



■ ■ ■ ADMINISTRATION GUIDE

Lifetime Key Management
Appliance 3.0

security

DRAFT ONLY - NOT FOR RELEASE

LKM Appliance Administration Guide

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

Part number: 210-03856 A0 (LKMA (081007)

Model Number: KM500

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

TRADEMARK NOTICE

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

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

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

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

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

Copyright © 1994-2003 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.

This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>).

Copyright © 2001 Carnegie Mellon University. All rights reserved.

Redistribution and use 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.

3. The name “Carnegie Mellon University” must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact:

Office of Technology Transfer

Carnegie Mellon University

5000 Forbes Avenue

Pittsburgh, PA 15213-3890

(412) 268-4387, fax: (412) 268-7395

tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment:
“This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>).”

NOTICES AND WARNINGS

Power Supply Notice

The appliance is suitable for IT power systems. Connect each power supply to a separate power source for failover support.

WARNING: The power supply cord is used as the main disconnect device. Ensure that the socket-outlet is located/installed near the equipment and is easily accessible.

ATTENTION: LE CORDON D'ALIMENTATION EST UTILISÉ COMME INTERRUPTEUR GÉNÉRAL. LA PRISE DE COURANT DOIT ÊTRE SITUÉE OU INSTALLÉE À PROXIMITÉ DU MATÉRIEL ET ÊTRE FACILE D'ACCÈS.

WARNUNG: Das Netzkabel dient als Netzschalter. Stellen Sie sicher, dass die Steckdose einfach zugänglich ist.

WARNING: This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).

ATTENTION: Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l'installation électrique du local. Vérifier qu'un fusible ou qu'un disjoncteur de 120 V alt., 15 A U.S. maximum (240 V alt., 10 A international) est utilisé sur les conducteurs de phase (conducteurs de charge).

WARNUNG: Dieses Produkt ist darauf angewiesen, daß im Gebäude ein Kurzschluß- bzw. Überstromschutz installiert ist. Stellen Sie sicher, daß eine Sicherung oder ein Unterbrecher von nicht mehr als 10 A ist.



WARNING: TO PREVENT BODILY INJURY WHEN MOUNTING OR SERVICING THE APPLIANCE, DO NOT LIFT OR CARRY THE UNIT BY THE FRONT PANEL. THE FRONT PANEL IS INTENDED TO BE AN EASILY DETACHABLE COMPONENT AND IS NOT DESIGNED TO CARRY PRODUCT WEIGHT.

Perchlorate Present

Important: Special handling may apply. See: <http://www.dtsc.ca.gov/hazardouswaste/perchlorate/>

Rack Mounting

Appropriate hardware is provided with the appliance to mount it in an EIA standard 19" rack. Follow instructions provided in the package to mount the slide rails to the sides of the LKM appliance, and attach the rail mounts to the rack. Then slide the appliance into the rack on the rails and secure the appliance in place using the provided screws.



WARNING: To prevent bodily injury when mounting or servicing this unit in a rack, take special precautions to ensure that the system remains stable. These guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

ATTENTION: Pour éviter toute blessure corporelle pendant les opérations de montage ou de réparation de cette unité en casier, il convient de prendre des précautions spéciales afin de maintenir la stabilité du système. Les directives ci-dessous sont destinées à assurer la protection du personnel.

- Si cette unité constitue la seule unité montée en casier, elle doit être placée dans le bas.
- Si cette unité est montée dans un casier partiellement rempli, charger le casier de bas en haut en plaçant l'élément le plus lourd dans le bas.
- Si le casier est équipé de dispositifs stabilisateurs, installer les stabilisateurs avant de monter ou de réparer l'unité en casier.

WARNUNG: Zur Vermeidung von Körperverletzung beim Anbringen oder Warten dieser Einheit in einem Gestell müssen Sie besondere Vorkehrungen treffen, um sicherzustellen, daß das System stabil bleibt. Die folgenden Richtlinien sollen zur Gewährleistung Ihrer Sicherheit dienen:

- Wenn diese Einheit die einzige im Gestell ist, sollte sie unten im Gestell angebracht werden.
- Bei Anbringung dieser Einheit in einem zum Teil gefüllten Gestell ist das Gestell von unten nach oben zu laden, wobei das schwerste Bauteil unten im Gestell anzubringen ist.
- Wird das Gestell mit Stabilisierungszubehör geliefert, sind zuerst die Stabilisatoren zu installieren, bevor Sie die Einheit im Gestell anbringen oder sie warten.

CONTENTS

Chapter 1 Lifetime Key Management[®] Appliance Overview	10
About the Lifetime Key Management [®] Appliance	11
Features at a Glance	11
About Management Interfaces	12
SecureView	12
Management Station	12
About Terms and Conventions	13
LKM Terminology	13
Conventions Used in this Manual	13
Chapter 2 Deploying an LKM Appliance	14
How the LKM Appliance Works	15
About Connection Types	15
How Key and Configuration Database Backups Work	16
Deployment Scenarios	17
Automatic Key Sharing	17
Manual Key Sharing	19
Enterprise Key Limits	20
Key Generation Frequency	20
Chapter 3 Installing an LKM Appliance	21
Notices and Warnings	22
Power Supply Notice	22
Power Cable Notice	22
Dual Power Supply Notice	22
Lithium Battery Notice for Service Personnel	22
Rack Mounting	22
Installing Hard Disk Drives	23
Rack Mounting the LKM Appliance	24
Connecting the LKM Appliance	24
System Card Insertion	24
Rear Panel Network Connections	25
Powering On and Shutting Down	26
Chapter 4 Setting up an Appliance	27
How to Set Up an Appliance	28
Assigning the IP Address	29
Setting the IP Address Using the LCD	29
Installing the Management Console	31
Management Station Requirements	31
Management Station Security	31
Using the Installer	32
Initializing an Appliance via the Setup Wizard	32

Adding an Appliance for the First Time	32
Using the Setup Wizard	33
Chapter 5 Getting Started	36
Launching the Decru Management Console	37
Exiting the Console	37
Adding Appliances to DMC	37
Adding Appliances	37
Adding Cluster Members	37
Adding Linked Appliances	38
Removing Appliances from DMC	38
Logging in to Appliances	38
Setting Preferences	38
Using Menus and Displays	39
State Displays	40
Using Table Columns	40
About the Appliances Table	40
Appliance Menu	41
Edit Menu	42
View Menu	42
Configuration Menu	43
Keys Menu	44
Topology Menu	45
Utilities Menu	45
Security Menu	46
Trustee Menu	46
Diagnostics	47
Help Menu	47
Chapter 6 Sharing Keys	48
How Keys are Shared	49
Creating Key Sharing Groups	50
Adding OpenKey Clients to Key Sharing Groups	50
Adding DataFort Appliances to Key Sharing Groups	51
Changing Key Sharing Groups	52
Creating Trustee Relationships	54
About Trustee Relationships between DataFort and LKM Appliances	54
About Trustee Relationships between DataFort Appliances	54
Creating Trustees using SecureView	54
Creating Trustees Relationships without SecureView	57
Creating Trustee Links	61
Monitoring Trustee Links	61
About the Linked Appliances Table	61
Viewing Appliance Links	62
Chapter 7 Managing Keys	63
Monitoring Keys	64

About Parent and Cryptainer Key Tables	64
Viewing Parent Keys	64
Viewing Cryptainer Keys	64
Archiving Parent Keys	66
About Parent Key Archives	66
Creating Parent Key Archive Files	67
Backing Up Keys to External Storage	69
About Exporting and Importing Keys	69
Exporting and Importing Keys	69
Transferring Keys	70
About Key Transfers	70
Transferring Cryptainer Keys	71
Chapter 8 Managing Appliances	73
Managing Licenses	74
About the License Table	74
Adding a License	74
Managing Administrators	75
About Administrators and Recovery Officers	75
About Administrator Roles	75
About the Administrators Table	76
Adding an Administrator	77
Modifying Administrators	78
Managing Appliances	79
Adding Lifetime Key Management® Software to DataFort appliances	80
Backing Up the Configuration Database Manually	80
Collecting Tech Support Info	81
Creating Custom Appliance Groups	81
Purging Unused Cryptainer Keys from DataFort appliances	81
Rebooting an Appliance	81
Setting Log Options	82
Setting SNMP Options	83
Upgrading an Appliance	83
Updating Date and Time Settings	84
Updating Network Settings	84
Viewing Appliance Details	84
Zeroizing an Appliance	84
Managing Smart Cards	85
About Smart Cards	85
Viewing Recovery Cards	85
Replacing a Recovery Card	86
Adding an Admin Card to an Administrator	87
Sharing an Admin Card	87
Resetting Smart Cards	88

Chapter 9 Using LKM CLI Commands	89
Using the Command Line Interface	90
Managing DataFort Appliances Linked to LKM	90
Managing SNMP	91
Viewing System Properties	91
Changing Backup Intervals	91
Assigning Names to Cryptainer Keys	92
Importing and Exporting Keys between Trustees	92
Authorizing an Administrator Log In	93
Shutting Down an LKM appliance	94
Appendix I Troubleshooting	95
Recovery Scenarios	96
Recovering LKM and DataFort Appliances	97
About Recovering Appliances	97
Using the Recovery Wizard	97
Initiating Remote Authorization for Recovery	99
Recovering LKM Appliance Keys	100
About Key Recovery	100
Recovering Keys	100
Responding to a Bad Connection Error	101
Viewing LED Displays	101
Front Panel LEDs	101
Back Panel LEDs	101
Appendix II Migrating from LKM Server to LKM Appliance	102
Requirements	103
Halting LKM Server Operations	103
Installing the Key Transfer Tool	103
Using the Key Transfer Tool	103
Appendix III Log Messages	104
LKM appliance Messages	105
Appliance Management Messages	106
Appendix IV Specifications	107
Appendix V Regulatory and Certifications	108
FCC B Declaration of Conformity	109
European Union	109
Canadian ICES-003	109
VCCI Class B Statement	110
CE Statement	110
Appendix VI Glossary	111



ABOUT THE LIFETIME KEY MANAGEMENT® APPLIANCE

The Lifetime Key Management® appliance (LKM appliance) manages encryption keys for multiple LKM clients (DataFort appliances and OpenKey clients), ensuring encryption key availability for the life of the secured data. The LKM appliance does this by providing a central location to store and send keys on demand to clients based on key sharing policies or by manually transferring keys. See [How the LKM Appliance Works](#) on page 15 and [How Keys are Shared](#) on page 49.

The Decru Management Console (DMC) provides a powerful tool for managing keys for multiple LKM clients from a single interface. See [About Management Interfaces](#) on page 12.

FEATURES AT A GLANCE

The LKM appliance offers the following features:

- Supports LKM clients across the enterprise
- Supports 100 DataFort appliances and 10 million keys per LKM appliance
- Up to 16 LKM appliances can be linked to support large DataFort appliance deployments (1000)
- Provides high availability through key replication and redundant components
- Provides centralized management for multiple DataFort and LKM appliances
- Provides global distributed backup, replication, and recovery of encryption keys
- Provides automated key distribution for information sharing
- Leverages Decru's FIPS 140-2 Level 3-certified Storage Encryption Processor (SEP) for encryption
- Provides role-based access controls for administrators
- Provides tamper-evident logging and auditing

ABOUT MANAGEMENT INTERFACES

The following table summarizes the management interfaces available for LKM appliances:

TABLE 1: MANAGEMENT INTERFACES

Interface	Function	Usage
Serial Console	Enter network settings for uninitialized appliances.	Set, clear, or reset IP address, gateway and subnet mask. Zeroize when other interfaces are not available.
LCD	Display touch panel functions and interactive messages.	View the Number of Keys (0-10M) and the CPU Load % (0-100) at a glance. Enter initial IP settings.
Decru Management Console (DMC)	Manage keys for multiple LKM clients from a single interface. A SecureView™ license supports the management of simultaneous LKM and DataFort appliances.	Manage all LKM and DataFort appliances in an installation and some features for OpenKey clients.

SECUREVIEW

SecureView™ is a licensed feature that allows the Decru Management Console to monitor and manage many appliances simultaneously. SecureView supports operations on multiple licensed appliances, whether local or remote, including appliance configurations, patches, licenses and administrators.

To manage multiple appliances using SecureView, add the same administrator (with the same name and password) to all appliances. Then select, log into and manage all appliances simultaneously. Different menu options appear depending on which appliance type is selected. If different appliance types are selected simultaneously, some menu items will be disabled. Attempts to multi-select appliances without the SecureView license will fail.

- Selecting several LKM and DataFort appliances with SecureView disables some menu items for both appliances.
- Selecting an LKM appliance with SecureView and a DataFort appliance without SecureView enables LKM menu items. The DataFort appliance without SecureView is considered unselected.

MANAGEMENT STATION

The Decru Management Console (DMC) provides the centralized management interface for the LKM appliance. DMC runs on a dedicated PC (the Management Station). The Management Station also provides a dock for smart cards, which are used during appliance setup and for authentication. See [Installing the Management Console](#) on page 31.

ABOUT TERMS AND CONVENTIONS

This section includes the following topics:

- [LKM Terminology](#)
- [Conventions Used in this Manual](#)

LKM TERMINOLOGY

Decru Management Console (DMC)

The DMC provides a centralized management interface for LKM clients and appliances.

See [Management Station](#) on page 12.

SecureView

SecureView™ is a licensed feature that allows DMC to monitor and manage many appliances simultaneously from a single console.

See [SecureView](#) on page 12.

Keys

LKM appliances automatically stores keys for all LKM clients in the enterprise.

See [How the LKM Appliance Works](#) on page 15.

Configuration Database

The LKM appliance automatically stores the most recent configuration database for any linked DataFort or LKM appliance.

See [How the LKM Appliance Works](#) on page 15.

Key Sharing

There are several ways to share keys between appliances depending on the level of trust set between appliances.

See [Sharing Keys](#) on page 48.

Parent Key Archives

Selecting any of the Parent Keys for an LKM client archives all of the Parent Keys for that client. Selecting a Cryptainer Key archives all of the Parent Keys for a DataFort Cryptainer Key.

See [Archiving Parent Keys](#) on page 66.

Administrators and Recovery Officers

There are two types of trusted individuals responsible for the security of the LKM appliance, LKM Administrators and Recovery Officers.

See [About Administrators and Recovery Officers](#) on page 75.

Smart Cards

Three types of smart cards are shipped with every LKM appliance, the System Card, Admin Card and Recovery Cards.

See [About Smart Cards](#) on page 85.

CONVENTIONS USED IN THIS MANUAL

This guide uses the following typographic conventions:

- Keyboard commands appear in mono-spaced font in **blue**.
- PDF links appear as [underlined purple](#) text.



■ ■ ■ ■ 2 DEPLOYING AN LKM APPLIANCE

This chapter includes the following topics:

- [How the LKM Appliance Works](#)
- [Deployment Scenarios](#)
- [Enterprise Key Limits](#)

How the LKM Appliance Works

The LKM appliance is positioned on the Ethernet portion of the network where LKM clients reside. Linking LKM appliances and clients provides a secure channel for key backup and replication since LKM clients can automatically share key data with a linked LKM appliance.

Note: Decru recommends that each LKM client have at least two LKM appliance peers, making LKM appliance connections across sites redundant. See [Figure 2-1](#).

The LKM appliance automatically stores all keys for the LKM client and the most recent configuration database for any DataFort appliance. LKM appliances maintain both a configuration and a key database of their own. Additionally, both key and configuration databases can be manually backed up to external storage. See [How Key and Configuration Database Backups Work](#) on page 16.

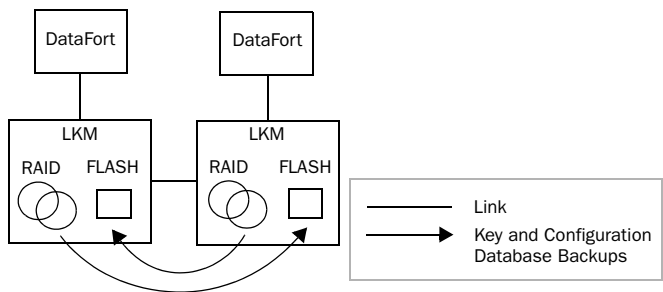


Figure 2-1: Key and Configuration Database Backups

About Connection Types

There are two ways clients can form connections to share keys. See [How Keys are Shared](#) on page 49.

TABLE 2: ABOUT CONNECTION TYPES

Connection Type	Details
Links	Links formed between LKM clients in a key sharing group and an LKM appliance allow group members to automatically share keys using a Secure Socket Layer (SSL) connection between appliances. See Automatic Key Sharing on page 17. Links formed between DataFort appliances and an LKM appliance outside of a key sharing group allow DataFort appliances to share keys by performing a one-way key transfer. See Key Translation on page 19.
Trustee Relationship	DataFort appliances must form a trustee relationship with an LKM appliance before creating a key sharing group. This allows them to share keys without manually importing and exporting keys or going through the key translation process. See Automatic Key Sharing on page 17. Unrelated DataFort appliances may form a trustee relationship. This allows appliances that may not even be on the same network to share keys by manually importing and exporting each key for each trustee. See Trustee Relationships on page 19.

How Key and Configuration Database Backups Work

The table below details how an LKM appliance uses automatic and manual back up methods to store keys and configuration data.

TABLE 3: KEY AND CONFIGURATION DATABASE BACKUP METHODS

Method	Details
Automatic Backups to LKM	Keys LKM clients are queried for new keys every five seconds by the LKM appliance. If a client returns a key, the LKM appliance asks for the new key immediately. If there is no new key, the LKM appliance waits five more seconds before sending another request. The LKM appliance does this for every client it is linked with, so that almost as soon as a new key is created on the LKM client, the key is synced to the LKM appliance.
	Configuration Database The LKM appliance retains only the most recent backup of the configuration database for the DataFort appliance. DataFort appliances initiate a backup of the configuration database to the LKM appliance approximately every two hours. The backup interval can be changed. See Changing Backup Intervals on page 91. Note, the DataFort configuration database can also be backed up remotely from the DataFort appliance.
Manual Backups to External Storage	Keys In the unlikely event that the LKM appliance and its peers are down, backing up the LKM key database to external storage makes recovery possible. See Backing Up Keys to External Storage on page 69.
	Configuration Database In the unlikely event that the LKM appliance and its peers are down, backing up the LKM appliance configuration database to external storage is useful in restoring key sharing groups. Backing up the DataFort configuration database to external storage is useful when multiple DataFort configuration database versions need to be archived, or if DataFort Cryptainers are frequently added or obsoleted. See Backing Up the Configuration Database Manually on page 80.

DEPLOYMENT SCENARIOS

This section includes the following topics:

- [Automatic Key Sharing](#)
- [Manual Key Sharing](#)

AUTOMATIC KEY SHARING

LKM clients may form key sharing groups when linking to an LKM appliance. This allows group members to automatically share keys.

Note: DataFort appliances must form a trustee relationship with an LKM appliance before creating a key sharing group. This allows them to share keys without manually importing and exporting keys or going through the key translation process. See [How Keys are Shared](#) on page 49.

This section includes the following topics:

- [Key Sharing Groups](#)
- [Hierarchical Key Sharing Groups](#)

Key Sharing Groups

LKM clients in a key sharing group with an LKM appliance request encryption keys from that LKM appliance. Each LKM client passes its encryption keys to either LKM appliance, and LKM appliances pass keys to clients as required to share keys between key sharing group members. See [Figure 2-2](#).

Note: Decru recommends using key sharing groups to share encryption keys between clients.

