

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.

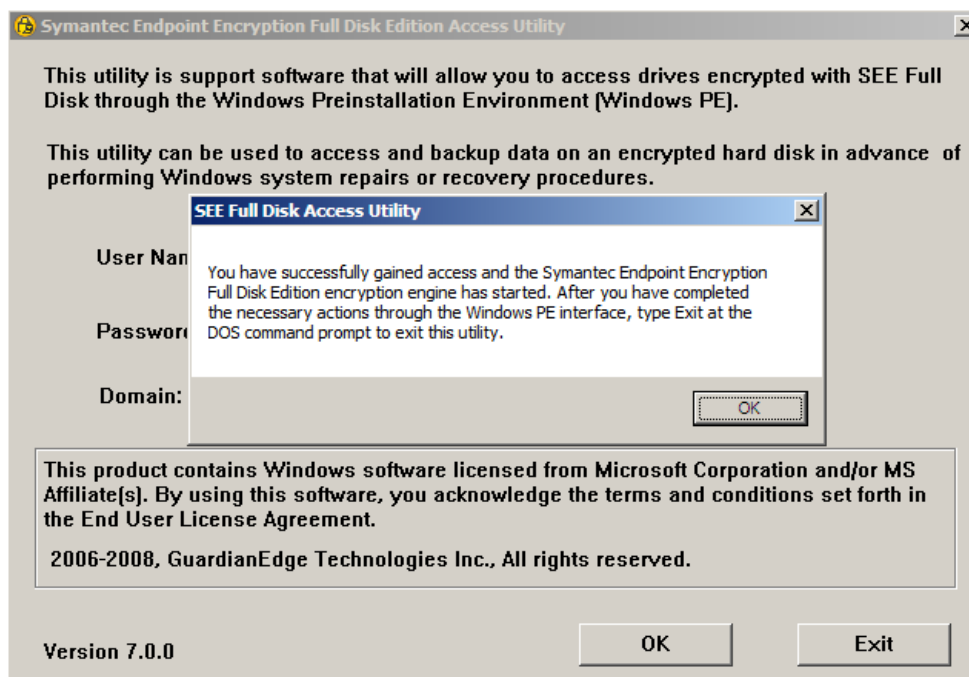
The command to run this utility is: "recover /a"

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.

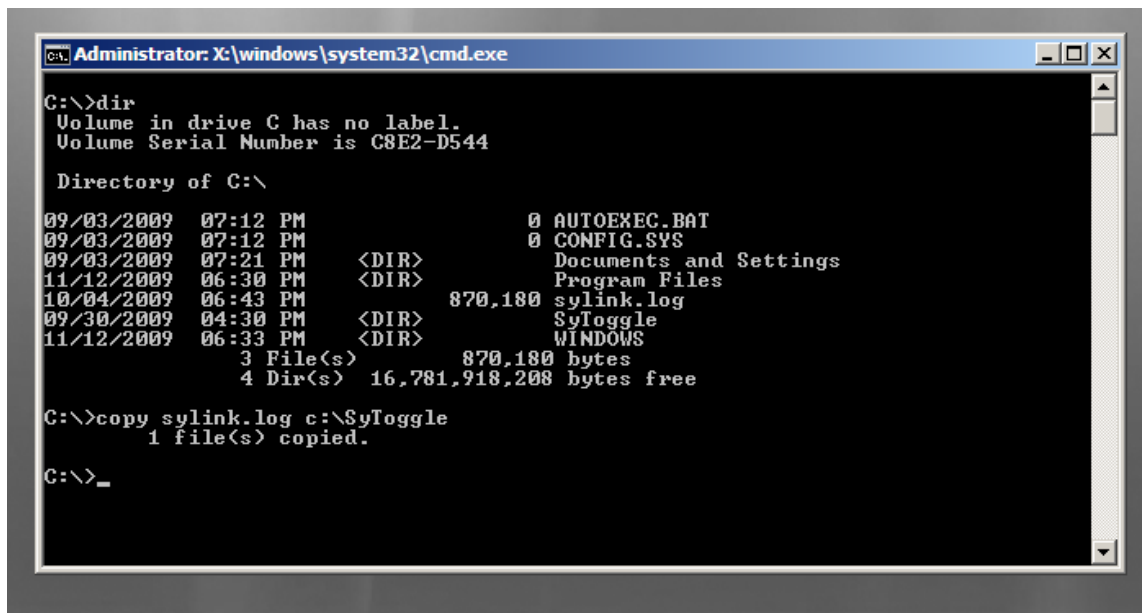
Endpoint Encryption Hard Disk Access Utility (Step 4)

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)



- 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.



