



ADMINISTRATION GUIDE

Data Decryption Software

security

Data Decryption Software (DDS) Guide

Copyright © 2003-2007 Decru, Inc. All rights reserved.

Part number: 30-000259 B0 (030207_DDS_30)

No part of this manual may be reproduced in any form or any means without the prior written permission of Decru, Inc.

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

Copyright© 2005 Sun Microsystems, Inc. All Rights Reserved.

This software is provided "AS IS," without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SUN MICROSYSTEMS, INC. ("SUN") AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Portions of this product are derived from FreeBSD, which is copyrighted by FreeBSD.

Copyright © 1994-2005 FreeBSD, Inc. All rights reserved.

Software derived from copyrighted material of FreeBSD is subject to the following license and disclaimer:

Redistribution and use of the software in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE FREEBSD PROJECT "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FREEBSD PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young.

This product includes software developed by the OpenSSL project for use in the OpenSSL Toolkit.

TRADEMARK NOTICE

Decru®, Decru DataFort®, Cryptainer®, CryptoShred®, Lifetime Key Management™, the Decru logo and/or any Decru products or services referenced herein are trademarks and/or service marks of Decru, Inc. and may be registered in certain jurisdictions. All other product names, company names, marks, logos and symbols are trademarks or registered trademarks of their respective owners.



CONTENTS

Decru Data Decryption Software	4
Installation Requirements	5
Installing DDS	5
Using DDS for NAS	6
Data Recovery for NAS	6
Using DDS for SAN/iSCSI	7
Before using DDS for SAN/iSCSI	8
Data Recovery for Disk	9
Data Recovery for Tape to Tape	10
Data Recovery for Tape to Disk	11
Using the DDS CLI	13
Index	14



■■■■ **DECRU DATA DECRYPTION SOFTWARE**

Decru's Data Decryption Software (DDS) is an emergency recovery solution that recovers data encrypted by a Decru DataFort™ storage security appliance when the DataFort appliance is unavailable. DDS is used to decrypt data in conjunction with either the Decru Lifetime Key Management™ appliance (LKM appliance), or the Decru Lifetime Key Management software (LKM software). Both manage encryption keys generated by multiple DataFort appliances and ensure encryption key availability for the life of the secured data.

This chapter contains the following sections:

- [Installation Requirements](#)
- [Installing DDS](#)
- [Using DDS for NAS](#)
- [Using DDS for SAN/iSCSI](#)
- [Using the DDS CLI](#)

INSTALLATION REQUIREMENTS

Install DDS on a work station that can access the encrypted data to be restored.

Note: Data recovery is CPU-intensive. Select a computer with a powerful processor and ample disk space. DDS does not require the smart card reader.

The DDS server should meet the following requirements:

TABLE 1: SOFTWARE SPECIFICATIONS

Operating System (select one)	Browser
Windows XP (latest service pack)	Internet Explorer, v6.0 or later
Windows 2000 (latest service pack)	
Windows Server 2003 (latest service pack)	

TABLE 2: HARDWARE SPECIFICATIONS

Hardware
Intel P4 processor
512M RAM
1G free hard drive space
Enough free space for the data being decrypted. Decryption speed is dependant on the processor speed of the DDS station.

INSTALLING DDS

1. On the User CD, follow the link to the Data Decryption Software page, and click the Windows link.

Note: If the installer doesn't start automatically, run setup.exe.

2. Enter the license key when prompted and choose the default options.

After the software has been installed, the **Start > Programs > Decru** menu displays the Data Decryption Software.

Note: If you are an advanced user, who needs finer grained options or prefer a command line interface, you can use the Data Decryption Tool from the command line by launching dds.exe available in the DDS installation directory.

USING DDS FOR NAS

Data recovery requires DDS and Cryptainer Key Archive files (.cka for LKM appliance) or Cryptainer Key files (.ckf for LKM Software), the passphrases used to encrypt them and the paths to the encrypted Cryptainers you want to recover.

Note: Cryptainer Key Files are generated using Decru Lifetime Key Management software or the Decru Lifetime Key Management appliance.

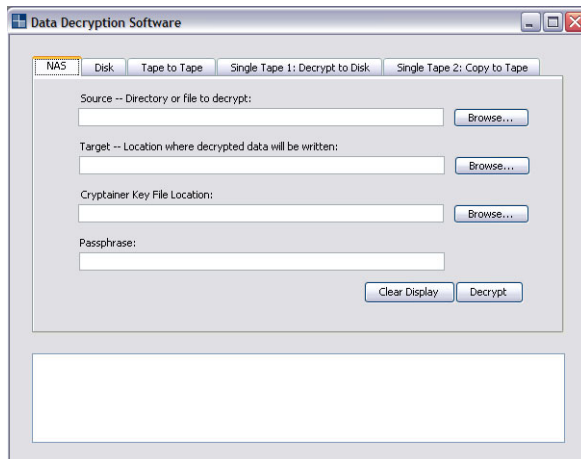
When copying encrypted data for decryption, be sure to copy over the entire Cryptainer. If a Cryptainer is of unknown origin, DDS will inform you which Cryptainer Key File to look for in LKM. Data Decryption Software decrypts one Cryptainer at a time. With the appropriate Cryptainer Key Files, DDS can decrypt all the Cryptainers associated with a DataFort.

