DECRU®

ADMINISTRATION GUIDE

Lifetime Key Management Tool

security

Decru Lifetime Key Management Guide

Copyright © 2003-2005 Decru, Inc. All rights reserved.

Part number: 30-000191 v 2.1 050305

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© 2003 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 © 1994-2003 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

The Decru Lifetime Key Management System **5**
Installing the LKM System 5
LKM Server Designation 5
LKM Server Specification 6
LKM Server Configuration 6
Preparing SQL Server for LKM Installation 7
Installing LKM Software 8
Accessing LKM Software 9
Starting the LKM UI 9
Initial Configuration 10
Configuring Backups to the LKM Server 10
Verifying Automated Backups 12
Loading Configurations in LKM Manually 13
After Initial Setup 15
Key Management 15

LKM Software **16**
Running the LKM UI 16
The LKM Display 17
Controlling the LKM Program Window Display 17
Summary of Menus and Options 21

LKM Archiving Functions **23**
Loading a DataFort Configuration Database 23
Backing up a Configuration Database 24
Generating a Recovery Key Archive 25

LKM Data Recovery Functions **28**
Decrypting Files and Cryptainer Vaults 29
Authentication for Data Recovery 29
Cryptainer Key Files 29
Recover Data Option 32
File Recovery with Recovery Cards 33
File Recovery with Recovery Key Archive 35
File Recovery with Cryptainer Key File 35
Identifying Recovery Cards 36
Import and Export of Cryptainer Keys 37
Exporting Cryptainer Keys 37
Importing Exported Cryptainer Keys 38
Key Translation Option 38
Translating All Cryptainer Keys 38

Translating Individual Keys 39
Restoring Cryptainers on the Target DataFort 40

Software Recovery Tool 41
Installing the Software Recovery Tool 41
Installing the Standalone Software Recovery Tool on Windows 41
Installing the Standalone Software Recovery Tool on Linux 41
Software Recovery Tool for NAS 42
Software Recovery for NAS Using Windows 42
Software Recovery for NAS Using Linux 43
Software Recovery Tool for SAN/iSCSI 43
Before Using the Software Recovery Tool for SAN/iSCSI 44
Software Recovery for Disk 44
Software Recovery for Tape to Tape 45
Software Recovery for Tape to Disk 46

LKM Options 48
DataFort Options 48
Delete DataFort Records 48
Open DataFort WebUI 49
View DataFort Properties 49
Delete Cryptainer from LKM 50
LKM Options 51
Save Latest Configuration Database to File 51
Import LKM Database 51
Export LKM Database 52
Sync a Primary and Secondary LKM Server 52
Zeroize LKM Database 52
Manage LKM Ports 53

LKM Administration 57
Administration Issues 57
Security Policy 57
Key Escrow 58
Troubleshooting 58
Managing the LKM Service 58
Backing Up LKM Archives 59
Changes in DataFort Deployment 59

Index 60

1 The Decru Lifetime Key Management System

The Decru DataFort™ appliance secures networked storage, protecting data at rest by encrypting it with strong algorithms. DataFort supports the creation of secured storage elements called Cryptainer vaults™, in which encrypted data is stored. Since DataFort offers persistent encryption for data in storage, a methodology for managing encryption keys over the long term is required.

The Decru Lifetime Key Management™ (LKM) software provides this functionality for a DataFort security administrator managing one or more DataFort appliances. LKM simplifies and centralizes two functions that make permanent data accessibility possible:

- Maintaining Cryptainer Key and DataFort configuration information.
- Under special circumstances, such as disaster recovery, providing additional tools for decrypting data that was encrypted by DataFort.

With LKM software, the security administrator can upload, view, manage and save DataFort configuration and key information as a form of insurance against future problems. If the need arises, LKM allows authorized persons to decrypt data in the absence of the usual decrypting mechanisms.

LKM creates a cumulative key archive based on information from DataFort configuration databases that are manually or automatically loaded into the LKM software, as part of regular updates that LKM receives from each DataFort.

A DataFort configuration database contains, in encrypted form, all of the key security and network information for the DataFort, including Cryptainer Keys, Tape Keys, Recovery Keys, and the secret shares required to recover the Master Key, which is used to decrypt other keys in the configuration database. By extracting key information from DataFort configuration databases over an extended period of time, LKM ensures that keys used to encrypt data are available for decryption throughout the life of the data. There ia a separate standalone Software Recovery Tool for data recovery.

Installing the LKM System

Setting up the LKM system consists of these steps:

- Designating an LKM server and installing LKM software on the server.
- Specifying the LKM server in a DataFort management interface.

LKM Server Designation

An LKM server is a Windows computer used for consolidating the key and configuration details of multiple DataFort appliances over extended periods of time. An LKM installation on one LKM server can manage multiple DataFort appliances. If desired, the LKM software and the database used to store LKM data can be divided between two servers.

The LKM server should be a dedicated machine used only for LKM and no other services. This server should be regularly inspected and patched, and physical access to it should be controlled. LKM software relies on the correctness of the server's operating system to authenticate the LKM administrator and to protect LKM from unauthorized tampering. Be sure that no hostile process or entity compromises the LKM server, especially when Recovery Cards are used, as keys are briefly exposed to software during Recovery Card procedures.

LKM Server Specification

Specifying the LKM server to a DataFort sends the current DataFort configuration to LKM automatically, and updates LKM automatically when the configuration changes. If the LKM server is not available when a DataFort is put into service, configuration database backups can be loaded into LKM software manually.

One LKM server can manage multiple DataFort appliances, and all DataFort cluster members update the same LKM server. For clustered DataFort appliances, specifying or changing LKM server settings on one cluster member automatically updates LKM settings on the other members.

After setup, familiarity with the *DataFort Administration Guide* will be helpful in understanding data recovery procedures that might be required in the future.

LKM Server Configuration

The LKM station must be dedicated to LKM use, and no other process must be allowed to run on this station, as any hostile local processes may issue destructive commands to the LKM server database.

> **Note:** The LKM server should be dedicated to key management and data recovery. Using a Management Station as an LKM server is not recommended. It is also feasible to select one computer for running LKM software and another for storing the key archives.

To configure the LKM server, choose a computer that meets the following requirements:

- Accessible via Ethernet to all DataFort appliances that LKM will serve.
- A fixed IP address. You will need the IP address when you configure DataFort appliances for automated backups.
- Windows 2000 Server or Windows Server 2003 operating system (preferred); a dedicated Windows 2000 or Windows XP workstation is acceptable.
- Internet Explorer, v6.0 or later.
- 2GB free disk space for the MySQL database if the database will reside on the LKM server. During installation you can also specify a different server to contain the database.
- 512MB RAM
- 1 GHz processor
- An available USB port for the smart card reader from Decru.
- A CD drive for installing software.
- Note that LKM server ports 15362 and 15363 need to be available to allow automated communication between the LKM server and DataFort appliances. If using a Windows XP server, you must add the ports used by LKM to Windows Firewall. Open Windows Firewall and click the Exceptions tab. Add ports 15362 and 15363 for clear communication and ports 15372 and 15373 for SSL using the Add port button.

Backup LKM Server

LKM supports automated configuration backups to a primary LKM server and an optional secondary backup server. The secondary server can be at a remote site. To use a backup LKM server, set it up just as you did the primary LKM server, and note its IP address. DataFort will ensure that the two LKM servers will be in sync going forward. If the secondary LKM Server is added at a later time, sync it with the existing server (see Sync a Primary and Secondary LKM Server on page 52).

Preparing SQL Server for LKM Installation

LKM can use a MySQL database to store data (this is the default), or it can be configured to use a Microsoft SQL Server. This designation is made during the installation wizard as described in Installing LKM Software. In order to configure LKM to use a Microsoft SQL Server as the database, the server must be prepared before installing LKM.

Note: The default installation using MySQL does not require this step. For ordinary installation, skip to Installing LKM Software on page 8.

1. From the left pane of the Microsoft SQL Server Enterprise Manager, expand the Microsoft SQL Servers entry in the Console Root tree.
2. Expand the entry for your SQL Server installation and right-click the Databases directory.
3. Select New Database from the right-click menu.
4. Create a database called Decru and click OK.
5. Right-click the Security directory under your SQL Server installation and right-click Logins.
6. Select New Login from the right-click menu.
7. Enter a name of your choice for this user. You will be prompted for this information during LKM installation.
8. Select the SQL Server Authentication button, and enter a password for this user. You will be prompted for this information during LKM installation.
9. Specify the Decru database as the default for this login by selecting it from the Database pull-down menu. Click OK.
10. Confirm the new password.
11. Expand the entry for your SQL Server installation, and expand the Databases directory.
12. Expand the Decru database directory and right-click the Users entry. Select New Database User from the right-click menu.
13. Select the new user from the pull-down menu of login names.
14. Check the boxes that will assign the following permissions to the user: public, db_owner, db_accessadmin, db_securityadmin, db_ddladmin, db_backupoperator, db_datareader, db_datawriter.
15. Click OK to complete the operation.
16. Ensure authentication settings are correct: Right-click your SQL Server entry in the left pane and select Properties.
17. Select the Security tab and be sure that the authentication button for SQL Server and Windows is selected.
18. Click OK.
19. Continue with Installing LKM Software.

Installing LKM Software

1. Insert the DataFort CD in a drive on the LKM server (or in a mapped drive). The CD will run automatically.
2. Click the Lifetime Key Management installer link. When prompted by the File Download screen to open or save the file, click the Open button to open the file.
3. Follow the prompts to start the installer and accept the terms of the license agreement.
4. Enter the LKM license key provided by Decru and click Next.
5. Click next to allow the system to be checked for software requirements.
6. Specify the installation directory or use the default. Click Next.
7. Click Install to begin installation.
8. Specify the database type to use with LKM (MySQL or Microsoft SQL) and click Next.

   MySQL: This is the default installation.

   - Enter a database user name of your choice.
   - Enter a password for that user.
   - Confirm the user password by entering it again.
   - Set the path to the data directory, or accept the default location and click Next.

   Microsoft SQL Server: Select this if a Microsoft SQL Server has been configured for use with LKM as described in Preparing SQL Server for LKM Installation. Enter the information for that server:

   - Enter the IP address of the Microsoft SQL Server.
   - Enter the user name (the same user name that was added to the Microsoft SQL Server).
   - Enter the user password (the same password that was added to the Microsoft SQL Server).
9. Follow the prompts to start the smart card reader installer (if the smart card reader driver is not already installed on the computer). Accept the license agreement, and select the model number of your smart card reader. The model number can be found on the underside of the smart card reader (i.e. GemPC413-SL).
10. Select the “Yes, I want to restart my computer now” radio button on the LKM installer page and click Finish to complete installation.
11. After the LKM server reboots, the LKM Service starts automatically. Click the LKM desktop icon or select **Start > Programs > Decru > Lifetime Key Management** to view LKM.

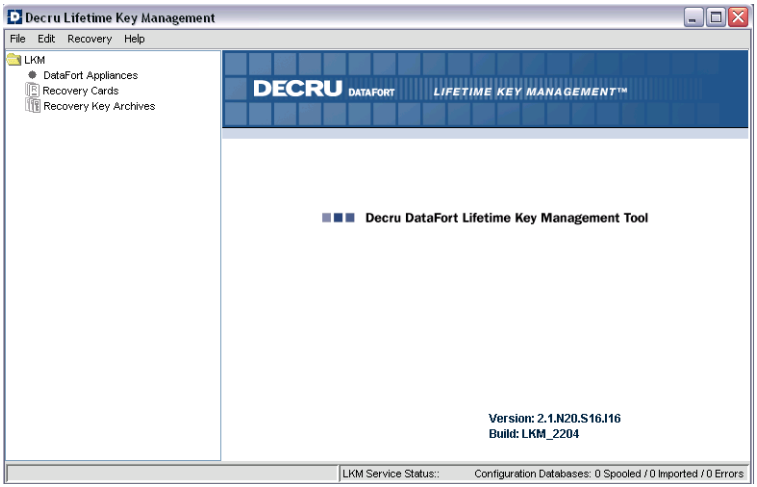
Accessing LKM Software

The Lifetime Key Management System runs as two components: a Windows Service that runs automatically whenever the LKM server is running, and a program user interface (UI) that you start when you wish to interact with LKM software. For information on the service component, see Managing the LKM Service.

Starting the LKM UI

1. To start the LKM UI, click the LKM program icon on the Windows desktop, or choose **Start > Programs > Decru > Lifetime Key Management**.

The tool offers drop-down menus for key functions, and the left pane lists DataFort appliances with configuration databases that have been added to LKM. Status is shown at the base of the screen. For more information, see LKM Software.



LKM Setup Guidelines

- Set up each DataFort using a setup wizard, as described in the *DataFort Administration Guide*.
- Specify LKM settings on each DataFort or DataFort cluster.
- To begin using LKM software, load a configuration database using one of the methods described in Initial Configuration.
- Leave the LKM server running at all times. LKM can receive updates from one or more DataFort appliances even after the server administrator logs out of the LKM server.
- You may leave the smart card reader attached to the LKM server's USB port, but it is not good practice to leave any smart cards in the reader.

Initial Configuration

After LKM software has been installed, load one or more DataFort configurations into the software. For more information about DataFort configuration and accessing management interfaces, see the *DataFort Administration Guide*. For configuring LKM, see the following sections of this guide:

- To specify the LKM server in DataFort WebUI, see Configuration from the DataFort WebUI.
- To specify the LKM server in DataFort CLI, see Configuration from the DataFort CLI.
- To upload previously-saved configurations in LKM manually, see Loading a Saved Configuration Database into LKM.

