

**EMC Solutions Enabler
Symmetrix Secure Erase CLI**
Version 6.0

PRODUCT GUIDE

**P/N 300-001-354
REV A03**

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.emc.com

Copyright © 2005 EMC Corporation. All rights reserved.

Printed January, 2005

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Trademark Information

EMC², EMC, Symmetrix, Celerra, CLARiiON, CLARAlert, Documentum, HighRoad, Legato, Navisphere, PowerPath, ResourcePak, SnapView/IP, SRDF, TimeFinder, VisualSAN, and where information lives are registered trademarks and EMC Automated Networked Storage, EMC ControlCenter, EMC Developers Program, EMC OnCourse, EMC Proven, EMC Snap, Access Logix, AutoAdvice, Automated Resource Manager, AutoSwap, AVALONidm, C-Clip, Celerra Replicator, Centera, CentraStar, CLARevent, Connectrix, CopyCross, CopyPoint, DatabaseXtender, Direct Matrix, Direct Matrix Architecture, EDM, E-Lab, Enginuity, FarPoint, FLARE, GeoSpan, InfoMover, MirrorView, NetWin, OnAlert, OpenScale, Powerlink, PowerVolume, RepliCare, SafeLine, SAN Architect, SAN Copy, SAN Manager, SDMS, SnapSure, SnapView, StorageScope, SupportMate, SymmAPI, SymmEnabler, Symmetrix DMX, Universal Data Tone, and VisualSRM are trademarks of EMC Corporation. All other trademarks used herein are the property of their respective owners.

Preface..... v

Chapter 1 Overview

 Overview 1-2

 Data Erase Utility..... 1-2

 Command Summary 1-3

Chapter 2 Symmetrix Secure Erase Operation

 Implementing EMC Symmetrix Secure Erase 2-2

 Symmetrix Secure Erase Restrictions..... 2-2

 Verifying Device Readiness 2-3

 Performing Erase Operations..... 2-3

 Confirming an Erase Operation 2-4

 symerase Example 2-5

Index..... i-1

As part of its effort to continuously improve and enhance the performance and capabilities of the EMC product line, EMC periodically releases new versions of both the EMC Enginuity Operating Environment and EMC Solutions Enabler. Therefore, some functions described in this guide may not be supported by all versions of Enginuity or Solutions Enabler currently in use. For the most up-to-date information on product features, see your product release notes.

If an EMC Solutions Enabler feature does not function properly or does not function as described in this guide, please contact the EMC Customer Support Center for assistance. If you are an EMC Development Partner, refer to the EMC Powerlink website.

Audience This manual provides both guide and reference information for command-line users and script programmers. The manual describes how to perform erase operations using the SYMCLI commands of the Solutions Enabler software.

Organization The following defines the structure of this manual:

Chapter 1, *Overview*, provides an introduction to the Symmetrix Secure Erase SYMCLI command (`symerase`).

Chapter 2, *Symmetrix Secure Erase Operation*, describes how to use the the Symmetrix Secure Erase operation using the `symerase` command.

Related Documentation Other Symmetrix publications of related interest are:

- ◆ *EMC Solutions Enabler Symmetrix CLI Command Reference*
- ◆ *EMC Solutions Enabler Support Matrix*
- ◆ *EMC Solutions Enabler Installation Guide*

- ◆ *EMC Solutions Enabler Symmetrix Base Management CLI Product Guide*
- ◆ Host Connectivity Guides, EMC Corporation

**Conventions Used in
this Manual**

The following conventions are used in this manual:

In this manual, every use of the word SYMCLI means EMC Solutions Enabler.

Note: A note calls attention to any item of information that may be of special importance to the reader.



CAUTION

A caution contains information essential to avoid damage or degraded integrity to storage of your data. The caution might also apply to protection of your software or hardware.

Typographical Conventions

This manual uses the following type style conventions in this guide:

bold text	Boldface text provides extra emphasis and emphasizes warnings, and specifies window names and menu items in text.
<i>italic text</i>	<i>Italic text and characters emphasizes new terms, identifies variables in a software syntax (non-literal notation), identifies unique word usage, and applies emphasis in examples and in references to book titles and sections.</i>
fixed space courier font	A fixed space font identifies files and path names, and is used in command line entries, displayed text, or program listings.

Where to Get Help

For questions about technical support, call your local sales office or service provider.

If you have a valid EMC service contract, contact EMC Customer Service at:

United States: (800) 782-4362 (SVC-4EMC)

Canada: (800) 543-4782 (543-4SVC)

Worldwide: (508) 497-7901

Follow the voice menu prompts to open a service call and select the applicable product support.

If you are located outside the North America, call the nearest EMC office for technical assistance.

