



ADMINISTRATION GUIDE

Lifetime Key Management
Appliance 3.0

security

LKM Appliance Administration Guide

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

Part number: 30-000311A0 (LKMA 011807)

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, das 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 240 V Wechselstrom, 10 A (bzw. in den USA 120 V Wechselstrom, 15 A) an den Phasenleitern (allen stromführenden Leitern) verwendet wird.

VARNING: Apparaten skall anslutas till jordat uttag när den ansluts till ett nätverk.

OPPMERKSAMHET: Apparaten må kun tilkoples jordet stikkontakt.

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.

WARNUNG: Diese Einheit verfügt über mehr als einen Stromanschluß; um Strom gänzlich von der Einheit fernzuhalten, müssen alle Stromzufuhren abgetrennt sein.

ATTENTION: Cette unité est équipée de plusieurs raccordements d'alimentation. Pour supprimer tout courant électrique de l'unité, tous les cordons d'alimentation doivent être débranchés.

Lithium Battery Notice for Service Personnel

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



CAUTION: 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.

ATTENTION: Il y a danger d'explosion s'il a remplacement incorrect de la batterie. Remplacer uniquement avec une batterie du meme type ou d'un type equivalent recommande par le constructeur. Mettre au rebut les batteries usagees conformement aux instructions du fabricant.

WARNUNG: Bei Einsetzen einer falschen Batterie besteht Explosionsgefahr. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.



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, you must 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 Introduction	10
Overview of the LKM Appliance	11
Features at a Glance	11
LKM Terms	12
About Configuration and Key Database Backups	13
About Management Interfaces	14
Conventions Used in this Manual	15
Chapter 2 Deploying an LKM Appliance	16
Enterprise Key Limits	17
Centralized Management	18
Operation Scenarios	19
Deployment Scenarios	22
Deploying a Single LKM Appliance	22
Deploying Linked LKM Appliance Peers	24
Chapter 3 Installation	27
Notices and Warnings	28
Power Supply Notice	28
Dual Power Supply Notice	28
Lithium Battery Notice for Service Personnel	28
Rack Mounting	28
Installing the RAID Disk Drives	29
Rack Mounting the LKM Appliance	30
Connecting the LKM Appliance	30
System Card Insertion	30
Rear Panel Network Connections	31
Powering On and Shutting Down	32
Chapter 4 Setting up Lifetime Key Management	33
How to Set Up an Appliance	34
Assigning the IP Address	35
Setting the IP Address Using the LCD	35
Setting the IP Address Using the Serial Console	36
Installing the Management Console	37
Management Station Requirements	37
Management Station Security	37
Running the Installer	38
Initializing an Appliance via the Setup Wizard	38
Adding Appliances for the First Time	38
Running the Setup Wizard	39

Chapter 5 Getting Started	42
Adding Appliances	43
Logging into Appliances	43
Linking Appliances to LKM	44
Using Drag and Drop	44
Using the LKM Menu	44
Using Menus and Displays	45
Appliance Tab	45
State Displays	46
Appliance Menu	47
Edit Menu	48
View Menu	48
Trustee Menu	48
Configuration Menu	49
LKM Menu	49
Help Menu	50
Chapter 6 Appliance Management	51
Using Management Interfaces	52
Accessing the Decru Management Console	52
Accessing the DataFort WebUI	52
Accessing the Command Line Interface	52
Managing Licenses	53
Adding a License	53
Viewing Licenses	53
Managing Administrators	54
About Administrators and Recovery Officers	54
About Administrator Roles	54
Adding an Administrator	55
Viewing Administrators	58
Setting Log Options	59
About Log Options	59
Setting the Logging Configuration	59
Maintaining Appliances	61
Removing an Appliance	61
Rebooting an Appliances	61
Zeroizing an Appliance	61
Viewing Appliance Details	61
Collecting Tech Support Info	62
Upgrading Appliances	62
Upgrading an Appliance	62
Verifying an Upgrade Package	62
Backing Up the Configuration Database Manually	63
Backing Up an Appliance	63
Backing Up All DataFort Appliances Linked to LKM	63