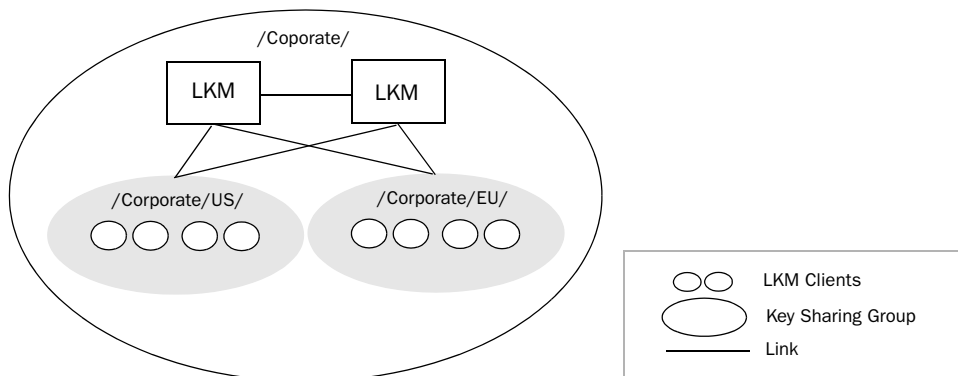


Figure 2-2: Key Sharing Groups

Hierarchical Key Sharing Groups

Hierarchical key sharing groups operate the same as with any key sharing group (see [Key Sharing Groups](#) on page 17). Additionally, key sharing group siblings cannot request keys from other siblings, but parent key sharing group members can request keys from siblings and from either LKM appliance. Also, remote recovery sites decrypt data encrypted with keys from either LKM appliance.

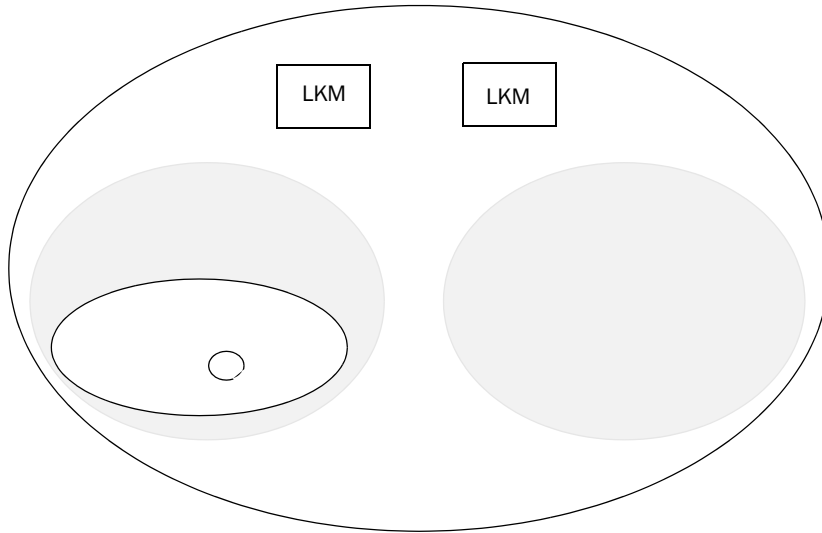


Figure 2-3: Hierarchical Key Sharing Groups

MANUAL KEY SHARING

DataFort appliances may form a trustee relationship or they may form a standalone link to an LKM appliance when sharing keys manually. See [How Keys are Shared](#) on page 49.

This section includes the following topics:

- [Trustee Relationships](#)
- [Key Translation](#)

Trustee Relationships

Unrelated DataFort appliances may share keys by forming a long-term trustee relationship. This allows appliances that reside in independent key domains to manually share keys by manually importing and exporting each key for each trustee. See [Creating Key Sharing Groups](#) on page 50.

Note: A Recovery Card quorum for each appliance is required for setup.

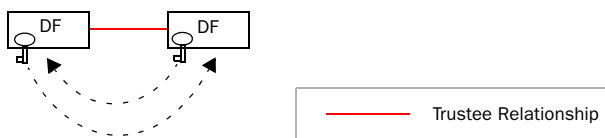


Figure 2-4: DataFort Trustees

Key Translation

Unrelated DataFort appliances that are linked to a shared LKM appliance may share keys by initiating a one-way key transfer. The LKM appliance enables the DataFort appliance receiving the keys to decrypt data encrypted by the DataFort appliance sending the keys. See [Creating Trustee Links](#) on page 61.

Note: Either a Recovery Card quorum or a Key Archive file for each DataFort appliance is required to transfer keys.

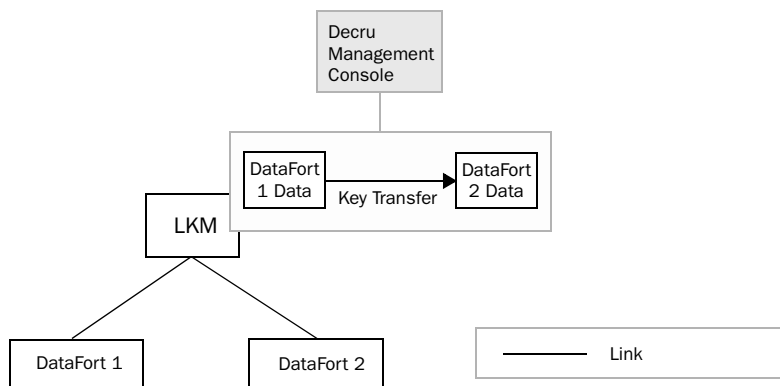


Figure 2-5: Key Translation

ENTERPRISE KEY LIMITS

One LKM appliance manages multiple LKM clients appliances, and multiple LKM appliances can share key information for the enterprise. The number of LKM clients and LKM appliances required across the entire installation is determined by the aggregate data throughput required by LKM clients, the frequency of key generation, and redundancy requirements.

Understanding the full life cycle of encryption keys in a deployment helps when determining the number of appliances to install. Factors to consider include requirements for an independent recovery site, key availability requirements, and the flow of encrypted data between sites.

When planning an installation, keep the following [Appliance Key Limits](#) in mind:

TABLE 4: APPLIANCE KEY LIMITS

Appliance Type	Item	Limit
Lifetime Key Management appliance	Number of LKM clients per LKM appliance	100
	Keys per LKM appliance	10 million
	Number of LKM appliances that can be linked together	16
DataFort appliance	Keys per DataFort.	4500 for E-Series
	The DataFort appliance will purge keys from the configuration database when the limit is reached.	8000 for FC-Series

KEY GENERATION FREQUENCY

For DataFort appliances, keys generate when a Cryptainer is created, rekeyed or translated from one DataFort to another. In some environments, such as those where new backup tapes are created each day, there is a high frequency of key generation. [Table 5](#) gives an example:

TABLE 5: HIGH FREQUENCY KEY GENERATION FOR FC-SERIES DATAFORT

Key Generation	Total
Keys Generated Per Tape	1
Tapes Generated Per Day	4
DataFort Appliances in Cluster	8
Keys Generated Per Day	32



■ ■ ■ ■ 3 INSTALLING AN LKM APPLIANCE

Ethernet connectivity is required between LKM appliances and all clients that send keys to LKM. Ethernet connectivity is also required between LKM appliances that replicate keys.

This chapter includes the following topics:

- [Notices and Warnings](#)
- [Installing Hard Disk Drives](#)
- [Rack Mounting the LKM Appliance](#)
- [Connecting the LKM Appliance](#)

NOTICES AND WARNINGS

POWER SUPPLY NOTICE

The appliance is suitable for IT power systems. Connect each power supply to a separate power source for failover support.



WARNING: THE POWER SUPPLY CORD IS USED AS THE MAIN DISCONNECT DEVICE. ENSURE THAT THE SOCKET-OUTLET IS LOCATED/INSTALLED NEAR THE EQUIPMENT AND IS EASILY ACCESSIBLE.

POWER CABLE NOTICE



WARNING: THE ELECTRIC CABLE CONTAINED IN THIS UNIT SHALL BE SOLELY FOR THE USE WITH THIS UNIT AND SHALL NOT BE USED WITH OTHER EQUIPMENT. THE USE OF THE ELECTRIC CABLE WITH OTHER EQUIPMENT OR FOR OTHER PURPOSES MAY CAUSE FIRE, ELECTROCUTION OR OTHER FATAL ACCIDENTS.

DUAL POWER SUPPLY NOTICE



WARNING: THIS UNIT HAS MORE THAN ONE POWER SUPPLY CONNECTION; ALL CONNECTIONS MUST BE REMOVED TO REMOVE ALL POWER FROM THE UNIT.

LITHIUM BATTERY NOTICE FOR SERVICE PERSONNEL

This product contains a lithium battery. Although the battery is not field-serviceable, observe the following warning:



WARNING: DANGER OF EXPLOSION IF BATTERY IS REPLACED WITH INCORRECT TYPE. REPLACE ONLY WITH THE SAME TYPE RECOMMENDED BY THE MANUFACTURER. DISPOSE OF USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

RACK MOUNTING



WARNING: TO PREVENT BODILY INJURY WHEN MOUNTING OR SERVICING THE APPLIANCE, DO NOT LIFT OR CARRY THE UNIT BY THE FRONT PANEL. THE FRONT PANEL IS INTENDED TO BE AN EASILY DETACHABLE COMPONENT AND IS NOT DESIGNED TO CARRY PRODUCT WEIGHT.

Appropriate hardware is provided with the appliance to mount it in an EIA standard 19" rack. Follow instructions provided in the package to mount the slide rails to the sides of the LKM appliance, and attach the rail mounts to the rack. Then slide the appliance into the rack on the rails and secure the appliance in place using the provided screws.



WARNING: TO PREVENT BODILY INJURY WHEN MOUNTING OR SERVICING THIS UNIT IN A RACK, TAKE SPECIAL PRECAUTIONS TO ENSURE THAT THE SYSTEM REMAINS STABLE. THESE GUIDELINES ARE PROVIDED TO ENSURE YOUR SAFETY:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

INSTALLING HARD DISK DRIVES

The LKM appliance automatically stores all encryption keys and the most recent configuration database for any linked appliance on the hard disk drives (RAID). See [How the LKM Appliance Works](#) on page 15.

WARNING: THE RAID IS NOT INTERCHANGEABLE WITHIN AN LKM APPLIANCE OR BETWEEN LKM APPLIANCES.

1. Remove the LKM appliance bezel by lifting it up from the bottom corners.
2. Locate the two drive slots in the chassis.
3. Remove the RAID from separate packaging in the LKM appliance shipping box.
4. Insert the RAID (labeled 1) into the top slot with the board facing down and the maroon tab facing right.
5. Secure the RAID in the top slot by completely inserting it and fastening the black handle to the right.

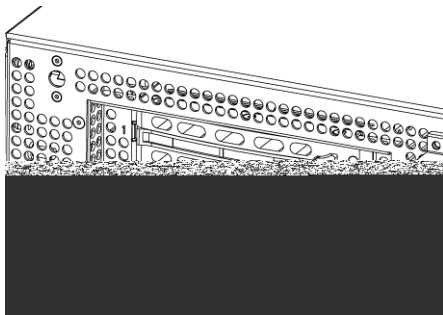


Figure 3-6: Front panel slots (with bezel removed) housing two drive slots for RAID

6. Repeat the process for the RAID (labeled 2), inserting it into the bottom slot.
7. Refasten the bezel to the chassis until it clicks in on both the top and bottom.

Note: The RAID can be replaced (hot-swap only) but working drives are not interchangeable. Contact Decru for service instructions the RAID needs to be replaced.

RACK MOUNTING THE LKM APPLIANCE

LKM appliance design allows for easy installation in an EIA standard 19" rack. When installing the unit in an equipment rack, select a location that meets the following requirements:

- Check that the ambient temperature around the unit (which may be higher than the room temperature) is within the limit specified for the unit:
 - Operating Temperature: +5°C to +40°C (41°F to 104°F)
 - Storage Temperature: -10°C to +60°C (+14°F to 140°F)
- Provide sufficient air flow around the unit. Do not block air flow from fans.
- Avoid overloading electrical circuits - consider the nameplate rating of all the connected equipment to ensure overcurrent protection.
- Ground the equipment properly.
- Do not place objects on top of the unit.
- Do not block access to the front panel smart card slot, LEDs or LCD panel.
- Allow access to rear panel ports, power supplies and fans.
- Avoid dusty or damp locations.

CONNECTING THE LKM APPLIANCE

Insert the System Card into the slot on the front panel, then connect the appliance as follows:

- [Rear Panel Network Connections](#)
- [Power Connection](#)
- [Powering On and Shutting Down](#)

SYSTEM CARD INSERTION

Insert the System Card before powering on the appliance.

1. Insert the System Card into the smart card slot on the front panel.
2. Slide the card into the slot firmly, with the gold contacts facing up and towards the back of the appliance. The card should fit snugly all the way into the slot, flush with the front bezel.

Leave the System Card inserted until after the appliance boots up.

REAR PANEL NETWORK CONNECTIONS

Connect the appliance to the network as described in the following sections:

- [Ethernet Connection](#)
- [Serial Console Port](#)
- [Power Connection](#)

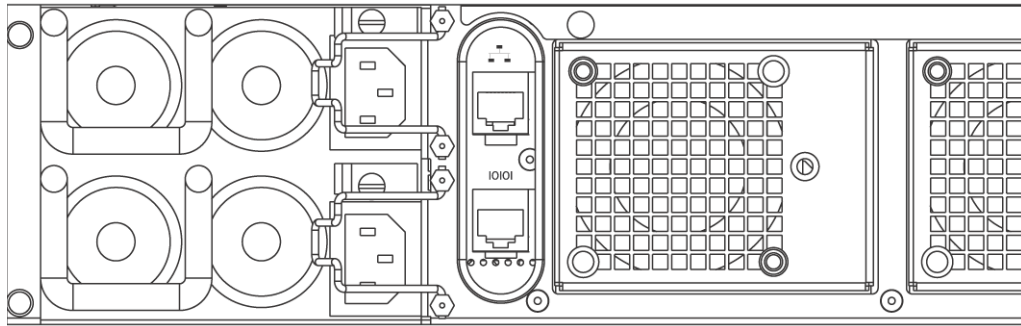


Figure 3-7: Rear panel connections

Ethernet Connection

Use a Category 6 Ethernet cable to connect the Management Port (the Ethernet port marked with the network icon) to the Ethernet network shared by the Management Station PC.

Serial Console Port

Use only the supplied RJ45 to DB9 adapter and standard straight through Ethernet cable to connect a workstation or serial switch to the serial console port on the rear panel.

1. Attach the provided RJ45 to DB9 adapter to the Category 5 cable.
2. Connect the DB9 end of the cable to a serial switch or the serial console port of a workstation.
3. Connect the RJ45 end of the cable to the serial console port (marked **IOIOI**) on the appliance.

Power Connection

The LKM appliance is equipped with three fans and two replaceable power supplies. For instructions on replacing fans and power supplies, contact Decru.

1. Use the provided cords to connect each power port on the rear panel to a separate grounded power supply and secure the power plug using the wire retaining clamp.
Note: The appliance operates with only one power cord, but the second cord provides failover protection when connected to a different circuit.
2. When the cords are connected, the appliance powers on automatically. See [Powering On and Shutting Down](#) on page 26.

Wait two to three minutes. When the LCD messages are complete then initialize the appliance.

POWERING ON AND SHUTTING DOWN

The LKM appliance is equipped with two power cords; the second cord provides failover protection when connected to a different circuit. For normal operation, leave the appliance powered on, with the System Card in the card slot.

Power on LKM

1. Connect each provided power cord to a LKM power port. Then connect the cord to an AC power source. See [Power Connection](#) on page 25.
2. Remove the LKM appliance bezel by lifting it up from the bottom corners and depress the recessed power button until the system turns on.

Note: The appliance may take up to 10 minutes to boot.

Power off LKM

Shut down using either the LKM appliance CLI shutdown command or the LCD.

WARNING: DO NOT SHUT DOWN THE LKM APPLIANCE USING THE POWER BUTTON, OR BY PULLING THE POWER CORDS. THIS IS TO AVOID RISK OF IMPROPER FILE SYSTEM SHUTDOWN, AND THE NEED TO PERFORM A FILE SYSTEM CHECK UPON NEXT STARTUP.

1. Back up the configuration database before shutting down the LKM appliance. See [Managing Smart Cards](#) on page 85.
2. Select from the following:
 - If using the CLI, see [Shutting Down an LKM appliance](#) on page 94.
 - If using the LCD, touch Menu, scroll to Shutdown and touch Select.
The LCD displays the message “Touch (OK) to shutdown system.” Touch OK to shut down the appliance.

WARNING: THERE IS NO CANCEL OPTION. TOUCHING OK WILL SHUT THE SYSTEM DOWN.

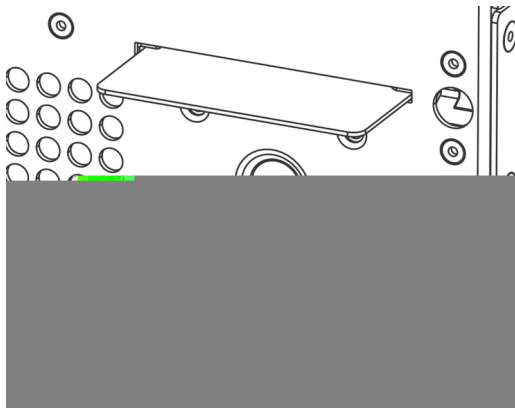


Figure 3-8: Front panel power button (bezel removed)



■ ■ ■ ■ 4 SETTING UP AN APPLIANCE

This chapter includes the following topics:

- [How to Set Up an Appliance](#)
- [Assigning the IP Address](#)
- [Installing the Management Console](#)
- [Initializing an Appliance via the Setup Wizard](#)

How to Set Up an Appliance

To set up an appliance:

1. Assign the appliance network settings using the LCD or Serial interface.
See [Assigning the IP Address](#) on page 29.
2. Install the Decru Management Console on the Management Station.
See [Installing the Management Console](#) on page 31.
3. Initialize an appliance by adding it and using the Setup Wizard.
See [Initializing an Appliance via the Setup Wizard](#) on page 32.
4. Log into and link the initialized appliances that are added to DMC.
See [Logging in to Appliances](#) on page 38 and [Sharing Keys](#) on page 48.

ASSIGNING THE IP ADDRESS

Assign an IP address so that the Decru Management Console can communicate with the appliance. Assign the appliance IP settings using the touch-sensitive buttons on the front panel LCD or the serial console port.

This section includes the following topics:

- [Setting the IP Address Using the LCD](#)
- [Setting the IP Address Using the Serial Console](#)

SETTING THE IP ADDRESS USING THE LCD

1. Touch the Details button.
2. Touch the Menu button.
The screen shows the Network Setting entry. (If not, touch either the up or down arrow to scroll the menu to the correct entry.)
3. Touch the Select button.
4. Touch the Edit button. The screen displays a keypad of numbers, and selectable fields for the Management Port IP address.
5. Touch the entry field to highlight it, and then touch the keypad buttons to enter each number.
Use the decimal point to tab to the next field automatically.
6. When the Management Port address are correct, touch Next.
The touch panel screen displays a keypad of numbers, and selectable fields for the Management Port netmask. A default entry of 255 is in place for the first field.
7. Touch the entry field to highlight it, and then touch the keypad buttons to enter each number.
8. Touch Next.
The touch panel screen displays a keypad of numbers and fields for the gateway.
9. Touch the entry field to highlight it, and then touch the keypad buttons to enter each number.
Use the decimal point to tab to the next field automatically.
10. Touch Next.
11. Review the appliance IP settings.
 - If settings are correct, touch Return to exit the menu.
 - If settings are incorrect, touch Edit and enter the settings again. When finished, touch Return to exit the menu.