```
Administrator: X:\windows\system32\cmd.exe

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:\$yToggle
        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:

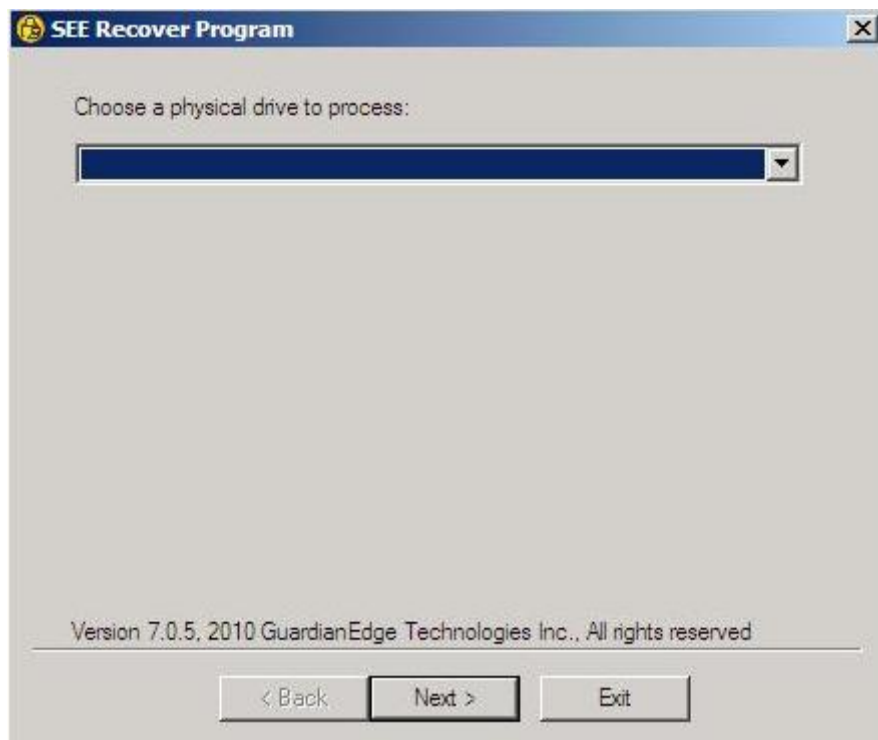
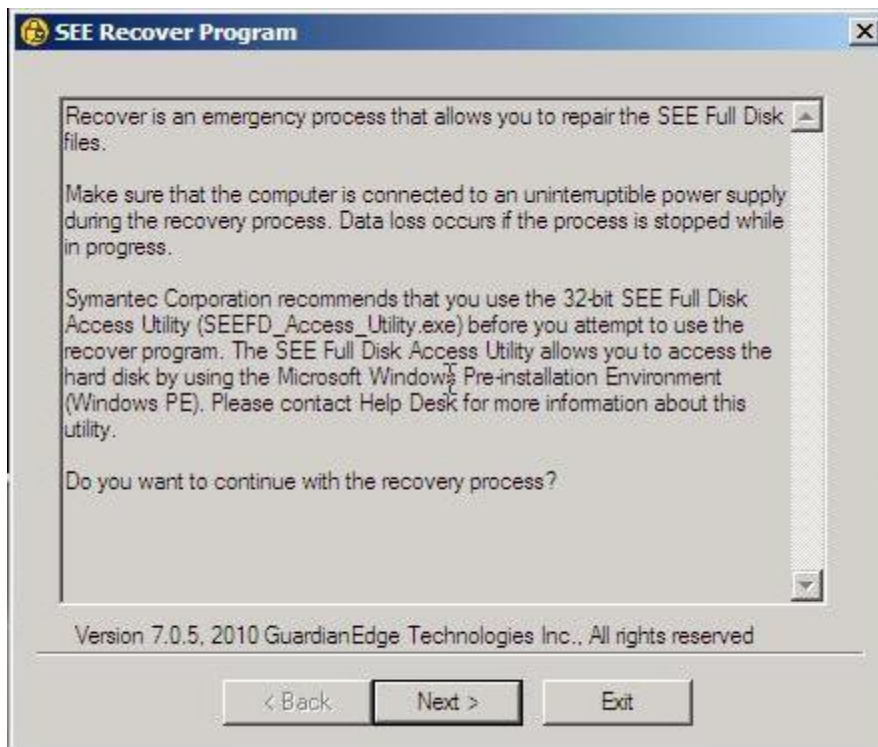
Never stop the emergency decryption process while in progress!