Managing Smart Cards	64
About Smart Cards	64
Viewing Recovery Cards	64
Replacing a Recovery Card	65
Adding an Admin Card to an Administrator	67
Resetting Smart Cards	67
Chapter 7 Key Management	68
About Keys and Key Files	69
About Sharing Keys Between Appliances	70
Archiving Keys	71
Viewing Keys	71
Generating a Parent Key Archive	73
Generating a Cryptainer Key Archive	75
Transferring Cryptainer Keys	76
About Translating Cryptainer Keys	76
Translating Cryptainer Keys	76
Managing Trustees	78
Creating Trustee Links with SecureView	79
Manually Creating Trustee Links	81
Sharing Keys between Trustees	85
Backing Up Keys to External Storage	86
Exporting and Importing Keys	86
Making a Cryptainer Key Archive From a Key File	87
Chapter 8 CLI Commands	89
Managing DataFort Appliances Linked to LKM	90
Managing SNMP	91
Viewing System Properties	91
Changing Backup Intervals	92
Assigning Names to Cryptainer Keys	92
Authorizing an Administrator Log In	92
Checking the Status of an LKM Appliance	93
Checking the Connectivity Status Between Appliances	93
Clearing Intrusion Alerts	93
Shutting Down an LKM Appliance	93
Appendix I Troubleshooting	94
Disaster Recovery Scenarios	95
Restoring an Appliance	96
Recovering Keys	97
Responding to a Bad Connection Error	98
Viewing LED Displays	98
Front Panel LEDs	98
Back Panel LEDs	98

Appendix II Migrating from LKM Server to LKM Appliance	99
Requirements	100
Halting LKM Server Operations	100
Installing the Key Transfer Tool	100
Running the Key Transfer Tool	100
Appendix III Log Messages	101
LKM Appliance Messages	102
Appliance Management Messages	103
Appendix IV Specifications	104
Appendix V Regulatory and Certifications	105
FCC B Declaration of Conformity	106
European Union	106
Canadian ICES-003	106
VCCI Class B Statement	107
CE Statement	107
Appendix VI Glossary	108
Index	112



■ ■ ■ ■ 1 INTRODUCTION

The Decru Lifetime Key Management™ appliance (LKM appliance) manages encryption keys for multiple Decru DataFort™ storage security appliances, ensuring encryption key availability for the life of the secured data.

This chapter includes the following topics:

- [Overview of the LKM Appliance](#)
- [About Configuration and Key Database Backups](#)
- [About Management Interfaces](#)
- [Conventions Used in this Manual](#)

OVERVIEW OF THE LKM APPLIANCE

The Decru DataFort™ appliance secures data at rest by encrypting it with strong algorithms and storing it in Cryptainer vaults™ managed by the appliance. Keys are generated before data is encrypted by DataFort. The presence of these keys is also required in order to decrypt the data. In an environment where multiple DataFort appliances manage large quantities of data, and therefore generate a large number of keys, a robust key management system is required.

The Decru Lifetime Key Management™ appliance (LKM appliance) manages encryption keys for multiple DataFort appliances, ensuring encryption key availability for the life of the secured data. The LKM appliance offers a central location for the administrator to load, view, manage, share and save all keys generated by DataFort appliances in an installation. When used in combination with the separate Decru Decryption Software (DDS), the LKM appliance also enables authorized administrators to decrypt data outside of the DataFort appliance.

The Decru Management Console (DMC) provides a powerful tool for managing multiple LKM and DataFort appliances from a single interface. This console displays at-a-glance status for all DataFort and LKM appliances in the installation, as well as providing centralized tools and menu operations for DataFort and LKM appliance management.

For an overview of LKM terms, see [LKM Terms](#) on page 12.

