

DECRU®



■ ■ ■ **ADMINISTRATION GUIDE**

Data Decryption Software

security

Data Decryption Software (DDS) Guide

Copyright © 2003-2006 Decru, Inc. All rights reserved.

Part number: 30-000259 v 2.5 051606

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™ software, 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
Installing the Data Decryption Software	4
Installing Data Decryption Software on Windows	4
Data Decryption Software WebUI	5
Data Decryption Software for NAS	5
Software Recovery for NAS Using Windows	5
Check the Target Disk	6
Data Decryption Software for SAN/iSCSI	7
Before Using the Data Decryption Software for SAN/iSCSI	7
Software Recovery for Disk	7
Software Recovery for Tape to Tape	8
Software Recovery for Tape to Disk	9



1 **DECRU DATA DECRYPTION SOFTWARE**

Decru’s Data Decryption Software (DDS) is used for emergency recovery of data encrypted using the Decru DataFort. Data recovery requires Cryptainer Key Files, which are generated by Decru Lifetime Key Management software as described in the *Lifetime Key Management Tool Guide*. You will also need to supply the passphrase that was provided when each Cryptainer Key File was created.

This document outlines the steps necessary to decrypt data on NAS and SAN/iSCSI devices:

- [Data Decryption Software for NAS](#)
- [Data Decryption Software for SAN/iSCSI](#)

INSTALLING THE DATA DECRYPTION SOFTWARE

Data decryption software is used under special circumstances to restore encrypted data when a DataFort is not available. The Data Decryption Software should be installed on a computer that is accessible to the data that is 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:

Operating System	Windows XP (latest service pack)
	Windows 2000 (latest service pack)
	Windows Server 2003 (latest service pack)
Hardware	Intel P4 processor
	512M RAM
	1G free hard drive space
	Enough free space for the data being decrypted. Note that decryption speed is dependant on the processor speed of the DDS station.

INSTALLING DATA DECRYPTION SOFTWARE ON WINDOWS

1. On the User CD, follow the link to the Data Decryption Software page, and click the Windows link.
2. If the installer doesn’t start automatically, run setup.exe.
3. 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 entry.

DATA DECRYPTION SOFTWARE WEBUI

The WebUI for DDS displays tabs for data recovery in different environments. For data recovery in the NAS environment, select NAS. For data recovery in the SAN or iSCSI environment, select the disk or tape options. The Clear Display button clears the GUI, providing for privacy without quitting DDS.

- [Data Decryption Software for NAS](#)
- [Data Decryption Software for SAN/iSCSI](#)

DATA DECRYPTION SOFTWARE FOR NAS

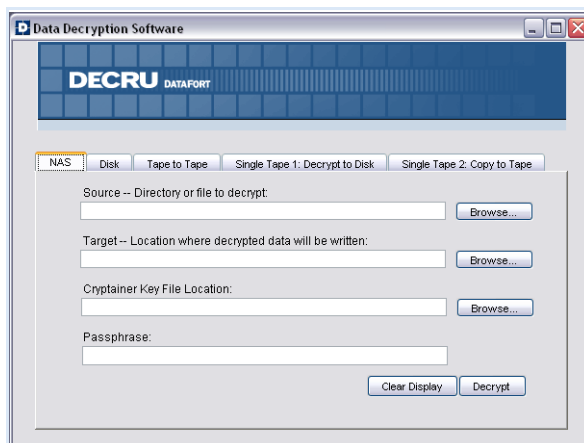
Before decrypting data, assemble the necessary Cryptainer Key Files and associated encrypted data. Cryptainer Key Files are generated using LKM. If you are copying encrypted data for decryption, be sure to copy over the entire Cryptainer.

If the Cryptainers that will be decrypted are of unknown origin, DDS will inform you which Cryptainer Key File to look for in LKM.

CAUTION: When you have finished decrypting files or Cryptainers, delete the Cryptainer Key File.

SOFTWARE RECOVERY FOR NAS USING WINDOWS

1. Choose **Start > Programs > Decru > Data Decryption Software**.
2. Select the NAS tab.



3. 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.
4. Click Decrypt.
 5. View the progress and the result of the operation in the lower window.
 6. To decrypt more files, specify new parameters and click Decrypt.
 7. Close the window to exit the tool.

CHECK THE TARGET DISK

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

1. Open a command prompt.
2. cd to the destination volume.
3. Execute the check disk command:
 - For NTFS volumes: `chkdsk /x`
 - For all other volumes: `chkdsk /f`

DATA DECRYPTION SOFTWARE FOR SAN/iSCSI

Data recovery in the SAN/iSCSI environment requires Cryptainer Key Files and the passphrase that was provided when each Cryptainer Key File was created. Note that metadata must be turned on for encrypted data in order to use the WebUI for DDS to decrypt data. See the *DataFort Administration Guide* for more information about metadata.

CAUTION: When you have finished decrypting files or Cryptainers, delete the Cryptainer Key File.

Data Decryption Software decrypts one Cryptainer at a time. With the appropriate Cryptainer or tape key files, DDS can decrypt all the Cryptainers associated with a DataFort. The following options exist in the SAN/iSCSI environment:

- [Software Recovery for Disk](#). Follow these instructions to recover an encrypted disk.
- [Software Recovery for Tape to Tape](#). Follow these instructions to recover an encrypted tape.
- [Software Recovery for Tape to Disk](#). Follow these instructions to recover an encrypted tape when only one tape drive is available.

Note: Advanced users who need finer grained options or prefer a command line interface can use the DataFort CLI, available in the SRT installation directory as dcrSWRTool.exe.