SETTING THE IP ADDRESS USING THE SERIAL CONSOLE

1. Open a serial console (such as HyperTerminal) on the workstation connected to the serial port. See [Serial Console Port](#) on page 25.
2. Set the new connection with the following properties:
 - Speed - **9600**
 - Data bits - **8**
 - Stop bits - **1**
 - Parity - **None**
 - Hardware or no flow control
3. At the shell prompt, log in using the default administrator name and password (note that these entries are space and case sensitive):
 - Login: **user**
 - Password: **PASSWORD**

The main menu appears. The serial console menu offers the following options:

```
1. Configure Network Interface - active
   IP Address                      : (not set)
   Netmask                        : (not set)
   Default Gateway Address        : (not set)
2. Ping Default Gateway
3. Save and Exit
-----
C. Clear Current Settings
F. fsck RAID filesystems
N. newfs RAID filesystems
R. Reboot appliance
S. Shutdown appliance
Z. Zeroize appliance
Q. Quit
```

4. Select option 1, and set an IP address, subnet mask and default gateway for the Network Interface.
5. Select option 3 to save the settings and exit the terminal window.

Note: Serial sessions time out after 90 seconds of inactivity. If this happens before completion, save the configuration and log in again. Settings are saved using the Save and Exit commands.

INSTALLING THE MANAGEMENT CONSOLE

Use the Decru Management Console (DMC) interface to run the Setup Wizard and initialize new appliances. The Decru Management Console runs on a dedicated PC (the Management Station).

Note: If [SecureView™](#) is enabled, setup and management functions can be performed on several appliances simultaneously.

This section includes the following topics:

- [Management Station Requirements](#)
- [Management Station Security](#)
- [Using the Installer](#)

MANAGEMENT STATION REQUIREMENTS

Select a computer that meets the following requirements to serve as the Management Station:

TABLE 6: MANAGEMENT STATION REQUIREMENTS

Software Requirements (select one of the following)	Hardware Requirements
Windows XP	2 Ghz
Windows 2000	1GB RAM
Windows Server 2003	4 GB free hard drive space
	An available USB port for the smart card reader from Decru

MANAGEMENT STATION SECURITY

Be sure that the Management Station's security patches are current and that unnecessary services are disabled or removed. Do not use the Management Station to browse untrusted web sites or run unverified code. Limit log ins to authorized administrators, and disable remote management.

WARNING: KEY MATERIAL IS EXPOSED DURING LKM OPERATIONS—BE SURE THE MANAGEMENT STATION IS A SECURE MACHINE.

USING THE INSTALLER

Before initializing an appliance, install the Decru Management Console and the driver for the smart card reader on the Management Station.

1. Insert the installation CD in a drive on the Management Station.
The CD will run automatically if autorun is on.
2. Click the installer link.
3. On the File Download screen, click the button to open or run the file.
4. Follow the prompts to start the installer.
5. Read and accept the terms of the license agreement.
6. Select the model number of the card reader.
The model number can be found on the underside of the card reader (i.e. GemPCUSB-SL).
7. Select "Yes, I want to restart my computer now" and click Finish to complete installation.

INITIALIZING AN APPLIANCE VIA THE SETUP WIZARD

To initialize an appliance, add the appliance(s) to the DMC console and run the Setup Wizard. To log into initialized appliances, see [Logging in to Appliances](#) on page 38.

See the sections below for details:

- [Adding an Appliance for the First Time](#)
- [Using the Setup Wizard](#)

ADDING AN APPLIANCE FOR THE FIRST TIME

Before using the Setup Wizard to initialize an appliance, add it to the Decru Management Console.

1. Select **Start > Programs > Decru > Decru Management Console** to view the console.
2. In the Decru Management Console, the Add screen appears automatically.
3. On the Add screen, select from the following:
 - To add appliances by IP address or hostname, enter the IP address(es) or hostname(s) of the appliance(s) in the text box and click OK.
 - To add appliances by IP range, enter the start and end addresses of the IP range and click OK.
4. On the Certificates screen, select whether to trust the certificate validating the connection between the appliance and the Management Console once or always.

USING THE SETUP WIZARD

Before using the Setup Wizard, add an appliance to the Decru Management Console. See [Adding an Appliance for the First Time](#) on page 32.

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Appliance menu, select Set up.
3. On the Decru Appliance Setup Wizard Step 1 of 12 (Welcome to the Decru Setup Wizard) screen, click Start.
4. On the Certificates screen, select whether to trust the certificate validating the connection between the appliance and the Management Console once or always.
5. On the Decru Appliance Setup Wizard Step 2 of 12 (Connect to Head of Cluster) screen, follow the instructions to enter the hostname or IP address of the appliance and click Next.

Note: This is the same hostname or IP address that was configured using the LCD or serial console during installation.

6. On the Decru Appliance Setup Wizard Step 3 of 12 (Sign the License Agreement) screen, read the license agreement and click Accept.
7. On the Decru Appliance Setup Wizard Step 4 of 12 (Recover from Database - Optional) screen, either browse to the path of the configuration database and click Next, or click Next to skip.
8. On the Decru Appliance Setup Wizard Step 5 of 12 (Create Administrator) screen, enter a username and password for the administrator and click Next.

Note: Record this information for future reference.

Passwords may be composed of upper and lower case characters, numbers and punctuation marks. Select a password consisting of at least 8 valid, randomly-chosen characters. This name and password will be used every time the administrator logs in to the appliance.

Note: When using SecureView licenses, Decru recommends that creating the same administrator on multiple appliances. This is to multi-select appliances and log into them as a group with one administrator profile.

9. On the Decru Appliance Setup Wizard Step 6 of 12 (Configure Cluster and Recovery Schema) screen, select the desired data recovery schema and shared secret, but **do not modify** the cluster size setting, and click Next.

Note: It is not necessary to set up a cluster when using LKM appliances.

WARNING: CLICKING NEXT MEANS THAT THIS SETTING CANNOT BE CHANGED. PLAN THE SETTING ACCORDING TO THE SECURITY POLICY OF YOUR ORGANIZATION.

Note: Decru recommends that 2 of the 5 Recovery Cards are present for sensitive data recovery operations. These same Recovery Cards, initialized during setup, are required to complete a recovery procedure. Give each card to a different individual, so that two people are present for data recovery procedures.

10. On the Decru Appliance Setup Wizard Step 7 of 12 (Network) screen, enter hostname of the appliance, the IP address of the appliance, and the netmask and gateway settings and click Next.
11. On the Decru Appliance Setup Wizard Step 8 of 12 (Add Decru provided Licenses) screen, enter

licenses and click Next.

To enter multiple licenses enter each license and then press Enter on the Management Station keyboard to start a new line for the next license. Each license must be on a consecutive and individual line.

12. On the Decru Appliance Setup Wizard Step 9 of 12 (Network and Certificate) screen, enter DNS information when using DNS and the values for the self-signed certificate and click Next.
13. On the Decru Appliance Setup Wizard Step 10 of 12 (Introduce Recovery Cards) screen, select a method to authorize the Setup Wizard:
 - To set up the appliance locally, see [Authorizing Setup Locally](#) on page 34.
 - To set up the appliance using Remote Authorization, see [Initiating Remote Authorization for Setup](#) on page 35.

Note: Both methods require using smart cards according to the recovery schema set for each appliance during initialization.

Authorizing Setup Locally

1. On the Decru Appliance Setup Wizard Step 10 of 12 (Introduce Recovery Cards) screen, insert a card into the card reader, enter the password and click Next.

Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader, it is selected (green). At this point, enter the password and click the Verify Password button. Cards remain selected after removal.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

Note: If the card is uninitialized, the Security Domain entered for the first card in the set is applied to the entire set of Recovery Cards. If the card is initialized, the Card Label and Security Domain appear and the Recovery Officer is prompted for the password.

2. On the Decru Appliance Setup Wizard Step 11 of 12 (Apply Settings) screen, click Next.
3. On the Decru Appliance Setup Wizard Step 12 of 12 (Wizard Completed Successfully) screen, click Finish.

Initiating Remote Authorization for Setup

1. On the Decru Appliance Setup Wizard Step 10 of 12 (Introduce Recovery Cards) screen, click Enable Remote Authorization.
Note: Previously entered data is saved locally, therefore Decru recommends that the Administrator initiating the remote authorization process be the last Recovery Card holder to supply a card.
2. When the Remote Authorization enabled message appears, close the Decru Appliance Setup Wizard Step 10 of 12 (Introduce Recovery Cards) screen.
3. Notify the outstanding Recovery Officer(s) that it is safe to continue the Setup Wizard approval and introduce Recovery Cards remotely. See [Authorizing Setup Remotely](#).

Authorizing Setup Remotely

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Appliance menu, select Set up.
3. On the Decru Appliance Setup Wizard Step 1 of 12 (Welcome to the Decru Setup Wizard) screen, click Start.
4. On the Certificates screen, select whether to trust the certificate validating the connection between the appliance and the Management Console once or always.
5. On the Decru Appliance Setup Wizard Step 2 of 12 (Connect to Head of Cluster) screen, click Next.
6. On the Question screen, to continue with the remote authorization process, click Yes.
7. On the Decru Appliance Setup Wizard Step 10 of 12 (Introduce Recovery Cards) screen, insert a card into the card reader, enter the password and click Next.

Note: When a card is inserted into the reader, it is selected (green). At this point, enter the password and click the Verify Password button. Cards remain selected after removal.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

8. Close the Decru Appliance Setup Wizard Step 10 of 12 (Introduce Recovery Cards) screen, and notify the outstanding Recovery Officer(s) that it is safe to continue the Setup Wizard approval.

Note: When the last card is introduced, verify that the information entered for Decru Appliance Setup Wizard screens 5 through 10 of 12 are correct before proceeding.

9. On the Decru Appliance Setup Wizard Step 11 of 12 (Apply Settings) screen, click Next.
10. On the Decru Appliance Setup Wizard Step 12 of 12 (Wizard Completed Successfully) screen, click Finish.



■ ■ ■ ■ 5 GETTING STARTED

Use the Decru Management Console (DMC) to perform centralized management functions for the enterprise.

Note: If [SecureView™](#) is enabled the administrator can perform management functions on several appliances simultaneously.

This chapter includes the following topics:

- [Launching the Decru Management Console](#)
- [Adding Appliances to DMC](#)
- [Logging in to Appliances](#)
- [Using Menus and Displays](#)

LAUNCHING THE DECRU MANAGEMENT CONSOLE

- Select **Start > Programs > Decru > Decru Management Console**.

EXITING THE CONSOLE

To exit the console, select from the following methods:

- In the Decru Management Console, from the Appliance menu, select Exit.
- Click the close box at the upper right-hand corner of the console screen.
- Double click the DMC icon at upper left-hand corner of the console screen.

ADDING APPLIANCES TO DMC

This section contains the following topics:

- [Adding Appliances](#)
- [Adding Cluster Members](#)
- [Adding Linked Appliances](#)
- [Removing Appliances from DMC](#)

ADDING APPLIANCES

To add an appliance to DMC for the first time, see [Adding an Appliance for the First Time](#) on page 32.

1. In the Decru Management Console, from the Appliance menu, select Add.
2. On the Add screen, select from the following and click OK.
 - To add appliances by IP address or hostname, enter the IP address(es) or hostname(s) of the appliance(s) in the text box.
 - To add appliances by IP range, enter the start and end addresses of the IP range.
3. On the Certificates screen, select whether to trust the certificate validating the connection between the appliance and the Management Console once or always.

Note: If adding more than one appliance, a trust certificate will appear for each appliance added.

Once added, appliances appear in the console listed under Resources as either LKM, E-series, FC-series or Unknown. Appliances appear offline until log in.

ADDING CLUSTER MEMBERS

1. In the Decru Management Console, select a DataFort appliance.
2. From the Appliance menu, select Add Cluster Members.

Once added, appliances appear in the console listed under Resources as either E-series, FC-series or Unknown. Appliances appear offline until log in.

ADDING LINKED APPLIANCES

1. In the Decru Management Console, select an appliance.
2. From the Appliance menu, select Add Linked Appliances.
Once added, appliances appear in the console listed under Resources as either LKM, E-series, FC-series or Unknown. Appliances appear offline until log in.

REMOVING APPLIANCES FROM DMC

1. In the Decru Management Console, in the Resources pane, select an appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Appliance menu, select Remove.

LOGGING IN TO APPLIANCES

Log into initialized appliances that are added to DMC. See [Initializing an Appliance via the Setup Wizard](#) on page 32.

1. In the Decru Management Console, in the Resources pane, select an appliance.
 - Shift- or Ctrl-click to select multiple appliances when logging in to appliances sharing a common administrator name and password simultaneously.
2. From the Appliance menu, select Log in.
 - Or, right-click the appliance and select Log in.
3. On the Log in screen, enter the user name and password and click OK.

If the correct credentials were entered and the appliance is correctly configured, the status of the appliance changes to online. See [State Displays](#) on page 40.

For the LKM appliance to manage keys it must share keys with the DataFort appliance(s) that it will serve. See [Sharing Keys](#) on page 48.

SETTING PREFERENCES

1. In the Decru Management Console, in the Resources pane, select an appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Edit menu, select Preferences.
3. Click the Stay Logged In check box and choose the refresh duration (up to 20 minutes).

USING MENUS AND DISPLAYS

Use the Decru Management Console to manage appliances from a central location.

This section includes the following topics:

- [State Displays](#)
- [Using Table Columns](#)
- [About the Appliances Table](#)
- [Appliance Menu](#)
- [Edit Menu](#)
- [View Menu](#)
- [Configuration Menu](#)
- [Keys Menu](#)
- [Topology Menu](#)
- [Utilities Menu](#)
- [Security Menu](#)
- [Trustee Menu](#)
- [Diagnostics](#)
- [Help Menu](#)

STATE DISPLAYS

The condition of each appliance is indicated in the DMC with an icon in the Resources pane of the DMC screen. [Table 7](#) shows possible state displays for appliances in the Management Console.

TABLE 7: APPLIANCE STATUS INDICATORS

Icon	Icon Appearance	Appliance State
	Blue	There are four online states that change the appearance of the the appliance font: Online - black, Linked - black bold, Policy Grouped - blue bold
	Blue with yellow alert	Online with error—See About the Appliances Table on page 40. for status details.
	Gray with exclamation	Logged off—Administrator name and/or password is incorrect, or log in is timed out (this occurs after 30 minutes if inactive).
	Yellow with open icon	Not initialized—IP address is set, but setup wizard not completed.
	Red	Offline
	Gray	Not logged in

USING TABLE COLUMNS

When information in a tab is displayed in table, the table can be customized. See [About the Appliances Table](#).

- To sort the table by a column, click on a column title.
- To add/remove columns, right-click on a column title.
 - From the Column Editor screen, select to add and remove columns and click OK.

ABOUT THE APPLIANCES TABLE

Most of the tab views in DMC display information in table format. Additionally, a status bar at the bottom of the Appliance table displays status messages. See [Using Table Columns](#).

The Appliance table contains the following default columns:

- Appliance—Displays the appliance by name.
- Availability—Displays the appliance state.
- Front Panel LCD—Displays the contents of the LCD on the front of the appliance. Includes the appliance name, status or error messages, Number of Keys, and CPU Load.
- Type—Displays the appliance type.
- Version—Displays the appliance operating system version.
- Serial Number—Displays the appliance serial number.

APPLIANCE MENU

Log in	Log in to an appliance as an administrator. See Logging in to Appliances on page 38.
Log out	Log out of an appliance.
Add	Add an appliance. See Adding Appliances to DMC on page 37.
Add Cluster Members	Add a DataFort appliance cluster member to DMC. See Adding Cluster Members on page 37.
Add Linked Appliances	Add appliances linked to an LKM appliance to DMC. See Adding Linked Appliances on page 38.
Remove	Remove an appliance in the Management Console. See Removing Appliances from DMC on page 38.
Link Appliances	Enable policy based key sharing between two appliances, one of which must be an LKM. See How Keys are Shared on page 49.
Add OpenKey clients	Add and OpenKey client to DMC. See Adding OpenKey Clients to Key Sharing Groups on page 50.
Add LKM Software	Add Lifetime Key Management® Software (LKM Software) to a DataFort appliance to manage a DataFort appliance's keys. See Adding Lifetime Key Management® Software to DataFort appliances on page 80.
Linked Appliances	View details about appliance links, including key sharing group, in the Linked Appliances table. See About the Linked Appliances Table on page 61.
Cluster	See the DataFort Administration Guide .
Set up	Set up an appliance by using the Setup Wizard. See Using the Setup Wizard on page 33.
Reboot	Reboot the selected appliance. See Rebooting an Appliance on page 81.
Zeroize	Zeroize the selected appliance. See Zeroizing an Appliance on page 84.
Exit	Exit the Management Console. See Exiting the Console on page 37.

EDIT MENU

Copy	Copy a text entry.
Cut	Cut a text entry.
Paste	Paste a text entry.
Find	Search for text in the active pane of the Management Console. The search is not case sensitive.
Find Again	Find next instance of same search.
Preferences	Check the stay logged in button and select a refresh duration for the session. See Setting Preferences on page 38.

VIEW MENU

The View setting determines how appliances display in the Resources pane. The default setting organizes appliances by type. Change the view to organize the display according to network, type and subnet information. Select an option to sort by, and deselect options that are not desired. More than one option can be selected at once. Appliances will appear once in each sorted list.

All	List all appliances.
Type (default)	Display appliances sorted by type, including LKM appliance, FC-Series Appliance, E-Series Appliance and S-Series Appliance.
Subnet	Display appliances sorted by subnet.
Custom Groups	Displays custom UI groups.
Add Custom Groups	Add a custom appliance group to monitor appliances based on organizational hierarchies. See Creating Custom Appliance Groups on page 81.
Remove Custom Group(s)	Remove a custom appliance group. See Removing a Custom Group on page 81.
Remove from Custom Group	Remove an appliance from a custom appliance group. See Removing an Appliance from a Custom Group on page 81.
Refresh	Refresh the view of appliances.

CONFIGURATION MENU

Administrators

View and manage administrators.
See [Editing Administrator Permissions](#) on page 78.

Add Admin

Add an administrator.
See [Adding an Administrator](#) on page 77.

License

View licenses.
See [About the License Table](#) on page 74.

License Usage

Nothing shows up?

Add License

Add licenses.
See [Adding a License](#) on page 74.

Network

Update the hostname of the appliance, the IP address, and the netmask and gateway settings of an appliance.
See [Updating Network Settings](#) on page 84.

Failover

See the [DataFort Administration Guide](#).

SNMP Agent

Set Net-SNMP agent options.
See [Setting SNMP Options](#) on page 83.

Date/Time

Update the date, time and time zone settings of an appliance.
See [Updating Date and Time Settings](#) on page 84.

Log Configuration

Select a log configuration.
Alex is documenting
See [Setting Log Options](#) on page 82.

KEYS MENU

Parent Keys

View all Parent Keys known to LKM appliance.
See [Viewing Parent Keys](#) on page 64.

Parent Keys from LKM

Cryptainer Keys

View all Cryptainer keys stored in LKM. This presents a dialog for filtering Cryptainer keys (find by DataFort, creation date or containing Key ID). The first 300 keys matching the attributes are returned. The Next/Previous Page options retrieve more results.
See [Viewing Cryptainer Keys](#) on page 64.

Translate Keys

Translate Cryptainer keys that have been decrypted from one DataFort appliance's Parent Key and encrypted with another DataFort's Parent Key, so that for both DataFort appliances can access the Cryptainer.
See [Transferring Keys](#) on page 70.

Change Key Sharing Group for Appliance

Change a policy based key sharing group for DataFort appliances that are Trustees of an LKM appliance.
See [Changing Key Sharing Groups](#) on page 52.

Change Key Sharing Group for Keys New

See [Changing a Key Sharing Group for Keys](#) on page 52.

Move Unshared Keys into Key Sharing Group

Move unshared keys into a key sharing group.
See [Moving Unshared Keys into a Key Sharing Group](#) on page 53.

Make Key Archive

Create an archive of Parent keys for an LKM client. See [Archiving Parent Keys](#) on page 66.

Make Cryptainer Key Archive

Create an archive of Parent keys for a Cryptainer
See [Archiving Parent Keys](#) on page 66.