FEATURES AT A GLANCE

The LKM appliance offers the following features:

- Supports DataFort appliances 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

LKM TERMS

Some of the most relevant LKM terms and how you can learn more about them are listed below:

Key Database	LKM appliances maintain a key database containing all encryption keys used by appliances in the enterprise. See About Configuration and Key Database Backups on page 13.
Configuration Database	The LKM appliance automatically stores all encryption keys and the most recent configuration database for any linked appliance. See About Configuration and Key Database Backups on page 13.
Decru Management Console (DMC)	The DMC provides centralized tools and menu operations for DataFort and LKM appliance management. See Management Station on page 15.
SecureView	SecureView™ is a licensed feature that allows DMC to monitor and manage many appliances simultaneously from a single console. See SecureView on page 15.
Key Types	There are three types of keys: Parent, Cryptainer and Translated Keys. See About Keys and Key Files on page 69.
Key Files	There are three types of key files: Parent Key Archive, Cryptainer Key Archive and Key Files. See About Keys and Key Files on page 69.
Key Sharing	There are several ways to share keys between appliances depending on the level of trust you want to create between appliances: via Cluster, Peer and/or Trustee Links and through Key Translation. See About Sharing Keys Between Appliances on page 70.
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 54.
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 64.

ABOUT CONFIGURATION AND KEY DATABASE BACKUPS

DataFort and LKM appliances both maintain a configuration database. LKM appliances also maintain a key database containing all encryption keys used by appliances in the enterprise. Creating a link between LKM and DataFort appliances allows automated key and configuration backups to be sent from DataFort to LKM appliances. The LKM appliance automatically stores all encryption keys and the most recent configuration database for any linked appliance.

TABLE 1: DATABASE TYPES STORED BY APPLIANCES

Database Type	Contains	Appliance Type
Configuration Database	• Network and security information • Access Control Lists (ACLs) • Encrypted key material	DataFort
	Network and security information	LKM
Key Database	Encryption keys used by linked appliances	LKM

In addition to the automatic backup that takes place between linked DataFort and LKM appliances, the configuration and key databases can be manually backed up to external storage.

The following back up methods are used to share configuration and key information between linked DataFort and LKM appliances:

Automatic DataFort Configuration Database Backup to LKM

A DataFort appliance linked to an LKM appliance initiates a backup of its configuration database approximately every two hours if certain items in the configuration database have changed. Note that the backup interval default can be changed. See [Changing Backup Intervals](#) on page 92.

An LKM appliance only retains the last backup of the configuration database for any linked DataFort appliance. The DataFort configuration database can also be backed up remotely from the DataFort appliance.

Automatic DataFort Key Backup to LKM

Every five seconds, the LKM appliance queries each DataFort appliance it is linked to for new keys. If an appliance returns a key, the LKM appliance asks for the next 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 appliance it is linked with, so that almost as soon as a new key is created on the DataFort, the key is synced to the LKM appliance.

The following back up methods are used to save DataFort and LKM configuration and key information:

- Manual DataFort or LKM Appliance Configuration Database Backup to External Storage**

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. Backing up the LKM appliance configuration database will aide in recovery should all LKM appliances need to be restored. See [Backing Up the Configuration Database Manually](#) on page 63.
- Manual LKM Key Backup to External Storage**

Backing up the LKM key database to external storage will make recovery possible if all LKM appliances and its peers are down. See [Backing Up Keys to External Storage](#) on page 86.

ABOUT MANAGEMENT INTERFACES

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

TABLE 2: MANAGEMENT INTERFACES

Interface	Description	Usage
Serial	A serial connection allows you to enter network settings for uninitialized appliances.	Set, clear, or reset IP address, gateway and subnet mask. Zeroize when other interfaces are not available.
LCD	A touch panel displays functions and interactive messages.	View the Number of Keys (0-10M) and the CPU Load % (0-100) at a glance. Enter initial IP settings.
Management Console	A Java tool allows you to use the Decru Management Console to manage appliances from a common location. A SecureView™ license supports simultaneous management of LKM and DataFort appliances.	Manage all LKM appliances in an installation, and use some additional management functions for DataFort appliances on the network.

SecureView

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

To facilitate management of multiple appliances using SecureView, add the same administrator (with the same name and password) to all appliances. This allows you to 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.

- Simultaneous selection of an LKM appliance with SecureView and a DataFort appliance with SecureView will disable the LKM menu items.
- Simultaneous selection of an LKM appliance with SecureView and a DataFort appliance without SecureView will enable LKM menu items, as the DataFort appliance without SecureView is not considered selected.

Management Station

The Decru Management Console (DMC) provides the 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 37.