If the LKM server is not yet in operation when you are entering LKM settings for the first time, back up DataFort configurations to another site, and load them into LKM later (see Saving the DataFort Configuration Database and Loading a Saved Configuration Database into LKM).

Configuring Backups to the LKM Server

Use the DataFort WebUI or the DataFort CLI to specify the LKM server and set up automated backups. The simplest way to ensure permanent retention of DataFort keys is to configure DataFort to automatically save backups of its configuration database to the LKM server.

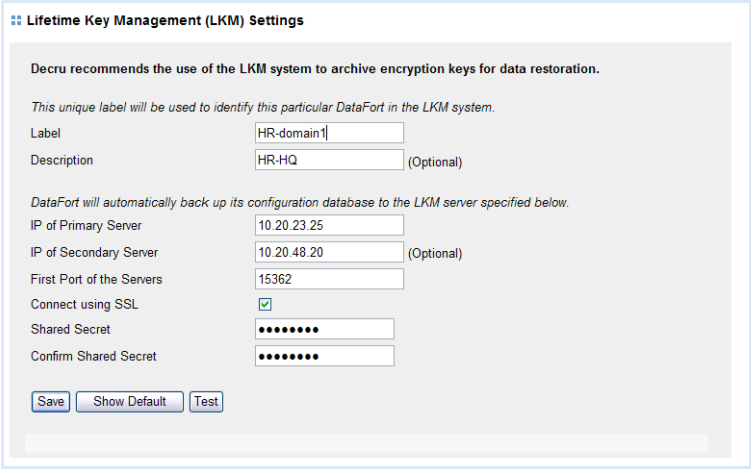
Note: If DataFort has been in operation for some time, postpone specifying automated backups until you have loaded earlier saved configurations to the LKM server.

Configuration from the DataFort WebUI

The following steps can be performed at any time after initial DataFort setup. See the *DataFort Administration Guide* for information about logging in to the DataFort WebUI.

1. From a Management Station, log in to the DataFort WebUI, and choose **System Config > Recovery > LKM Settings**.

   Note: Log in to any member of a cluster to enter these settings.



2. Assign a unique name for the DataFort that will identify it in LKM. Enter a description (optional).
3. Enter the IP address of the LKM server.
4. If you have configured a secondary backup LKM server, enter the IP address of the secondary server. If the first LKM server is already in operation when you add a secondary server, sync the secondary server (see Sync a Primary and Secondary LKM Server).
5. Enter LKM information at the LKM Settings page of one member of each cluster whose keys you want LKM to manage. Configure Regular or Secure Backups by completing the appropriate procedure below.

Configuring Regular Backups

1. On the LKM Settings page, leave the First Port of the Servers at its default (15362). If this port will not be available, change it here and also in LKM (see Configuring LKM Server Ports).

   Note: This setting defines three successive ports (on the LKM server) used for communication between all connected DataFort appliances and the LKM server, and within LKM.

2. The Settings page sets up the connection but does not send data immediately. To test the connection between DataFort and the LKM server right away, click Test. The status line indicates whether the connection succeeded.
3. Click Save.

   Clicking Save on this screen saves the configuration database to the LKM server automatically, and every 10 minutes thereafter if there are configuration changes.

   Note: If the LKM server is not yet up and running when you specify the LKM server from this screen, back up the first configuration database to another site (see Saving the DataFort Configuration Database on page 13) and load it manually in LKM (see Loading a Saved Configuration Database into LKM).

Configuring Secure Backups

Unlike regular backups, secure backups must be explicitly enabled both at DataFort and in the LKM UI. Note that since configuration database backups contain no plaintext key material, SSL backups are not essential for the security of your data or key material.

1. On the LKM Settings page, leave the First Port of the Servers at its default setting (15362).
2. Select Connect using SSL, and enter and confirm a shared secret. The shared secret can be a string of any characters of any length, including spaces.

   Note: Secure backups use the base port (First Port of the Servers) + 10 and the base port + 11. The status of LKM server ports can be checked from the LKM UI. If these ports will not be available, change them from the LKM UI (see Configuring LKM Server Ports) as well as in the First Port of the Servers field.

3. The LKM Settings page sets up the connection but does not send data immediately. To test the connection between DataFort and the LKM server right away, click Test. The status line indicates whether the connection succeeded.
4. Click Save.

   Clicking Save on this screen specifies that the DataFort configuration database should be backed up to the LKM server automatically, over the secure channel.

5. As soon as possible, plan to enable SSL and enter the same shared secret in the LKM UI. Until this is done, secure backups to the LKM server will not proceed.

   After SSL is enabled and its shared secret entered for both parties to this communication (DataFort and LKM), the configuration database is backed up to LKM, and every 10 minutes thereafter if there are configuration changes.

   Note: If the LKM server is not yet up and running when you specify the LKM server from the LKM Settings screen, back up the first configuration database to another site (see Saving the DataFort Configuration Database on page 13), and load it manually in LKM as soon as possible (see Loading a Saved Configuration Database into LKM).

Configuration from the DataFort CLI

CLI configuration can be used after initial DataFort setup. Complete one of these LKM configuration procedures for every DataFort cluster.

1. Log in to the DataFort CLI. For instructions, see the *DataFort Administration Guide*.
2. Enter the following commands to set DataFort properties for LKM, and to specify the LKM server:

```
system property set sys.datafort.label <label-name>
system property set sys.datafort.description <description>
system property set sys.lkm.server.ip <IP address>
system property set sys.lkm.server.port <port>
```

   These commands parallel the entries in the LKM Settings screen of the DataFort WebUI. The description and port commands are optional. The default ports will be used if not otherwise specified.

3. To set up an optional secondary LKM server:

```
sys pro set sys.lkm.secondary.ip <IP address>
```

   The remaining properties, including the base port, are taken from the properties of the primary server.

4. For secure automated backups, enter:

```
sys pro set sys.lkm.usessl 1
sys pro set sys.lkm.secret <secret>
```

5. Save the current configuration to the LKM server:

```
db backup --lkm
```

Verifying Automated Backups

The previously described methods specify automated configuration database backups to the LKM server. They signal DataFort to back up its current configuration and check its configuration database every 10 minutes for changes. If DataFort detects changes from its previous configuration, the new configuration database is automatically sent to the LKM server.

If the LKM server is online and LKM software is running, the changes are incorporated into LKM configuration archives. However, if the LKM server is not yet set up, or if the LKM server or LKM software has been shut down, LKM cannot receive configuration updates.

Verifying DataFort Configuration in LKM

You can make sure that the configuration has been loaded and that LKM archives are being updated.

1. At the LKM server, display the LKM program window (click the LKM program icon from the Windows desktop).
2. Click the DataFort Appliances folder in the left pane.

   The list will include the DataFort you just configured for LKM. When you select the DataFort, the right pane displays the Cryptainers associated with it. At the same time, all Recovery Cards connected with this DataFort are added to the Recovery Cards List.

   If you don't see a DataFort that was just added, right-click DataFort Appliances in the left frame, and choose Refresh List.
3. Right-click the DataFort you want to check, and choose Properties.

   The DataFort Properties dialog displays information about the DataFort, including the date and time of the most recent configuration update. The date and time should correspond approximately to the most recent configuration changes.

   Note: If a DataFort does not appear in the list of DataFort Appliances, or if its records are not being updated, make sure the communication ports specified on the LKM server match those specified on the DataFort. For more information, see Troubleshooting.

Loading Configurations in LKM Manually

Under the following circumstances, load saved DataFort configurations into LKM manually:

- A DataFort configuration was backed up to another site and the LKM server was not specified in the DataFort WebUI.
- The LKM server was specified in the DataFort WebUI, but the LKM server was not in operation at the time.
- The DataFort has been in use for some time (without backup to LKM), Cryptainer vaults may have been deleted or changed, and multiple configuration database backups have been saved. In this case, see Loading a Saved Configuration Database into LKM.
- You prefer to perform regular backups of the DataFort configuration database to a remote site rather than automatically updating the LKM archives. For example, you can load configurations manually if the LKM server is kept offline except when it is used for acquiring backups or recovering data. For more guidelines when using this option, see Backing up a Configuration Database.

Saving the DataFort Configuration Database

If a DataFort configuration is backed up to a location other than the LKM server, the saved DataFort configuration database can be added to the LKM archive later. A new DataFort configuration is backed up at the conclusion of the setup wizard. If LKM has been configured, the backup will be sent to the LKM server automatically at the conclusion of the wizard, and automatically thereafter. After setup, a DataFort configuration can be manually backed up:

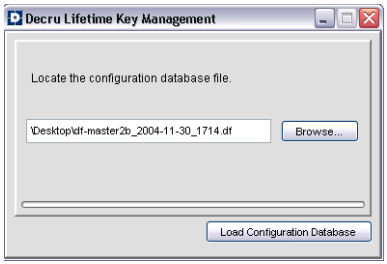
- From the DataFort WebUI, in the Back Up Configurations screen. Choose **System Config > Recovery > Backup**, and click Download.
- From the DataFort CLI, use the `db backup` command. For example, to back up to an FTP server:

```
db backup --ftp ftp://user:pass@server/myconfigdb.df
```

Loading a Saved Configuration Database into LKM

Load a saved configuration into LKM if it was backed up to a site other than the LKM server.

1. At the LKM server, display the LKM program window.
2. Choose **File > New DataFort DB**.
3. Browse or enter the path to the saved configuration database file.
4. Click Load Configuration Database, and wait for the file to be processed.



Note: If more than one configuration database exists for the DataFort, repeat the previous steps until you have loaded the most recently saved configuration. Each time you load a configuration, the LKM archive is updated to become a cumulative record of Cryptainer vaults created with that DataFort.

After loading is complete, the list of Datafort Appliances in the left frame of LKM includes the DataFort whose configuration you just loaded. For a more detailed description of the LKM UI, see Running the LKM UI.

5. If you have not already done so, enable automated updates by specifying the LKM server in the DataFort WebUI (see Configuration from the DataFort WebUI).

Triggering a Backup to LKM Manually

The current DataFort configuration is loaded into LKM automatically when the LKM server is specified in the DataFort WebUI or the DataFort CLI, and updated with any changes at 10 minute intervals thereafter. There is no need to load current configurations manually. However, if you have any doubt as to whether the current configuration has been sent to LKM, or wish to load it manually, use the WebUI or the CLI.

When you back up the current configuration to LKM manually, there is an additional option: you can choose to purge unused keys from the DataFort configuration database after the backup is complete. The unused keys can be keys for deleted or rekeyed Cryptainers.

Backing up to LKM Manually Using DataFort WebUI

Loading the current configuration to LKM can be accomplished by clicking the Back Up to LKM button at any time after the LKM settings are specified. See the *DataFort Administration Guide* for details.

1. Log in to the WebUI of the DataFort whose configuration you wish to load, and choose **System Config > Recovery > Backup**.
2. If you wish to purge unused keys, click the check box to Purge unused Cryptainer Keys.

The purged Cryptainer Keys are preserved in the LKM database, but deleted from the DataFort database.

3. Click Back Up to LKM.

   The current configuration of this DataFort is sent to the LKM server immediately. A confirmation message is displayed. If a secondary LKM server has been configured, the current configuration is sent to the secondary server at the same time.

Backing up to LKM Manually Using DataFort CLI

A DataFort CLI backup command can be used if the LKM server and DataFort properties have already been specified (in the DataFort WebUI or DataFort CLI).

1. Log in to DataFort CLI.
2. Enter the command

```
db backup --lkm
```

3. If you wish to purge unused keys, back up using the `-p` option:

```
db backup --lkm --purge
```

After Initial Setup

At a convenient time after LKM displays a DataFort in its list of DataFort Appliances, arrange for secure long-term storage of DataFort key information. Assemble the Recovery Officers and use LKM to create a Recovery Key Archive for the DataFort. For more information, see Generating a Recovery Key Archive.

Key Management

When it is set up as described in the previous sections, LKM maintains an encrypted copy of all keys from every designated DataFort. LKM extracts the keys and identifying information about Cryptainers from configuration database backups.

When the DataFort configuration is changed and a revised configuration database is loaded into LKM software, new Cryptainer and key information is added to the previous information.

LKM also saves the most recent configuration database in a form that can be used to restore a DataFort. However, the primary function of LKM is key management. Accordingly, LKM does not archive all previous configuration databases and cannot be used to restore a DataFort to any configuration other than the latest one.

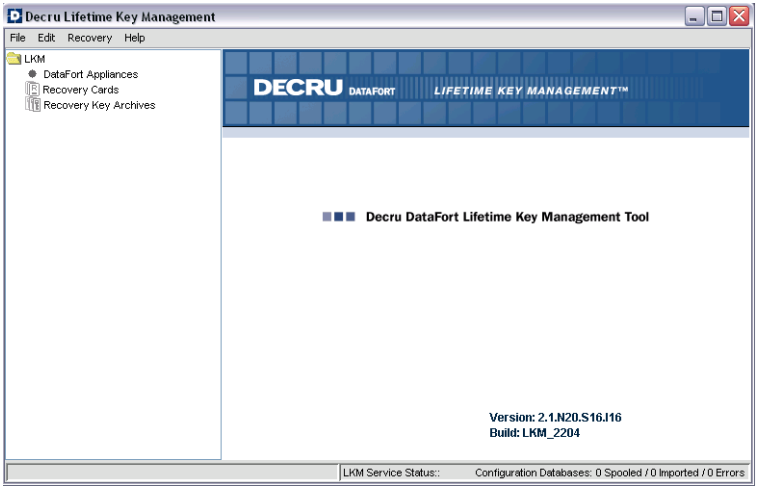
LKM never deletes any keys unless requested to do so, even if the original Cryptainer vaults are purged from the DataFort or the source DataFort is decommissioned. However, you can choose to delete a Cryptainer or a DataFort from LKM records. When you delete a Cryptainer or DataFort from LKM, LKM deletes the keys associated with them.