Export Keys

Exports key files to a local hard drive. The files can then be deleted from the LKM appliance, or imported back into an LKM appliance (the original or another one). Only key information is shared.
See [Exporting and Importing Keys](#) on page 69.

Import Keys

Imports key files that have been exported from another LKM appliance.
See [Exporting and Importing Keys](#) on page 69.

Key Recovery

Recovers key files in the rare event the LKM appliance and its peers are down.
See [Recovering LKM Appliance Keys](#) on page 100.

Purge Unused Keys

Purge unused Cryptainer keys from DataFort appliances.
See [Purging Unused Cryptainer Keys from DataFort appliances](#) on page 81.

TOPOLOGY MENU

See the *DataFort Administration Guide*.

UTILITIES MENU

Command Line	Open the CLI to run commands on selected appliances. See Using the Command Line Interface on page 90.
WebUI	See the <i>DataFort Administration Guide</i> .
Back up	Back up the configuration database of a DataFort or LKM appliance. See Backing Up an Appliance on page 80.
Back up appliances to LKM	Back up keys and configuration databases of all appliances linked to an LKM appliance to that LKM appliance. See Backing Up Appliances to LKM on page 80.
Back up appliances from LKM	Back up the most recent configuration database of all appliances backed up to an LKM appliance to a secondary location. See Backing Up Appliances from LKM on page 80.
Upgrade/Downgrade	Upgrade or downgrade an appliance. Perform upgrades and downgrades only after consulting Decru support. See Upgrading an Appliance on page 83.
Verify	Verify the validity of an upgrade package before upgrading. See Verifying an Upgrade Package on page 84.

SECURITY MENU

Smart Card Required	See Policy
Recovery Cards	View all Recovery Cards associated with an appliance. See Viewing Recovery Cards on page 85.
Recovery Cards from LKM	more . . .
Replace Recovery Officer	Replace Recovery Officers. See Replacing a Recovery Card on page 86.
Change Recovery Card Password	Borrow from DF
Smart Card Utilities	Reset a smart card and display card information. See Resetting Smart Cards on page 88.
Policy	Alex.
Defense	Alex
Certificates	Alex

TRUSTEE MENU

A trustee relationship between two appliances allows encryption keys to be shared between those appliances even if they have no Recovery Cards in common, and are not on the same network. Trustees send messages to establish a relationship before key sharing. The first message is the Trustee Establishment Package (TEP). The second message is the Trustee Acceptance Package (TAP).

Create Trustee Link	Create a Trustee relationship between two appliances. This allows the appliances to share key information. Both appliances must be selected. See Creating Key Sharing Groups on page 50.
Start Trustee Creation	Create trustee relationship. See Start Trustee Creation (Create TEP) on page 57.
Receive TEP	Allow selected appliance(s) to receive a Trustee Establishment Package. See Receive TEP on page 57.
Receive TAP	Allow selected appliance(s) to receive a Trustee Acceptance Package. See Receive TAP on page 59.
Unapproved Trustee List	Display list of trustees not yet approved (waiting to accept a TAP). See Delete Unapproved TAP Trustee on page 61.
Trustee List	Display list of trustees.

DIAGNOSTICS

Appliques to DF and LKM.

Details Show the system version for the selected appliance.

Log [more . . .](#)

Crypto [more . . .](#)

Storage [more . . .](#)

Sensor [more . . .](#)

Collect Tech Support Info Create a file containing information useful to technical support when troubleshooting for the selected appliance. The file is by default placed in the tech support folder of the Decru Management Console directory. See [Collecting Tech Support Info](#) on page 81.

HELP MENU

Help Contents Opens online help as a .pdf file for selected appliance type. The administrative guide for the selected appliance type will open.

About Show information about this version of the Management Console.



■ ■ ■ ■ 6 SHARING KEYS

This chapter includes the following topics:

- [How Keys are Shared](#)
- [Creating Key Sharing Groups](#)
- [Creating Trustee Relationships](#)
- [Creating Trustee Links](#)
- [Monitoring Trustee Links](#)

How Keys Are Shared

Keys are shared by using key sharing groups, by creating a trustee relationship between unrelated DataFort appliances, and by linking DataFort appliances to an LKM appliance and performing the key translation process. See [Table 8](#).

Note: Decru recommends using key sharing groups to share encryption keys between LKM clients. See [Deployment Scenarios](#) on page 17.

TABLE 8: HOW KEYS ARE SHARED

Key Sharing Method	Key Sharing Feature
Automatic	Key Sharing Groups Linking OpenKey clients to an LKM appliance allows third-party clients to use the LKM as a secure key management service and to form key sharing groups. DataFort appliances must form a trustee relationship with an LKM appliance before creating a key sharing group. This allows them to share keys without manually importing and exporting keys or going through the key translation process. See Automatic Key Sharing on page 17, Adding OpenKey Clients to Key Sharing Groups on page 50, Creating Trustee Relationships on page 54, and Adding DataFort Appliances to Key Sharing Groups on page 51. Requirement: A certificate package for each OpenKey client or a Recovery Card quorum for each DataFort appliance.
Manual	Trustee Relationships (DataFort only) Unrelated DataFort appliances may share keys by forming a long-term trustee relationship with each other. This allows appliances that reside in independent key domains to manually share keys by manually importing and exporting each key for each trustee. See Trustee Relationships on page 19, Creating Key Sharing Groups on page 50 and Importing and Exporting Keys between Trustees on page 92. Requirement: A Recovery Card quorum for each DataFort appliance. Key Translation Unrelated DataFort appliances that are linked to a shared LKM appliance may share keys by initiating a one-way key transfer. See Key Translation on page 19, Creating Trustee Links on page 61, and Transferring Keys on page 70. Requirement: Either a Recovery Card quorum or a Key Archive file for each DataFort appliance.

CREATING KEY SHARING GROUPS

LKM clients may form key sharing groups when linking to an LKM appliance. This allows group members to automatically share keys.

Note: DataFort appliances must form a trustee relationship with an LKM appliance before creating a key sharing group. This allows them to share keys without manually importing and exporting keys or going through the key translation process. See [How Keys are Shared](#) on page 49.

This section includes the following topics:

- [Adding OpenKey Clients to Key Sharing Groups](#)
- [Adding DataFort Appliances to Key Sharing Groups](#)
- [Changing Key Sharing Groups](#)

ADDING OPENKEY CLIENTS TO KEY SHARING GROUPS

Linking an OpenKey client to an LKM appliance allows third-party LKM clients to use the LKM as a secure key management service. To add an OpenKey Client to a key sharing group on an LKM appliance, a certificate package is required.

Note: OpenKey clients are not viewable in the Resources pane since they are added to an LKM appliance only and not to DMC. To view an OpenKey client, see [About the Linked Appliances Table](#) on page 61.

1. In the Decru Management Console, in the Resources pane, select an LKM appliance.
2. From the Appliance menu, select Add OpenKey clients.
3. On the Add OpenKey Client screen, enter the client IP address of the client.
4. In the Key Sharing Group combo box, type or select a group name.

The following options apply:

Appliances in ' ' can only see keys in ' '

Empty group can only see its keys.

Appliances in '/' can see all keys

Root can see all keys.

Appliances in '/x/' can only see keys in '/x/' but not in '/y/'

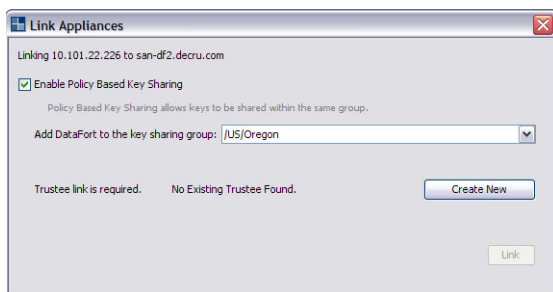
Key sharing group siblings cannot share keys, but child key sharing group members can share keys with parent groups '/'.

5. In the Path to Package text box, browse to or copy and paste the certificate package and click Apply.

ADDING DATAFORT APPLIANCES TO KEY SHARING GROUPS

DataFort appliances must form a trustee relationship with an LKM appliance before creating a key sharing group. This allows them to share keys without manually importing and exporting keys or going through the key translation process. See [Creating Trustee Relationships](#) on page 54.

1. In the Decru Management Console, in the Resources pane, select an LKM appliance.
 - Alternatively, drag and drop an appliance to an LKM appliance and skip to step 4.
2. From the Appliance menu, select Link Appliances.
3. From the Select an appliance to link screen, select an appliance and click OK.
4. On the Link Appliances screen, see that the Enable Policy-Based Key Sharing check box is selected.



5. In the Add DataFort to the key sharing group combo box, type or select a group name.
The following options apply:

Appliances in ' ' can only see keys in ' '

Empty group can only see its keys.

Appliances in '/' can see all keys

Root can see all keys.

Appliances in '/x/' can only see keys in '/x/' but not in '/y/'

Key sharing group siblings cannot share keys, but child key sharing group members can share keys with parent groups '/'.

6. Click Link.
7. On the Appliance Link screen, verify that a connection is established between the selected appliances and click OK.

CHANGING KEY SHARING GROUPS

View details about appliance links, including key sharing groups, in the Linked Appliances tab. See [Monitoring Trustee Links](#) on page 61.

To view key sharing groups

- [Changing Key Sharing Groups between OpenKey Clients](#)
- [Changing Key Sharing Groups between DataFort Appliances](#)
- [Changing a Key Sharing Group for Keys](#)
- [Moving Unshared Keys into a Key Sharing Group](#)

Changing Key Sharing Groups between OpenKey Clients

Should be UI command in v13.

Changing Key Sharing Groups between DataFort Appliances

1. In the Decru Management Console, in the Resources pane, click to select a DataFort appliance.
2. From the Configuration menu, select Change Key Sharing Group.
3. On the Change Key Sharing Group screen, in the Key Sharing Group combo box, type or select a group name.

The following options apply:

Appliances in ' ' can only see keys in ' '	Empty group can only see it's keys.
Appliances in '/' can see all keys	Root can see all keys.
Appliances in '/x/' can only see keys in '/x/' but not in '/y/'	Key sharing group siblings cannot share keys, but child key sharing group members can share keys with parent groups '/'.

4. Click Apply.

Changing a Key Sharing Group for Keys

Moving Unshared Keys into a Key Sharing Group

Would I do this if I changed the group for an appliance and still had keys backed up to LKM that needed to be moved?

1. In the Decru Management Console, in the Resources pane, click to select an LKM appliance.
2. From the LKM menu, select Cryptainer Keys.
3. On the Key Find screen, click one or more of the following check boxes to locate keys:

keys from:	Locates all keys for a specific DataFort. Selections contain the hostname of the appliance for reference.
key with ID containing:	Locates a key by partial key ID. The key ID identifies the encryption key. It is a global unique ID
key with creation dates after or before:	Locates a key by date.
key with descriptions containing:	Locates a key by partial description.
4. In the Cryptainer Keys table, select a key and right-click to select Change Key Sharing Group.
5. On the Change Key Sharing Group screen, in the Key Sharing Group combo box, type or select a group name.

The following options apply:

Appliances in ' ' can only see keys in ' '	Empty group can only see it's keys.
Appliances in '/' can see all keys	Root can see all keys.
Appliances in '/x/' can only see keys in '/x/' but not in '/y/'	Key sharing group siblings cannot share keys, but child key sharing group members can share keys with parent groups '/'.
6. Click Apply.

CREATING TRUSTEE RELATIONSHIPS

This section includes the following topics:

- [About Trustee Relationships between DataFort Appliances](#)
- [Creating Trustees using SecureView](#)
- [Creating Trustees Relationships without SecureView](#)

ABOUT TRUSTEE RELATIONSHIPS BETWEEN DATAFORT AND LKM APPLIANCES

DataFort appliances must form a trustee relationship with an LKM appliance before creating a key sharing group. This allows them to share keys without manually importing and exporting keys or going through the key translation process. See [Creating Key Sharing Groups](#) on page 50.

Note: A Recovery Card quorum for each DataFort appliance is required to setup.

ABOUT TRUSTEE RELATIONSHIPS BETWEEN DATAFORT APPLIANCES

Unrelated DataFort appliances may form a trustee relationship. This allows appliances that may not even be on the same network to share keys by manually importing and exporting each key for each trustee. See [Importing and Exporting Keys between Trustees](#) on page 92.

Note: A Recovery Card quorum for each appliance is required.

DataFort appliances that form a trustee relationships offer several enterprise solutions:

- | | |
|------------------------------|--|
| HQ with branches | Where there are many branch offices and it is preferable to share a different encryption key with each branch exclusively. |
| Vendors/Third parties | Where a vendor and supplier both have DataFort appliances. Data is protected via Cryptainers, but it is not desirable to share all keys. |

CREATING TRUSTEES USING SECUREVIEW

When enabled, create DataFort trustees using [SecureView](#)™ if both appliances are in the same local network.

Note: A Recovery Card quorum for each appliance is required for setup.

1. In the Decru Management Console, in the Resources pane, Shift- or Ctrl-click to select both appliances.
2. From the Trustee menu, select Create Trustee Link.
3. On the Trustee Setup screen, notice that both appliances appear and click Create Link. Edit the trustee label. By default it shows the hostname or IP address of the other appliance.
4. Select a method to authorize trustees:
 - To authorize trustees locally, see [Authorizing Trustees Locally](#) on page 55.
 - To authorize trustees using Remote Authorization, see [Initiating Remote Authorization to Approve TEP](#) on page 55.

Note: Both methods require using smart cards according to the recovery schema set for each appliance during initialization.

Authorizing Trustees Locally

1. On the Approve TEP (Trustee Establishment Package) screen, select from the following:
 - If you have multiple card readers, insert the quorum of cards into the readers, enter the passwords and click Start.
 - If you have a single card reader, select a quorum of cards from the Recovery Officers list, enter the passwords and click Start.

Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader, it is selected (green). Cards remain selected after removal. Enter the password and click the Verify Password button.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

2. On the Approve TAP (Trustee Acceptance Package) screen, select from the following:
 - If you have multiple card readers, insert a quorum of cards into the readers, enter the passwords and click Start.
 - If you have a single card reader, select a quorum of cards from the Recovery Officers list, enter the passwords and click Start.

Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader, it is selected (green). Cards remain selected after removal. Enter the password and click the Verify Password button.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

3. On the Trustee screen, a message appears indicating that the trustee is created, click OK.

Initiating Remote Authorization to Approve TEP

1. On the Approve TEP (Trustee Establishment Package) screen, select a quorum of cards from the Recovery Officers list and click Enable Remote Authorization.

Note: Previously entered data is saved locally, therefore Decru recommends that the Administrator initiating the remote authorization process be the last Recovery Card holder to supply a card.
2. When the Remote Authorization enabled message appears, close the Approve TEP screen.
3. Notify the Recovery Officer who will approve the TEP that it is safe to continue the TEP approval process and introduce Recovery Cards remotely. See [Authorizing TEP Approval Remotely](#) on page 56.

Authorizing TEP Approval Remotely

1. In the Decru Management Console, in the Resources pane, select both appliances.
2. From the Trustee menu, select Create Trustee Link.
3. On Approve TEP screen, insert a card into the card reader, enter the password and click Start.

Note: When a card is inserted into the reader, it is selected (green). At this point, enter the password and click the Verify Password button. Cards remain selected after removal.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

4. When the progress bar is complete, close the Approve TEP screen.
5. Notify the Recovery Officer(s) who will approve the TEP that it is safe to continue the TEP approval process.

Note: The last officer to supply a card, must initiate the TAP approval process. See [Initiating Remote Authorization to Approve TAP](#).

Initiating Remote Authorization to Approve TAP

1. In the Decru Management Console, in the Resources pane, select both appliances.
2. From the Trustee menu, select Create Trustee Link.
3. On the Approve TAP (Trustee Acceptance Package) screen, select a quorum of cards from the Recovery Officers list and click Enable Remote Authorization.
4. When the Remote Authorization enabled message appears, close the Approve TAP screen and notify the Recovery Officer(s) who will approve the TAP that it is safe to continue. See [Authorizing TAP Approval Remotely](#).

Authorizing TAP Approval Remotely

1. In the Decru Management Console, in the Resources pane, select both appliances.
2. From the Trustee menu, select Create Trustee Link.
3. On the Approve TAP screen, insert a card into the card reader, enter the password and click Start.

Note: When a card is inserted into the reader, it is selected (green). At this point, enter the password and click the Verify Password button. Cards remain selected after removal.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

4. When the progress bar is complete, close the Approve TAP screen.
5. Notify the Recovery Officer(s) who will approve the TEP that it is safe to continue the TEP approval process.

Note: The last officer to supply a card, must complete the TAP approval process by performing the last step.

6. On the Trustee screen, a message appears indicating that the trustee is created, click OK.

CREATING TRUSTEES RELATIONSHIPS WITHOUT SECUREVIEW

If both appliances are not on the same local network and SecureView is unavailable, follow the steps to create a trustee relationship.

Note: A Recovery Card quorum for each appliance is required for setup.

This section includes the following topics:

- [Start Trustee Creation \(Create TEP\)](#)
- [Receive TEP](#)
- [Receive TAP](#)
- [Delete Unapproved TAP Trustee](#)

Start Trustee Creation (Create TEP)

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Trustee menu, select Start Trustee Creation.
3. On the Start Trustee (Create TEP) screen, enter the following and click Create.
 - A Trustee Label or hostname for the appliance.
 - A Package Label or hostname for the package.
4. On the Select File screen, select a TEP file name and location and click Save.
5. From the Trustee menu, select Unapproved Trustee List.
6. On the Unapproved Trustee List tab, right-click the correct Trustee Label and select Copy Verifier.
7. Paste the verifier into a text file and save it.
8. Send the verifier file and the TEP file separately to the second appliance. See [Receive TEP](#).

Note: Communicate the verifier in a secure manner; by phone or direct contact rather than email. This is the only way to confidentially authenticate trustees for key sharing.

Receive TEP

To receive the TEP (Trustee Establishment Package), the second appliance needs the TEP file and verifier received from the first appliance. See [Start Trustee Creation \(Create TEP\)](#) on page 57.

Note: After receiving and approving the TEP, this process automatically creates the TAP (Trustee Acceptance Package).

1. In the Decru Management Console, in the Resources pane, select the second appliance.
2. From the Trustee menu, select Receive TEP
3. On the Receive TEP screen enter the following and click Begin Approval.
 - Browse to the path of the TEP file.
 - Paste the verifier.
 - A Trustee Label or hostname for the appliance.
 - A Package Label or hostname for the package.

4. Select a method to authorize trustees:

- To authorize trustees locally, see [Authorizing Trustees Locally to Receive TEP](#) on page 58.
- To authorize trustees using Remote Authorization, see [Initiating Remote Authorization to Receive TEP](#) on page 58.

Authorizing Trustees Locally to Receive TEP

1. On the Approve TEP (Trustee Establishment Package) screen, select from the following:

- If you have multiple card readers, insert the quorum of cards into the readers, enter the passwords and click Start.
- If you have a single card reader, select a quorum of cards from the Recovery Officers list, enter the passwords and click Start.

Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader, it is selected (green). At this point, enter the password and click the Verify Password button. Cards remain selected after removal.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

2. On the Select File screen, select a TAP file name and location and click Save.
3. From the Trustee menu, select Unapproved Trustee List.
4. On the Unapproved Trustee List tab, right-click the trustee and select Copy Verifier.
5. Paste the verifier into a text file and save it.
6. Send the verifier file and the TAP file separately to the first appliance.

Note: Communicate the verifier in a secure manner; by phone or direct contact rather than email. This is the only form of authentication for key sharing and is considered sensitive material.

Initiating Remote Authorization to Receive TEP

1. On the Approve TEP (Trustee Establishment Package), select a quorum of cards from the Recovery Officers list and click Enable Remote Authorization.