CONVENTIONS USED IN THIS MANUAL

This guide uses the following typographic conventions:

- Commands that you enter from the keyboard appear in monospaced font in **blue**.
- Active links that you can click in the PDF version of this guide appear as underlined purple text.

2 DEPLOYING AN LKM APPLIANCE

The LKM appliance is positioned on the Ethernet portion of the network where the DataFort appliance resides. Linking DataFort and LKM appliances provides a secure channel for key backup and replication between appliances. The DataFort appliance automatically shares key data with a linked LKM appliance. See [About Sharing Keys Between Appliances](#) on page 70.

Note: Decru recommends that each DataFort appliance have at least two LKM appliance peers, making LKM appliance connections across sites redundant.

This chapter includes the following topics:

- [Enterprise Key Limits](#)
- [Centralized Management](#)
- [Operation Scenarios](#)
- [Deployment Scenarios](#)

ENTERPRISE KEY LIMITS

One LKM appliance can support the management of multiple DataFort appliances, and multiple LKM appliances can share key information for the enterprise. The number of DataFort and LKM appliances required across the entire installation is determined by the aggregate data throughput required by DataFort appliances, the frequency of key generation, and redundancy requirements. It is important to understand the full life cycle of encryption keys in the deployment in order to accurately plan for the number of appliances to install. Factors to consider include the 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 3: APPLIANCE KEY LIMITS

Appliance Type	Item	Limit
Lifetime Key Management Appliance	Number of DataFort appliances 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. The DataFort appliance will purge keys from the configuration database when the limit is reached.	4500 for E-Series 8000 for FC-Series

Keys generate when a Cryptainer is created, rekeyed or translated from one DataFort to another. Some environments, such as those where new backup tapes are created each day, generate many keys. The following table provides an example of high frequency key generation by an FC-Series DataFort:

TABLE 4: EXAMPLE OF HIGH FREQUENCY KEY GENERATION

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

CENTRALIZED MANAGEMENT

Multiple LKM appliances provide key replication for a single installation, and can be employed to offer key management across multiple sites, and multiple DataFort cluster locations. A single instance of the Decru Management Console running on the Management Station manages all appliances in use.

Multiple LKM appliances can share keys across a large configuration which includes DataFort clusters encrypting data stored on disk and tape. LKM appliances store all encryption keys for the entire enterprise, and can share them between remote sites. Once LKM appliances are linked in this type of deployment, the appliances provide seamless key management across the entire enterprise.

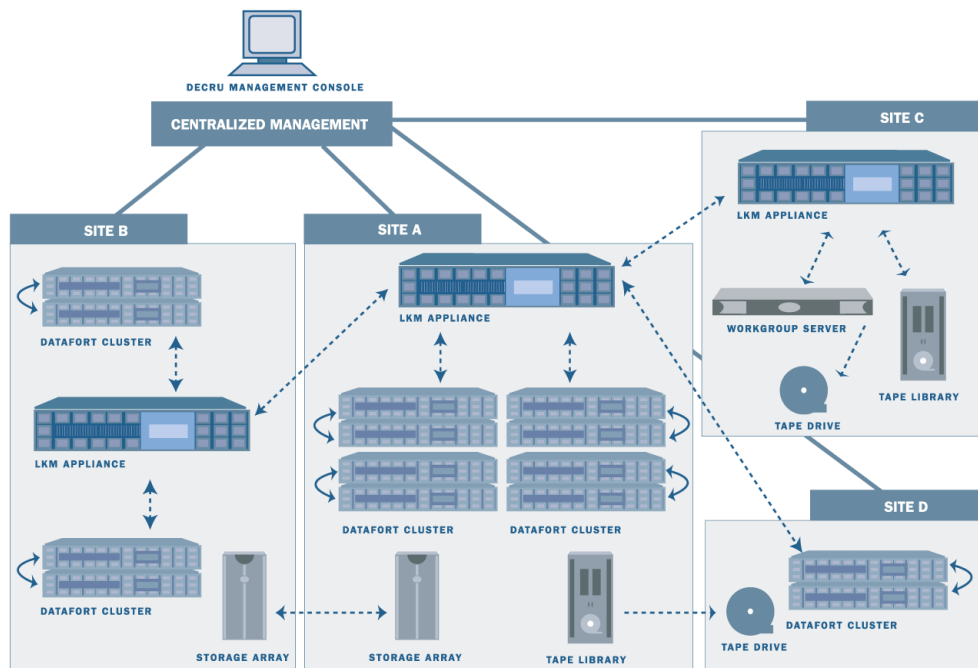


Figure 2-1: Centralized key management for large enterprise deployment

OPERATION SCENARIOS

This section includes the following topics:

- [Key Translation and Trustee Links](#)
- [Key Translation](#)
- [Configuration Database Backups](#)

Key Translation and Trustee Links

Both Key Translation and a Trustee Link allow you to make keys available to non-clustered DataFort appliances that are peer-linked to the same LKM appliance. The difference is that a Trustee Link is an established relationship that allows for continual bi-directional key sharing, while Key Translation is useful only one time and only in one direction. The trustee link is established using the Decru Management Console. Once the trustee link is established, DataFort appliances share keys directly.

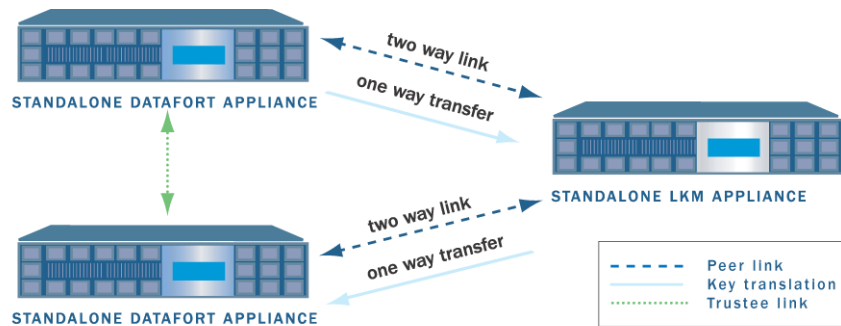


Figure 2-2: Key Translation and Trustee Link

For more about links between DataFort and LKM appliances, see [About Sharing Keys Between Appliances](#) on page 70.

Key Translation

The LKM appliance translates keys between linked DataFort appliances that are not in a cluster. The LKM appliance translates a key from one DataFort to the other. Keys travel over the peer link between the LKM appliance and each of the DataFort appliances.

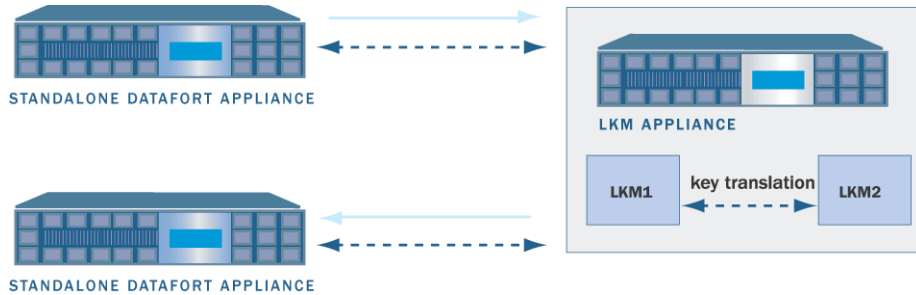


Figure 2-3: Key Translation with Standalone DataFort Appliances and Single LKM Appliance

Within the LKM appliance, keys are available for translation between DataFort clusters only if there is a prior peer link between both cluster members and the LKM appliance that is performing the key translation, or if there is a prior peer link between the LKM appliances supporting both cluster members. See [About Sharing Keys Between Appliances](#) on page 70.