LKM can be used to create Cryptainer Key Files, which when used with the Software Recovery Tool, allow LKM to recover data even if its origin is not currently known, or the originating DataFort is no longer in operation. If data recovery is needed in NAS environments, LKM can analyze encrypted files and trace the source Cryptainer Key, provided the Cryptainer was recorded in the LKM system at some time.

2 LKM Software

Running the LKM UI

To start the LKM UI, click the LKM program icon on the Windows desktop, or choose **Start > Programs > Decru > Lifetime Key Management**.



The left pane displays:

- DataFort Appliances
- Recovery Cards
- Recovery Key Archives

Right-clicking an object displays a menu of commands and options available for that object. Additional commands are available from the menu bar. See LKM Options on page 51. After LKM has been in use for a time, information is displayed in the right pane, according to the selection in the left pane:

Table 1: LKM Display

Object selected in left pane	Right pane display
DataFort Appliances	List of DataFort appliances with configurations loaded into LKM.
Individual DataFort	Cumulative list of Cryptainers, Cryptainer and tape keys and related information for the selected DataFort. Additional detail about a selected DataFort is displayed by right-clicking a DataFort and selecting Properties.

TABLE 1: LKM DISPLAY (CONTINUED)

Object selected in left pane	Right pane display
Recovery Cards	Cumulative list of Recovery Cards.
Recovery Key Archives	List of Recovery Key Archive files that were created by this instance of LKM.

To exit the LKM UI, choose **File > Exit**, click the Close box, or choose Close from the taskbar menu.

Note: The LKM server continues to receive configuration updates when the LKM UI is closed, as long as the LKM server is on (the Windows Service component is running). For more information on the service component, see Managing the LKM Service.

THE LKM DISPLAY

Once one or more DataFort configurations have been loaded into LKM, the display shows the contents of the LKM database. You can flag or sort the information in the program window.

CONTROLLING THE LKM PROGRAM WINDOW DISPLAY

DataFort Appliances When **DataFort Appliances** is selected in the left pane, the right pane identifies every DataFort that has been described in a configuration database loaded into LKM. For each DataFort, the right pane lists the DataFort ID, the DataFort Name, the Type (DataFort model and network type), and the optional description (that was entered in a DataFort setup wizard, the WebUI, or the CLI system property command).

Delete Records If you have decommissioned a DataFort and want to remove it from this cumulative list, you can delete it. Right-click the DataFort and choose Delete Records. All listings and records for this DataFort will be deleted from the LKM database. For more information, see Deleting a DataFort from LKM.

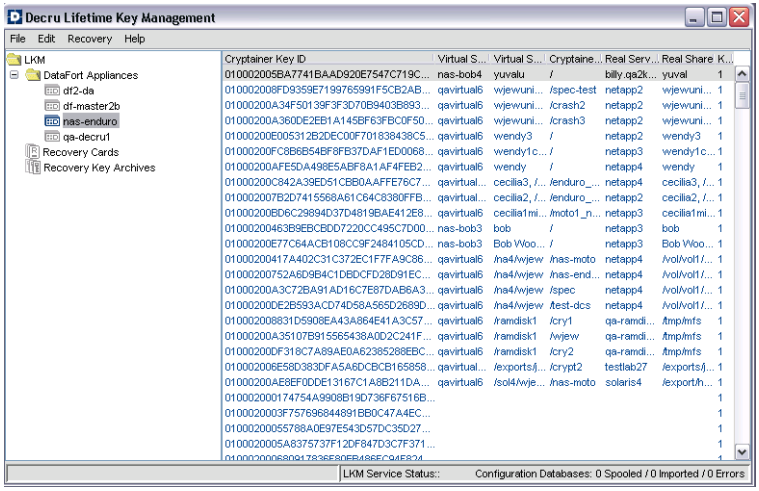
Individual DataFort When a DataFort is selected in the left pane, the right pane shows a cumulative list of Cryptainers for the selected DataFort. If a Cryptainer is listed, LKM can be used for emergency recovery of its data. The display information differs for each DataFort product as described in NAS Display, SAN Disk Display, SAN Tape Display and iSCSI Display below.

To change the display:

- To widen a column, click the column separator and drag it to the right.
- To widen the entire display, drag the corner of the frame to resize the window.
- To sort the entries in a column, click the column heading.
- To flag a DataFort as inactive, see Marking a DataFort Inactive.

NAS Display

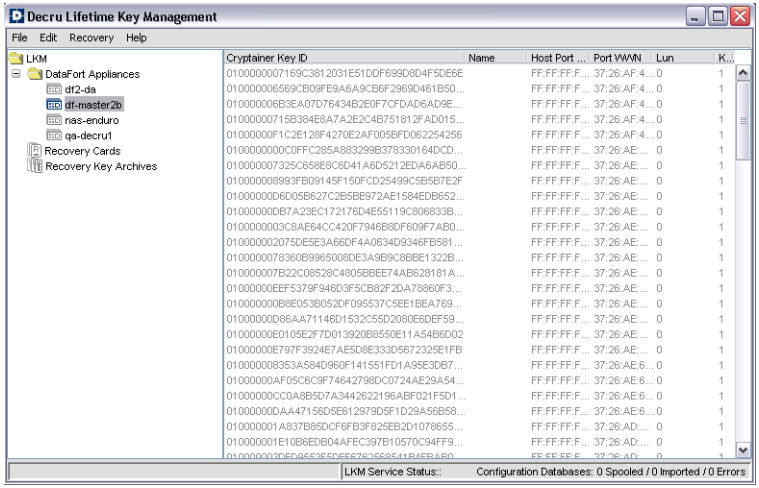
For each Cryptainer, LKM displays the unique Cryptainer Key ID, Virtual Server, Virtual Share name, Cryptainer Name, Real Server name, Real Share name, and the Key Version. The Key Version is 1 unless the Cryptainer has been rekeyed.



LKM interface with NAS appliance selected

SAN Disk Display

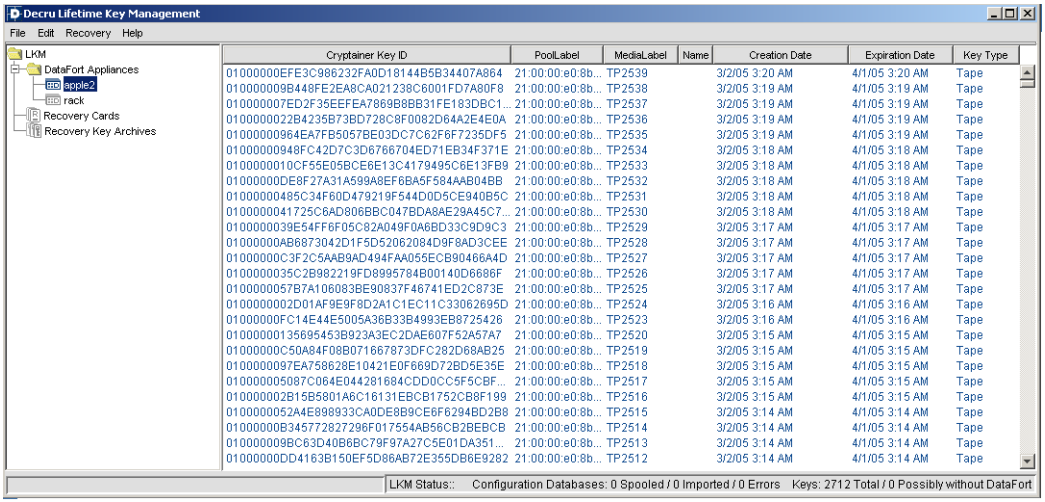
For each Cryptainer, LKM displays Host Port WWN, Port WWN, LUN, Cryptainer Name, Cryptainer ID, and Key Version. The Key Version is 1 unless the Cryptainer has been rekeyed. A SAN DataFort can have disk Cryptainer Keys and Tape Keys. Tape Keys do not have a Port WWN or a LUN listed, because they are associated with a host rather than a specific storage device. A tape-only DataFort will display pool information. See SAN Tape Display on page 19.



LKM interface with SAN appliance selected

SAN Tape Display

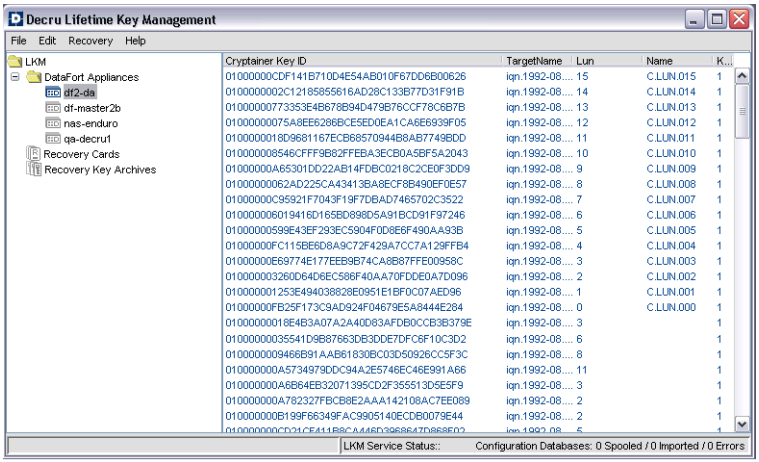
For each Cryptainer, LKM displays Pool Label, Media Label, Name, Creation Date, Expiration Date and Key Type. Expiration dates for keys are set using the DataFort WebUI as described in the *DataFort Administration Guide*.



LKM interface with SAN tape appliance selected

iSCSI Display

For each Cryptainer, LKM displays the name of the target where the Cryptainer is stored, the LUN number of the Cryptainer and the Key Version. The Key Version is 1 unless the Cryptainer has been rekeyed.



LKM interface with iSCSI appliance selected

Individual Cryptainer Cryptainer entries are color-coded: **blue** by default, **gray** if the Cryptainer has been deleted from a DataFort configuration, and **red** if the Cryptainer was translated from a different DataFort (see Key Translation Option). Translated Cryptainers are also identified by the word "translated" in parentheses. Delete a Cryptainer from the LKM database and the listing by right-clicking it and choosing Delete from LKM.

Recovery Cards LKM displays all the Recovery Cards connected with each DataFort, including their labels and Security Domain.

Recovery Key Archives The right pane lists every Recovery Key Archive that was created with the current instance of LKM. The listing includes the Key Archive ID (a sequential autonumber), the creator's comment, DataFort Name, Master Key ID, and time of creation. The list indicates only that a Recovery Key Archive was created; it cannot be used to retrieve the Recovery Key.

DataFort Properties Right-click a DataFort in the left or right pane and choose Properties to display the current properties of the selected DataFort.

The General tab provides summary information including the date and time of the last configuration update, and the number of known Cryptainers and keys. The Recovery Cards tab indicates the number of Recovery Cards or Recovery Officers (the quorum) required for data recovery. The Recovery Key Archive tab lists the Recovery Key Archives created for the selected DataFort, and the Cluster tab lists known cluster information for the DataFort.

Summary of Menus and Options

LKM menus and options are summarized in the tables that follow, and are described in more detail on the linked pages.

Table 3 lists LKM drop-down menus. Table 3 lists the right-click menu options that are available in the context of a particular LKM item.

Table 2: LKM Menus

Menu Name	Drop-down Option	Function
File	New DataFort DB	Loads a saved DataFort configuration database into LKM. See Loading a DataFort Configuration Database.
	Import	Allows LKM to import Cryptainer Keys and Tape Keys that were exported from another LKM server. See Import LKM Database.
	Export	Allows LKM to export Cryptainer Keys and Tape Keys for import into another LKM server. See Export LKM Database.
	Zeroize	Clears the contents of the LKM database. See Zeroize LKM Database.
	Exit	Quits LKM WebUI.
Edit	Port	Allows the port and SSL connections of LKM server to be configured. See Manage LKM Ports. Tests the LKM query and update ports.
Recovery	Recover Data	Examines an encrypted file and identifies the requirements for decryption. See Recover Data Option.
	Recovery Cards	Displays all Recovery Cards associated with configuration databases loaded into LKM.
	Identify Card	Displays attributes of a Recovery Card inserted in the smart card reader. See Identifying Recovery Cards.
	Recovery Key Archives	Displays requirements for recovering data from an encrypted file, and begins the data recovery process (NAS only).
Help	Contents	Opens the PDF file of this document: *Lifetime Key Management Guide.*
	About LKM	Displays the LKM software version.