Note: Previously entered data is saved locally, therefore Decru recommends that the Administrator initiating the remote authorization process be the last Recovery Card holder to supply a card.

2. When the Remote Authorization enabled message appears, close the Approve TEP screen.
3. Notify the outstanding Recovery Officer that it is safe to continue the TEP approval process using the procedure to introduce Recovery Cards remotely. See [Authorizing TEP Reception Remotely](#).

Authorizing TEP Reception Remotely

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Trustee menu, select Receive TEP
3. On the Receive TEP screen, insert a card into the card reader, enter the password and click Start.

Note: When a card is inserted into the reader, it is selected (green). At this point, enter the password and click the Verify Password button. Cards remain selected after removal.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

4. On the Select File screen, select a TAP file name and location and click Save.
5. From the Trustee menu, select Unapproved Trustee List.
6. On the Unapproved Trustee List tab, right-click the trustee and select Copy Verifier.
7. Paste the verifier into a text file and save it.
8. Send the verifier file and the TAP file separately to the first appliance. [Receive TEP](#) on page 57.

Note: Communicate the verifier in a secure manner; by phone or direct contact rather than email. This is the only form of authentication for key sharing and is considered sensitive material.

Receive TAP

To receive the TAP (Trustee Acceptance Package), the first appliance needs the TAP file and verifier received from the second appliance. See [Receive TEP](#) on page 57.

1. In the Decru Management Console, in the Resources pane, select the first appliance.
2. From the Trustee menu, select Receive TAP
3. On the Receive TAP screen, browse to the TAP file and copy the verifier into the provided field.
4. Click Begin Approval.
5. Select a method to authorize trustees:
 - To authorize trustees locally, see [Authorizing Trustees Locally](#) on page 60.
 - To authorize trustees using Remote Authorization, see [Authorizing Trustee Remotely](#) on page 60.

Note: Both methods require using smart cards according to the recovery schema set for each appliance during initialization.

Authorizing Trustees Locally

1. On the Approve TAP screen, select from the following:

- If you have multiple card readers, insert the quorum of cards into the readers, enter the passwords and click Start.
- If you have a single card reader, select a quorum of cards from the Recovery Officers list, enter the passwords and click Start.

Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader, it is selected (green). At this point, you may enter the password and click the Verify Password button. Cards remain selected after removal.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

2. A message appears indicating the trustee is approved, click OK.

Note: When the first appliance approves the TAP, it is recommended they notify the second appliance so that they can [Delete Unapproved TAP Trustee](#).

Authorizing Trustee Remotely

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Trustee menu, select Receive TAP
3. On the Approve TAP screen, select a quorum of cards from the Recovery Officers list and click Enable Remote Authorization.

Note: Previously entered data is saved locally, therefore Decru recommends that the Administrator initiating the remote authorization process be the last Recovery Card holder to supply a card.

4. When the Remote Authorization enabled message appears, close the Approve TAP screen.
5. Notify the outstanding Recovery Officer(s) that it is safe to continue the TAP approval process using the procedure to introduce Recovery Cards remotely. See [Introducing Recovery Cards Remotely \(Receive TAP\)](#).

Introducing Recovery Cards Remotely (Receive TAP)

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Trustee menu, select Receive TAP
3. On the Approve TAP screen, insert a card into the card reader, enter the password and click Start.

Note: When a card is inserted into the reader, it is selected (green). At this point, you may enter the password and click the Verify Password button. Cards remain selected after removal.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

4. A message appears indicating the trustee is approved, click OK.

Note: When the first appliance approves the TAP, it is recommended they notify the second appliance so that they can [Delete Unapproved TAP Trustee](#).

Delete Unapproved TAP Trustee

Decru recommends that the first appliance approve the TAP before the second appliance deletes the unapproved TAP trustee. This retains a backup TAP trustee file until the process is complete. See [Receive TAP](#) on page 59.

1. In the Decru Management Console, in the Resources pane, select the second appliance.
2. From the Trustee menu, select Unapproved Trustee List.
3. On the Unapproved Trustee List tab, right-click the trustee and select Delete.

CREATING TRUSTEE LINKS

1. In the Decru Management Console, in the Resources pane, select an LKM appliance.
 - Alternatively, drag and drop an appliance to an LKM appliance and skip to step 4.
2. From the Appliance menu, select Link Appliances.
3. From the Select an appliance to link screen, select an appliance and click OK.
4. On the Link Appliances screen, unselect the Enable Policy-Based Key Sharing check box.
5. Click Link.
6. On the Appliance Link screen, verify that a connection is established between the selected appliances and click OK.

MONITORING TRUSTEE LINKS

Can we see OpenKey Links here?

This section contains the following topics:

- [About the Linked Appliances Table](#)
- [Viewing Appliance Links](#)

ABOUT THE LINKED APPLIANCES TABLE

Most of the tab views in DMC display information in table format. See [Using Table Columns](#) on page 40.

The Linked Appliances table contains the following default columns:

- From—Displays the appliance IP address of the appliance being linked from.
- To—Displays the IP address of the appliance being linked to.
- Status—Displays the link status. For example, Linked, Trusteed, Key Sharing Group or Link Broken.
- Key Sharing Group—Displays the key sharing group which is stored on the LKM appliance.
- Percent Complete—*what is this?*
- Last Complete—*what is this?*

VIEWING APPLIANCE LINKS

1. In the Decru Management Console, in the Resources pane, click to select an appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Appliance menu, select Linked Appliances. See [About the Linked Appliances Table](#) on page 61.

Removing an Appliance Link

1. In the Decru Management Console, in the Resources pane, click to select an appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Appliance menu, select Linked Appliances.
3. On the Linked Appliances table, click on a linked appliance and right click to select Remove.
See [About the Linked Appliances Table](#) on page 61.
4. In the Action (Remove link from selected appliance links) screen, in the Link(s) box, verify that the appliance links you selected are highlighted and click Apply.

7 MANAGING KEYS

The LKM appliance and the Management Console provide tools to manage keys in the enterprise. A search tool allows you to view and archive keys. You may also backup keys to external storage and perform a one-way key transfer between DataFort appliances when it is not possible to form a key sharing group between them. See [How Keys are Shared](#) on page 49.

The chapter includes the following topics:

- [Monitoring Keys](#)
- [Archiving Parent Keys](#)
- [Backing Up Keys to External Storage](#)
- [Transferring Keys](#)

MONITORING KEYS

This section includes the following topics:

- [About Parent and Cryptainer Key Tables](#)
- [Viewing Parent Keys](#)
- [Viewing Cryptainer Keys](#)

ABOUT PARENT AND CRYPTAINER KEY TABLES

Most of the tab views in DMC display information in table format. See [Using Table Columns](#) on page 40.

The Parent or Cryptainer key tables contain the following default columns:

- Key ID—Displays the primary ID of the key.
- Key Class—Displays the type of key contained in the key.
- Key Format—Displays the wrapping of the key. For example, plaintext, encrypted with Domain Key, etc.
- Key Description—Displays . . . ? *For Parent Keys?*
- Key Version—Displays changes in the key properties. *For Cryptainer Keys?*
- *What about OpenKeys???*

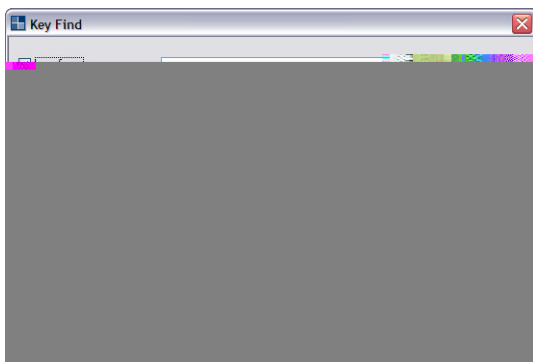
VIEWING PARENT KEYS

Are we going to do this? Being decided.

VIEWING CRYPTAINER KEYS

The Key Find window allows you to search and locate Cryptainer keys. If necessary, you can rename Cryptainer keys for easier identification. See [Assigning Names to Cryptainer Keys](#) on page 92.

1. In the Decru Management Console, in the Resources pane, select an LKM appliance.
2. From the Keys menu, select Cryptainer Keys.



3. On the Key Find screen, click one or more of the following check boxes to locate keys:

- | | |
|--|---|
| keys from: | Locates all keys for a specific DataFort. Selections contain the hostname of the appliance for reference. |
| key with ID containing: | Locates a key by partial key ID. The key ID identifies the encryption key. It is a global unique ID |
| key with creation dates after or before: | Locates a key by date. |
| key with descriptions containing: | Locates a key by partial description. |

4. After making your selections, click Find.

ARCHIVING PARENT KEYS

In the event that an LKM client unavailable, the LKM appliance uses a parent key archive to supply the keys needed to decrypt data. Selecting any of the parent keys for an LKM client archives all of the parent keys for that client. Selecting a Cryptainer key archives all of the parent keys for a DataFort Cryptainer key.

WARNING: BECAUSE THE PARENT KEY ARCHIVE COMPROMISES THE DISTRIBUTED SECURITY DESIGN OF THE SYSTEM AND DATAFORT RECOVERY CARDS, CREATE AND USE A KEY ARCHIVE FOR ONLY TWO PURPOSES: IMMEDIATE DATA RECOVERY IF AN LKM CLIENT IS NO LONGER FUNCTIONING, AND PLACEMENT IN KEY ESCROW OR ANOTHER FORM OF TRUSTED LONG-TERM STORAGE, FOR USE IN AN EMERGENCY. DELETE KEY ARCHIVES IMMEDIATELY AFTER USE OR UPON SUBMISSION TO ESCROW.

WARNING: GENERATE KEY ARCHIVES ON A SECURE WINDOWS PC THAT IS SCANNED FOR VIRUSES AND IS THOROUGHLY CHECKED FOR THE PRESENCE OF MALICIOUS CODE THAT COULD COMPROMISE THE SECURITY OF ENCRYPTED DATA. DECRU RECOMMENDS REBOOTING THE MANAGEMENT STATION AFTER CREATING ANY KIND OF KEY ARCHIVE.

This section includes the following topics:

- [About Parent Key Archives](#)
- [Creating Parent Key Archive Files](#)

ABOUT PARENT KEY ARCHIVES

TABLE 9: PARENT KEY ARCHIVES

Type	Details	Requirements
Archive of Parent Keys for an LKM client	Selecting any of the Parent keys for an LKM client archives all of the Parent Keys for that client.	One of the following is required: • A quorum of Recovery Officers and Recovery Cards for each DataFort. Each Recovery Officer is required to present a Recovery Card and its password. • A passphrase, the security administrator supplies when generating the Key Archive, to encrypt the Key Archive.
Archive of Parent Keys for a Cryptainer	Selecting a Cryptainer key archives all of the Parent keys for a DataFort Cryptainer key. This is useful when recovering data using Decru Data Decryption Software (DDS). See the Decru Data Decryption Software Administration Guide for details.	

CREATING PARENT KEY ARCHIVE FILES

1. In the Decru Management Console, in the Resources pane, select an LKM appliance.
Note: The LKM appliance must be linked to a DataFort appliance. See [Using Menus and Displays](#) on page 39.
2. From the Keys menu, select from the following:
 - Parent Keys
 - Cryptainer Keys (See [Monitoring Keys](#) on page 64.)**Note:** Selecting any of the Parent Keys for an LKM client archives all of the Parent Keys for that client. Selecting a Cryptainer Key archives all of the Parent Keys for a DataFort Cryptainer Key.
3. Select from the following:
 - On the Parent Keys tab, right-click the key you would like to archive and select Make Key Archive.
 - On the Cryptainer Keys tab, right-click the key you would like to archive and select Make Cryptainer Key Archive.
4. Select a method to create a key archive:
 - To use an archive file, see [Using an Archive File to Create a Parent Key Archive](#).
 - To use recovery cards, see [Using Recovery Cards to Create a Parent Key Archive](#) on page 68.

Using an Archive File to Create a Parent Key Archive

You can use a Key Archive file generated by a DataFort appliance (.ka file) or a Master Key Archive file generated by LKM server software (.mka file) to make a parent key archive.

1. On the Key Recovery screen, select Key Archive or Master Key Archive file and browse to the file, or enter the path and file name into the text box.
2. In the password text box, enter the password for the selected file, and click Recover.
3. When prompted, select a name and location for the key archive file.
4. Enter a password for the archive and click Save.

Note: Move the key file archive to escrow or secure long-term storage, making sure you store the passphrase as well.

WARNING: DELETE KEY ARCHIVES IMMEDIATELY AFTER USE OR UPON SUBMISSION TO ESCROW. DO NOT LEAVE ARCHIVE KEY FILES OPENLY ACCESSIBLE OR THEY MAY COMPROMISE THE SECURITY OF ENCRYPTED DATA.

Using Recovery Cards to Create a Parent Key Archive

1. On the Key Recovery screen, select Recovery Cards and click Recover.
2. On the Recover Secret Shares screen, select from the following:
 - If you have multiple card readers, insert a quorum of cards into the readers, enter the passwords and click Start.
 - If you have a single card reader, select a quorum of cards from the Recovery Officers list, enter the passwords and click Start.

When prompted, insert the requested card into the reader and click Start.

Repeat until all cards are processed.

Note: When a card is inserted into the reader, it is selected (green). At this point, you may enter the password and click the Verify Password button. Cards remain selected after removal.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

3. When prompted, select a name and location for the key archive file.
4. Enter a password for the archive and click Save.

Note: Move the key file archive to escrow or secure long-term storage, making sure you store the passphrase as well.

WARNING: DELETE KEY ARCHIVES IMMEDIATELY AFTER USE OR UPON SUBMISSION TO ESCROW. DO NOT LEAVE ARCHIVE KEY FILES OPENLY ACCESSIBLE OR THEY MAY COMPROMISE THE SECURITY OF ENCRYPTED DATA.

BACKING UP KEYS TO EXTERNAL STORAGE

This section includes the following topics:

- [About Exporting and Importing Keys](#)
- [Exporting and Importing Keys](#)

ABOUT EXPORTING AND IMPORTING KEYS

You may export and import both Parent Keys and Cryptainer Keys when backing up keys from the LKM appliance to external storage. This is useful if you do not have a redundant topology and you must rely on manually exporting keys to external storage to regularly back them up.

Note: In the rare event that the key database gets corrupted on the LKM appliance, it is not possible to manually back up keys from the LKM appliance to a key export file. In this case, the LKM appliance has a second database of keys on its hard drives containing the last one million keys to use when recovering keys that have not been manually backed up. To insure a complete key recovery, Decru recommends limiting keys that have not been manually backed up to less than one million. See [Recovering LKM Appliance Keys](#) on page 100.

EXPORTING AND IMPORTING KEYS

Note: When importing keys, if you have LKM key administrator permissions, you must request that LKM administrator temporarily change the `lkm.appliance.key.allow_unsigned_add` property to true.

1. In the Decru Management Console, in the Resources pane, select an LKM appliance.
2. From the Keys menu, select Export Keys or Import Keys.
3. On the Select Directory screen, select a folder location and click Select.

A message prompt notifies you of the number of keys currently exported or imported from the total number of keys available for export or import.

4. To pause the export or import at any time, click the Cancel button.

Note: You may resume this procedure, picking up where you left off at anytime, by selecting the same appliance and export or import folder. Any new keys added to the LKM between pausing and resuming the key export or import are added to the total number of keys available for export or import in the progress bar. This is also useful when you want to incrementally export and import new keys only.

TRANSFERRING KEYS

Trustee links formed between DataFort appliances and an LKM appliance outside of a key sharing group allow DataFort appliances to share keys by performing a one-way key transfer. The LKM appliance enables the DataFort appliance receiving the keys to decrypt data encrypted by the DataFort sending the keys. This does not disable Cryptainer Keys from the source DataFort.

See [Manual Key Sharing](#) on page 19 and [Creating Trustee Links](#) on page 61.

Note: Either a Recovery Card quorum or a Key Archive file for each appliance is required. Additionally, if you have LKM key administrator permissions, you must request that LKM administrator temporarily change the `lkm.appliance.key.allow_unsigned_add` property to true to transfer Cryptainer keys. See [Managing Administrators](#) on page 75.

This section includes the following topics:

- [About Key Transfers](#)
- [Transferring Cryptainer Keys](#)

ABOUT KEY TRANSFERS

Key transfers allows administrators to share Cryptainer keys that are decrypted from one DataFort's Parent Key and encrypted with another DataFort's Parent Key.

There are two possible scenarios:

**Transferring Keys
between DataFort
appliances**

The LKM appliance transfers keys between linked DataFort appliances. The LKM appliance transfers a key from one DataFort to the other. Keys travel over the peer link between the LKM appliance and each of the DataFort appliances.

**Transferring Keys
between DataFort
clusters**

Within the LKM appliance, keys are available for transfers between DataFort appliances only if there is a prior peer link between both appliances and the LKM appliance that is performing the key transfers, or if there is a prior peer link between the LKM appliances supporting both DataForts.

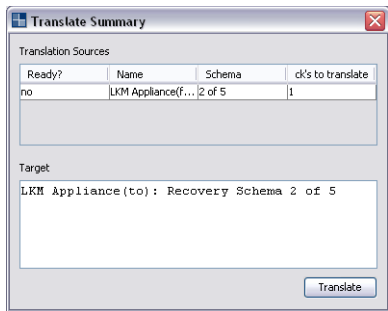
TRANSFERRING CRYPTAINER KEYS

WARNING: TRANSFER CRYPTAINER KEYS ON A SECURE WINDOWS PC THAT IS SCANNED FOR VIRUSES AND IS THOROUGHLY CHECKED FOR THE PRESENCE OF MALICIOUS CODE THAT COULD COMPROMISE THE SECURITY OF ENCRYPTED DATA. AFTER A KEY TRANSFER, CLEARTEXT KEYS ARE ZEROIZED IN RAM.

1. In the Decru Management Console, in the Resources pane, select the LKM appliance.
2. From the Keys menu, select Cryptainer Keys. See [Creating Parent Key Archive Files](#) on page 67.
3. On the Cryptainer Keys tab, right-click the key you would like to distribute (share), and select Translate Key(s).
 - To select more than one key, Ctrl-click and then right-click.



4. On the Select a Destination Key screen, highlight a destination key for the target appliance and click OK.



5. On the Translate Summary screen, review the translation activity and if correct, click Translate.
6. Select a method to recover keys:
 - [Using an Archive File to Transfer Cryptainer Keys](#)
 - [Using Recovery Cards to Transfer Cryptainer Keys](#)

Using an Archive File to Transfer Cryptainer Keys

You can use a Key Archive file generated by a DataFort appliance (.ka file) or a Master Key Archive file generated by LKM server software (.mka file) to distribute Cryptainer keys.

1. On the Prepare Source DataFort Appliance (from) screen, select Key Archive or Master Key Archive file.
2. Click the Select ka or Select mka button to browse for the file, or enter the path and file name into the text box.
3. In the password text box, enter the password for the selected file, and click Recover.
4. When prompted, select a name and location for the file.
5. Enter a password for the archive and click Save.
6. On the Prepare Target DataFort screen, select a method to recover keys.
7. A message appears indicating the number of keys successfully distributes, click OK.

Using Recovery Cards to Transfer Cryptainer Keys

1. On the Prepare Source DataFort Appliance (from) screen, select Recovery Cards and click Recover.
2. On the Recover Secret Shares screen, select from the following:
 - If you have multiple card readers, insert a quorum of cards into the readers, enter the passwords and click Start.
 - If you have a single card reader, select a quorum of cards from the Recovery Officers list, enter the passwords and click Start.When prompted, insert the requested card into the reader and click Start.
Repeat until all cards are processed.

Note: When a card is inserted into the reader, it is selected (green). At this point, you may enter the password and click the Verify Password button. Cards remain selected after removal.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

3. When prompted, select a name and location for the file.
4. Enter a password for the archive and click Save.
5. On the Prepare Target DataFort screen, select a method to recover keys.