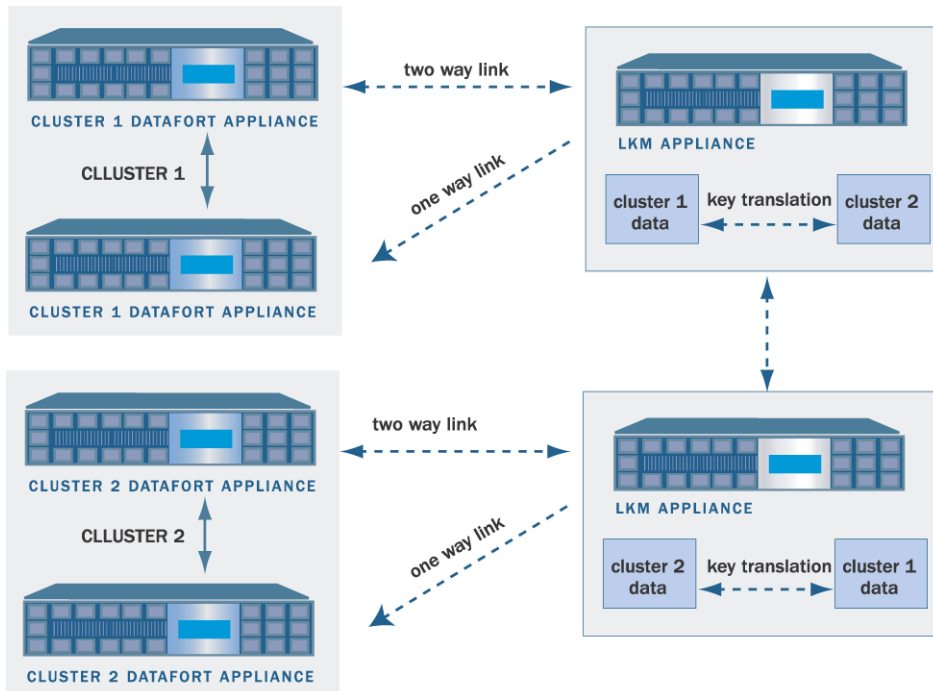


Figure 2-4: Key Translation with Linked LKM Appliances and DataFort Cluster

CONFIGURATION DATABASE BACKUPS

Each DataFort appliance configuration database is backed up to its peer-linked LKM appliance. Peer-linked LKM appliance configuration databases are backed up to each other. See [About Configuration and Key Database Backups](#) on page 13.

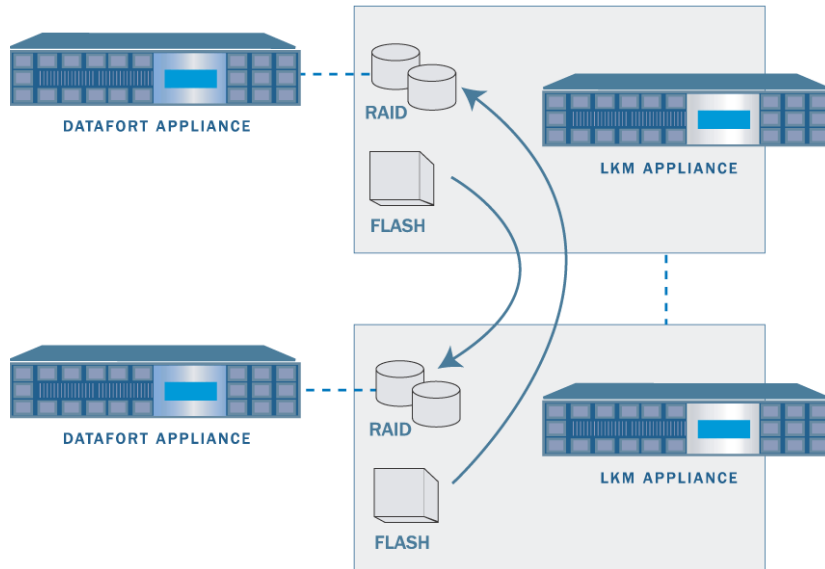


Figure 2-5: Configuration Database Backups

DEPLOYMENT SCENARIOS

This section includes the following topics:

- [Deploying a Single LKM Appliance](#)
- [Deploying Linked LKM Appliance Peers](#)

DEPLOYING A SINGLE LKM APPLIANCE

This section includes the following topics:

- [Single LKM Appliance Linked to Standalone DataFort Appliance](#)
- [Single LKM Appliance Linked to DataFort Cluster](#)
- [Single LKM Appliance Linked to Multiple Standalone DataFort Appliances](#)
- [Single LKM Appliance with Multiple DataFort Clusters](#)

Single LKM Appliance Linked to Standalone DataFort Appliance

Linking a standalone DataFort appliance to an LKM appliance creates a peer link between the appliances. See [Linking Appliances to LKM](#) on page 44. The DataFort appliance passes encrypted keys and configuration database backups to the peer-linked LKM for storage. The LKM appliance will pass keys to the peer-linked DataFort as required to restore deleted Cryptainer vaults.



