other use of storage, as a safeguard against faults or errors, or in connection with debugging.

E

E1. Enterprise Format 1 recording technology. See EFMT1.

E2. Enterprise Format 2 recording technology. See EFMT2.

E3. Enterprise Format 3 recording technology. See EFMT3.

EEDK. Externally Encrypted Data Key. A Data Key that has been encrypted (wrapped) by a Key Encryption Key prior to being stored in the data cartridge. See KEK.

EEFMT2. Enterprise Encryption Format. AES 256-bit encrypted data written recorded at the performance and capacity format used by the native 3592 Model E05.

EEFMT3. Enterprise Encryption Format. AES 256-bit encrypted data written recorded at the performance and capacity format used by the native 3592 Model E06.

effective data rate. The average number of bits, bytes, characters, or blocks per unit time transferred from a data source to a data sink and accepted as valid. The rate is expressed in bits, bytes, characters, or blocks per second, minute, or hour.

effective data rate. The average number of bits, bytes, characters, or blocks per unit time transferred from a data source to a data sink and accepted as valid. The rate is expressed in bits, bytes, characters, or blocks per second, minute, or hour.

effective recording density. The number of user bytes per unit of length of the recording medium.

EFMT1. Enterprise Format 1 recording technology. The performance and capacity format used by the 3592 Model J1A and the 3592 Model E05 when emulating Model J1A.

EFMT2. Enterprise Format 2 recording technology. The performance and capacity format used by the native 3592 Model E05.

EFMT3. Enterprise Format 3 recording technology. The performance and capacity format used by the native 3592 Model E06 to record at increased density.

Encryption Key Manager. Enterprise Key Manager. A Java application supplying public and private keys and certificates for use in encrypting and decrypting data on the TS1130 and TS1120 tape drives.

enable. To provide the means or opportunity. The modification of system, control unit, or device action through the change of a software module or a hardware switch (circuit jumper) position.

encryrption-capable. A TS1130 or TS1120 tape drive functionally able, but not yet set up by IBM, to encrypt and decrypt data.

encryrption-enabled. An encryption-capable TS1130 or TS1120 tape drive that has been set up by IBM to encrypt and decrypt data.

ERA. Error-recovery action performed by the host.

ESCON. Enterprise System Connection architecture.

F

Fabric, Fibre Channel. An interconnection that receives addressed information which, in turn, routes the information to its appropriate destination.

FC. Feature code.

Fibre Channel. A technology for transmitting data between computer devices at a data rate of up to 4 Gbps. It is especially suited for attaching computer servers to shared storage devices and for interconnecting storage controllers and drives. Often the term is used to refer to an optics cable utilizing filaments to transmit data.

Fibre Channel arbitrated loop (FC-AL). In this topology, two or more Fibre Channel end points are interconnected through a looped interface. Information is routed through the loop to its destination.

Fibre Channel hub. In this topology, the hub provides ports similar to switch ports and uses a Fibre Channel arbitrated loop structure.

Fibre Channel switch (switched fabric). In this topology, two or more end points are interconnected through one or more switches.

Fibre Channel topologies. Shared loop host and storage controllers.

Fiber Connectivity (FICON). A high-speed input/output (I/O) interface for mainframe computer connections to storage devices.

FICON. See *Fiber Connectivity*.

FID. Failure ID

fiducial. A reference point which guides the cartridge-handling device to the tape system location.

field microcode replacement (FMR) tape. A tape cartridge that contains new or revised firmware (microcode).

field replaceable unit (FRU). An assembly that is replaced in its entirety when any one of its components fails. In some cases a field replaceable unit may contain other field replaceable units; for example, a brush and a brush block that can be replaced individually or as a single unit.

file. A set of related records, treated as a unit, for example, in stock control, a file could consist of a set of invoices.

file protected. See write-protect.

firmware. Proprietary code that is usually delivered as firmware as part of an operating system. Firmware is more efficient than software loaded from an alterable medium and more adaptable to change than pure hardware circuitry. An example of firmware is the Basic Input/Output System (BIOS) in read-only memory (ROM) on a PC motherboard.