WARNING: WHEN YOU HAVE FINISHED DECRYPTING FILES OR CRYPTAINERS, DELETE THE CRYPTAINER KEY FILE.

DATA RECOVERY FOR NAS

DDS displays tabs for data recovery in different environments.

1. On the Windows taskbar, select **Start > Programs > Decru > Data Decryption Software**.



2. On the NAS tab, enter or browse to the required information:
 - The directory or file to decrypt.
 - The location to store the decrypted directory/file.
 - The location of the Cryptainer Key File containing the Cryptainer Key needed for decryption.
 - The passphrase to recover the Cryptainer Key from the Cryptainer Key File.
3. Click Decrypt.

Note: The Clear Display button clears the GUI, to provide privacy without quitting DDS.

4. View the progress and the result of the operation in the lower window.
5. To decrypt more files, specify new parameters and click Decrypt.
6. Close the window to exit the tool.

Check the Target Disk

After decrypting data, run the check disk command on the destination disk.

1. At the CLI, cd to the destination volume.
2. Run the check disk command:
 - For NTFS volumes: `chkdsk /x`
 - For all other volumes: `chkdsk /f`

Using DDS for SAN/iSCSI

Data recovery requires DDS and Cryptainer Key Archive files (.cka for LKM appliance) or Cryptainer Key files (.ckf for LKM Software), the passphrases used to encrypt them and the paths to the encrypted Cryptainers you want to recover.

Note: Cryptainer Key Files are generated using Decru Lifetime Key Management software or the Decru Lifetime Key Management appliance.

When copying encrypted data for decryption, be sure to copy over the entire Cryptainer. If a Cryptainer is of unknown origin, DDS will inform you which Cryptainer Key File to look for in LKM. Data Decryption Software decrypts one Cryptainer at a time. With the appropriate Cryptainer Key Files, DDS can decrypt all the Cryptainers associated with a DataFort.

WARNING: WHEN YOU HAVE FINISHED DECRYPTING FILES OR CRYPTAINERS, DELETE THE CRYPTAINER KEY FILE.

This section includes the following topics:

- [Before using DDS for SAN/iSCSI](#)
- [Data Recovery for Disk](#)
- [Data Recovery for Tape to Disk](#)

BEFORE USING DDS FOR SAN/iSCSI

Before you run DDS for SAN/iSCSI, make the following additional preparations:

- Metadata must be turned on for encrypted data in order to use DDS to decrypt data. See the [DataFort Administration Guide](#) for more information about metadata.
- Obtain the identifying numbers of the source and target disks or tapes from Windows Administrative Tools.

This section includes the following topics:

- [Obtaining Identifying Numbers from Disk](#)
- [Obtaining Identifying Numbers from Veritas Volume Manager Disks](#)
- [Obtaining Identifying Numbers from Tape](#)

Obtaining Identifying Numbers from Disk

1. On the Windows taskbar, select **Start > Settings > Control Panel**
2. Select **Administrative Tools > Computer Management > Storage > Disk Management**.
3. Notice the disk number which is listed to the left of the bottom pane.
For example, the disk number is '2' for 'Disk 2'.

Obtaining Identifying Numbers from Veritas Volume Manager Disks

1. Start the Veritas Enterprise Administrator and connect to the system to which the encrypted drive is attached.
2. In the navigation pane on the left side of the Veritas UI, select the "Disks" tab under the system with the drive to be restored.
3. Identify the desired disk number by looking at the list of drives in the right-hand pane.
For example, the disk number would be '5' for 'Harddisk5'.

Obtaining Identifying Numbers from Tape

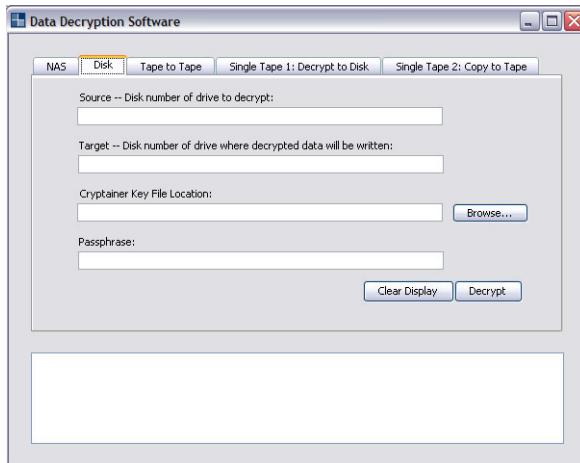
1. On the Windows taskbar, select **Start > Settings > Control Panel**
1. Select **Administrative Tools > Computer Management > Storage > Removable Storage > Physical Location**.
2. Right-click the source or target tape drive, and choose Properties.
3. Notice the tape drive number which is listed in the Device Info pane under Device Name.
For example, the tape drive number is '0' for '\\.\Tape0'.