BEFORE USING THE DATA DECRYPTION SOFTWARE FOR SAN/iSCSI

Before you run the tool, make the following preparations:

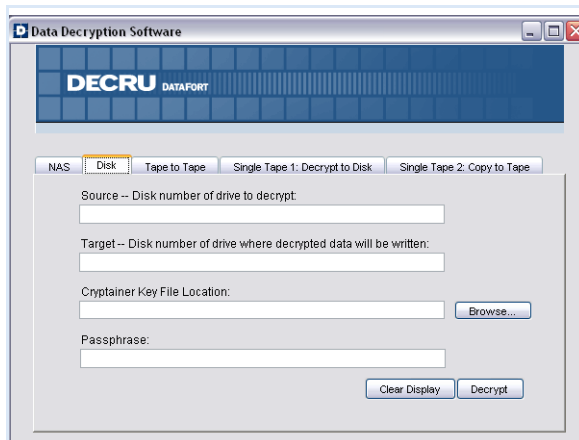
- Create and assemble the necessary Cryptainer Key Files, their passphrases, and the paths to the encrypted Cryptainers you want to recover.
- Obtain the identifying numbers of the source and target disks or tapes from Windows Administrative Tools.
 - **Disk:** From Administrative Tools, choose **Computer Management > Storage > Disk Management**. The disk number is listed in the left column of the Disk Management pane. For example, the disk number is '2' for 'Disk 2'.
 - **Veritas Volume Manager disks:** Start the Veritas Enterprise Administrator and connect to the system to which the encrypted drive is attached. 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. 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'.
 - **Tape:** From Administrative Tools, choose **Computer Management > Storage > Removable Storage > Physical Location**. Right-click the source or target tape drive, and choose Properties. The tape drive number is listed in the Device Info pane under Device Name. For example, the tape drive number is '0' for '\\.\Tape0'.

SOFTWARE RECOVERY FOR DISK

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. To open the tool from the Windows Start menu, choose **Start > Programs > Decru > Data Decryption Software**.

2. Click the Disk tab.

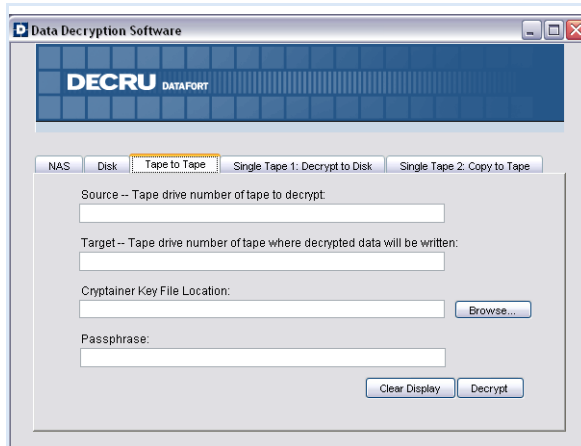


3. Specify the following:
 - The source disk number which is to be recovered.
 - A destination disk number for the disk to which data is to be written (Note: the disk must be identical to the source disk).
 - A Cryptainer Key file that contains the appropriate key.
 - The passphrase used to encrypt that Cryptainer Key File.
4. Press Decrypt to begin decryption.
5. View the progress and the result of the operation in the lower window.

SOFTWARE 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 [Software Recovery for Tape to Disk](#).

1. To open the tool from the Windows Start menu, choose **Start > Programs > Decru > Data Decryption Software**.
2. Click the Tape to Tape tab.



3. Specify the following:
 - 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.
4. Press Decrypt to begin decryption.
5. View the progress and the result of the operation in the lower window.

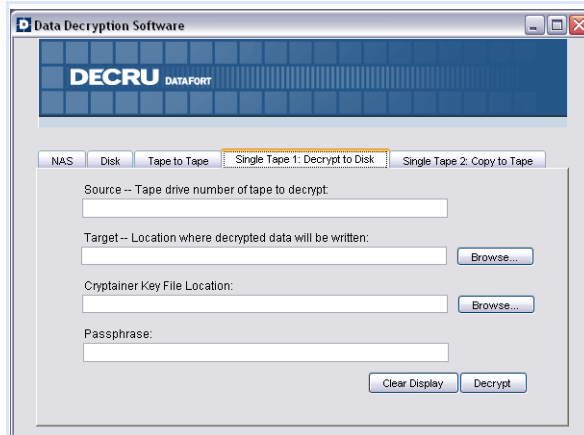
SOFTWARE RECOVERY FOR TAPE TO DISK

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. To open the tool from the Windows Start menu, choose **Start > Programs > Decru > Data Decryption Software**.
2. Click the Single Tape 1: Decrypt to Disk tab.

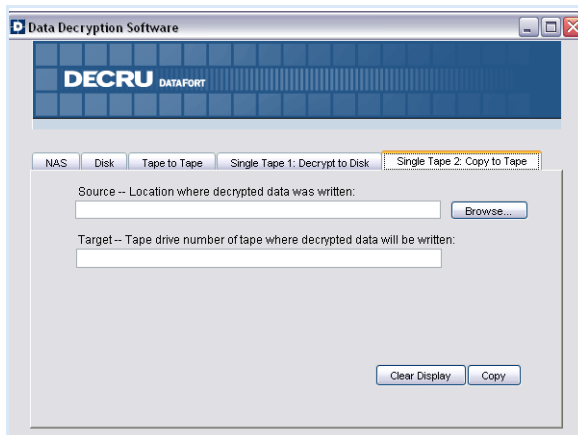


3. Specify the following:
 - The source tape drive number which is to be recovered.
 - A destination file to which the data is to be written.
 - A Cryptainer Key file that contains the appropriate key.
 - The passphrase used to encrypt that Cryptainer Key File.
4. Press Decrypt data to begin decryption.
5. 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. Click the Single Tape 2: Copy to Tape tab.



2. Specify the following:
 - 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.