FMR tape. See *field microcode replacement tape*.

format. The arrangement or layout of data on a data medium.

formatted tape volume. A tape volume that has been initialized with certain formatting information which is required to exist for the recording technique used on the volume before any data can be recorded. Depending on the format and medium, formatting may or may not be required to utilize the medium for data recording purposes.

FRU. Field replaceable unit.

FTP site. Any electronic repository of information that uses the File Transfer Protocol (FTP) for transferring files to and from servers. Use of an FTP site generally requires a user ID and possibly a password.

G

GB. Gigabyte; 1 000 000 000 bytes.

GBIC. See *gigabit interface converter*.

GiB. One gibibyte (GiB) = 2^{30} bytes = 1,073,741,824 bytes.

gigabit interface converter (GBIC). A device that converts data from electrical signals to optical signals.

H

host. The controlling or highest-level system in a data communication configuration. Synonymous with *server*.

host system. A data-processing system that is used to prepare programs and the operating environments for use on another computer or control unit.

I

index. A function performed by the cartridge loader that moves cartridges down the input or output stack one cartridge position. A loader can perform multiple consecutive indexes.

input/output channel. In a data-processing system, a functional unit, controlled by the processing unit, that handles the transfer of data between main storage and peripheral equipment.

install. To set up for use or service. The act of adding a product, feature, or function to a system or device either by a singular change or by the addition of multiple components or devices.

interchange. The ability to process (read or write) a given tape volume on any one of a set of tape devices that support the form factor and recording format on the tape volume.

interchange application. The preparation of tapes for use on other systems or devices, either local or remote, or the use of tape data prepared by another system.

I/O. Input/output.

ISV. independent software vendors

K

KB. Kilobyte; 1 024 bytes of storage.

KEK. Key Encrypting Key. An alphanumeric string used to encrypt the Data Key. See EEDK.

keystore. A database of private keys and their associated X.509 digital certificate chains used to authenticate the corresponding public keys.

KiB. One kibibyte (KiB) = 210 bytes = 1,024 bytes.

L

LCD. See *liquid crystal display*.

leader pin. A small metal rod attached to the end of the magnetic tape. During tape processing, the leader pin is grasped by a threading mechanism, which pulls the pin and the tape out of the cartridge, across the drive head, and onto a take-up reel. The head can then read or write data from or to the tape.

LED. Common abbreviation for light-emitting diode.

liquid crystal display (LCD). A low-power display technology used in computers and other I/O devices.

load point. The beginning of the recording area on magnetic tape.

logical block. A logical block is an independently accessible unit of information created by the program within a file. A logical block may be either a data logical block or a mark logical block.

logical end of tape. A point on the tape where written data normally ends.

logical record. A logical record is a string of concatenated data bytes that is passed between an application program and a control program or access method as the result of an I/O request.

logical-write protection. Logical-write protection is a facility provided by the device that allows a program to write-protect a tape volume through some device command. Logical-write protection persists for the duration of a tape mount or until deactivated by the program.

long wave. A Fibre Channel cable that has a 1400-nm wave length.

LUN. Logical unit number.

M

MB. Megabyte; 1 000 000 bytes.

magnetic tape. A tape with a magnetizable surface layer on which data can be stored by magnetic recording.

manual mode. A mode of operation that can be selected on the cartridge loader. This mode allows a single tape cartridge feed, performed by the operator.

media capacity. The amount of data that can be contained on storage media and expressed in bytes of data.

MiB. One mebibyte (MiB) = 2^{20} bytes = 1,048,576 bytes.

Mibit/s. One Mebibit per second (Mibit/s) = 2^{20} bits = 1,048,576 bits per second.

microcode. A code, representing the instructions of an instruction set, that is implemented in a part of storage that is not program-addressable.

migration. See *conversion*.