DATA RECOVERY FOR DISK

Note: For Decru DataFort FC-Series appliance 2.x to decrypt disk data, you must make a key file with only one key entry (DDS will automatically use this key), or use the CLI to pick a key from the key file. See [Using the DDS CLI](#) on page 13.

This procedure will decrypt data from a source (encrypted) disk to a target disk. Be sure the target disk has the same or greater capacity as the source disk containing the encrypted files.

1. On the Windows taskbar, select **Start > Programs > Decru > Data Decryption Software**.



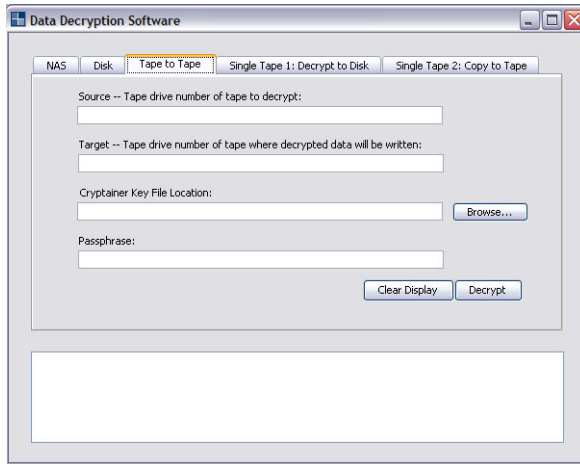
2. On the Disk tab, enter or browse to the required information:
 - The source disk number which is to be recovered.
 - A destination disk number for the disk to which data is to be written (Note: the disk must be identical to the source disk).
 - A Cryptainer Key file that contains the appropriate key.
 - The passphrase used to encrypt that Cryptainer Key File.
3. Press Decrypt to begin decryption.

Note: The Clear Display button clears the GUI, to provide privacy without quitting DDS.
4. View the progress and the result of the operation in the lower window.

DATA RECOVERY FOR TAPE TO TAPE

This procedure will decrypt data from a source (encrypted) tape to a target tape drive. Be sure the target tape drive is at least as large as the source tape drive. You can use a disk for intermediate data storage between the source and target tape drive. See [Data Recovery for Tape to Disk](#).

1. On the Windows taskbar, select **Start > Programs > Decru > Data Decryption Software**.



2. On the Tape to Tape tab, enter or browse to the required information:
 - The source tape drive number which is to be recovered.
 - A destination tape drive number for the tape to which data is to be written (Note: the tape must be greater in size than the source tape).
 - A Cryptainer Key file that contains the appropriate key.
 - The passphrase used to encrypt that Cryptainer Key File.
3. Press Decrypt to begin decryption.

Note: The Clear Display button clears the GUI, to provide privacy without quitting DDS.
4. View the progress and the result of the operation in the lower window.

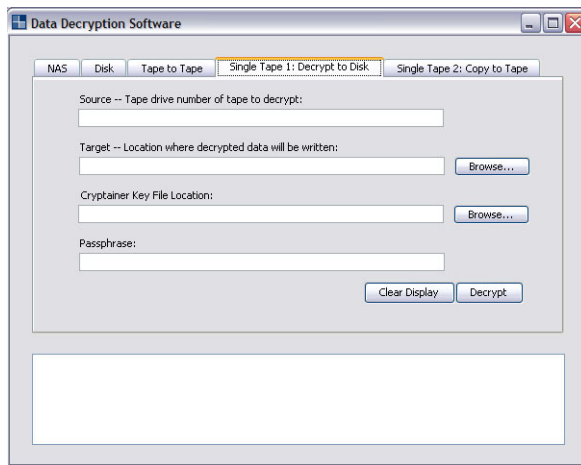
DATA RECOVERY FOR TAPE TO DISK

This procedure can be used when only one tape drive is available. Make sure the disk has adequate space for the data that will be transferred. The process is broken up into two steps, [Decrypting Data to a Temporary Disk File](#) and [Writing Decrypted Data to Tape](#).

Decrypting Data to a Temporary Disk File

First decrypt the tape to a temporary disk file. Please make sure that you have enough free disk space to decrypt this tape to disk.