Figure 2-6: Single LKM Appliance with Standalone DataFort Appliance

Single LKM Appliance Linked to DataFort Cluster

Keys are replicated between DataFort cluster members. Only one DataFort within the cluster will pass keys to a peer-linked LKM, but LKM will pass keys to either DataFort cluster member as required to restore deleted Cryptainer vaults.

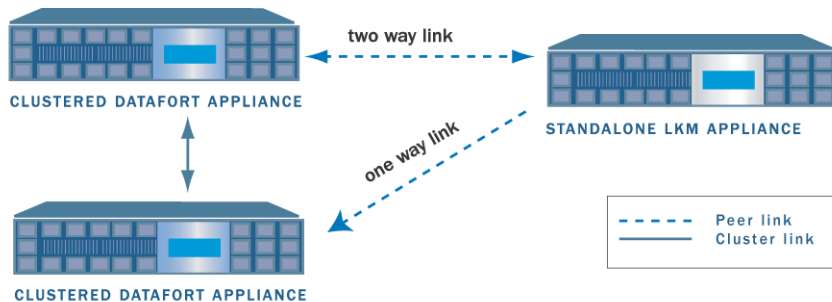


Figure 2-7: Single LKM Appliance with Clustered DataFort Appliances

Single LKM Appliance Linked to Multiple Standalone DataFort Appliances

Both standalone DataFort appliances are peer-linked to LKM and so pass encrypted keys to the LKM appliance for storage. The LKM appliance will pass keys to each DataFort respectively to restore deleted Cryptainer vaults.

A one-way key transfer of a limited number of keys between DataFort appliances via the LKM appliance is supported. This enables the DataFort receiving the keys to decrypt data encrypted by the DataFort sending the keys.

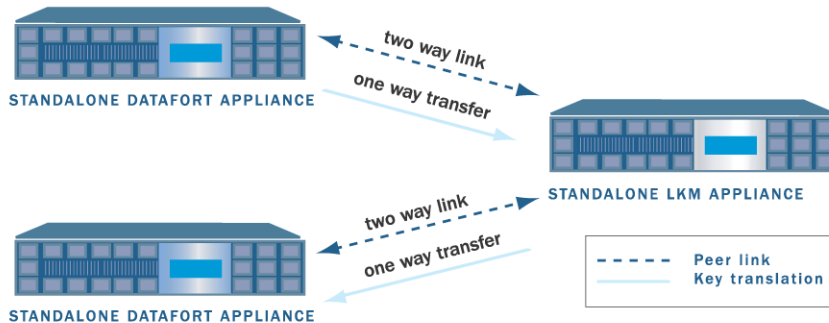


Figure 2-8: Single LKM Appliance with Standalone DataFort Appliances

A trustee link can be added to this configuration to allow direct continual bi-directional key sharing between the two DataFort appliances. See [Key Translation and Trustee Links](#) on page 19.

Single LKM Appliance with Multiple DataFort Clusters

Keys are replicated between DataFort cluster members. One DataFort per cluster will pass encrypted keys to a peer-linked LKM. The LKM appliance will pass keys to either DataFort cluster member as required to restore deleted Cryptainer vaults.

A one-way key transfer of a limited number of keys between DataFort clusters via the LKM appliance is supported. This enables the DataFort cluster receiving the keys to decrypt data encrypted by the DataFort cluster sending the keys.