TABLE 3: LKM OPTIONS IN CONTEXT

Item	Name	Description/Function
DataFort Appliances	Refresh List	Refreshes the display of DataFort appliances.
DataFort	Export Keys	Enables an export of all Cryptainer Keys to another LKM server. See Import and Export of Cryptainer Keys.
	Translate Keys	Makes the selected DataFort's Cryptainers accessible from another DataFort. See Key Translation Option.
	Generate Key File	Generates a Cryptainer Key file for all Cryptainer vaults associated with selected DataFort. See Cryptainer Key Files.
	Generate Recovery Key Archive	Creates a file containing a passphrase-encrypted Recovery Key. See Generating a Recovery Key Archive.
	Launch WebUI	Opens WebUI of selected DataFort. See Open DataFort WebUI.
	Save DB	Creates a configuration database file of the last configuration database loaded in LKM from selected DataFort. See Save Latest Configuration Database to File.
	Mark Inactive/Active	Marks DataFort status. See Marking a DataFort Inactive.
	Delete Records	Deletes records of the selected DataFort from the LKM system. See Delete DataFort Records.
	Refresh	Refreshes the Cryptainer and key list in the right pane and refreshes DataFort Properties.
	Properties	Displays the DataFort properties that are recorded in LKM. See View DataFort Properties.
Cryptainer	Export Key	Enables an export of Cryptainer Key to another LKM server. See Import and Export of Cryptainer Keys.
	Translate Key	Makes the selected Cryptainer accessible to another DataFort. See Key Translation Option.
	Generate Key file	Generates key file for selected Cryptainer. See Cryptainer Key Files.
	Delete from LKM	Deletes record of selected Cryptainer from LKM. See Delete Cryptainer from LKM.
Recovery Cards	Refresh Cards List	Refreshes the display of Recovery Cards.
Recovery Key Archives	Refresh Archives List	Refreshes the display of archived Recovery Key files.

3 LKM Archiving Functions

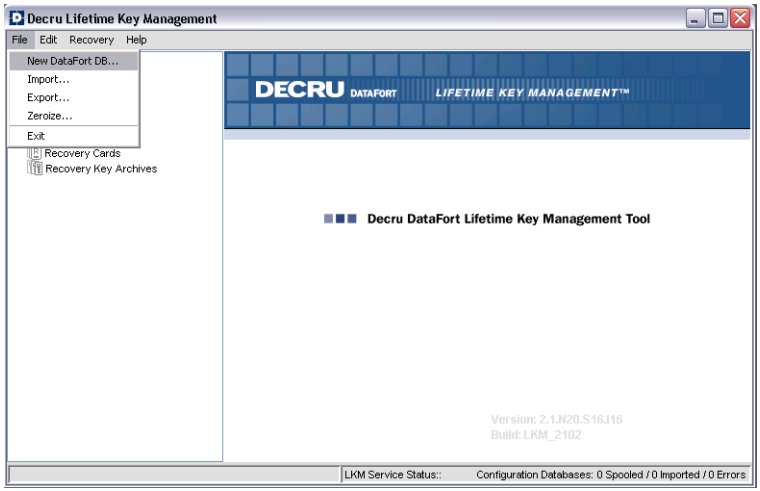
LKM archiving functions are used in conjunction with manual and automated backups from each DataFort appliance. If you set up automated backups immediately initializing a DataFort, you will not need to load a configuration database manually. LKM archiving is described in the following sections:

- Loading a DataFort Configuration Database
- Backing up a Configuration Database
- Generating a Recovery Key Archive

Loading a DataFort Configuration Database

A configuration database saved from a DataFort appliance can be manually loaded into LKM at any time. The process was outlined earlier, and is described in a little more detail here.

1. Choose **File > New DataFort DB**.



   The software prompts for the location of the saved configuration database.

2. Browse or enter the path to the saved file and click Load Configuration Database.

   LKM displays progress bars while it extracts Cryptainer and key information from the uploaded configuration, and saves that information in the LKM internal database. LKM also retains the most recent configuration database in case it is needed for restoration of the DataFort. Some time may be required to process a large configuration database; please be patient.

3. To verify the upload, click DataFort Appliances.

After a configuration is uploaded for the first time, the source DataFort and associated Recovery Cards will be listed in the LKM UI. Subsequent uploads update the initial information.

If you don't see the DataFort associated with the configuration that was just added, right-click DataFort Appliances and choose Refresh List. If the DataFort does not appear, check the log files (see Troubleshooting on page 58).

4. Select the DataFort associated with the configuration you loaded. After loading a configuration in which Cryptainer vaults are defined, the right pane displays information about each Cryptainer Key.

   Whether configurations are updated manually or automatically, the list of Cryptainer vaults is updated with any changes since the last upload. New Cryptainers are added to the list; deleted Cryptainers are grayed.

5. Right-click the DataFort and choose Properties.

   The Properties window shows the date and time of the most recent configuration update, the number of Cryptainers and keys, as well as other information obtained from the uploaded configuration.

Backing up a Configuration Database

Data recovery with LKM relies on the availability of current key information. To maintain current key information, DataFort configuration databases must be backed up on a regular basis. DataFort's automated backups to LKM take care of this for you. If you prefer to use manual backups, be sure to back up the configuration database from the DataFort after the following events:

- DataFort initialization
- Cryptainer creation, deletion, restoration, or rekey operations
- DataFort recovery
- Smart card replacement

Store the configuration database backups in a location that is managed by your organization's existing backup infrastructure and backup policies.

If you are working in a dynamic environment, and think you may have to restore an earlier configuration, back up the configuration database independently of LKM. See Saving the DataFort Configuration Database on page 13 for a summary, and see the *DataFort Administration Guide* for additional information.

Retain the three most recent configuration database backups in case you need to restore an earlier configuration or replace a failed standalone DataFort.

Generating a Recovery Key Archive

The Recovery Key, encrypted and securely stored in a tamper-proof part of the DataFort hardware, is used to encrypt each unique Cryptainer Key or tape key in a DataFort's configuration. Outside of the DataFort, the Recovery Key is stored as a shared secret among a quorum of Recovery Cards.

Access to the Recovery Key is critical for recovering data that has been encrypted if the original DataFort is no longer available. LKM can retrieve the Recovery Key from a DataFort configuration and a quorum of Recovery Cards, and save it in the form of a passphrase-encrypted Recovery Key Archive file. In the event of complete hardware unavailability or failure (including both the DataFort and the Recovery Cards), LKM can use the Recovery Key Archive to supply the keys for decrypting data.

> **CAUTION:** Because the Recovery Key Archive file compromises the distributed security design of the DataFort System Card and Recovery Cards, a Recovery Key Archive should be created and used for only two purposes: immediate data recovery if a DataFort is no longer functioning, and placement in key escrow or another form of trusted long-term storage, for use in an emergency.

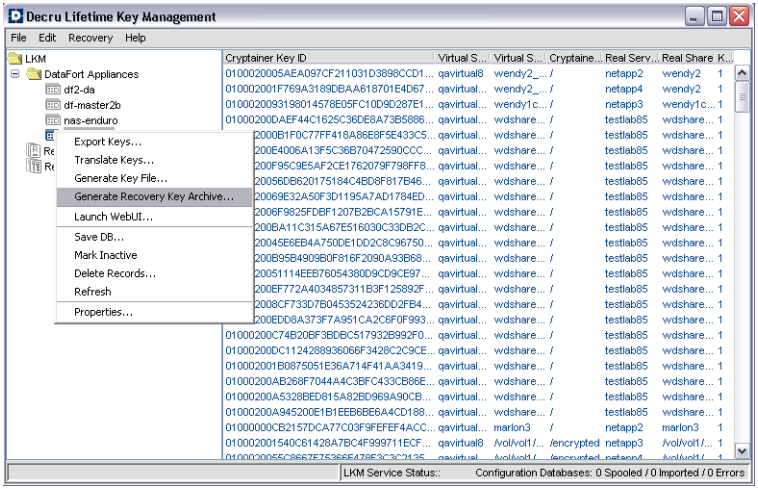
A Recovery Key Archive should be created after every DataFort is initialized. The Recovery Key Archive is generally valid for the life of the DataFort. A new Recovery Key Archive is needed only if the DataFort is zeroized and subsequently reinitialized.

Generating a Recovery Key Archive requires:

- The configuration database of a DataFort already loaded into the LKM software.
- The quorum of Recovery Officers and Recovery Cards (as configured during DataFort setup). Each Recovery Officer will be required to present a Recovery Card and its password.
- A passphrase that the security administrator will supply in the course of generating the Recovery Key Archive to encrypt the Recovery Key Archive.

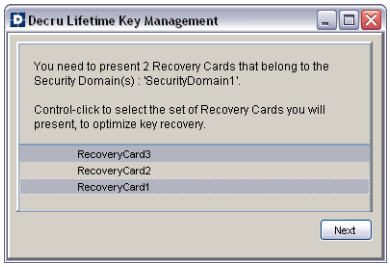
> **CAUTION:** Before inserting Recovery Cards in the reader connected to the LKM server, the LKM server should be thoroughly checked for the presence of malicious code that could compromise the security of encrypted data.

1. Right-click the DataFort whose Recovery Key you want to archive, and choose Generate Recovery Key Archive.

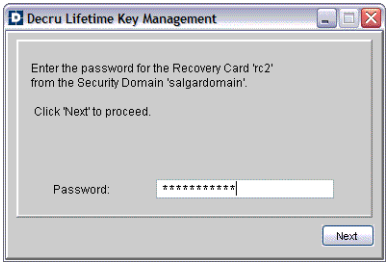


You are informed of the quorum of Recovery Cards required for the Security Domain of the selected DataFort.

2. A scrollbar lists the Recovery Cards in the Security Domain. If desired, control-click to select the particular Recovery Cards you will present to speed up the process. Click Next.



3. When prompted, a Recovery Officer should insert a Recovery Card in the smart card reader, and click OK.
4. Enter the Recovery Card password. Click Next.



The previous two steps are repeated for all the Recovery Cards in the quorum. You are alerted to remove and store the Recovery Cards safely.

5. When prompted for a passphrase for the Recovery Key Archive, enter it twice and make a note of it. Click Next.
6. Enter a comment or identifying name to help identify the Recovery Key Archive, and browse or enter the path to the directory where the file should be saved.
7. Enter a descriptive filename and click Save. Click Finish.

   With the Recovery Cards LKM decrypts the secret shares and recovers the Recovery Key. A file is generated that contains the Recovery Key, re-encrypted with the supplied passphrase.

   The name of the Recovery Key Archive is added to the left frame, and to the DataFort Properties.

   Note: For security reasons, LKM does not retain the location of the saved file.
8. Move the Recovery Key Archive file to escrow or secure long-term storage, making sure you store the passphrase as well.
9. If necessary, use the Recovery Key Archive immediately for data recovery. The Recovery Key Archive can be used to generate a Cryptainer Key File, or it can be used directly to decrypt one or more files or Cryptainers, using the Recover Data Option (NAS only).

> **CAUTION:** Delete every Recovery Key Archive immediately after use or submission to escrow. Do not leave Recovery Key Archive files on the LKM server or any other accessible location, as they may compromise the security of encrypted data.

Recovery Key Archives function as a substitute for Recovery Cards in their emergency data recovery function, ensuring access to encrypted data even if the DataFort appliance, Recovery Cards, or Recovery Officers are not available. However, Recovery Key Archives do not substitute for Recovery Cards in other DataFort management functions, such as zeroizing and reconfiguring a DataFort, changing cluster configurations, or replacing other smart cards.

4 LKM Data Recovery Functions

LKM archiving functions have a single purpose: to make encrypted data permanently accessible. While DataFort appliances with established Cryptainers take care of encrypting and decrypting data with no administrative input, there are occasions when normal methods are not adequate. LKM software can provide long-term access to encrypted data under those special circumstances.

The following situations might render data unusable without LKM:

- A replaced or reconfigured DataFort appliance
- Purged encryption keys that are needed again
- Data transfer from one Cryptainer to another
- Lost Recovery Cards
- Theft or destruction of the only DataFort appliance

LKM functions provide the necessary components of emergency data recovery including:

Generate Key File LKM can generate a Cryptainer Key File to decrypt a single Cryptainer or all Cryptainers in a DataFort configuration. A Cryptainer Key File is used in conjunction with the LKM Recover Data function or the standalone Software Recovery Tool. Cryptainer Key Files are an intermediate component of data recovery. Note that a Cryptainer Key File for all Cryptainers can only be used to decrypt Cryptainers that were in LKM when the Cryptainer Key File was created.

Recover Data The Recover Data Option (NAS only) analyzes an encrypted file or Cryptainer, displays the name of the DataFort and the authentication needed to decrypt it, and allows you to initiate data recovery. When you supply the necessary authentication, LKM decrypts and saves one or more files from a Cryptainer. Use this function to repeatedly to decrypt multiple Cryptainers.

Translate Keys The Key Translation Option enables all Cryptainers on a selected DataFort to be accessible from another DataFort.

Software Recovery The standalone Software Recovery Tool will decrypt a file or a Cryptainer, using a Cryptainer Key File and its passphrase. The standalone Software Recovery Tool is independent of the LKM UI. The tool can be run on a computer that is not acting as an LKM server, although it must have access to encryption key files and to the data that will be restored.

CAUTION: Generation of Recovery Key Archives and Cryptainer Key Files reveals the plaintext Recovery Key to the recovery software; accordingly, these processes should be executed only on a secure machine that has been scanned for viruses and preferably is not on the network. Decru recommends rebooting the machine after either process.

Decrypting Files and Cryptainer Vaults

Choose an appropriate recovery procedure as follows:

- In general, use a two-stage data recovery process. First, at the LKM server, generate and save one or more Cryptainer Key Files. After you have generated Cryptainer Key Files, use a computer with access to those Cryptainer Key Files and to the encrypted data and run the standalone Software Recovery Tool to decrypt the files or Cryptainers.
- (NAS only) If you have one file or one or more Cryptainers that need to be decrypted immediately, use the Recover Data Option. If the file or Cryptainer is of unknown origin, this provides the necessary recovery information.
- To translate Cryptainer Keys to another DataFort for normal access through DataFort or for data recovery, use the Key Translation Option.