1. On the Windows taskbar, select **Start > Programs > Decru > Data Decryption Software**.



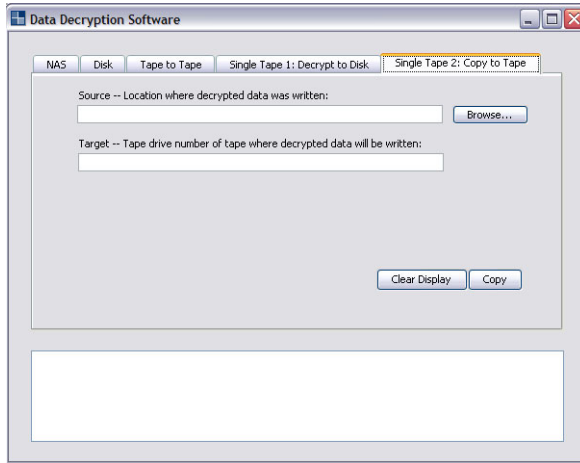
2. On the Single Tape 1: Decrypt to Disk tab, enter or browse to the required information:
 - The source tape drive number which is to be recovered.
 - A destination file to which the data is to be written.
 - A Cryptainer Key file that contains the appropriate key.
 - The passphrase used to encrypt that Cryptainer Key File.
3. Press Decrypt data to begin decryption.

Note: The Clear Display button clears the GUI, to provide privacy without quitting DDS.
4. View the progress and the result of the operation in the lower window.

Writing Decrypted Data to Tape

Next use the tool to write the decrypted data from the file to tape.

1. On the Windows taskbar, select **Start > Programs > Decru > Data Decryption Software**.



2. On the Single Tape 2: Copy to Tape tab, enter or browse to the required information:
 - The destination tape drive number where data is to be written.
 - The destination file to which the data was written in the previous step.
 3. Click Copy to begin writing to the tape.
 4. View the progress and the result of the operation in the lower window.
- Note:** The Clear Display button clears the GUI, to provide privacy without quitting DDS.

USING THE DDS CLI

1. On the Windows taskbar, select Run.
2. Enter or browse to the DDS.exe file.
For example: C:\Program Files\Decru\Decru Data Decryption Software\dds.exe
3. At the CLI, run the dds.exe with the following command using the desired recovery type:

```
dds [options] [<recovery_type> [args]]
```

For example, here is a command to recover a disk:

```
dds.exe disk 0 1 test.cka 12345678
```

Valid options are:

<code>[-b/--blocksize <size>]</code>	Sets tape block size. Valid values: 32, 64, 128, 256, 512, 1024, 2048, 4096
<code>[-v]</code>	Enables verbose mode. These details may be sent to your local support engineer.
<code>[-q <queue_size>]</code>	Sets the size of the read-ahead queue.
<code>[--nowrite]</code>	Reads the data only.

Valid recovery types are:

```
read-tape [<src_tape>]
```

Performs a read performance test on the tape.

```
tape [<src_tape> <tgt_tape> <key_file> [<password>]]
```

Recovers data from the source tape and writes to the destination tape.

```
tape-disk [<src_tape> <temp_file> <key_file> [<password>]]
```

Recovers data from the source tape and writes to a temporary file.

```
disk-tape [<temp_file> <tgt_tape>]
```

Restores data from the a temporary file to the tape.

```
disk [<src_disk> <tgt_disk> <key_file> [<password>]]
```

Recovers data from the source disk and writes to the target disk.

```
nas [<src_dir/src_file> <tgt_dir> <key_file> [<password>]]
```

Recovers a file or directory.



INDEX

Symbols

- .cka
 - cryptainer key archive file, LKM appliance 6, 7
- .ckf
 - cryptainer key file, LKM software 6, 7

C

- CLI
 - use of for decryption 13
- copy to tape
 - tab 12
- cryptainer key archive file
 - LKM appliance 6, 7
- cryptainer key file
 - LKM software 6, 7

D

- DDS
 - copy to tape tab 12
 - decrypt to disk tab 11
 - disk tab 9
 - install 5
 - NAS tab 6
 - tape to tape tab 10
 - using software 6
- decrypt
 - data from disk to disk 9
 - data from tape to tape 10
 - data to temporary disk file 11
 - NAS data 6
 - write decrypted data to tape 12
- decrypt to disk
 - tab 11
- decryption
 - via CLI 13
- disk
 - tab 9

I

- install
 - DDS 5
 - hardware specifications 5
 - requirements 5
 - software specifications 5

L

- LKM appliance
 - .cka file 6, 7
 - cryptainer key archive file 6, 7
- LKM software
 - .ckf file 6, 7
 - cryptainer key file 6, 7

N

- NAS
 - check target disk 7
 - tab 6

T

- tab
 - copy to tape 12
 - decrypt to disk 11
 - disk 9
 - NAS 6
 - tape to tape 10
- tape to tape
 - tab 10