MIM. Media information message.

mount. The act of making a tape volume available for processing by a specific tape device.

mounted. The state of a tape volume while it is available for processing by a specific tape device.

N

native data capacity. The amount of data that can be stored without data compression on a cartridge.

O

Oe. Oersted. The unit of magnetic intensity in the centimeter-gram-second system.

OEM. Original equipment manufacturer.

operating environment.   The temperature, relative humidity, and wet bulb temperature of the room in which the tape library routinely conducts processing.

P

partitions.   One or more non-overlapped mini-volumes, each with its own beginning and ending points, contained within a single physical tape volume.

PDF.   Portable Document Format. A standard specified by Adobe Systems, Incorporated, for the electronic distribution of documents. PDF files are compact; can be distributed globally via e-mail, the Web, intranets, or CD-ROM; and can be viewed with the Acrobat Reader, which is software from Adobe Systems that can be downloaded at no cost from the Adobe Systems home page.

physical end of tape.   A point on the tape beyond which the tape is not permitted to move.

physical-write protection.   A facility provided by the mechanical housing of the tape volume that allows a human being or robotics device to write-protect a tape volume. Physical-write protection persists until the state of the facility on the tape volume is changed.

POST.   Power On Self-Test. A series of diagnostic tests which are run automatically each time power is provided to the device.

PostScript.   A standard specified by Adobe Systems, Incorporated, that defines how text and graphics are presented on printers and display devices.

public/private keys.   A cryptography system that uses two keys: a public key known to everyone and a private or secret key known only to the recipient of the message. The public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Also known as asymmetric keys.

R

random access.   Random access refers to the processing of information on a volume in a manner that requires the device to access nonconsecutive storage locations on the medium.

read-type commands.   Any commands that cause data to be read from tape.

record.   A collection of related data or words, treated as a unit; for example, in stock control, each invoice could constitute one record.

recording density.   The number of bits in a single linear track measured per unit of length of the recording medium.

rekey.   The process of changing the asymmetric Key Encrypting Key (KEK) that protects the Data Key (DK) stored on an already encrypted tape, thereby allowing different entities access to the data.

relative humidity.   The ratio of the amount of water vapor actually present in the air to the greatest amount possible at the same temperature.

removable media.   Recording media that can be added to or removed from a recording device.

RSA.   Rivest-Shamir-Adleman algorithm. A system for asymmetric, public-key cryptography used for encryption and authentication. It was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The security of the system depends on the difficulty of factoring the product of two large prime numbers.

S

SAN.   Storage Area Network

SARS.   Statistical Analysis and Reporting System

SCSI.   Small computer system interface.

SCSI address.   The hexadecimal representation of the unique address (0–F) assigned to a SCSI device. This address would normally be assigned and set in the SCSI device during system installation.

SCSI device.   A host adapter or a target controller that can be attached to the SCSI bus.

SCSI ID.   The bit-significant representation of the SCSI address referring to one of the signal lines DB (F–0).

sequential access.   Refers to the processing of information on a volume in a manner that requires the device to access consecutive storage locations (e.g. logical blocks) on the medium.

server.   A functional unit that provides services to one or more clients over a network. Examples include a file server, a print server, and a mail server. The pSeries, iSeries, HP, and Sun are servers. Synonymous with *host*.

shipping environment.   The temperature, relative humidity rate, and wet bulb temperature of the environment to which the tape library is exposed when being transferred from one location to another.

short wave.   A Fibre Channel cable that has an 850-nm wave length.

SIM.   Service Information Message

storage environment.   The temperature, relative humidity rate, and wet bulb temperature of the environment in which the tape library is non-operational and being kept for future use.

T

TapeAlert. A patented technology from Hewlett-Packard that monitors the status of a tape device and media, and detects problems as they occur.