Authentication for Data Recovery

Data recovery operations are sensitive procedures that require a quorum of Recovery Officers and Recovery Cards at some stage.

> **CAUTION:** Before inserting Recovery Cards in the smart card reader connected to the LKM server, the LKM server should be thoroughly checked for the presence of malicious code that could compromise the security of encrypted data.

You can supply a Recovery Key Archive file (and its passphrase) to create Cryptainer Key files in lieu of presenting Recovery Officers and Recovery Cards, because those officers were required in order to create the Recovery Key Archive file in the first place.

Similarly, you can supply a Cryptainer Key File and its passphrase to a recovery tool in lieu of presenting Recovery Officers and Recovery Cards.

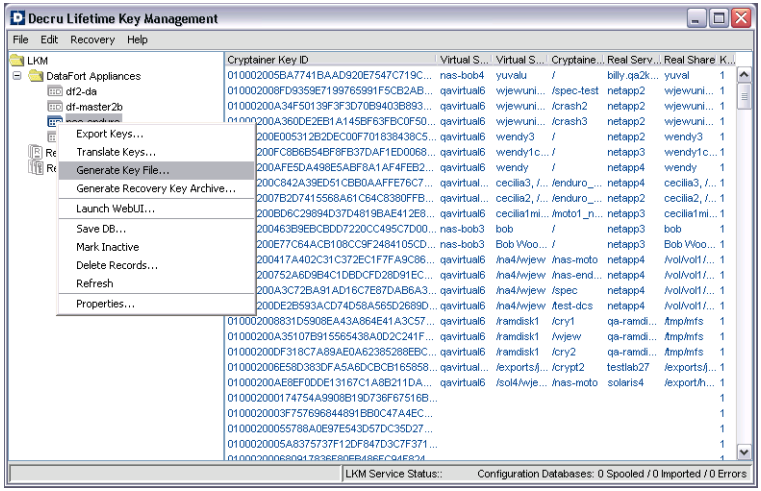
Cryptainer Key Files

LKM can generate a Cryptainer Key File that contains passphrase-encrypted Cryptainer Keys or tape keys. These keys allow the recovery of encrypted data under special circumstances without a DataFort. Cryptainer Key Files created with this procedure can be saved for use on the same or a different computer.

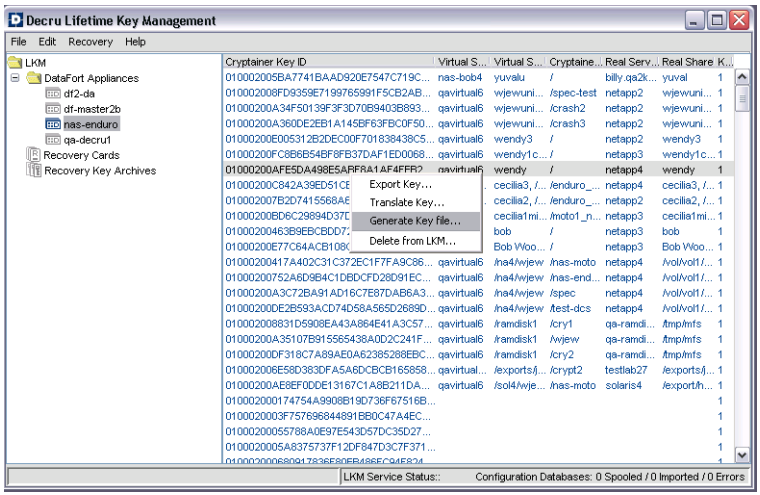
Before a Cryptainer Key can be recovered and used, the Recovery Key must be introduced into the LKM software. This is done by presenting either a quorum of Recovery Cards or a Recovery Key Archive file. In the NAS environment, if the Cryptainer or Cryptainers you need to decrypt are of unknown origin, use the Recover Data Option to analyze the file before generating a Cryptainer Key File.

1. Generate a Cryptainer Key File for a single Cryptainer, or for all Cryptainers in a configuration database.

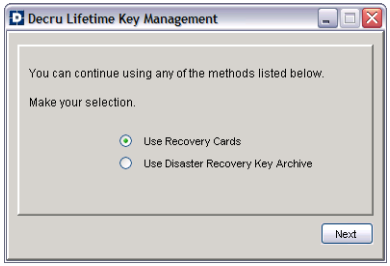
- To generate Cryptainer Keys for all Cryptainers associated with a DataFort, right-click the DataFort in the left pane, and choose Generate Key File. Note that such a Cryptainer Key File can only be used to decrypt Cryptainers recorded in LKM at the time the Cryptainer Key File was created.



- To generate a Cryptainer Key File for a single Cryptainer, select the DataFort in the left pane. A list of Cryptainer vaults for that DataFort is shown on the right. Right-click the Cryptainer you wish to recover, and choose Generate Key file.

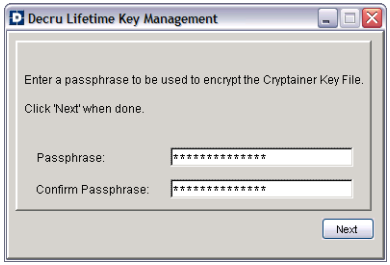


2. Select the method by which the Recovery Key will be introduced.



- If you are using Recovery Cards to supply the Recovery Key, you are told how many Recovery Cards will be required. Pre-selecting the Recovery Cards that will be used speeds up the process. Recovery Officers should follow the screen prompts to insert Recovery Cards in the smart card reader and authenticate them with their passwords. You are alerted to remove and store the Recovery Cards safely. Do so, and click OK.
- Alternatively, if you are using the Recovery Key Archive to supply the Recovery Key, follow the screen prompts to locate the Recovery Key Archive file, and enter the Recovery Key Archive passphrase. Click Next.

3. Whether you used Recovery Cards or the Recovery Key Archive, enter a passphrase for LKM to use to encrypt the Cryptainer Key File. Enter it again to confirm, make a note of it, and click Next.



4. Browse or enter a location for storing the Key File. Enter a filename, and click Save. Record the passphrase, the filename, and the nature of the Key File so you can identify and use it later.
5. Click Finish.

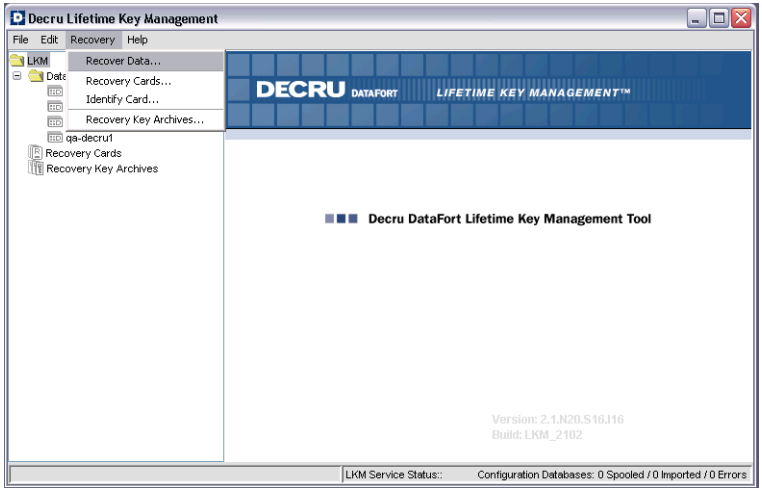
The Key File is stored in the designated location.

Recover Data Option

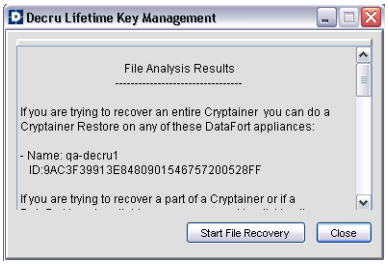
The Recover Data option examines an encrypted file and identifies the requirements for decryption (NAS only). It also allows you to begin the decryption process. For authentication, you can choose to provide Recovery Cards, a Recovery Key Archive, or a Cryptainer Key File. If you choose to use Recovery Cards or a Recovery Key Archive, the Recover Data function creates a temporary internal version of a Cryptainer Key File and deletes it after use.

Note: Before beginning file recovery, close other applications (including any browser windows).

1. Select **Recovery > Recover Data** from the LKM menu bar.



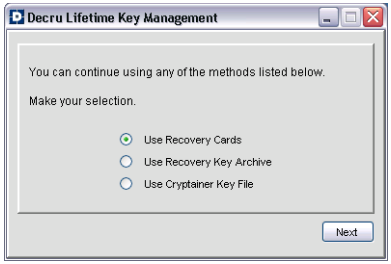
2. Provide the path or browse to the file, directory, or Cryptainer directory containing files that need to be analyzed and decrypted.
3. Click Next.



4. Examine the File Analysis Results.

If the named DataFort is still in operation, it can be used to decrypt the file or Cryptainer (see instructions for restoring a Cryptainer in the *DataFort Administration Guide*). If not, you will need to use an LKM data recovery process (either this tool or the standalone Software Recovery Tool). Key Translation is another option if you have a second DataFort.

5. Click Start File Recovery if you meet the requirements and want to decrypt the file immediately. Click Close if you wish to decrypt the file later.
6. Choose whether you will authenticate data recovery by using Recovery Cards (a quorum of Recovery Officers and Recovery Cards), a Recovery Key Archive, or a Cryptainer Key File.
   - If you can provide Recovery Cards, choose the Use Recovery Cards radio button. See File Recovery with Recovery Cards.
   - If you are providing a Recovery Key Archive, choose the Use Recovery Key Archive radio button. See File Recovery with Recovery Key Archive.
   - If you are providing a Cryptainer Key File, choose the Use Cryptainer Key File radio button. See File Recovery with Cryptainer Key File.



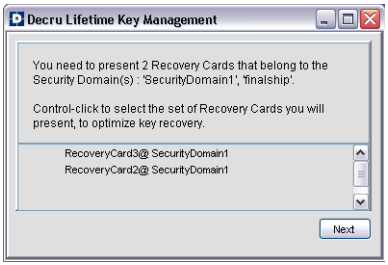
Whichever method of authentication you choose, LKM screens prompt with the next step. See:

- File Recovery with Recovery Cards
- File Recovery with Recovery Key Archive
- File Recovery with Cryptainer Key File

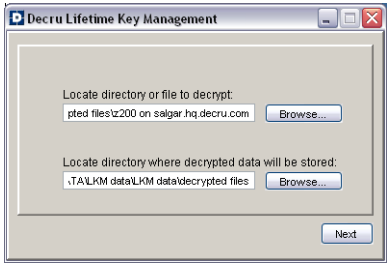
File Recovery with Recovery Cards

1. If you can provide Recovery Cards, choose the Use Recovery Cards radio button. Click Next.

   You are informed of the quorum of Recovery Cards required for the Security Domain of the DataFort associated with the encrypted file. A scrollbar lists the Recovery Cards in the Security Domain. If desired, control-click to pre-select the particular Recovery Cards you will present.



2. Follow the screen prompts to insert each Recovery Card in the smart card reader and authenticate it with its password. At the reminder, return the Recovery Cards to the Recovery Officers and click OK.
3. Choose a location to store the decrypted file. Navigate to a location for the decrypted file, and click Open.



4. Click Start Decryption. You are alerted that any file with the same name in the target directory you designated will be overwritten. Click OK.

   The decrypted file or files are stored in the specified location.
5. An information dialog box indicates the number of files that were successfully decrypted, and asks if you would like to decrypt another file or Cryptainer. Click Yes to continue; click No to close the tool.

   Note: Using Recovery Cards for authentication, only one Cryptainer can be decrypted at a time, because the internal Cryptainer Key File that was generated has keys for only one Cryptainer (the one containing the selected directory or file).
6. If you clicked Yes to continue, the dialog box with the source and target paths is displayed again. Change one or both paths as needed, and choose Start Decryption.

File Recovery with Recovery Key Archive

1. If you are providing a Recovery Key Archive, choose the Use Recovery Key Archive radio button. Click Next.

2. Locate the Recovery Key Archive and enter its passphrase, to decrypt the data. Click Next.

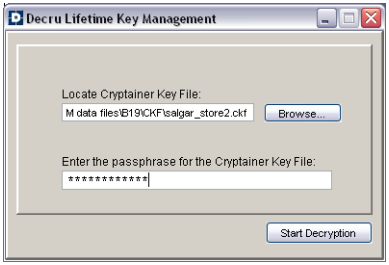
3. Choose a location to store the decrypted file. The path to the file or directory you want to decrypt is already filled in. Navigate to a folder for the decrypted file, and click Open.
4. Click Start Decryption.
5. An information dialog box indicates the number of files that were successfully decrypted, and asks if you would like to decrypt another file or Cryptainer. Click Yes to continue; click No to close the tool.

File Recovery with Cryptainer Key File

1. If you are providing a Cryptainer Key File, choose the Use Cryptainer Key File radio button. Click Next.

   To create a Cryptainer Key File for a Cryptainer or for a DataFort, see the previous section, Cryptainer Key Files.

2. Choose a location to store the decrypted file. The path to the file you want to decrypt is already filled in. Navigate to a folder for the decrypted file, and click Open.
3. Browse or enter the path to the Cryptainer Key File.