Sales and Customer Service Contacts

For the list of EMC sales locations, please access the EMC home page at:

<http://www.emc.com/contact/>

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

<http://powerlink.emc.com>

Your Comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send a message to **techpub_comments@emc.com** with your opinions of this guide.

Your technical enhancement suggestions for future development consideration are also welcome. To send a suggestion, log on to **<http://powerlink.emc.com>**, follow the path **Support, Contact Support**, and choose **Software Product Enhancement Request** from the Subject menu.

This chapter provides an introduction to the Symmetrix Secure Erase utility (`symerase` command).

- ◆ Overview 1-2

Overview

The EMC® Symmetrix® Secure Erase (`symerase` command) for Enginuity™ version 5670 and above, provides a method to quickly erase all the data on a Symmetrix device. This erase utility meets the Department of Defense clearing and sanitizing requirements for a non-removable rigid disk (DOD requirement 5220.22-M), which are as follows:

Overwrite all addressable locations with a character, its complement, then a random character, and confirm the erase operation.

The `symerase` command can be used to erase specific devices by specifying a Symmetrix device, a physical device, or a logical device member of a group. For Windows systems, a filesystem drive letter can also be specified.

This functionality requires an Erase license.

Note: For a detailed introduction to the Solutions Enabler, SYMCLI, and the Symmetrix array, refer to the *EMC Solutions Enabler Symmetrix Base Management CLI Product Guide*.

Data Erase Utility

Erasing data from electronic media is not as simple as deleting the data, because deleted data can still be recovered with some work. Erasing of an address is properly done by writing a character to it, overwriting that character with its complement, then writing a random character and confirming the operation by reading back the random character.

Because an erase operation is a multi-step process, it is important to manage the process as close to the data as possible. For this reason, Symmetrix Secure Erase is performed at the disk-media-level inside the Symmetrix array. This is especially important when large quantities of mirrored data need to be erased. Typical non-EMC host-based erase applications that currently exist are not fast enough to be a viable option, due to the communications delay between the application and the storage location.

The Symmetrix Secure Erase utility provides a quick means for an authorized user to launch an erase operation for a data set. When this initial request is sent to the Symmetrix array, the Symmetrix array rapidly handles the request, requiring no further user intervention.

Command Summary

Table 1-1 summarizes the Secure Erase actions.

Table 1-1 **`symerase` Command Summary**

Option	Description
commit	Commits the erase operation for the specified device.
verify	Verifies that the specified device can be erased prior to the operation.

For information about performing Symmetrix Secure Erase control operations, refer to Chapter 2. For details about the `symerase` command syntax and available options, refer to the *EMC Solutions Enabler Symmetrix CLI Command Reference*.

Symmetrix Secure Erase Operation

This chapter provides instructions for using the Symmetrix Secure Erase command, identifies any device or system restrictions, and shows several examples of using the `symerase` command.

- ◆ Implementing EMC Symmetrix Secure Erase.....2-2

Implementing EMC Symmetrix Secure Erase

The `symerase` command allows you to perform erase operations on Symmetrix devices and device groups. Using this command you can do the following:

- ◆ Verify that a device can be erased
- ◆ Perform an erase operation
- ◆ Confirm a successful erase operation

This section provides the restrictions for using Symmetrix Secure Erase, and explains the operations you can perform using the `symerase` command.

Note: For detailed syntax of the `symerase` command, refer to the *EMC Solutions Enabler Symmetrix CLI Command Reference* manual.

Symmetrix Secure Erase Restrictions

The following are current restrictions for using Symmetrix Secure Erase:

- ◆ Engenuity version 5670 and Solutions Enabler V5.4 (minimum).
- ◆ TimeFinder®, TimeFinder/Snap, and clone operations on the involved devices are prohibited during an erase operation.
- ◆ The Symmetrix containing the volume to be erased must be local to the host.
- ◆ The volume being erased must be visible to the host.
- ◆ The device state must be `WRITE_DISABLED`, and cannot be `NOT_READY`.
- ◆ The erase operation cannot be performed on the specified device if the device is any of the following:
 - A RAID-S/RAID-5, CKD, or RDF device
 - A source or target device of a clone session
 - A virtual device (VDEV) that is in use
 - A WORM-protected device
 - A device that is part of an enabled RDF CG group
 - A device that is a meta member
 - A device with an attached BCV or DRV

- A VCM database device
- A device with checksum extents defined on it

Refer to the *EMC Solutions Enabler CLI Release Notes* for any additional restrictions.

Verifying Device Readiness

Prior to performing an erase operation, you can verify that the devices are available, adhere to the erase restrictions, and that extent definitions meet the Enginuity code requirements. Devices to be erased must be visible to the host from which the command is being issued.