TapeAlert flags. Status and error messages that are generated by the TapeAlert utility and display on the host console. The messages indicate the type of problem and tell how to resolve it.

tape cartridge. A container holding magnetic tape that can be processed without separating it from the container.

tape device. A computer peripheral device that supports reading or writing of a removable recording medium called a tape volume. A tape device has a model number.

tape drive. A device that is used for moving magnetic tape and includes the mechanisms for writing and reading data to and from the tape.

tape format. The tape format defines the way that information is physical recorded and arranged on a tape volume. It includes the physical representation for all constructs associated with the tape data model as well as other constructs that are format dependent.

tape library. A structure that provides for the storage of tape volumes and facilitates the movement of tape volumes between the storage structure and the tape device.

tape mount. The operation associated with mounting a tape volume on a tape device.

tape synchronous mode. The tape synchronous mode transfers records whose length is greater than the limits defined for buffered records. The device operates in the tape synchronous mode, if the format being processed is supported.

tape unit. A device that contains tape drives and their associated power supplies and electronics.

terminator. A part used to end a channel or connection on a computer system.

TSM. Tivoli® Storage Manager

U

unique cartridge identifier (UCID). See WWCID.

unformatted tape volume. A tape volume that has not been initialized with certain formatting information (for example, servo tracks), which is required to exist for the recording technique used on the volume before any data can be recorded. Depending on the format and medium, formatting may be required to utilize the medium for data recording purposes.

uniform resource locator (URL). The address of an item on the World Wide Web. It includes the protocol followed by the fully qualified domain name (sometimes called the host name) and the request. The web server typically maps the request portion of the URL to a path and file name. For example, if the URL is http://www.storage.ibm.com/tape/index.html, the protocol is http; the fully qualified domain name is www.storage.ibm.com; and the request is /tape/index.html.

unique cartridge identifier (UCID). A permanent identifier associated with a specific tape cartridge, typically stored on the tape itself and the non-volatile cartridge memory.

URL. See *Uniform resource locator*.

V

VOLSER. Volume serial number. The serial number of the specific tape cartridge.

volume. (1) A certain portion of data, together with its data carrier, that can be handled conveniently as a unit. (2) A data carrier that is mounted and demounted as a unit, for example, a reel of magnetic tape, a disk pack.

W

World-wide Unique Cartridge Identifier. See WWCID

Write Once, Read Many (WORM). A technology to allow data to be written once to storage media. After that, data is permanent and cannot be altered, but can be read any number of times.

write-protected. A logical or physical setting on a tape volume to prevent writing or erasing data from the tape.

write protect unit check. The tape cartridge is physically or logically write protected and the command is subject to write protect unit checks, unit check initial status is presented to the command, and the associated sense data indicates ERA code 30.

write-type commands. Any commands that cause data to be written on tape or affect buffered write data.

WWCID. An identifier that uniquely identifies a cartridge.

Index

Numerics

Readers' Comments — We'd Like to Hear from You

IBM System Storage TS1120 and TS1130 Tape Drives and TS1120 Controller
Operator Guide
3592 Models J1A, E05, E06, EU6, J70 and C06

Publication No. GA32-0556-03

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Send your comments to the address on the reverse side of this form.

If you would like a response from IBM, please fill in the following information:

Name

Address

Company or Organization

Phone No.

E-mail address

IBM

Fold and Tape   **Please do not staple**   Fold and Tape
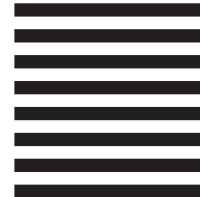
NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL   PERMIT NO. 40   ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machine Corporation
Information Development
Building 9032-2, Department GZW
9032 South Rita Road
Tucson, Arizona U.S.A.   85744-0002

Fold and Tape   **Please do not staple**   Fold and Tape

IBM

Spine information:

IBM

IBM System Storage TS1120 and
TS1130 Tape Drives and TS1120
Controller

3592 Operator Guide