WARNING: A message appears indicating the number of keys successfully distributes, click OK.



■ ■ ■ ■ 8 MANAGING APPLIANCES

Use the Decru Management Console to manage appliances including administrators and licenses.

Note: If [SecureView™](#) licenses are enabled, management functions are available to appliances simultaneously.

The chapter includes the following topics:

- [Managing Licenses](#)
- [Managing Administrators](#)
- [Managing Appliances](#)
- [Managing Smart Cards](#)

MANAGING LICENSES

This section includes the following topics:

- [About the License Table](#)
- [Adding a License](#)

ABOUT THE LICENSE TABLE

Most of the tab views in DMC display information in table format. See [Using Table Columns](#) on page 40.

The License table contains the following default columns:

- License ID—*Displays*
- Is Valid—*Displays*
- Serial Number—*Displays*
- Expiration—*Displays*
- Feature—*Displays*
- Quantity—*Displays*

ADDING A LICENSE

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, select Add License.
 - If adding site-wide license, apply the same license for each DataFort.
3. On the Add License screen, in the License ID field, enter the license and click Apply.

Deleting a License

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Configuration menu, select License.

On the License tab, all known licenses for the selected appliance(s) appear. See [Managing Administrators](#).

 - To remove a license, right-click the license and select Delete.

MANAGING ADMINISTRATORS

There are three administrator roles used to define administrative permissions; Read-Only, Specialty and Full Admin.

This section includes the following topics:

- [About Administrators and Recovery Officers](#)
- [About Administrator Roles](#)
- [About the Administrators Table](#)
- [Adding an Administrator](#)
- [Modifying Administrators](#)

ABOUT ADMINISTRATORS AND RECOVERY OFFICERS

There are two types of trusted individuals responsible for the security of the appliance: Administrators and Recovery Officers.

Administrators Administrators have varying degrees of privilege depending on their role. A Full Administrator can complete all operations necessary to set up, manage and maintain the system, while other administrators may execute a limited set of specific functions.

Recovery Officers A Recovery Officer retains an initialized Recovery Card after appliance setup is complete. Each Recovery Officer is authenticated by a Recovery Card and its associated password. A set minimum of Recovery Officers must be present with their associated cards in order to complete sensitive operations such as data recovery and cluster formation.

ABOUT ADMINISTRATOR ROLES

There are three administrator roles used to define administrative permissions; Read-Only, Specialty and Full Admin. Every administrator is authenticated with a login name and password. Additionally, administrators can be authenticated with physical possession of an Admin Card.

Read-Only	Allow read-only permissions.
Specialty	Create an administrator with limited permissions.
Full Admin	Allow full administrative permissions.

About Specialty Administrators

A Full Administrator can assign select permissions to a Specialty Administrator. While they can be created for LKM appliances, Specialty Admins are mainly used for DataFort management, supporting task specialization for increased security. See the [DataFort Administration Guide](#) for more information about special administrator roles.

TABLE 10: SPECIAL ADMIN TYPES

Admin Type	Responsibility	Appliance Type
Key Admin	Apply security-related settings.	DataFort and LKM
Security Admin	Apply physical security-related settings.	DataFort and LKM
Accounts Admin	Add, delete and manage administrators.	DataFort and LKM
Storage Admin	Manage hosts/clients and storage to create Cryptainers.	DataFort
Backup Admin	Manage backups of configuration and key databases.	DataFort and LKM
Machine Admin	Manage system properties and non-security sensitive cluster operations. Change local network settings.	DataFort and LKM

ABOUT THE ADMINISTRATORS TABLE

Most of the tab views in DMC display information in table format. See [Using Table Columns](#) on page 40, and [Editing Administrator Permissions](#) on page 78.

The Administrators table contains the following default columns:

- Username—Displays the username of the administrator.
- Role—Displays the administrative roles associated with the administrator.
- Card Associated—Displays if an Admin Card is associated with the administrator.

Right-Click Options

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, select Administrators.
3. On the Administrators tab, select an administrator from the table and right-click to perform the following actions:

See [About the Administrators Table](#).

- To add an Admin Card to an administrator, see [Adding an Admin Card to an Administrator](#) on page 87.
- To remove an Admin Card from an administrator, see [Removing an Admin Card from an Administrator](#) on page 87.
- To move an Admin Card to an administrator, see [Sharing an Admin Card](#) on page 87.
- To change administrator permissions, see [Editing Administrator Permissions](#) on page 78.
- To change a password for an administrator, see [Changing an Administrator Password](#) on page 79.

- To delete an administrator, see [Deleting an Administrator](#) on page 79.

ADDING AN ADMINISTRATOR

Add administrators to any LKM appliance in the Management Console. Full Administrators can perform all administration tasks.

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, select Add Admin.

Add Admin

Add administrator for selected appliances

Username:

Password:

Confirm Password:

Role:

- ☐ Read Only
- ☒ Specialty
- ☐ Full Admin

Specialty Role:

- ☐ Key
- ☐ Security
- ☐ Accounts
- ☐ Storage
- ☐ Backup
- ☐ Machine

Full Name:

Login:

- ☒ Direct
- ☐ Requires Prior Authorization

Items in **bold** are required.

3. On the Add Administrator screen, enter the username and password of the administrator.
4. Select from the following administrator roles:
 - Select Read-only to create an administrator with read-only permissions.
 - Select Specialty and then check any of the Specialty Roles to create an administrator with limited permissions. See [About Administrator Roles](#) on page 75.
 - Select Full Admin to create an administrator with full permissions.
5. Enter the Full name and select from the following Login options:
 - Select Direct to allow the administrator to log in without authorization.

- Select Requires Prior Authorization to pre-authorize an administrator's log in.

Note: Any Full Admin who can log in without authorization can grant any administrator the right to log in. See [Authorizing an Administrator Log In](#) on page 93.

6. Click Apply.

MODIFYING ADMINISTRATORS

Administrator options are available by right-clicking on the Administrator tab. See [Right-Click Options](#) on page 76.

The section contains the following topics:

- [Editing Administrator Permissions](#)
- [Changing an Administrator Password](#)
- [Deleting an Administrator](#)

Editing Administrator Permissions

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, select Administrators.
3. On the Administrators tab, select an administrator from the table and right-click to select Edit.
4. On the Edit Administrator screen, select from the following administrator roles:
 - Select Read-only to create an administrator with read-only permissions.
 - Select Specialty and then check any of the Specialty Roles to create an administrator with limited permissions. See [About Administrator Roles](#) on page 75.
 - Select Full Admin to create an administrator with full permissions.
5. Enter the Full name and select from the following Login options:
 - Select Direct to allow the administrator to log in without authorization.
 - Select Requires Prior Authorization to pre-authorize an administrator's log in.

Note: Any Full Admin who can log in without authorization can grant any administrator the right to log in. See [Authorizing an Administrator Log In](#) on page 93.
6. Click Apply.

Changing an Administrator Password

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, select Administrators.
3. On the Administrators tab, select an administrator from the table and right-click to select Change Password.
4. On the Change Password screen, enter the current password, new password and confirm the new password of the administrator.

Deleting an Administrator

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, select Administrators.
3. On the Administrators tab, right-click an administrator from the table and select Remove.
 - Shift-click and then right-click to multi-select.

MANAGING APPLIANCES

This section includes the following topics:

- [Adding Lifetime Key Management® Software to DataFort appliances](#)
- [Collecting Tech Support Info](#)
- [Creating Custom Appliance Groups](#)
- [Purging Unused Cryptainer Keys from DataFort appliances](#)
- [Rebooting an Appliance](#)
- [Setting Log Options](#)
- [Setting SNMP Options](#)
- [Updating Network Settings](#)
- [Viewing Appliance Details](#)
- [Zeroizing an Appliance](#)

ADDING LIFETIME KEY MANAGEMENT® SOFTWARE TO DATAFORT APPLIANCES

Adding Lifetime Key Management® Software (LKM Software) to a DataFort appliance allows the manage a DataFort appliance's keys from the LKM Software client.

1. In the Decru Management Console, in the Resources pane, select a DataFort appliance.
2. From the Appliance menu, select Add LKM Software.
3. On the Add LKM Software screen, enter the IP address of the client and click Apply.
 - Optionally, enter the client port and password.

BACKING UP THE CONFIGURATION DATABASE MANUALLY

You may back up both the LKM and the DataFort appliance configuration databases. However, an LKM appliance may access only the last backup of the configuration database for any DataFort appliance it is linked to.

This section includes the following topics:

- [Backing Up an Appliance](#)
- [Backing Up Appliances to LKM](#)

Backing Up an Appliance

Back up the configuration database of a DataFort or LKM appliance.

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Utilities menu, select Back Up.
3. On the Select File screen, select a location for the file and click Save.

Backing Up Appliances to LKM

Back up keys and configuration databases of all appliances linked to an LKM appliance to that LKM appliance.

1. In the Decru Management Console, in the Resources pane, select an DataFort appliance.
2. From the Utilities menu, select Back up appliances to LKM.
3. On the Select Directory screen, select a location for the folder and click Save.

Backing Up Appliances from LKM

Back up the most recent configuration database of all appliances backed up to an LKM appliance to a secondary location.

1. In the Decru Management Console, in the Resources pane, select an LKM appliance.
2. From the Utilities menu, select Back up appliances from LKM.
3. On the Select Directory screen, select a location for the folder and click Save.

COLLECTING TECH SUPPORT INFO

To assist Decru Technical Support in evaluating a problem, run a script on the selected appliance.

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Diagnostics menu, select Collect Tech Support Info.
3. Select a location for the file and click Save.

CREATING CUSTOM APPLIANCE GROUPS

Custom appliance groups are useful when quickly accessing or monitoring appliances based on organizational hierarchies.

1. In the Decru Management Console, from the Appliance menu, select Add Group.
You can add nested groups within custom groups.
2. On the Input screen, type in a group name and click Ok.
3. In the resources pane, select an appliance.
 - Shift-click to select multiple appliances.
4. Drag the appliance icon(s) into the group.

Removing an Appliance from a Custom Group

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Appliance menu, select Remove from Group(s).
3. In the Remove Selected Appliance(s) from Group screen, click Yes.

Removing a Custom Group

1. In the Decru Management Console, in the Resources pane, select an appliance group or nested group.
2. From the Appliance menu, select Remove Group(s).
3. In the Remove Groups screen, click Yes.

PURGING UNUSED CRYPTAINER KEYS FROM DATAFORT APPLIANCES

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Key menu, select Purge Unused Keys.
3. In the Purge Unused Keys from Database screen, click Yes.
4. The Performing Action screen appears, and a message that the action completed successfully appears at the bottom of the Appliance tab.

REBOOTING AN APPLIANCE

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.

2. From the Appliance menu, select Reboot.

SETTING LOG OPTIONS

Appliances log events in three categories; Security, Operations and Performance. Within each category, there are priority levels. Elect to store DataFort log information (according to category and priority level) in one or more of these possible locations:

- Temporary (RAM inside DataFort)
- Database (DataFort configuration database)
- Remote Logging Host (remote syslog server)
- Event Log Host (remote event log server)

Note: Decru recommends that logs be stored in more than one location.

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Configuration menu, select Log Configuration.

The screenshot shows the 'Logging Configuration' window. At the top, it says 'Decru recommends storing critical logs in a permanent, remote location.' Below this is the 'Windows Event Log User' section with fields for Domain, Username, Password, and Confirm Password, and a checkbox for 'Modify Event Log User'. The main configuration area has a header row with 'Temporary Database', 'Remote Logging Host', 'Event Log Host', and 'Signed'. It is divided into three sections: 'Security' with 'Low (6)' and 'High (4)' priority levels, 'Operations' with 'Trace (7)' and 'Information (6)' priority levels, and 'Performance' (partially visible). Each priority level has checkboxes for the four storage locations and input fields for the Remote Logging Host and Event Log Host.

	Temporary Database	Remote Logging Host	Event Log Host	Signed
Security				
Low (6)	☐	☒		
High (4)	☐	☒		
Operations				
Trace (7)	☒	☐		
Information (6)	☐	☒		
Performance				

3. On the Logging Configuration screen, select the desired settings and click Apply.

Note: For instruction on Windows event logging, see the [DataFort Administration Guide](#).

Setting SNMP Options

Decru uses Net-SNMP agent with the following protocols:

- MD5/SHA authentication and DES/AES privacy protocols
- SNMPv3 queries (GET, WALK) using MD5 as the authentication protocol and DES as the privacy protocol

Note: Decru does not support sending SNMPv3 traps.

For more information, see [DataFort Appliance SNMP Alarms Reference Guide](#).

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Configuration menu, select SNMP Agent.
3. On the SNMP Agent screen, enable or disable SNMP for the appliance.
4. Enter the following:

System

- System—Enter the location of and contact person for the SNMP agent.

Trap

- Host and Community—Enter the destination host IP address and the SNMP community name to send with the trap.

Version: SNMPv1/v2c

- Read Community—A single read-only community string may be configured for SNMPv1 and SNMPv2.

SNMPv3

- Optional, check if you would like to send queries using SNMPv3.
- Username and Password—A single user and password can be configured for SNMPv3.

UPGRADING AN APPLIANCE

Each upgrade package comes with its own set of instructions from Decru. Download the provided software package to the Management Station and complete the steps outlined in the upgrade instruction packet. See [Verifying an Upgrade Package](#) on page 84.

Note: While the appliance is being upgraded, there is a small window of time during which the appliance's intrusion detection is disabled. Upgrades should only be performed when the administrator can maintain physical security of the appliance.

Note: To prevent upgrades from failing, Decru recommends selecting the Stay login option in DMC, otherwise the upgrade session may expire before it is complete. See [Setting Preferences](#) on page 38.

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Utilities menu, select Upgrade.

3. Browse to the upgrade file.
4. Select if you would like to zeroize the appliance or not and click Apply.
5. When prompted enter the user name and password for the appliance and click Ok.
6. In the Upgrade Successful screen, click Ok.

Verifying an Upgrade Package

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Utilities menu, select Verify.
3. Browse to the upgrade file and click Apply.
Note: After the package is verified, the hash will display in an screen allowing you to verify the hash number with the known valid hash number.
4. Copy and paste this number into a text editor and click Ok to close the screen.

UPDATING DATE AND TIME SETTINGS

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Configuration menu, select Date/Time.
3. On the Date/Time screen, update the date, time and time zone settings and click Next.
4. Click Apply.

UPDATING NETWORK SETTINGS

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Configuration menu, select Network.
3. On the Network screen, update the hostname of the appliance, the IP address of the appliance, and the netmask and gateway settings and click Next.
4. Click Apply.

VIEWING APPLIANCE DETAILS

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Appliance menu, select Details.
3. The system version command runs in the CLI and the output displays.

ZEROIZING AN APPLIANCE

Zeroizing an appliance erases and invalidates all encryption keys and configuration data in the system. After zeroizing, you must run the Setup Wizard. See [Using the Setup Wizard](#) on page 33.

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Appliance menu, select Zeroize.
3. On the Zeroize screen, select whether to keep the appliance's IP Address.
4. Enter the confirmation code listed on the screen (ZeroizeYes) and click Apply.

MANAGING SMART CARDS

Three types of smart cards are shipped with every appliance: the System Card, Admin Card and Recovery Cards.

This section includes the following topics:

- [About Smart Cards](#)
- [Viewing Recovery Cards](#)
- [Replacing a Recovery Card](#)
- [Adding an Admin Card to an Administrator](#)
- [Sharing an Admin Card](#)
- [Resetting Smart Cards](#)

ABOUT SMART CARDS

The appliance incorporates smart cards into network management, backup and recovery procedures. This provides a second layer of authentication beyond username and password credentials. Decru supplies a smart card reader and software that convert a Windows PC into a Management Station, providing a dock for the smart cards.

Three types of smart cards are shipped with every appliance: the System Card, Admin Card and Recovery Cards.

System Card

Each appliance has a unique System Card that is used to handle key data. The System Card is required for the appliance to boot and provides physical security for the appliance.

Admin Card

The Admin Card authenticates communication between the administrator and appliance.

Recovery Cards

Recovery Cards are used in sets to restore encrypted data or appliances, and to replace other smart cards. Each Recovery Card belongs to a Recovery Officer, who is a highly trusted individual in the organization. Officers must present cards and passwords before any sensitive procedures can be performed.

VIEWING RECOVERY CARDS

1. From the Security menu, select Recovery Cards.
2. On the Recovery Cards tab, right-click on a row to change the password of a card.

Note: Password changes require using Recovery Card.

3. Click on a column to order keys by that column.
 - To add and remove columns, right-click on a column title, from the Column Editor screen, select to add and remove columns and click OK.

REPLACING A RECOVERY CARD

This option replaces the Recovery Card and its associated Recovery Officer.

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Security menu, select Replace Recovery Officer.

The screenshot shows a Windows-style dialog box titled "Replace Recovery Card". It is divided into three numbered sections. Section 1, "1. Select a Recovery Card to Remove", features a list box containing five email addresses: "Jim@Finance", "Alan@Finance", "Bob@Finance", "Cecilia@Legal", and "Warren@Legal". Section 2, "2. Identify replacement Recovery Card", contains two text input fields labeled "Card Label" and "Security Domain". Below these fields is a "Select" button and the text "Current Selection: None". Section 3, "3. Authorize Replacement with Quorum of Recovery Cards", contains an "Authorize" button.

3. On the Replace Recovery Card screen, click to select the card that will be replaced.
4. Insert the card that will replace the deleted card into the card reader and click Select, then click Authorize.

Note: The next steps require that the minimum number of Recovery Officers, responsible for the Recovery Cards used to initialize this appliance, be prepared to enter Card Label and password information into the provided fields.

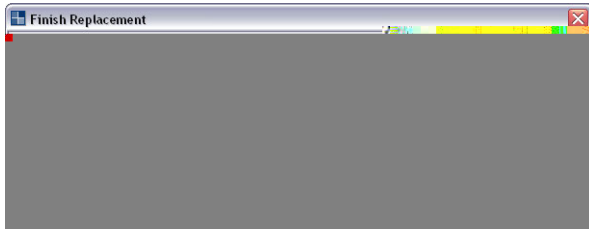
5. On the Authorize Recovery Card Replacement screen, select from the following:
 - For multiple card readers, insert a quorum of cards into the readers, enter the passwords and click Start.
 - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the passwords and click Start.

When prompted, insert the requested card into the reader and click Start.

Repeat until all cards are processed.

Note: When a card is inserted into the reader, it is selected (green). At this point, enter the password and click the Verify Password button. Cards remain selected after removal.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.



6. On the Finish Replacement screen, insert the replacement card and enter the Card Label, security domain and password and click Add Card.
 - If the card is already initialized, enter the security domain and/or password only and click Add Card.

A message appears stating that the card has been replaced successfully.

7. Click OK.

ADDING AN ADMIN CARD TO AN ADMINISTRATOR

After adding an Admin Card to an administrator you may share it with one or more administrators. See [Sharing an Admin Card](#) on page 87.

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Security menu, select Administrators.
3. On the Administrators tab, right-click an administrator and select Add Admin Card.
4. On the Add Admin Card screen, insert the Admin Card into the Management Station's card reader and click Apply.

Note: Smart cards must be fully inserted into the reader. If a card is not recognized, re-insert it for better contact.

5. On the Question screen, select to turn on Secure Login or not.
 - To verify that the Admin Card is added to an administrator, on the Administrator tab, notice that the Card Associated column is set to y (yes).

Removing an Admin Card from an Administrator

1. On the Security tab, right-click an administrator and select Remove Admin Card.
2. On the Remove Admin Card screen, select an appliance and click Apply.

SHARING AN ADMIN CARD

1. In the Decru Management Console, in the Resources pane, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Security menu, select Administrators.
3. On the Administrators tab, right-click an administrator and select Move Admin Card To.