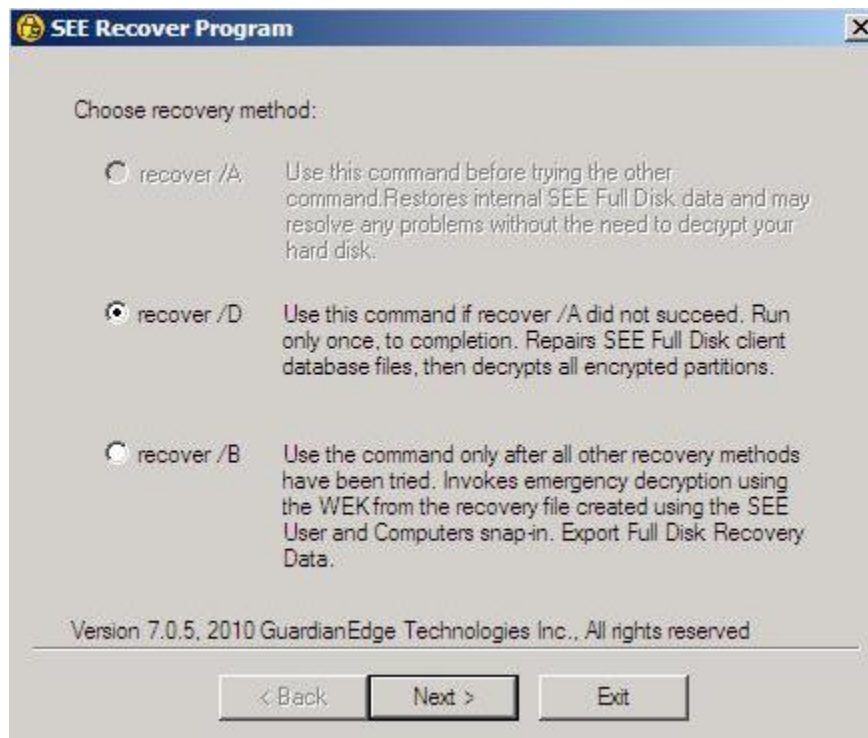
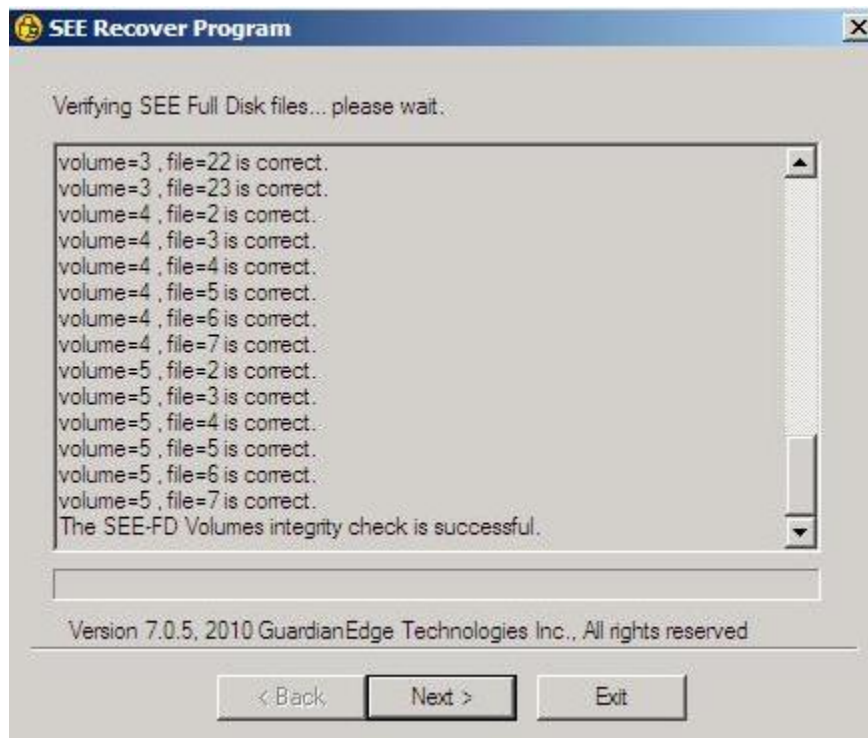
Do not run the "recover /d" command more than once, even if it did not appear to work.

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!

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





The screenshot shows the 'SEE Recover Program' window. At the top, there is a title bar with the program name and a close button. Below the title bar, the text 'Enter your client administrator credentials and click Next.' is displayed. There are two input fields: 'User name : ' followed by a text box, and 'Password : ' followed by a text box. At the bottom, there is a version string 'Version 7.0.5, 2010 GuardianEdge Technologies Inc., All rights reserved' and three buttons: '< Back', 'Next >', and 'Exit'.

SEE Recover Program

Enter your client administrator credentials and click Next.

User name :

Password :

Version 7.0.5, 2010 GuardianEdge Technologies Inc., All rights reserved

< Back Next > Exit

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

The screenshot shows the 'SEE Recover Program' window with a warning dialog box open. The dialog box has a title bar 'SEE Recover Program' and contains the text: '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.' There is an 'OK' button at the bottom right of the dialog box. The background window is partially obscured by the dialog box. The version string and navigation buttons are visible at the bottom of the main window.