4. Enter the Cryptainer Key File passphrase, and click Start Decryption.

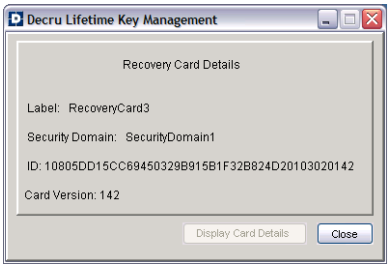
   The decrypted file is stored in the specified location.
5. An information dialog box indicates the number of files that were successfully decrypted, and asks if you would like to decrypt another file or Cryptainer. Click Yes to continue; click No to close the tool.
6. If you clicked Yes, the dialog box with the source and target paths is displayed again. Change one or both paths as needed, enter the Cryptainer Key File passphrase again, and click Start Decryption.

Identifying Recovery Cards

LKM can identify unmarked or unknown DataFort Recovery Cards.

1. Choose **Recovery > Identify Card** from the LKM menu.
2. When prompted, insert the unidentified Recovery Card in the smart card reader.
3. Click Display Card Details.

LKM displays the card label, its Security Domain, card ID, (and, when applicable, card version).



Import and Export of Cryptainer Keys

LKM allows you to selectively export and import Cryptainer Keys and Tape Keys from one LKM server to another. This can be used to grant a remote DataFort clone (typically created early in the life of a DataFort) access to encryption keys that were created later on the original DataFort. Access is provided through LKM software. A sample scenario might be:

1. A DataFort configuration database is backed up to a disk, and its encryption keys are managed by LKM.
2. You clone the DataFort at the remote site, and set up another LKM server connected to the remote DataFort. One way to clone a DataFort is to use a DataFort that has been restored with a configuration database from an existing DataFort.
3. In the course of time, additional Cryptainers are created, and there is a requirement to share some of the new Cryptainer Keys with the clone at the remote site.
4. You selectively export Cryptainer Keys from the original LKM server and import them to LKM at the remote site, which makes these keys accessible to the remote DataFort.

Exporting Cryptainer Keys

You can export individual Cryptainer or tape keys or export all the keys associated with a DataFort.

1. At the source LKM server:
   - To export all the keys of a DataFort, right-click a DataFort in the left pane of the LKM UI, and choose Export Keys.
   - To export one Cryptainer Key or tape key, select a DataFort in the left pane of the LKM UI and right-click a Cryptainer or tape key in the right pane. Choose Export Key.
2. Enter and then confirm a passphrase in the dialog that follows.
3. Click Choose Save Location.
4. Specify a location to save the export file. Enter a new filename or accept the default filename (which is based on the DataFort name or key name), and click Save.

Importing Exported Cryptainer Keys

The saved export file can be imported into another LKM installation.

1. At the target LKM server, choose **File > Import**.
2. Enter the passphrase you supplied when you exported the Cryptainer Keys. Click Choose File Location.
3. Browse to the export file you saved in the previous procedure, and click Open.

   The imported keys now appear in the right pane, associated with the appropriate DataFort.

Key Translation Option

Key Translation transfers one or more Cryptainer or Tape Keys from one DataFort to another. In the event that one DataFort is unavailable or has been reassigned (for example to secure data for a different group), an administrator may transfer the Cryptainers protected by that DataFort (the source DataFort) to another DataFort (the target). Key Translation may also be used as a backup for a DataFort; it does not disable the Cryptainer Keys from the source DataFort.

Key Translation can be performed for one or more Cryptainers, and the target can be one or more DataFort appliances. Key translation can be performed for all Cryptainers at once, or one at a time.

Key Translation is initiated from the LKM server that contains key information for both the source and target DataFort appliances. It requires a quorum of Recovery Officers and Recovery Cards for both the source and target DataFort, if they are secured by different individuals and cards.

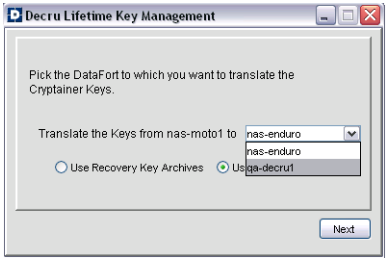
> **CAUTION:** In the Key Translation process, two Recovery Keys, as well as a Cryptainer Key, are exposed to software on the LKM server. Therefore, before initiating Key Translation, the LKM server should be thoroughly checked to ensure that no malicious code has been installed on it.

After the key or keys are translated to the target DataFort, the administrator must perform a Cryptainer Restore operation on each of the translated Cryptainers, in order to make them accessible from the target DataFort. The steps are outlined below.

Translating All Cryptainer Keys

Key translation can be authenticated either with Recovery Cards or Recovery Key Archives. In the first case, assemble the Recovery Officers and Recovery Cards for both the source DataFort and the target DataFort. In the second case, obtain Recovery Key Archives for the source and target DataFort.

1. Right-click the source DataFort in the LKM UI, and choose Translate Keys.
2. From the drop-down list, choose the target DataFort. The list includes all the DataFort appliances known to the LKM server.



3. Choose the method of authenticating the Key Translation and click Next. Choose Use Recovery Cards unless you have already created a Recovery Key Archive.

- If you choose Use Recovery Cards, LKM displays the names of the Security Domains of the source and target DataFort appliances, and the quorum of Recovery Cards that will be needed. When prompted to insert Recovery Cards, a quorum of Recovery Officers will insert their Recovery Cards in the smart card reader attached to the LKM server, and enter their passwords. If a separate set of Recovery Cards is required for the target DataFort, you are prompted for both sets of cards.

  In either case, control-click to pre-select the cards you will present, if desired, to speed up the process. Click Next. Follow the prompts to insert each card and enter its password.

- If you choose Use Recovery Key Archives, browse or enter the path to the Recovery Key Archive for the source DataFort, and enter the Recovery Key Archive passphrase. Click Next.

  Then browse or enter the path to the Recovery Key Archive for the target DataFort, and enter its passphrase. Click Next.

  A message confirms that the keys have been successfully translated.

  The LKM UI reflects the new set of translated Cryptainer Keys. Clicking the target DataFort displays all the translated Cryptainers and their identifying information, in red. Each translated Cryptainer is also identified by the word “translated.” Proceed to Restoring Cryptainers on the Target DataFort.

Translating Individual Keys

The procedure for translating individual keys, or translating keys one at a time, is the same as for translating all the Cryptainer Keys of a DataFort. As before, key translation can be authenticated either with Recovery Cards or Recovery Key Archives. Either assemble the Recovery Officers and Recovery Cards for both the source DataFort and the target DataFort, or locate the Recovery Key Archives for the source and the target DataFort.

1. Click the source DataFort in the LKM UI, and in the right pane, right-click a Cryptainer or tape key to be translated. Choose Translate Key.
2. Select the target DataFort from the drop-down list.
3. Choose the authentication method. Click Next.
4. Follow the screen prompts to translate the keys. When the keys are translated, Restoring Cryptainers on the Target DataFort.

Restoring Cryptainers on the Target DataFort

For a full explanation, see the section on restoring a Cryptainer in the *DataFort Administration Guide*.

Restore Newly translated Cryptainers in the NAS Environment

1. Verify that the DataFort domain access user has read access to the .decru file in the share to be restored.
2. At a Management Station, log in to the DataFort WebUI of the target DataFort. If the file server has not been added to the DataFort configuration database, access the NAS Topology page of the WebUI, right-click the domain where the file server with the data resides and choose Add Server.
3. From the NAS Topology page in the WebUI, right-click the server and choose Add Share to add the share to be restored.
4. Right-click the share and Virtualize the share on a virtual server.
5. Right-click the share and select Restore Cryptainer to restore it.
   - If only one share is selected, you can enter the path and owner.
   - If multiple shares are selected, there is no option to edit paths.
   - For CIFS Cryptainers, entering the owner is optional. If the owner is not specified, the administrator performing the restore becomes the owner.

Permissions for a newly restored Cryptainer are not synced with the ACL on the server. The ACL of each translated and restored Cryptainer must be reset or synced individually after a Cryptainer is restored. To sync the ACLs of CIFS and NFS Cryptainers, see the explanation of restoring a Cryptainer in the *DataFort Administration Guide*.

Restore Newly translated Cryptainers in the SAN Environment

1. Log in to the target DataFort using CLI and import the translated Cryptainer Key:

   ```
   keyman lkm import --ck-id <Cryptainer Key ID>
   ```

2. Now log in to the WebUI of the target DataFort and select **Storage > Network**.
3. Right-click the translated Cryptainer in the Storage Management pane, and choose **Advanced > Restore Cryptainer**. Follow the prompts to restore the newly translated Cryptainer.

After restoring Cryptainers, open the LKM UI and click a target DataFort. The right pane shows a new (duplicate) entry for each restored Cryptainer, with updated settings.

The restored Cryptainer shares the Cryptainer Key ID with the translated Cryptainer, but other settings are different. If a translated and restored Cryptainer is active, the formerly red entry will be blue; if it is inactive, it will be gray. Future uploads of the configuration database from the target DataFort will update these settings.

5 Software Recovery Tool

The standalone Software Recovery Tool provides additional flexibility in data recovery. It can be used for emergency data recovery on the LKM server, or it can be installed and used on a separate computer. A smart card reader is not required for running the standalone Software Recovery Tool.

Note: Data recovery requires Cryptainer Key Files (generated as described in Cryptainer Key Files on page 29). You will also need to supply the passphrase that was provided when each Cryptainer Key File was created.

Instructions for using the Software Recovery Tool in the following environments follow:

- Software Recovery Tool for NAS
- Software Recovery Tool for SAN/iSCSI

Installing the Software Recovery Tool

Software data recovery is used under special circumstances to restore encrypted data when a DataFort is not available. The Software Recovery Tool is available with a separate installation. The tool should be installed on a computer that is accessible to the data that is to be restored.

Installing the Standalone Software Recovery Tool on Windows

The Software Recovery Tool can be installed on the LKM server or on a different Windows machine.

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

1. On the User CD, follow the LKM link to the Software Recovery Tool page, and click the link for the standalone Windows tool.
2. If the installer doesn't start automatically, run setup.exe. Accept the license agreement and choose the default options.

After the software has been installed, the **Start > Programs > Decru** menu displays a new Software Recovery Tool entry.

Installing the Standalone Software Recovery Tool on Linux

The Linux Software Recovery Tool comes packaged as an RPM. It is supported only for the NAS environment.

1. On the User CD, follow the LKM link to the Software Recovery Tool page, and click the link for the directory containing the standalone Linux tool.
2. Copy the file `dcrSWRTool-linux-2.0.0-1.i386.rpm` to the machine on which data recovery will be performed.
3. To install the tool, type:

   ```
   rpm -i dcrSWRTool-linux-2.0.0-1.i386.rpm
   ```

   The Linux Software Recovery Tool will be installed in the /usr/local/decru/bin directory.

Note: To uninstall the tool, type:

```
rpm -e dcrSWRTool-linux
```

Software Recovery Tool for NAS

The standalone Software Recovery Tool can be installed on any computer that has access to the encrypted data and the necessary Cryptainer Key Files. Before you run the tool, create and assemble the necessary Cryptainer Key Files and the encrypted files you want to recover.

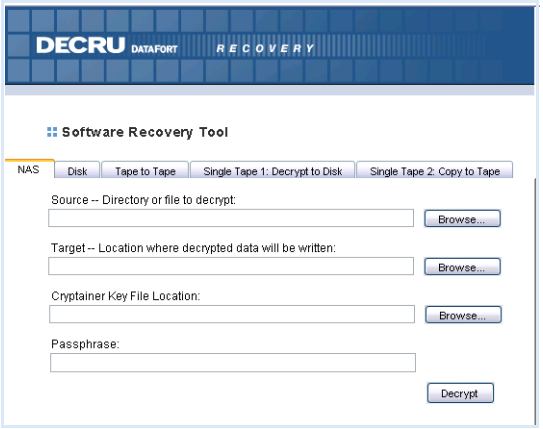
> **CAUTION:** When you have finished decrypting files or Cryptainers, delete the Cryptainer Key File.

If the Cryptainer or Cryptainers you need to decrypt are of unknown origin, use the Recover Data Option to analyze a file before using a software recovery tool.

If you are copying encrypted data for decryption, be sure to copy over the entire Cryptainer. Trying to decrypt individual files from a partially encrypted Cryptainer may fail or produce incorrect results. Partially encrypted Cryptainers should be recovered using the LKM (see Chapter 4), not the Software Recovery Tool.

Software Recovery for NAS Using Windows

1. Choose **Start > Programs > Decru > Software Recovery Tool**.
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.

Software Recovery for NAS Using Linux

1. Go to **/usr/local/decru/bin**.

   You will run the RPM executable that you copied from the DataFort install CD.
2. To use the tool, type:

   ```
   ./dcrSWRTool-linux
   ```
3. The Decru Decryption Engine displays general instructions and prompts you for the required file and directory locations. Provide them as absolute paths.
4. Follow the prompts to indicate the required paths to:

- The source (the file to be decrypted).
- The destination (the location to store the decrypted directory/file).
- The Recovery Key file (the Cryptainer Key File containing the Cryptainer Key needed for decryption).
- The password (the passphrase to recover the Cryptainer Key from the Cryptainer Key File).

After decryption, a decryption status message is displayed, with the name of the log file.

5. Press **Y** if you wish to decrypt another Cryptainer, or press any other key to exit the tool.

Software Recovery Tool 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.