4. On the Move Admin Card To screen, select an appliance and a user and click Apply.
 - To verify that the Admin Card is added to an administrator, on the Administrator tab, notice that the Card Associated column is set to y (yes).

RESETTING SMART CARDS

Resetting smart cards, erases username and password settings.

1. In the Decru Management Console, from the Security menu, select Smart Card Utilities.
2. At the zeroize Smart Cards screen, insert the card to be reset.
 - Clicking the Manufacturing Info button shows Smart Card factory details.
3. Click Zeroize for each card.
4. Agree to zeroize key material for the smart card by clicking Yes.

The card state changes to New.
5. Remove the card and close the window.

■ ■ ■ ■ 9 USING LKM CLI COMMANDS

This chapter contains CLI commands that cannot be completed using the Decru Management Console menus. See the [DataFort Administration Guide](#) for instructions on using the Command Line Interface (CLI) to manage DataFort appliances.

The chapter includes the following topics:

- [Using the Command Line Interface](#)
- [Managing DataFort Appliances Linked to LKM](#)
- [Managing SNMP](#)
- [Viewing System Properties](#)
- [Changing Backup Intervals](#)
- [Assigning Names to Cryptainer Keys](#)
- [Importing and Exporting Keys between Trustees](#)
- [Authorizing an Administrator Log In](#)
- [Checking the Status of an LKM appliance](#)
- [Checking the Connectivity Status Between Appliances](#)
- [Clearing Intrusion Alerts](#)
- [Shutting Down an LKM appliance](#)

USING THE COMMAND LINE INTERFACE

1. In the Decru Management Console, in the Resources pane, select an appliance.
Note: Selecting more than one DataFort appliance disables the command line option.
2. From the Utilities menu, select Command Line.
3. On the Command Line tab, enter the command into the command field.
 - Click Execute to execute the command. The command will be run on the selected appliance and the output returned on the screen.
 - Click File to open a command file to run on the selected appliance. The commands will run when the file is opened.
 - Click Save to save the output of the command to a file.
 - Click the check box to save the command to a .zip file.

MANAGING DATAFORT APPLIANCES LINKED TO LKM

If a member of a DataFort cluster that is linked to LKM is replaced, you must sever the link between the DataFort appliance cluster member and LKM via the CLI.

Note: The Decru Management Console is the only method for linking LKM and DataFort appliances. See [Importing and Exporting Keys between Trustees](#) on page 92.

To sever the link between the DataFort appliance cluster member and LKM:

1. Select the LKM appliance in DMC and access the CLI.
2. At the CLI, run the following commands:
 - To list all appliances linked to the LKM appliance:
`lkm server list`
 - To sever the link between the DataFort appliance cluster member and LKM:
`lkm server remove <IP of DataFort appliance>`
3. Select the DataFort appliance in DMC and access the CLI.
4. At the CLI, run the following commands:
 - To list all appliances linked to the DataFort appliance:
`lkm server list`
 - To sever the link between the DataFort appliance cluster member and LKM:
`lkm server remove <IP of LKM appliance>`

After replacing a DataFort cluster member, set up Lifetime Key Management for that new cluster member. See [Setting up an Appliance](#) on page 27.

MANAGING SNMP

To manage SNMP settings for the LKM appliance:

1. Select the LKM appliance in DMC and access the CLI.
2. At the CLI, run the following SNMP commands:

To turn on SNMP:

```
system property set sys.snmp.enabled 1
system snmp restart
```

To turn off SNMP:

```
system property set sys.snmp.enabled 0
system snmp restart
```

To configure SNMP v1 and v2c:

```
system property set sys.snmp.rocommunity <SecureString>
system snmp restart
```

To configure SNMP trap to point to a server:

```
system property set sys.snmp.traplocation <IPAddress>
system snmp restart
```

To configure SNMP v3:

```
system property set -g sys.snmp.rouser <Username>
system property set -g sys.snmp.ropass <Password>
system snmp restart
```

Note: The -g is needed because these properties do not exist by default.

VIEWING SYSTEM PROPERTIES

To view the system properties of an LKM appliance:

1. Select the LKM appliance in DMC and access the CLI.
2. At the CLI, run the following command:

```
system property get -k lkm
```

CHANGING BACKUP INTERVALS

By default, a linked DataFort appliance will send its configuration database to the LKM appliance every 7200 seconds if certain items in the configuration database have changed. To change the interval at which the DataFort appliance sends a backup of its configuration database to a linked LKM appliance:

1. Select the DataFort appliance in DMC and access the CLI.
2. At the CLI, run the following command:

```
system property set lkm.db.backup.interval <seconds>
```

ASSIGNING NAMES TO CRYPTAINER KEYS

To improve Cryptainer Key identification, you can assign a new name to an existing Cryptainer Key via the DataFort CLI. The updated name will automatically be synced to the LKM appliance. See the [DataFort Administration Guide](#) for details on using the DataFort CLI.

To assign names to Cryptainer Keys:

1. Select the DataFort appliance in DMC and access the CLI.
2. At the CLI, run the following command:

```
keyman cryptainerkeys rename <ck-id> <new-name>
```

Parameters:

<ck-id>	ID of the Cryptainer key to be renamed.
<new-name>	New name to be associated with this Cryptainer key.

For example:

```
keyman cryptainerkeys rename
010002025012a876d828d95be81616550a4eb8c9 cryptainer_rename
```

IMPORTING AND EXPORTING KEYS BETWEEN TRUSTEES

A trustee may export Cryptainer keys to or import Cryptainer keys from another trustee. Imported keys cannot be exported once they are imported.

Note: To export a Cryptainer key for a specific trustee using the DataFort WebUI, see the [DataFort Appliance Administration Guide](#).

1. To export a trustee key to an ftp server using the key id, run the following command:

```
trustee keys export -u <username> -f <servername> -k <keyID>
<trustee label>
```

Note: You must export keys per trustee.

2. Enter the password.

The name of the export file appears with the following message:

```
<appliance_name_date_time.kdf>
Notice: Keys export to FTP server completed successfully.
```

3. To import the exported key file from the ftp server, enter the following command:

```
trustee keys import -u <username> -f <path/>
<appliance_name_date_time.kdf>
```

4. Enter the password.

The following message appears:

```
WARNING: Naming keys that are not yet associated with storage is
highly recommended.
```

5. To verify that the exported key was imported to the LKM appliance, run the following command:

```
keyman cryptainerkeys list -k <keyID of exported key>
```

You may now use the imported keys to restore Cryptainers. See [DataFort Appliance Administration Guide](#).

AUTHORIZING AN ADMINISTRATOR LOG IN

To authorize an administrator log in:

1. Select the LKM appliance in DMC and access the CLI.
2. At the CLI, run the following command:

```
authorize <admin name>
```

For example:

```
authorize admin1
```

Upon authorization, the administrator has approximately a minute to log in with the correct password.

WARNING: A BAD PASSWORD, A LOGOUT, OR ENDING A SESSION ALL REQUIRE REAUTHORIZATION.

CHECKING THE STATUS OF AN LKM APPLIANCE

If keys are not syncing and you suspect that there's a connectivity problem, use the following command to check whether a connection exists to each of the known peers.

To check the status of the LKM:

1. Select the LKM appliance in DMC and access the CLI.
2. At the CLI, run the following command:

```
lkm status
```

CHECKING THE CONNECTIVITY STATUS BETWEEN APPLIANCES

If you're still seeing an error, then you may check to the network connectivity status between appliances.

To check the connectivity status between appliances:

1. Select an appliance in DMC and access the CLI.
2. At the CLI, run the following command for the appliance you want to connect to:

```
net util ping <IP of appliance>
```

CLEARING INTRUSION ALERTS

If the LKM appliance chassis is opened, an automatic defense response triggers. If chassis intrusion is detected, look for physical evidence (such as scratches, a broken lock or a stolen chassis key). If an intrusion alert appears, reset the tamper alert using CLI commands.

To clear an intrusion alert:

1. Select the LKM appliance in DMC and access the CLI.
2. At the CLI, run the following commands:

To check the appliance intrusion state:

```
system tamper status
```

To reset the appliance tamper alarm if an intrusion has occurred:

```
system tamper reset
```

SHUTTING DOWN AN LKM APPLIANCE

To shut down the LKM appliance:

1. Select the LKM appliance in DMC and access the CLI.
2. At the CLI, run the following command:

```
system shutdown
```

Note: After shutting down, power the LKM on again using the power button. See [Powering On and Shutting Down](#) on page 26.



■ ■ ■ ■ **APPENDIX I TROUBLESHOOTING**

This chapter includes troubleshooting information specific to the LKM appliance. For more information contact Decru Technical Support.

The chapter includes the following topics:

- [Recovery Scenarios](#)
- [Recovering LKM and DataFort Appliances](#)
- [Recovering LKM Appliance Keys](#)
- [Responding to a Bad Connection Error](#)
- [Viewing LED Displays](#)

RECOVERY SCENARIOS

Save for later

TABLE 11: HIERARCHICAL KEY SHARING GROUPS RECOVERY PLAN

DataFort Cluster Fails	DataFort appliance Fails	LKM appliance Fails
Replace DataFort appliances.	Replace DataFort appliance.	Replace LKM appliance.
Run Setup Wizard.	Run Add Cluster Member Wizard.	Run Recovery Wizard
Enable Policy Based Key Sharing: • Link appliances • Select a Key Sharing Group • Create a Trustee Relationship	Set Peer Link.	Set Peer Links
Restore Cryptainer		
Run Add Cluster Member Wizard.		

TABLE 12: KEY SHARING GROUPS WITH TWO LKMs RECOVERY PLAN

DataFort Cluster Fails	DataFort appliance Fails	LKM appliance Fails
Replace DataFort appliances.	Replace DataFort appliance.	Replace LKM appliance.
Run Setup Wizard.	Run Add Cluster Member Wizard.	Run Recovery Wizard
Enable Policy Based Key Sharing: • Link appliances • Select a Key Sharing Group • Create a Trustee Relationship	Set Peer Link.	Set Peer Links
Restore Cryptainer		
Run Add Cluster Member Wizard.		

TABLE 13: SOFTWARE KEY TRANSLATION RECOVERY PLAN

DataFort Cluster Fails	DataFort appliance Fails	LKM appliance Fails
Replace DataFort appliances.	Replace DataFort appliance.	Replace LKM appliance.
Export Configuration Database from LKM	Run Add Cluster Member Wizard.	Run Recovery Wizard • Import archived Configuration Database from LKM 2.
Run Setup Wizard. • Import Configuration Database from LKM.		Set Peer Links.
Peer Link appliance to LKM.		
Restore Cryptainer		
Run Add Cluster Member Wizard.		
Set Peer Link.		

RECOVERING LKM AND DATAFORT APPLIANCES

You can recover LKM and DataFort appliances in the unlikely event that they go down.

This section contains the following topics:

- [About Recovering Appliances](#)
- [Using the Recovery Wizard](#)

ABOUT RECOVERING APPLIANCES

If an appliance is lost, a saved configuration database from that appliance can be used to configure a replacement. The Setup Wizard assigns a new appliance the configuration from a pre-existing appliance. The replacement will retain all parameters stored in the configuration database of the original appliance. The following are required when restoring an appliance:

- A new or zeroized appliance and System Card.
- Decru-provided licenses.
- The minimum set of Recovery Officers and Recovery Cards as determined by the recovery schema.
- A saved database from the appliance that is to be restored.

Before you begin, you must connect the new or zeroized appliance to the network and assign it the IP settings of the old appliance. See [Assigning the IP Address](#) on page 29.

After restoring the appliance you may restore its keys by importing the last key backup of the LKM appliance. See [Exporting and Importing Keys](#) on page 69.

Additionally, you may need to recover keys. See [Recovering LKM Appliance Keys](#) on page 100.

USING THE RECOVERY WIZARD

For requirements, [About Recovering Appliances](#).

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Appliance menu, select Set up.
3. On the Decru Appliance Setup Wizard Step 1 of 12 (Welcome to the Decru Setup Wizard) screen, click Start.
4. On the Certificates screen, select whether to trust the certificate validating the connection between the appliance and the Management Console once or always.
5. On the Decru Appliance Setup Wizard Step 2 of 12 (Connect to Head of Cluster) screen, follow the instructions to enter the hostname or IP address of the appliance and click Next.
Note: This is the same hostname or IP address you configured using the LCD or serial console during installation.
6. On the Decru Appliance Setup Wizard Step 3 of 12 (Sign the License Agreement) screen, read the license agreement and click Accept.
7. On the Decru Appliance Setup Wizard Step 4 of 12 (Recover from Database - Optional) screen, either browse to the path of the configuration database and click Next, or click Next to skip.

8. On the Decru Appliance Setup Wizard Step 5 of 12 (Create Administrator) screen, enter a username and password for the administrator and click Next.

Note: Record this information for future reference.

Passwords may be composed of upper and lower case characters, numbers and punctuation marks. Select a password consisting of at least 8 valid, randomly-chosen characters. This name and password will be used every time the administrator logs in to the appliance.

Note: When using SecureView licenses, Decru recommends that you create the same administrator on multiple appliances. This allows you to multi-select appliances and log into them as a group with one administrator profile.

9. On the Decru Appliance Setup Wizard Step 6 of 12 (Configure Cluster and Recovery Schema) screen, click Next.
10. On the Decru Appliance Setup Wizard Step 7 of 12 (Network) screen, click Next.
11. On the Decru Appliance Setup Wizard Step 8 of 12 (Add Decru provided Licenses) screen, enter licenses and click Next.

To enter multiple licenses enter each license and then press Enter on the Management Station keyboard to start a new line for the next license. Each license must be on a consecutive and individual line.
12. On the Decru Appliance Setup Wizard Step 9 of 12 (Network and Certificate) screen, click Next.
13. On the Decru Appliance Setup Wizard Step 10 of 12 (Introduce Recovery Cards) screen, select a method to authorize the Setup Wizard:
 - To set up the appliance locally, see [Authorizing Recovery Locally](#) on page 98.
 - To set up the appliance using Remote Authorization, see [Initiating Remote Authorization for Recovery](#) on page 99.

Note: Both methods require using smart cards according to the recovery schema set for each appliance during initialization.

Authorizing Recovery Locally

1. On the Decru Appliance Setup Wizard Step 10 of 12 (Introduce Recovery Cards) screen, insert a card into the card reader, enter the password and click Next.

Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader, it is selected (green). At this point, you may enter the password and click the Verify Password button. Cards remain selected after removal.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

Note: If the card is uninitialized, the Security Domain entered for the first card in the set is applied to the entire set of Recovery Cards. If the card is initialized, the Card Label and Security Domain appear and the Recovery Officer is prompted for the password.

2. On the Decru Appliance Setup Wizard Step 11 of 12 (Apply Settings) screen, click Next.

3. On the Decru Appliance Setup Wizard Step 12 of 12 (Wizard Completed Successfully) screen, click Finish.

INITIATING REMOTE AUTHORIZATION FOR RECOVERY

1. On the Decru Appliance Setup Wizard Step 10 of 12 (Introduce Recovery Cards) screen, click Enable Remote Authorization.
Note: Previously entered data is saved locally, therefore Decru recommends that the Administrator initiating the remote authorization process be the last Recovery Card holder to supply a card.
2. When the Remote Authorization enabled message appears, close the Decru Appliance Setup Wizard Step 10 of 12 (Introduce Recovery Cards) screen.
3. Notify the outstanding Recovery Officer(s) that it is safe to continue the Setup Wizard approval and introduce Recovery Cards remotely. See [Authorizing Recovery Remotely](#).

Authorizing Recovery Remotely

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Appliance menu, select Set up.
3. On the Decru Appliance Setup Wizard Step 1 of 12 (Welcome to the Decru Setup Wizard) screen, click Start.
4. On the Certificates screen, select whether to trust the certificate validating the connection between the appliance and the Management Console once or always.
5. On the Decru Appliance Setup Wizard Step 2 of 12 (Connect to Head of Cluster) screen, click Next.
6. On the Question screen, verify that you want to continue with the remote authorization process by clicking Yes.
7. On the Decru Appliance Setup Wizard Step 10 of 12 (Introduce Recovery Cards) screen, insert a card into the card reader, enter the password and click Next.

Note: When a card is inserted into the reader, it is selected (green). At this point, you may enter the password and click the Verify Password button. Cards remain selected after removal.

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER.

8. Close the Decru Appliance Setup Wizard Step 10 of 12 (Introduce Recovery Cards) screen, and notify the outstanding Recovery Officer(s) that it is safe to continue the Setup Wizard approval.
Note: When the last card is introduced, verify that the information entered for Decru Appliance Setup Wizard screens 5 through 10 of 12 are correct before proceeding.
9. On the Decru Appliance Setup Wizard Step 11 of 12 (Apply Settings) screen, click Next.
10. On the Decru Appliance Setup Wizard Step 12 of 12 (Wizard Completed Successfully) screen, click Finish.

RECOVERING LKM APPLIANCE KEYS

This section includes the following topics:

- [About Recovering Appliances](#)
- [Recovering Keys](#)

ABOUT KEY RECOVERY

The key recovery procedure is intended for use only in the following conditions:

- You need to zeroize the LKM appliance.
- Some of the keys in LKM are not backed up to external storage and are not replicated in another LKM appliance.
- The Export Key procedure fails.

Note: In the rare event that the key database gets corrupted on the LKM appliance, it is not possible to manually back up keys from the LKM appliance to a key export file. In this case, the LKM appliance has a second database of keys on its hard drives, containing the last one million keys, to use when recovering keys that have not been manually backed up. To insure a complete key recovery, Decru recommends limiting keys that have not been manually backed up to less than one million.

To recover keys you will need:

- The last key backup of the LKM appliance. See [Exporting and Importing Keys](#) on page 69.
- The recovery key backup. See procedure below.

WARNING: WHEN PERFORMING THIS PROCEDURE, DO NOT OVERWRITE THE LAST KEY BACKUP OF THE LKM APPLIANCE.

RECOVERING KEYS

For requirements, see [About Key Recovery](#).

1. In the Decru Management Console, in the Resources pane, select the LKM appliance.
2. From the Keys menu, select Key Recovery.
3. A message appears asking if you would like to continue with key recovery, click Yes.
4. On the Select Directory screen, select a folder location and click Select.

A message prompt notifies you of the number of keys currently exported from the total number of keys available for export.

Note: Clicking Cancel ends the procedure. Unlike the Export Key procedure, you may not pause this procedure to incrementally export keys.

RESPONDING TO A BAD CONNECTION ERROR

You may use the procedure below to respond to a “ERROR: Bad connection to DB3” message. The following conditions may be present:

- The lkm key statistics command produces an ERROR: Bad connection to DB3 message.
- When using the system util df command, neither /var/chroot/pgsql/mnt/db3_data nor /var/chroot/pgsql/mnt/lkm_tablespace are present.
- The LKM appliance does not connect to DataFort appliances in its peer list, preventing DataFort key backups to LKM.

To respond to Bad connection to DB3 Error Message:

1. In the serial console, log into the appliance. See [Serial Console Port](#) on page 25.
2. From the menu, select “F. fsck RAID filesystems”.

VIEWING LED DISPLAYS

This section includes the following topics:

- [Front Panel LEDs](#)
- [Back Panel LEDs](#)

FRONT PANEL LEDs

There are four front panel LEDs, see the table below for details.

TABLE 14: FRONT PANEL LED

LED Name	Position	Color	State	Indication
Status LED	Top	Green	Solid	On network, no errors
		Red	Solid	Error or warning
	Bottom	Green	Solid	On network, no errors
		Red	Solid	Network error or lost network connection

BACK PANEL LEDs

The back panel of the LKM appliance features one or two bicolored LEDs that signal the status of the appliance, see the table below for details.