To verify a device prior to an erase operation, use the following form:

```
# symerase pd PdevName verify
```

To verify that all the logical devices in a device group can be erased, use the following form:

```
# symerase -g DgName ld ALL -pattern ONES verify
```

The system displays an error if the device does not qualify for an erase operation.

Performing Erase Operations

The Department of Defense (DOD) data erase requirements can be viewed as four steps:

1. Write all addressable locations with a character.
2. Write again with its complement.
3. Write all addresses a third time with a random character.
4. Read the random character back.

The `symerase` command automatically performs steps 1, 2, and 3.

The third (random) character can be selected by using the `-pattern` option and specifying a parameter (ONES, ZEROS, RANDOM, or a hexadecimal character). If RANDOM is specified, the system will generate a random character.

The fourth step is optional (`-confirm`). If you need to comply with the DOD requirements, you must use this option.

You can erase data on a device (`dev`), a logical device (`ld`) using the device group (`-g`), a physical device (`pd`), or a filesystem (`X:`).

Prior to performing the erase operation, the system returns information about all devices that will be erased. For example, if you entered a command to erase a device that was a meta head, the system would list all the meta members.

Erasing Devices

The following are some examples of commands to use for erase operations. A complete example, including system output, is at the end of this chapter.

To commit an erase operation for a device, use the following form:

```
# symerase -sid SymmID dev SymDevName -pattern 0x2B commit
```

To commit an erase operation for a physical device, use the following form:

```
# symerase pd /dev/rdisk/c2t0d1s2 -pattern RANDOM commit
```

Erasing a Filesystem

The erasing of filesystems is supported on Windows platforms only. The filesystem is indicated by referencing its drive letter. The filesystems must be created using the `diskpart` CLI utility, (not the Windows Disk Manager interface). The Disk Manager interface reserves space at the end of the device, causing the resulting device to not be created on track boundaries. The `symerase` utility requires that the object being erased reside on track boundaries.

The filesystems must also be created on *basic* disks, not *dynamic* disks. This option is set through the **Settings -> Control Panel -> Administrative Tools -> Storage Management -> Disk Manager**.

The following example shows a `symerase` operation for filesystem N: on Symmetrix 120800005605, using a hexadecimal pattern 0x2A:

```
symerase filesystem N: -pattern 0x2A commit
```

Confirming an Erase Operation

To confirm the erase operation, add the `-confirm` option to the command, as shown:

```
# symerase -sid 000187900769 dev 021 -pattern 0x2B commit -confirm
```

When you add the `-confirm` option, an additional step of internal processing is performed, where the system reads back from the device the random pattern to confirm that the original data is overwritten. This additional step is necessary for compliance with the DOD verification requirements.

symerase Example

The following example shows a `symerase commit` operation which uses a hexadecimal pattern to overwrite the data on device 021 on Symmetrix 000187900769:

```
# symerase -sid 000187900769 dev 021 -pattern 0x2B commit
```

As shown in the sample output below, prior to performing the erase operation the system identifies the devices to be erased. The user must agree to continue by entering `y` (yes) or `n` (no) on the command line. (Using the `-noprompt` option omits this step.)

```
Proceed with erasing device(s)
  Symid: 000187900769 Meta devname: 021, pdevname: /dev/rdisk/clt0d10s2
  Metamembers: [022, 023, 024]
(y/[n]) ? y
```

```
Starting an erase session. Please wait...
```

```
Session percent complete..... 0.00
Session percent complete..... 5.43
Session percent complete..... 10.86
Session percent complete..... 16.29
Session percent complete..... 21.72
Session percent complete..... 27.15
Session percent complete..... 32.58
Session percent complete..... 38.01
Session percent complete..... 43.44
Session percent complete..... 48.87
Session percent complete..... 54.30
Session percent complete..... 59.73
Session percent complete..... 65.16
Session percent complete..... 70.59
Session percent complete..... 76.02
Session percent complete..... 81.45
Session percent complete..... 86.88
Session percent complete..... 92.32
Session percent complete..... 97.75
Session percent complete.....100.00
```

```
The erase session has completed.
```

Using the `-noecho` option allows the erase operation to run without progress updates on the screen.

A

Array restrictions
 when using symerase 2-3

D

Device readiness
 possible errors about 2-3
Device restrictions
 when using symerase 2-3

F

Filesystem
 erasing data from 2-4

S

Sample output 2-5
symerase
 Command Syntax 1-3
 for a filesystem 2-4
 restrictions 2-2
 sample output from 2-5
 using commit 2-4
 using confirm 2-4
 using verify 2-3

V

Verifying device readiness 2-3