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

The Software Recovery Tool decrypts one Cryptainer at a time. With the appropriate Cryptainer or tape key files, a software recovery tool 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 Software Recovery Tool for SAN/iSCSI

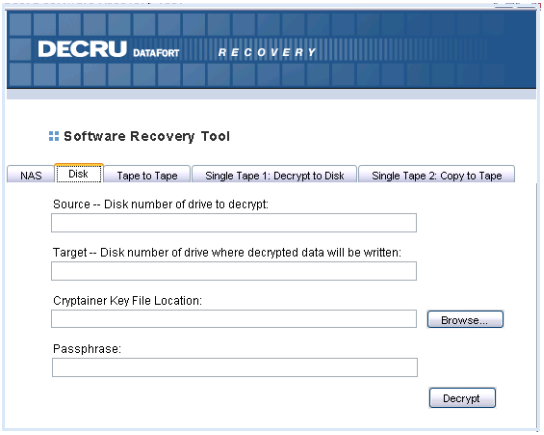
Before you run the tool, make the following preparations:

- 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 > Software Recovery Tool**.
2. Click the Disk tab.



3. Specify the following:

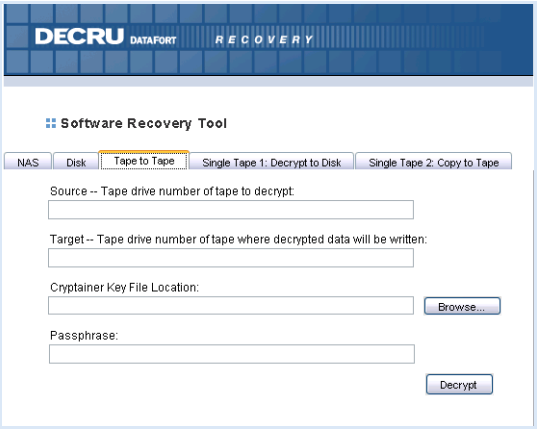
- The source disk number which is to be recovered.
- A destination disk number for the disk to which data is to be written (Note: the disk must be identical to the source disk).
- A Cryptainer Key file that contains the appropriate key.
- The passphrase used to encrypt that Cryptainer Key File.

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 > Software Recovery Tool**.
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.

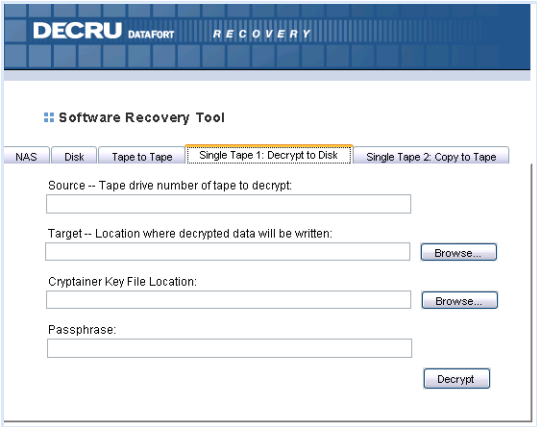
Software Recovery for Tape to Disk

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 > Software Recovery Tool**.
2. Click the Single Tape 1: Decrypt to Disk tab.



3. Specify the following:

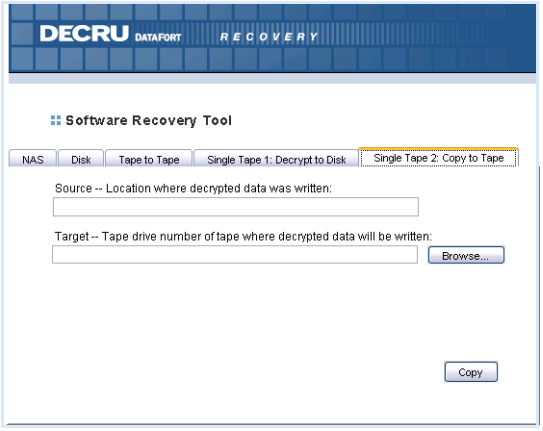
- The source tape drive number which is to be recovered.
- A destination file to which the data is to be written.
- A Cryptainer Key file that contains the appropriate key.
- The passphrase used to encrypt that Cryptainer Key File.

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.

6 LKM Options

Optional LKM commands are available in the right-click or main menus. Options include:

- DataFort Options
- LKM Options

DataFort Options

- Delete DataFort Records
- Open DataFort WebUI
- View DataFort Properties
- Delete Cryptainer from LKM

Delete DataFort Records

LKM keeps a cumulative record of Cryptainer and tape keys for all DataFort appliances from which configurations were loaded. After a period of time, the list of DataFort appliances may include units that are no longer in use, or no longer in the same Security Domain. If you prefer not to view records of inactive DataFort appliances, LKM gives you two options: Deleting a DataFort from LKM, or Marking a DataFort Inactive.

Deleting a DataFort from LKM

1. As a precaution (optional) before you delete, right-click the DataFort in the left or right frame of the LKM window, and choose Properties. Review the properties to verify the identity of the DataFort you intend to delete. Click Close.
2. Right-click the DataFort again, and choose Delete Records.

   You are warned that the information will be deleted permanently from LKM software, and asked if you want to continue.
3. To delete the records, click Yes.

   You are alerted to delete the IP address from the LKM Settings page in the DataFort WebUI if this DataFort is still in use. If you do not, the deleted records will be restored with the next automatic update, provided there has been a change to the DataFort configuration.

   The DataFort is deleted from the list of DataFort Appliances, together with any Recovery Cards that were associated exclusively with that DataFort.

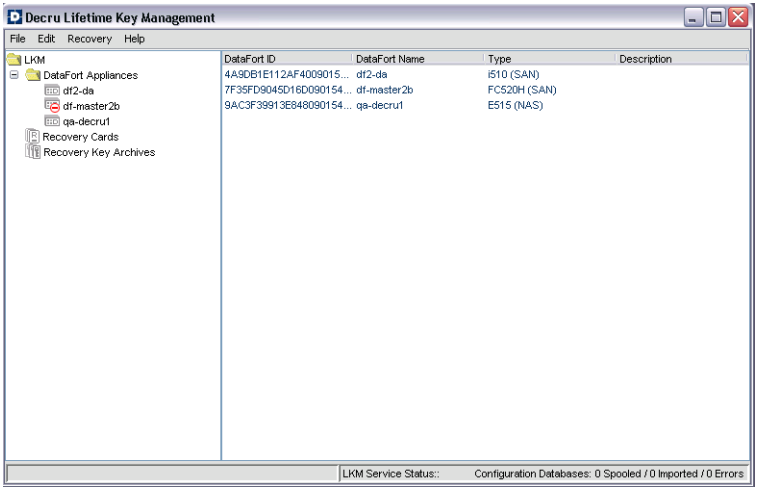
   Note: If you change your mind after deleting, and the LKM server is still connected to the DataFort, you can load a current DataFort configuration into LKM (see Loading a Saved Configuration Database into LKM). This will restore many (if not all) of the records that you deleted.

Marking a DataFort Inactive

If you do not wish to delete any DataFort records from LKM, you can mark inactive DataFort appliances with a red Inactive flag, so you can easily distinguish them in the list. The flag is reversible, and is just a visual sign that you confer—LKM cannot query a DataFort to find out if it is active.

1. Right-click a DataFort in the left or right frame of the LKM window, and choose Mark Inactive.

   Just as with Delete DataFort Records, you are alerted to change LKM settings in the DataFort WebUI if this DataFort is still in use. If you do not, the DataFort will be restored to active status with the next automated update, provided there has been a configuration change.



   The DataFort you selected is marked with an Inactive icon.

   Note: If you right-click the DataFort again, the menu now reads Mark Active. If you choose Mark Active, the Inactive flag is removed.

Open DataFort WebUI

Opening the DataFort WebUI from LKM permits you to log in to a DataFort from the LKM server.

1. Right-click a DataFort in the list on the left side of the LKM main screen, and choose Launch WebUI.

   LKM opens Internet Explorer to the domain name listed for the selected DataFort.

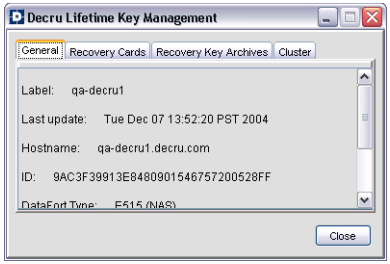
2. Log in as administrator and navigate the WebUI as usual.

View DataFort Properties

You can view general information that LKM has recorded for a selected DataFort appliance.

1. Right-click a DataFort and choose Properties.
2. Click the tabs to view:

- The DataFort label that was entered in the DataFort WebUI
- Date and time the last configuration update was sent to LKM
- Hostname
- ID
- DataFort Type
- DataFort description
- Number of Cryptainer Keys known and Number of Cryptainers known
- Recovery Cards (labels and size of quorum)
- Known Recovery Key Archives and the dates on which they were created
- Cluster information, if any



Delete Cryptainer from LKM

Just as you can delete DataFort records from LKM, you can also delete individual Cryptainer and tape key records. Cryptainer vaults that have been deleted from a DataFort are recorded as a change in DataFort configuration. When LKM updates its database with a new DataFort configuration, it indicates deleted Cryptainer status by graying the name of the Cryptainer in the list in the right frame.

However, you can delete Cryptainer records from LKM entirely, as follows:

1. Select the DataFort in the left pane. From the list of Cryptainers in the right frame, right-click the Cryptainer or tape key you wish to delete, and choose Delete from LKM.

   You are alerted, as when you delete a DataFort from LKM, that the information will be deleted from LKM software, and asked if you want to continue.

2. Click Yes.

   The Cryptainer is deleted from the list and from LKM records. LKM reminds you that if this is an active Cryptainer, it will reappear with the next configuration update from that DataFort.

LKM Options

The main LKM menus contain LKM tools and commands that apply to the LKM server and database.

- Save Latest Configuration Database to File
- Import LKM Database
- Export LKM Database
- Sync a Primary and Secondary LKM Server
- Zeroize LKM Database
- Manage LKM Ports (including setting SSL)

Save Latest Configuration Database to File

When LKM loads a DataFort configuration database, new information is added to its records. At the same time, LKM saves the most recent version of the DataFort configuration database in its own format.

If a DataFort has to be restored to its most recent configuration, the Restore Wizard in the DataFort WebUI prompts the administrator to locate a configuration database backup. If this backup is not available, or if all backups were made to LKM, use LKM to create a configuration database file for restoring a DataFort. From the Restore Wizard (accessed from the DataFort WebUI), browse to the location where you save the configuration file at the end of this operation.

1. Right-click the DataFort in the list of DataFort appliances in the left frame of LKM, and choose Save DB.
2. Browse to the location where you wish to save the file, and enter a filename. Click Save.

   Note: LKM can create a configuration database file only if a current or saved configuration database was loaded in LKM. If LKM data comes from an imported LKM database, it cannot be saved as a configuration database and used to restore a DataFort.

Import LKM Database

The Import command imports an LKM database that was previously exported as a file, adding the data to the current LKM database. The LKM Database Export file (*.lkm) may be a complete LKM database or may contain only selected records from an LKM database. You will need to provide the passphrase that LKM used to encrypt the file.

You can use the Import menu option:

- To add LKM records from one LKM server to LKM running on another.

  For example, if you import records to an LKM server in a different Security Domain, the imported records will be merged with the existing records. This works best if you are importing records of different DataFort appliances.

  You can import Cryptainer Keys exported from one LKM server to another LKM server managing the keys of a DataFort clone. See Import and Export of Cryptainer Keys on page 37.
- To transfer an entire LKM archive from one computer to another (for example, to sync two LKM servers (see Sync a Primary and Secondary LKM Server).
- To reconstitute an LKM archive from an export file that you created as a backup.

1. Choose **File > Import**.
2. Click Yes to continue.
3. Enter the passphrase that was supplied when the LKM Data was exported to a file.
4. Click Choose File Location.
5. Enter or browse to the file you wish to import. Click Save.

   The LKM Database is imported. DataFort appliances in the imported database are listed, along with Cryptainers and Recovery Cards.

   Note: Import can take a while if the LKM database is large. Please wait.

Export LKM Database

The Export command exports the entire LKM Database as a file encrypted with a passphrase.

You can use the Export command to create a file:

- To add records from one LKM server to LKM running on another.
- To move an entire LKM database from one LKM server to another.
- To sync a primary and secondary LKM server.
- To back up the LKM database.

1. Choose **File > Export**.
2. Enter a passphrase that LKM will use to encrypt the export file. Enter it again to confirm.
3. Click Choose Save Location.
4. Enter or browse to the directory where you will store the file. Enter a filename and click Save.
5. Note the filename and the passphrase. You will need them when you are ready to import the file.

Sync a Primary and Secondary LKM Server

If both LKM servers are put in operation at the same time, DataFort keeps them in sync. If the secondary LKM server is added after the primary server, sync them up once:

- At the primary LKM server, export the LKM Database (choose **File > Export**).
- At the secondary LKM server, import the LKM Database (choose **File > Import**).

This ensures that all data is available from both servers. DataFort will keep them in sync thereafter.

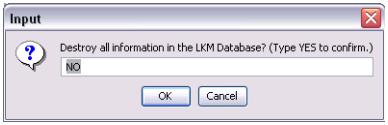
Zeroize LKM Database

The Zeroize command clears the contents of the LKM database. Use this command to:

- Avoid duplicate entries if you plan to import an LKM database that includes records for the same DataFort appliances.
- Restore a blank database after you have exported an existing database.

  Note: If you have any reservations about clearing the database, perform an Export LKM Database command first, so you have a backup file.

1. Choose **File > Zeroize**.



LKM warns that all the data will be destroyed.