TABLE 15: BACK PANEL LED

LED Name	Position	Color	State	Indication
Power supply	Top	Green	Solid	On
Network LED	Bottom	Green	Blinks	Network activity



REQUIREMENTS

The process requires that the following be configured and/or accessible:

- LKM Server
- LKM appliance
- Empty directory—Keys are saved from the LKM Server into this directory before they are imported by the LKM appliance.
- LKM Key Transfer tool

HALTING LKM SERVER OPERATIONS

Before translating keys, stop LKM services on the LKM server PC.

1. From the LKM Server, open the Administrative Tools by selecting **Start > Settings > Control Panel > Administrative Tools**.
2. Select Services.
3. Select Decru Lifetime Key Management Service and select Stop from the Action menu.

INSTALLING THE KEY TRANSFER TOOL

1. Insert the LKM appliance CD into a drive on the LKM Server. The CD will run automatically if autorun is enabled on the PC.
2. Click the LKM Key Transfer installer link.
3. Follow the prompts to start the installer and accept the terms of the license agreement.
4. Specify the installation directory or use the default. Click Next.
5. Click Install to begin installation.
6. Click Finish when installation concludes.

USING THE KEY TRANSFER TOOL

Before using the Key Transfer Tool, halt LKM server operations.

1. Start LKM Key Transfer by selecting **Start > Programs > Decru > LKM Key Transfer** from the Windows Start menu of the LKM Server.
2. On the Select Directory screen, select a folder location and click Save.

A message prompt notifies you of the number of keys written to the directory. This number is defined by the number of keys in the LKM Server database.

3. Click OK.

Note: Key files will appear in the selected directory for import into the LKM appliance. Keys must be manually imported into the LKM appliance. See [Exporting and Importing Keys](#) on page 69.



■ ■ ■ ■ **APPENDIX III LOG MESSAGES**

This chapter includes the following topics:

- [LKM appliance Messages](#)
- [Appliance Management Messages](#)

LKM APPLIANCE MESSAGES

Logs are generated from the LKM process which runs on both LKM and DataFort appliances. The lkmd process is a program running on the DataFort and LKM appliances that handles the network communication for key synchronization, backup and restoration.

TABLE 16: LKM PROCESS MESSAGES

Message	Details
LKM: Started	lkmd process has started.
LKM: Stopped	lkmd process has shut down.

The logs in [Table 17](#) address the network connections between appliances. These logs are generated on both the initiating end and the accepting end of connections. DMC allows the creation of only SSL connections, and automatically makes sure that the certificate matches. Although you won't see many messages concerning cleartext connections, or SSL/cleartext mismatches or certificate mismatches, they are also included.

The following conventions apply:

- X.X.X.X is an IP address
- X.X.X.X:Y is an IP address followed by a TCP port number

TABLE 17: LKM APPLIANCE CONNECTION MESSAGES

Message	Details
LKM: SSL connection to X.X.X.X:Y succeeded	SSL connection is established.
LKM: SSL connection to X.X.X.X:Y rejected	SSL connection has failed.
LKM: SSL connection from X.X.X.X rejected (unknown peer)	SSL connection has failed, peer is unknown.
LKM: SSL connection from X.X.X.X:Y accepted	SSL connection is established.
LKM: SSL connection from X.X.X.X rejected (no certificate stored for peer)	SSL connection has failed, certificate is not stored.
LKM: SSL connection from X.X.X.X rejected (unmatched certificate for peer)	SSL connection has failed, certificate is unmatched.
LKM: Cleartext connection from X.X.X.X:Y accepted	Cleartext connection is established.
LKM: Cleartext connection from X.X.X.X rejected (unknown peer)	Cleartext connection has failed, peer is unknown.
LKM: Cleartext connection from X.X.X.X rejected (SSL required)	Cleartext connection has failed, SSL connection required.

APPLIANCE MANAGEMENT MESSAGES

Appliances include a management program that acts as the central hub for all user-interface and database activity. The following messages address the process that manages the appliance.

TABLE 18: PROCESS MESSAGES

Log Message	Details
Deleting LKM key database: <msg>	All the keys are being deleted; you should see this when you zeroize.
Deleting LKM Configdbs: <msg>	All the stored remote configuration databases are being deleted; you should see this when you zeroize.
boxmanager is now connected to the lkmd process	The central management program established a connection with the LKM channel.
boxmanager is now disconnected to the lkmd process	The central management program terminated a connection with the LKM channel.

The LKM database resides on the RAID disks which stores the keys. The following messages address the central management program's connection to the LKM database.

TABLE 19: CONNECTION MESSAGES

Log Message	Details
Closing bad connection to LKMDB	Closing bad connection to the LKM database.
Opening connection to LKMDB	Opening connection to the LKM database.
Failed to connect to LKMDB	Failed to connect to the LKM database.
Failed to initialize LKMDB: <msg>	Fail to initialize the LKM database.
Closing connection to inconsistent LKMDB	Closing connection to inconsistent LKM database.
Closing connection to LKMDB	Closing connection to LKM database.
LKM: Inserted server X.X.X.X	Added LKM peer: LKM appliance, LKM software, or DataFort.
LKM: Updated server X.X.X.X: Shared secret '****' -> '****'	Updated LKM peer to change shared secret.
LKM: Updated server X.X.X.X: Port Y -> Z	Updated LKM peer to change port.
LKM: Updated server X.X.X.X: Type <type> -> <type>	Updated LKM peer to change type: LKM appliance, LKM software, or DataFort.
Updated server X.X.X.X: Use SECRET <on/off> -> <on/off>	Updated LKM peer to change SSL on/off.
LKM: Deleted server X.X.X.X	Deleted LKM peer.

APPENDIX IV SPECIFICATIONS

TABLE 20: LKM 500 SPECIFICATIONS

Item	Detail	Specification
Hardware	Rack mountable	Standard 19" EIA rack
	Weight	48 lbs (21.8 kg)
	Size	43.2 cm (17") W x 8.8 cm (3.5") H x 79.5 cm (31.3") D
	Security	FIPS Level 3 Physical Security, Tamper Evident Label, Intrusion Detection Circuit
	Management Port	1 10/100/1000 Base-T Ethernet Port
	Serial Port	RJ45 serial console port
	Power Supply	2 Universal: 100-240V/5A, 50/60 Hz Redundant/Hot Swappable
	RAID Drives	2 SCSI RAID 1 Hot Swappable
	FAN	3 Redundant Hot Swappable
	LED	Power status, network activity, fault status
	LCD	Liquid Crystal display with touch-panel capability
	Smart Card	1 internal smart card reader
Environment	Temperature	Operating Temperature 5°C to 40°C (41°F to 104°F) Storage Temperature -10°C to 60°C (14°F to 140°F)
	Humidity	Operating Humidity: 85% RH at 40°C
	Shock	Non-Operating ASTM D3332, Method B
	Vibration	ASTM D3580-95, Method B
	Altitude	10,000ft at 23C
	Transportation	ISTA-2A
	RoHS	R5, China 2007
Regulatory Compliance	WEEE	Europe, China 2007
	EMC	United States FCC Class B Canada ICES-003 Class B Japan VCCI Class B Korea RRL Class B EU Community CE (EN55022 Class B, EN55024, EN61000-3-2 Class A, & EN61000-3-3) Australia/New Zealand AS/NZS 3548 Class B China CCC Taiwan BSMI International IEC 60950-1
	Safety	United States UL 60950-1 Canada CSA 60950-1 Japan IEC 60950-1 EU Community EN60950-1 +A11 China CCC International CB: IEC 60950-1





FCC B DECLARATION OF CONFORMITY

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

In order to maintain compliance with FCC regulations, shielded cables must be used with this equipment. Operation with non-approved equipment or unshielded cables is likely to result in interference to radio and TV reception. The user is cautioned that changes and modifications made to the equipment without the approval of manufacturer could void the user's authority to operate this equipment.

EUROPEAN UNION

This equipment is intended to operate under the following environmental conditions with respect to EMC:

1. A separate defined location under user's control.
2. Earthing and bonding shall meet the requirements of ETS 300 253 or CCITT K27.
3. Where applicable, AC power distribution shall be one of the following types: TN-S and TN-C [as defined in IEC 364-3] In addition, if equipment is operated in a domestic environment, interference may occur.

CANADIAN ICES-003

This Class A digital apparatus meets all requirements of the Canadian ICES-003 Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

VCCI CLASS B STATEMENT

This is a Class B product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take corrective actions. VCCI-B

CE STATEMENT

The standards compliance label on the Lifetime Key Mangement™ appliance contains the CE mark that indicates that this system conforms to the provisions of all European Council Directives, laws, and standards.

The appliance is in conformity with the provisions of the following EC Directives, including all amendments, and national legislation implementing these directives:

- 89/336/EEC
- 93/68/EEC
- 73/23/EEC

The following harmonized standards have been applied

- EN55022: 1998 Plus A1: 2000 & A2: 2003
- EN61000-3-2: 2001
- EN61000-3-3: 1995 Plus A1: 2001
- EN55024: 1998 Plus A1: 2000 & A2: 2003
- EN60950-1: 2001+A11: 2004

■ ■ ■ ■ APPENDIX VI GLOSSARY

administrator	A type of user with specific privileges. manage, create and delete user accounts, to create and delete Cryptainers, to control user access to certain Cryptainers, and to configure and maintain the DataFort.
Admin Card	A smart card used to authenticate a DataFort administrator. An individual possessing the Admin Card and the username and password for that card has privileges of a DataFort administrator. DataFort detects the presence of this card in the card reader attached to the Management Station.
AES	Advanced Encryption Standard. The official U.S. replacement for DES (and 3DES). AES allows for significantly stronger encryption than 3DES or DES, which was the official U.S. encryption algorithm until it was replaced by AES.
authentication	The process by which identity is established on a network. Typically, identity is established with username/password combinations (logging in to a computer) or using physical tokens (keys, smart cards). By default, DataFort requires both a username/password combination and a token to authenticate the DataFort administrator and Recovery Officers. DataFort can be configured to require only a username and password for management.
block cipher	An encryption algorithm in which data is segmented into fixed size blocks before processing. An algorithm is applied to each block.
chassis	The physical encasement of a device. DataFort is designed to resist and detect any attempt to open the chassis.
ciphertext	Encrypted data. A cryptographic cipher transforms cleartext data into ciphertext. Ciphertext appears to be random, obscuring the meaning of the original data. After encryption, only those with access to the encryption key can read the data.
cleartext	Data before encryption. Unencrypted data is clear in the sense that anyone with access to the data can read it.
CLI	The command line interface used to manage the DataFort device. The CLI allows remote users to log in to DataFort and administer it by entering text commands over SSH.

client	A device that initiates requests as part of a client/server model. In this model, one entity (the client) requests a resource from a second entity (the server). An example of this model can be found when a workstation makes a request for data from a storage device: the workstation is the client, and the storage device is the server.
cluster	A cluster is a set of interconnected devices. If one fails, the other can continue providing the service. By clustering DataFort devices, total system redundancy is increased, decreasing the probability of any downtime.
configuration database	The database stored inside an appliance and contains network and security information, ACLs and (on DataFort) encrypted key material.
Cryptainer	A Cryptainer is a specially designated directory or LUN. Data within a Cryptainer is encrypted by DataFort with a Cryptainer Key, using AES.
cryptography	The science of rearranging data by applying algorithms mathematically to combine cleartext and an encryption key. The resulting ciphertext appears to be random, but contains all of the original information.
failover	The ability to withstand the failure of one or several system components by transferring access to data from a failed path to a healthy one. To provide redundancy in case of failure, the DataFort can be connected to the fabric via two ports, allowing the same LUN to be addressed via two or more WWNs or port addresses.
Fibre Channel	Fibre Channel is a physical layer (fabric) that connects servers, switches and hubs, storage devices and appliances (such as DataFort). Fibre Channel carries SCSI-3 traffic. Hosts in the fabric see storage devices as if they were locally attached storage.
IPsec	Internet Protocol Security. A standard for secure network communication. Communication between clustered DataFort devices occurs over IPsec; IPsec communication is a licensed option between DataFort and clients.
key	In cryptography, a key is a value applied to cleartext (using an algorithm) in order to generate ciphertext, or applied to ciphertext to generate cleartext. Each cipher requires a key in order to encrypt or decrypt data.
Lifetime Key Management® appliance (LKM)	Decru's proprietary solution for encryption key management. LKM software and the LKM appliance both store key information.
Management Station	A Windows PC equipped with a smart card reader, from which a DataFort administrator can manage the DataFort via the DataFort WebUI.
NAS	Network Attached Storage. Hard disk storage connected to a LAN (Local Area Network) and assigned an IP address, not attached directly to a computer.

quorum

The minimum number of Recovery Officers required to complete sensitive DataFort and LKM management procedures.

RAID Disk Drives

**Trustee Acceptance
Package (TAP)**

The second message between DataFort and LKM appliances when setting up a trustee relationship.

**Trustee Establishment
Package (TEPT)**

The first message sent between DataFort and LKM appliances when setting up a trustee relationship.

UDP

User Datagram Protocol. User Datagram Protocol is a communications protocol for messages between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP). Services that can be run on both TCP and on UDP (such as NFS) are often deployed with UDP when speed is a concern and deployed with TCP when on a lossy network.

WebUI

A graphical user interface used to manage the appliance via a web browser using SSL. Commands are entered by selecting from drop-down menus and filling out web forms.

INDEX

A

- access
 - CLI 90
- adaptor
 - RJ45 to DB9 25
- add
 - administrator 77
 - administrator card 87
 - license 74
 - LKM appliance to DMC 37
 - LKM appliance, first time 32, 37
- Admin Card
 - about 111
- administrator
 - about 111
 - add 77
 - add card 87
 - permissions 77
 - remove card 87
 - types 77
- administrators
 - about 75
- AES
 - about 111
- appliance
 - back up 80
 - menu 41
 - remove 38
 - verify upgrade package 84
 - zeroize 84
- archive
 - keys 66
 - parent keys 66
- authentication
 - about 111

B

- back panel
 - LED 101
- back up
 - appliance 80
 - configuration database to external storage 16
 - DataFort appliance 80

- LKM appliance 80
- backup interval
 - configuration database 91
- backups
 - frequency of configuration database 16
- battery iv, 22
- block cipher
 - about 111

C

- Canadian ICES-003
 - certification 109
- Category 5 cable 25
- CE
 - certification 110
- certification
 - Canadian ICES-003 109
 - CE 110
 - declaration of conformity 109
 - European Union 109
 - VCCI Class A 110
- chassis
 - about 111
- ciphertext
 - about 111
- cleartext
 - about 111
- CLI
 - access 90
 - commands 89
- client
 - about 112
- cluster
 - about 112
- collect
 - tech support info 81
- commands
 - CLI 89
 - intrusion alerts 94
 - SNMP 91
- configuration
 - menu 43
- configuration database

- about 112
- backup interval 91
- frequency of automatic backups 16
- manual back up 16
- conventions
 - LKM appliance guide 13
- create
 - trustee links with SecureView 54
- Cryptainer
 - about 112
- Cryptainer keys
 - assign names to 92
 - transfer 71
 - view 64
- cryptography
 - about 112

D

- DataFort
 - assign IP address 29
 - assign IP settings from LCD 29
 - assign IP settings from serial console 30
 - back panel connections 25
 - back up 80
 - diagram, back panel 25
 - link to LKM 90
 - purge keys 20
 - restore 97
 - specifications 107
- declaration of conformity
 - certification 109
- Decru Management Console 12
- display
 - state 40

E

- edit
 - menu 42
- European Union
 - certification 109
- exit
 - management console 37
- export
 - keys to external storage 69
 - trustee keys 92

F

- failover 111

- about 112
- fibre channel
 - about 112
- front panel
 - assign IP address 29
- LED 101
- System Card slot 24

H

- help
 - menu 47

I

- import
 - keys from external storage 69
 - trustee keys 92
- installation
 - key transfer tool 103
 - management console 31
 - precautions v, 23
 - rack mount 24
 - run installer 32
- intrusion alerts
 - clear 94
 - commands from CLI 94
- IP settings
 - assign from LCD 29
 - assign from serial console 30
- IPsec
 - about 112
- IT power systems 22

K

- keys
 - about 112
 - archive 66
 - export to external storage 69
 - import from external storage 69
 - install transfer tool 103
 - limits for enterprise 20
 - manage 63
 - recover 100
 - run transfer tool 103
 - transfer from LKM 2.5 to 3.0 102

L

- LCD
 - assign DataFort IP settings 29

LED

- back panel 101
- front panel 101

license

- add 74

Lifetime Key Management

- about 112

link

- DataFort appliances to LKM 90

lithium battery iv, 22

LKM appliance

- add to DMC 37
 - add to DMC, first time 32, 37
 - back up 80
 - boxmanager connection messages 106
 - boxmanager process messages 106
 - check connectivity status of 93
 - check status of 93
 - connect 24
 - deployment of 14
 - features overview 11
 - guide conventions 13
 - LKM connection messages 105
 - LKM process messages 105
 - log into 38
 - menu 44
 - shut down 94
 - troubleshooting 95
 - understanding 13
- ## LKM server
- halt operations 103
- ## lkmd 105
- ## log in
- authorizing administrator log in 93
 - to LKM appliance 38

M

manage

- administrator 74
- keys 63
- licenses 74
- Smart Cards 85
- the LKM appliance 79

management

- console, exit 37
- console, install 31
- from console 12
- interface 12

port 25

- SecureView 12
- station 31

management interface

- console 12

LCD 12

- serial 12

management port

- connect to Ethernet 25

Management Station 12

management station

- about 112
- requirements 31
- security 31

menu

- appliance 41
- configuration 43
- edit 42
- help 47
- LKM appliance 44
- security 46
- topology 45
- trustee 46
- use 39
- view 42

N

names

- assign to Cryptainer keys 92

NAS

- about 112

O

online help 47

P

parent keys

- archive 66

permissions

- administrator 77

port

- management 25

power

- cords 25
- LKM appliance on 26
- on after shut down 26
- precautions 22
- supply notice 22

- purge keys
 - DataFort appliance 20

Q

- quorum
 - about 113

R

- rack mount
 - DataFort 24
 - installation 24
 - standard 24
- RAID
 - about 113
- recover
 - keys 100
- Recovery Card
 - about 113
 - replace 86
- recovery officers
 - about 75, 113
- remove
 - administrator card 87
 - appliance 38
- replace
 - Recovery Card 86
- requirements
 - management station 31
- reset
 - Smart Cards 88
- restore
 - DataFort 97
- run
 - installer 32
 - key transfer tool 103
 - Setup Wizard 33

S

- SAN
 - about 113
- security
 - management station 31
 - menu 46
- security domain
 - about 113
- SEP
 - about 113
- serial console

- connect serial port 25
- DataFort settings 30
- Setup Wizard
 - run 33
- shut down
 - LKM appliance 26, 94
- Smart Cards
 - about 85, 113
 - admin 85
 - manage 85
 - recovery 85
 - reset 88
 - system 85
- SNMP
 - about 113
 - commands 91
- SSH
 - about 113
- SSL
 - about 113
- state displays 40
 - use 39
- System Card
 - about 113
 - insert 24
- system details
 - view 84
- system properties
 - view 91

T

- TAP
 - about 114
- tech support info
 - collect 81
- TEP
 - about 114
- topology
 - menu 45
- transfer
 - Cryptainer keys 71
- transfer keys
 - from LKM 2.5 to 3.0 102
- troubleshooting
 - LKM appliance 95
- trustee
 - about 113
 - create links with SecureView 54

- export keys 92
- import keys 92
- menu 46
- Trustee Acceptance Package (TAP) 55
- Trustee Establishment Package (TEP) 55, 56, 58

U

- UDP
 - about 114

V

- VCCI Class A
 - certification 110
- verify
 - appliance upgrade package 84
- view
 - Cryptainer keys 64
 - menu 42
 - system details 84
 - system properties 91

W

- WebUI
 - about 114
- wizard
 - use Setup Wizard 32

Z

- zeroize appliance 84