Best Practices for Data Recovery using Symantec Endpoint Encryption - Full Disk (SEE-FD)

When a computer encrypted with Symantec Endpoint Encryption - Full Disk experiences a failure of any type, it is the policy of Symantec Technical Support to use a step-by-step approach to attempt to access and backup the computer's encrypted files prior to any attempts to restore the system so as to protect against possible data loss during the repair process.

IMPORTANT NOTE: Symantec highly recommends that you contact technical support at the earliest possible convenience when dealing with a technical issue that involves critical data. Please document all events that preceded the problem, list any actions taken, and error messages encountered.

The Recovery Process Steps Summary:

It is recommended that the following actions take place in the order listed for the best possible chance at recovering data.

- 1. Contact your internal help desk for assistance.
- 2. Contact Symantec Technical Support for assistance.
- 3. Run "Recover /a".
- 4. Run the SEE Hard Disk Access utility and back up any data.
- 5. Perform a Hard Drive consistency check.
- 6. Perform a hard drive backup using a "sector by sector" copy method.
- 7. Run "Recover /d" emergency decryption.

Contacting internal help desk (Step 1)

The Contact your internal help desk for assistance

Contacting Symantec (Step 2)

Contact Symantec Technical Support for assistance by calling 1-800-342-0652.

Run "Recover /a" (Step 3)

The recommended first step, after contacting your internal company help desk and the Symantec technical support team, will be to attempt to repair the SEE Hard Disk Operating System (RTOS) if it has been damaged. The use of the recover utility with the /a parameter will not harm the drive or any data it contains.

The command to run this utility is: "recover /a"

WARNING: Do not run the recovery program with the "/d" or "/b" parameters until instructed to do so, or there could be the risk of data loss.

Endpoint Encryption Hard Disk Access Utility (Step 4)

Symantec recommends running the Hard Disk Access Utility and attempting to back up the data to a secondary location for safe keeping.

- Boot the system with SEE-FD-Access-7.X.X.iso

(The SEE-FD Access Utility is available on request from Symantec Support)

🚯 Symantec Endpoin	It Encryption Full Disk Edition Access Utility		×
This utility is su Disk through the	upport software that will allow you to acc e Windows Preinstallation Environment	cess drives encrypted (Windows PE).	with SEE Full
This utility can performing Win	be used to access and backup data on a dows system repairs or recovery proce	an encrypted hard dis dures.	k in advance of
User Nam	e :		
Password	:		
Domain:		•	
This product co Affiliate(s). By u the End User Li	ntains Windows software licensed from Ising this software, you acknowledge the cense Agreement.	Microsoft Corporation e terms and condition	and/or MS s set forth in
2006-2008, Gu	ardianEdge Technologies Inc., All rights	reserved.	
Version 7.0.0		ОК	Exit
🔒 Symantec Endpoir	nt Encryption Full Disk Edition Access Utility		×
This utility is s Disk through th	upport software that will allow you to a e Windows Preinstallation Environmer	ccess drives encrypt nt (Windows PE).	ed with SEE Full
This utility can performing Wir	be used to access and backup data or ndows system repairs or recovery proc	n an encrypted hard d cedures.	isk in advance of
	SEE Full Disk Access Utility		×
User Nan Password	You have successfully gained access and the Sym Full Disk Edition encryption engine has started. Af the necessary actions through the Windows PE int DOS command prompt to exit this utility.	antec Endpoint Encryption ter you have completed terface, type Exit at the	
Domain:		OK	
This product co Affiliate(s). By u the End User L	ntains Windows software licensed from using this software, you acknowledge t icense Agreement.	n Microsoft Corporati he terms and conditio	on and/or MS ons set forth in
2006-2008, Gu	ardianEdge Technologies Inc., All right	s reserved.	
Version 7.0.0		ок	Exit

- MS DOS commands like **copy** and **xcopy** can then be used to backup data to a network share (by mapping a drive using the **NET USE** command) or to a USB storage device. This allows data to be backed up and retrieved in case a user experiences a failure within Windows.

C:∖≻dir Volume in drive C has no label. Volume Serial Number is C8E2-D544	
Directory of C:\	
09/03/2009 07:12 PM 0 AUTOEXEC.BAT 09/03/2009 07:12 PM 0 CONFIG.SYS 09/03/2009 07:21 PM (DIR) Documents and Settings 11/12/2009 06:30 PM (DIR) Program Files 10/04/2009 06:43 PM 870,180 sylink.log 09/30/2009 04:30 PM (DIR) SyToggle 11/12/2009 06:33 PM (DIR) WINDOWS 3 File(s) 870,180 bytes 4 Dir(s) 16,781,918,208 bytes free C:\>copy_sylink.log c:\SyToggle	
1 file(s) copied. C:∖>_	
	_

Hard Drive Consistency Check (Step 5)

Using the hard drive manufacturers recommended method, perform a low level consistency check to verify that the hard drive hardware is operating normally. This is to eliminate the possibility that a mechanical failure is the root cause of the problem. This will usually require a separate boot disk with the manufacturer's utility on it.

Hard Drive Backup (Step 6)

At this point, a backup of the hard drive should be taken for protection against possible data corruption. Further attempts at recovering data will involve writing to the drive and will increase the risk of data loss. Symantec recommends that Symantec Ghost be used to create a "sector-by-sector" copy of the hard drive.