2. Type YES to confirm, and click OK.

Manage LKM Ports

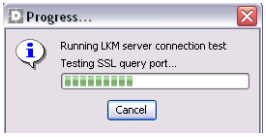
The Edit menu manages LKM server ports. Use this menu to test and configure LKM server ports:

- Testing LKM Server Ports
- Configuring the SSL Connection
- Configuring LKM Server Ports

Testing LKM Server Ports

The LKM server port configuration can be tested and edited as follows:

- Test the availability of LKM server ports and reporting status
- Configure a secure connection to DataFort appliances (SSL)
- Change the base port number
- Choose **Edit > Port**.

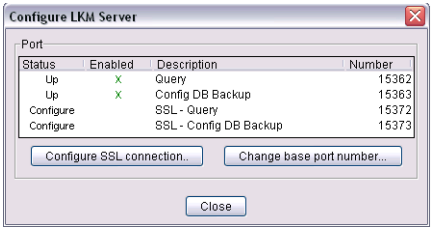


LKM quickly tests four LKM server ports for availability: the ports for regular communication and the ports for secure communication to and from DataFort appliances.

Configuration Database Backup Port This port on the LKM server is assigned to listen for DataFort configuration databases to load. It receives updates automatically and adds them to the configurations stored in LKM.

Query Port If a Datafort does not have access to a particular key when asked to restore a Cryptainer, it will use this port to query the LKM server for the key. If the LKM server has the key, it will send it to the DataFort in encrypted form. This communication is not visible to a user.

The results are shown in the Configure LKM Server dialog box. By default, the Query and Config DB Backup ports are enabled, but the two SSL ports are not available until the SSL connection has been configured in LKM.



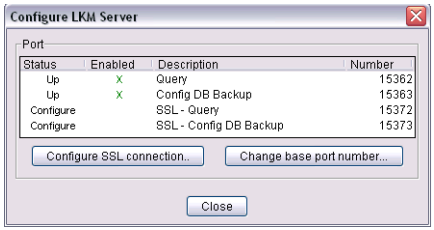
The status of the DataFort Query and DataFort Config DB Backup ports is shown as Up unless there is a port conflict. A status of Configure means that the SSL ports have not yet been configured. The designated port numbers are shown on the right side of the Port window.

Configuring the SSL Connection

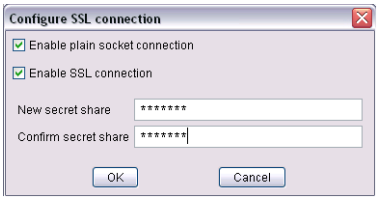
To enable secure communication between DataFort appliances and the LKM server, you must configure the SSL connection at the LKM server once, and also enable SSL at one member of each DataFort cluster. It doesn't matter in what order you do this, but secure backups of the configuration database will not proceed until SSL is enabled and the shared secret registered for both parties to the communication.

1. Choose **Edit > Port**.

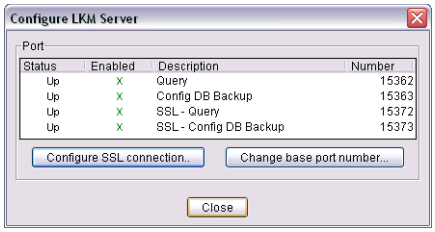
   A connection test will run. The Configure LKM Server window appears.



2. Click Configure SSL Connection. The Configure SSL Connection window appears.
3. Click to check the Enable SSL Connection box.
4. Enter and confirm the secret that will be used to authenticate the SSL connection. The shared secret can be a string of any characters of any length, including spaces.



A connection test will run. The Configure LKM Server dialog box now shows the status of the SSL ports as Enabled and Up.



5. Click Close.

   Note: Enable SSL and enter the identical shared secret, LKM server IP and First Port of the Servers at all connected DataFort clusters. See Configuration from the DataFort WebUI.

Requiring SSL

It is possible to set the ports so that SSL communication is required, not optional.

1. Choose **Edit > Port**.

   A connection test will run. The Configure LKM Server window appears.

2. Click Configure SSL Connection. The Configure SSL Connection window appears.
3. Click to check the Enable SSL connection and enter and verify the secret share.
4. Click to uncheck the Enable plain socket connection box. Click OK.
5. Verify that only the SSL ports are enabled.
6. Click Close.
7. Make sure that one member of each cluster of DataFort appliances has SSL enabled with the same secret.

   Note: If any of the DataFort clusters contain appliances running previous versions of software (1.6 or earlier), they will not be able use SSL to communicate with the LKM server. In that case, leave Enable plain socket connection selected.

Configuring LKM Server Ports

For communication with connected DataFort appliances the default listening ports on the LKM server are 15362 and 15363. Port 15364 is reserved for internal communication. The ports reserved for secure connection with DataFort appliances are the base port + 10 and base port + 11 (by default ports 15372 and 15373).

In the unlikely event that the LKM server requires these ports for another application, you can configure the LKM server to use a different base port. You must make the same modification for all connected DataFort appliances. To change the base port number:

1. Choose **Edit > Port**.

   A connection test will run. The Configure LKM Server window appears.

2. Click Change base port number.
3. Enter the new base port number and click OK.
4. Click Close.

   Note: Be sure the new base port number is entered at one member of every connected DataFort cluster. See Configuration from the DataFort WebUI.

Secondary Server Ports

If you configure and use a secondary backup LKM server, the secondary server uses the same set of ports and the same configuration as the primary LKM server.

7 LKM Administration

Administration Issues

With a minimum of management, LKM archives maintain Cryptainer and key information in a central location for the life of the data. The following topics touch on issues that pertain to LKM administration:

- Security Policy
- Key Escrow
- Troubleshooting
- Managing the LKM Service
- Backing Up LKM Archives
- Changes in DataFort Deployment.

Security Policy

Administering LKM from the LKM server does not require special DataFort permissions or smart cards, however data recovery procedures have the same requirements as recovery procedures performed from the DataFort—a quorum of Recovery Officers and their Recovery Cards.

Recovery Officers For the highest security, make sure the Recovery Officers retain and do not share their Recovery Cards and passwords, or that possession of the card and possession of the password are entrusted to different individuals. If redundancy is desired, initialize a quorum of Recovery Cards with passwords and send them to a key escrow service. Since Recovery Officers will be required only on rare occasions, periodically remind the Recovery Officers to locate their Recovery Card and recall the password. The*DataFort Administration Guide* presents additional options for smart card management.

A Windows PC (for example, one used as an LKM server) does not have the security features of a DataFort appliance. Before inserting Recovery Cards in a smart card reader connected to a Windows PC, check the computer thoroughly to make sure that no malicious code has been installed on it.

Two types of files created by LKM contain encrypted sensitive information: Cryptainer Key Files and Recovery Key Archive files. To minimize the potential for misusing these files, observe the following precautions:

Recovery Key Archive File As soon as a Recovery Key Archive is created, send it to a key escrow service and delete the file from local storage. Make the passphrase available to the escrow service, but do not share it with anyone else.

Cryptainer Key File If you are restoring one or more files within one Cryptainer, use the Recover Data Tool in LKM instead of the option to create a Cryptainer Key File. The LKM server creates an internal copy of the Cryptainer Key File and deletes it automatically after use. If you need to create a Cryptainer Key file, create it for a single Cryptainer if you don't need to decrypt all the Cryptainers of a DataFort. Do not share the passphrase for a Cryptainer Key File. After it has served its purpose, be sure to delete the Cryptainer Key File.

Key Escrow

To ensure recoverability, Recovery Key Archives, Recovery Cards, passwords and backups of the configuration database may be escrowed or placed in trusted long term storage. Contact Decru for more information about escrowing services.

Troubleshooting

If a DataFort does not appear in the list of DataFort Appliances in the LKM UI, or if its records are not being updated, or if an LKM alert appears on the DataFort Home page, check the following:

Communication Ports If you have set up a DataFort for automatic backup to the LKM server, make sure that the same ports were specified on the LKM server. Choose **Edit > Port** to check the number of the base port. If the port is not responding, change the base port number. If the number is doesn't match the number registered with DataFort, enter a matching base port. For more information, see Configuring LKM Server Ports on page 55.

If one of the ports is down, try restarting the server port. If the error persists, it means some other application is using one of the LKM ports. Either choose to use another set of ports for LKM (by changing the base ports to unused ports) or re-configure the other application.

When using a Windows XP server, you must configure Windows Firewall as follows: From the Windows Control Panel, select Windows Firewall. Click the Exceptions tab and add the ports used by LKM by clicking Add port. Add ports 15362 and 15363 for clear communication and ports 15372 and 15373 for SSL. Restart LKM.

SSL Communication Secure automatic backup using SSL must be explicitly enabled in LKM as well as in connected DataFort appliances. For secure backup to the LKM server, make sure that SSL is enabled and configured with the same base port and shared secret at both parties to the connection. For information on DataFort configuration, see Configuring Backups to the LKM Server on page 10.

When using a Windows XP server with SSL, you must configure Windows Firewall as follows: From the Windows Control Panel, select Windows Firewall. Click the Exceptions tab and add the ports used by LKM by clicking Add port. Add ports 15362 and 15363 for clear communication and ports 15372 and 15373 for SSL. Restart LKM.

Temporary Files Configuration databases loaded or backed up to the LKM server are initially stored in temporary files (tempxxx.df) in the q\cfgdb subdirectory of the LKM application folder. When there are many backups of large configuration databases, you may see one or more of these temporary files. After the configuration is loaded in LKM, the temporary file no longer appears in the folder.

Log Files Every time a configuration database is loaded or backed up to the LKM server, LKM creates a log entry in a file named LKM.log, which is also found in the LKM application folder. Open the log file with any text editor to check the status of a particular configuration database loading operation. The log file lkmService.log contains more detailed information from the LKM service.

Managing the LKM Service

LKM software has two components: the Lifetime Key Management Windows Service, and the LKM UI. The Lifetime Key Management service starts automatically when the LKM server is booted, and remains running as long as the server is on. Lifetime Key Management service allows the LKM server to continue to receive configuration updates from connected DataFort appliances regardless of whether the server administrator is logged in.

The Lifetime Key Management service is reset automatically if you change LKM communication ports. In common with other Windows Services, the Lifetime Key Management service can be manually stopped and restarted. To reset the service manually, open the Administrative Tools Control Panel and choose Services. Select Decru Lifetime Key Management Service and choose Stop from the Action menu. To restart, select Decru Lifetime Key Management Service again and choose Restart.

The UI component is started from the Decru Lifetime Key Management desktop icon or the Start menu (**Start > Programs > Decru > Lifetime Key Management**). It provides all the LKM functions that originate from the LKM server. Multiple instances of the LKM UI can be run at the same time. Both components communicate with the LKM internal database.

Backing Up LKM Archives

For automatic backup of LKM archives, set up a secondary (backup) LKM server (see Backup LKM Server). Whether or not you use a secondary LKM server, you can make the LKM server part of your organization's existing backup infrastructure and backup policies. If you wish to store incremental backups periodically, use the Export LKM Database command. The exported database will include the contents of the LKM internal database, but will not include the latest saved configuration database(s).

Changes in DataFort Deployment

Some DataFort changes affect what you see in the LKM UI. Since LKM does not initiate queries to DataFort, continuity of communication between a DataFort and the LKM server is ensured by specifying settings for LKM server IP and base port from a DataFort management interface.

All DataFort configuration changes are saved in the internal configuration database of the DataFort, and these changes are sent to LKM automatically, but only the changes relevant to key management are incorporated into the LKM internal database. For example, changes in administrators, networks and ACLs are not reflected in the LKM UI.

- For a new or zeroized DataFort appliance, follow the setup procedures outlined in Initial Configuration.
- Cluster changes (failing over a cluster and re-forming from the same DataFort appliances) will not be apparent in the LKM UI. Since both cluster members maintain configuration information for the entire cluster, either cluster member can continue to operate in standalone mode, or the cluster can be re-formed, with no effect on the LKM archive.

INDEX

A
Archiving Tools
- Generate Recovery Key Archive 25
- Load Configuration Database 23

C
CLI
- database backup 13, 15
- LKM configuration 12

clone 37
configuration database 5
- automated backup 12
- backups to LKM server 10
- loaded in LKM manually 13
- secure backup 11
- when to back up 24

Configuring the SSL Connection 54
Cryptainer Key 5, 17, 24, 38
Cryptainer Key File 29

D
Data Recovery Tool
- Software Recovery Tool 41

Data Recovery Tools
- Identify Recovery Card 36
- Recover Data Tool 32

DataFort Properties 49
Delete Cryptainer from LKM 50
Delete DataFort Records 48

E
Export Cryptainer Keys to Clone 37
Export LKM Database 52

G
Generate Recovery Key Archive 25

I
Identify Recovery Card 36
Import Cryptainer Keys 38
initial configuration, LKM system 10

K
key management 15
key translation 38

L
LKM server 6
- IP address 6
- ports 6
- secondary (backup) 6, 11

LKM software
- accessing 9
- controlling the display 17
- installing 8
- menu bar 51
- tools and options 21

LKM system
- administration 57
- initial configuration 10
- maintaining automatically 12
- using for data recovery 28

Load Configuration Database 23

M
Mark Active 49
Mark Inactive 49
Marking a DataFort Inactive or Active 49
MS SQL Server 8
MySQL 8

O
Open DataFort WebUI 49

P
port configuration 6

R
Recover Data Tool 32
Recovery Key Archive 25
Requiring SSL 55
Reset LKM Database 52

S
Save Latest Configuration Database to File 51
secure communication, configuring 11, 54
Software Recovery Tool 41
Software Recovery Tools
- installing 41
- iSCSI 43
- NAS 42

SAN 43
SQL Server 7
SSL 58
configuring 11, 54

T

Tape Key 5, 17, 24, 38

W

Windows Firewall 6, 58
Windows XP 6