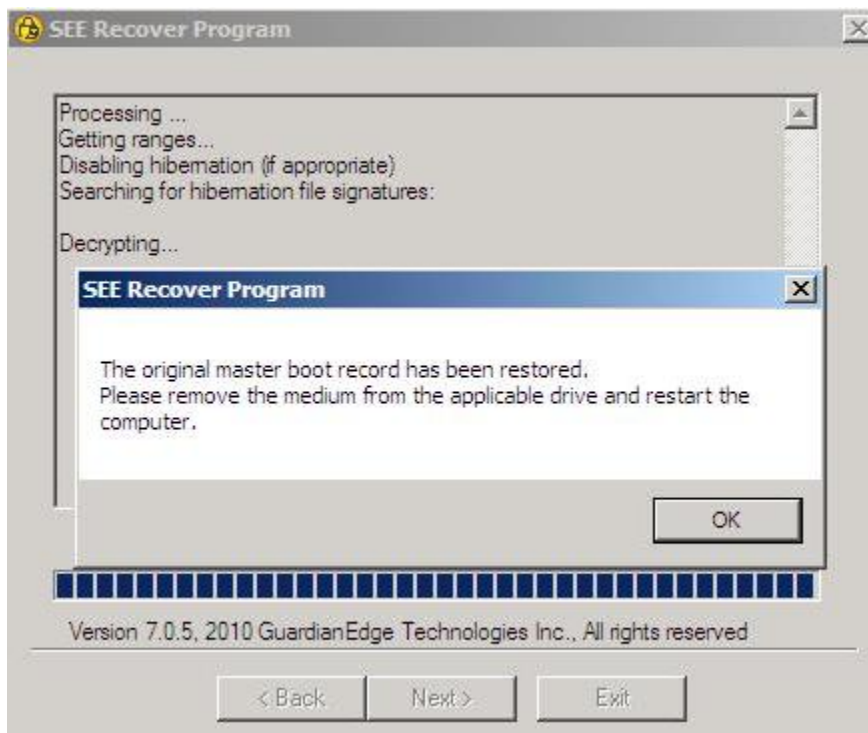
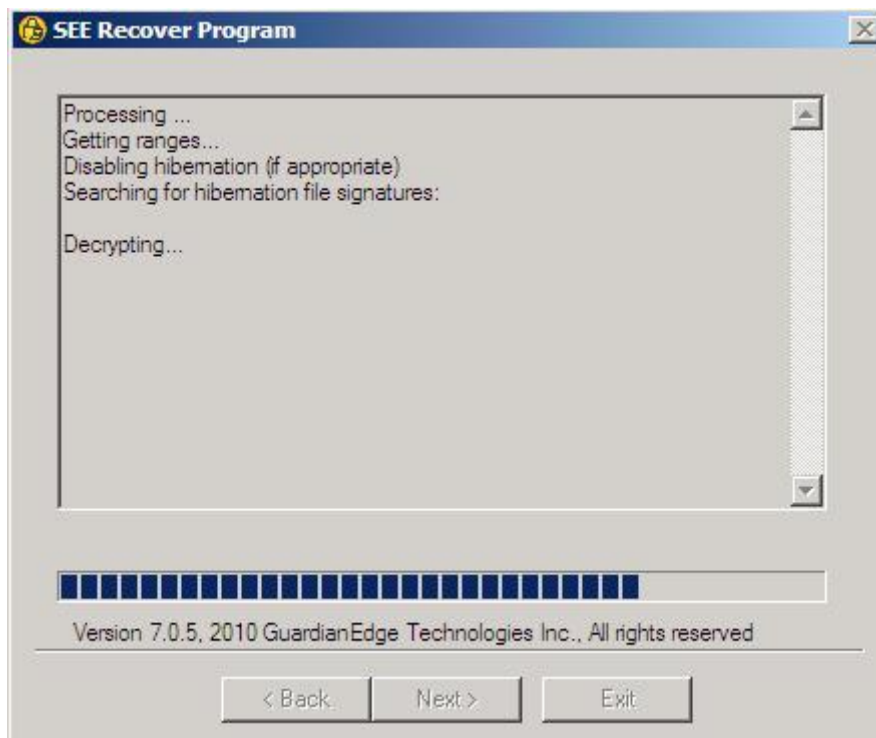
SEE Recover Program

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.

OK

Version 7.0.5, 2010 GuardianEdge Technologies Inc., All rights reserved

< Back Next > Exit





- 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/en-us/net_use.msp?mfr=true