Symantec Technical Support can provide instructions on performing a sector-by-sector backup of the hard drive.

Run "Recover /d" (Step 7 - Emergency decryption)

The emergency decryption process is used to decrypt a hard drive in the event that normal decryption methods are unsuccessful. The emergency decryption utility is a very powerful tool that will decrypt the entire hard drive when authorized by a Hard Disk administrator. There are some very important points to keep in mind when using this utility:

Never stop the emergency decryption process while in progress!

Do not run the "recover /d" command more than once, even if it did not appear to work.

Be patient! The program may appear to be working slowly or not at all at certain points, but the program is most likely still running.

Warning!

<u>Do not run Recover /d more than once – it will cause file corruption on the hard drive (making any data unrecoverable).</u>

Recover is an emergency process that allows you to repair the SEE Full Disk files.	
Make sure that the computer is connected to an uninterruptible power supply during the recovery process. Data loss occurs if the process is stopped while in progress.	
Symantec Corporation recommends that you use the 32-bit SEE Full Disk Access Utility (SEEFD_Access_Utility.exe) before you attempt to use the recover program. The SEE Full Disk Access Utility allows you to access the hard disk by using the Microsoft Window Pre-installation Environment (Windows PE). Please contact Help Desk for more information about this utility.	
Do you want to continue with the recovery process?	
Version 7.0.5, 2010 Guardian Edge, Technologies, Inc., All rights reserved	

uma-3 fila-22 ia	correct
olume=3 , file=23 is	correct.
olume=4 , file=2 is c olume=4 , file=3 is c	omect.
olume=4 , file=4 is o	correct.
olume=4 , file=6 is o	conect.
olume=4 , file=7 is c olume=5 _file=2 is c	correct.
olume=5 , file=3 is c	orrect.
olume=5 , file=4 is c olume=5 , file=5 is c	correct.
olume=5 , file=6 is o olume=5 , file=7 is o	correct.
ne SEE-FD Volume	is integrity check is successful.
(amine 705 2010	Guardian Edge Technologian Inc. All debte mean of
/ersion 7.0.5, 2010	GuardianEdge Technologies Inc., All rights reserved
/ersion 7.0.5, 2010	GuardianEdge Technologies Inc., All rights reserved Sack Next > Exit
/ersion 7.0.5, 2010	GuardianEdge Technologies Inc., All rights reserved KBack Next > Exit
/ersion 7.0.5, 2010	GuardianEdge Technologies Inc., All rights reserved < Black Next > Exit
/ersion 7.0.5, 2010	GuardianEdge Technologies Inc., All rights reserved < Black Next > Exit ram
E Recover Prog	GuardianEdge Technologies Inc., All rights reserved < Back Next > Exit ram
/ersion 7.0.5, 2010	GuardianEdge Technologies Inc., All rights reserved < Back Next > Exit ram nethod:
/ersion 7.0.5, 2010	GuardianEdge Technologies Inc., All rights reserved
E Recover Progr Choose recovery m	GuardianEdge Technologies Inc., All rights reserved
/ersion 7.0.5, 2010	GuardianEdge Technologies Inc., All rights reserved < Back
E Recover Progr Choose recovery m	GuardianEdge Technologies Inc., All rights reserved
/ersion 7.0.5, 2010	GuardianEdge Technologies Inc., All rights reserved
/ersion 7.0.5, 2010	GuardianEdge Technologies Inc., All rights reserved < Back
/ersion 7.0.5, 2010	GuardianEdge Technologies Inc., All rights reserved < Back
/ersion 7.0.5, 2010	GuardianEdge Technologies Inc., All rights reserved < Back
/ersion 7.0.5, 2010	GuardianEdge Technologies Inc., All rights reserved < Back

Next >

Exit

< Back

- This is the Admin credentials for SEE package not system Admin credentials.

SEE Recover	Program		X
Make sure th	at the computer is conne	cted to an uninter	uptible power
supply during	the recovery process. I	ata loss occurs if t	he process is
supply during stopped while	the recovery process. [e in progress.	oata loss occurs if t	he process is

Getting ranges Disabling hibema Searching for hib	tion (if appropri emation file sig	ate) natures:			4
Decrypting					
					-
Version 7.0.5, 2	010 Guardian E	dge Technolog	gies Inc., A	l rights reserve	ed
		2011 - C.	4-1 C		



Disabling hibemation (if appropriate Searching for hibemation file signat) ures:	_
Decrypting		
The SEE-FD Recover process is su	iccessful.	
		*

- The system is now ready to boot up in normal mode.

References:

Best Practices for Data Recovery using Symantec Endpoint Encryption - Full Disk (SEE-FD) http://service1.symantec.com/support/ent-security.nsf/docid/2008022909242448

Information about the 32-bit Symantec Endpoint Encryption-Full Disk Access Utility http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008021914571748

How to get the 32-bit Symantec Endpoint Encryption - Full Disk (SEE-FD) Access Utility (WinPE) CD http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008021915141248

How to recover all data from an encrypted system when recover /d fails http://service1.symantec.com/support/ent-security.nsf/docid/2008021915563748

Commands used with Net Use and Symantec Endpoint Encryption http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008022015225848

Microsoft DOS copy command http://www.computerhope.com/copyhlp.htm

NET USE http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/enus/net_use.mspx?mfr=true