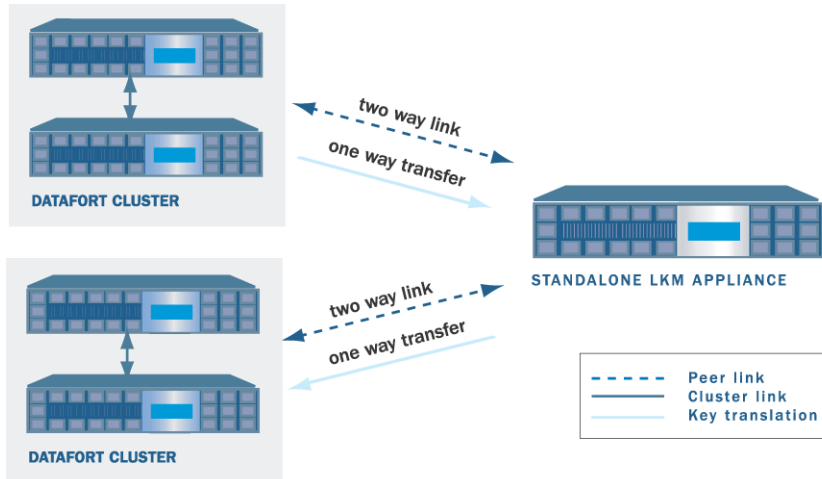


Figure 2-9: Single LKM Appliance with Multiple Clustered DataFort Appliances

A trustee link can be added to this configuration to allow direct continual bi-directional key sharing between the two DataFort clusters. See [Key Translation and Trustee Links](#) on page 19

DEPLOYING LINKED LKM APPLIANCE PEERS

This section includes the following topics:

- [Linked LKM Appliances with Standalone DataFort Appliances](#)
- [Linked LKM Appliances with DataFort Cluster](#)

Linked LKM Appliances with Standalone DataFort Appliances

Linked LKM appliances provide failover protection for encryption key and configuration database backups. Each DataFort appliance will pass encrypted keys to its peer-linked LKM appliance for storage. Peer-linked LKM appliances will replicate keys to store both of the DataFort appliances' keys on both of the LKM appliances. Each LKM appliance will pass keys to either peer-linked DataFort cluster member as required to restore deleted Cryptainer vaults.

A one-way key transfer of a limited number of keys between DataFort appliances via the LKM peers is supported. This enables the DataFort receiving the keys to decrypt data encrypted by the DataFort sending the keys. See [Key Translation and Trustee Links](#) on page 19

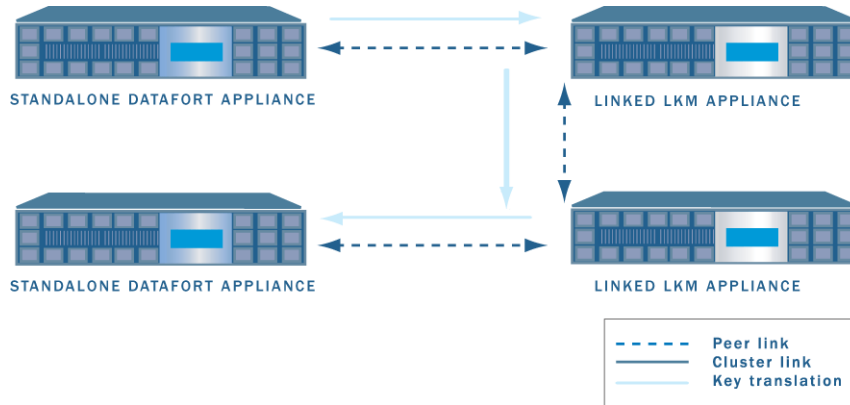


Figure 2-10: Linked LKM Appliances with Standalone DataFort Appliances

Linked LKM Appliances with DataFort Cluster

Linked LKM appliances provide failover protection for encryption key and configuration database backups. Keys are replicated between DataFort cluster members. One DataFort per cluster will pass encrypted keys to a peer-linked LKM. The LKM appliance will pass keys to either DataFort cluster member as required to restore deleted Cryptainer vaults.

A one-way key transfer of a limited number of keys between DataFort clusters via the LKM appliance is supported. This enables the DataFort cluster receiving the keys to decrypt data encrypted by the DataFort cluster sending the keys. See [Key Translation and Trustee Links](#) on page 19

Peer-linked LKM appliances will replicate keys to store both of the DataFort cluster keys on both of the LKM appliances. Each LKM appliance will pass encrypted keys back to either peer-linked DataFort cluster for decryption.

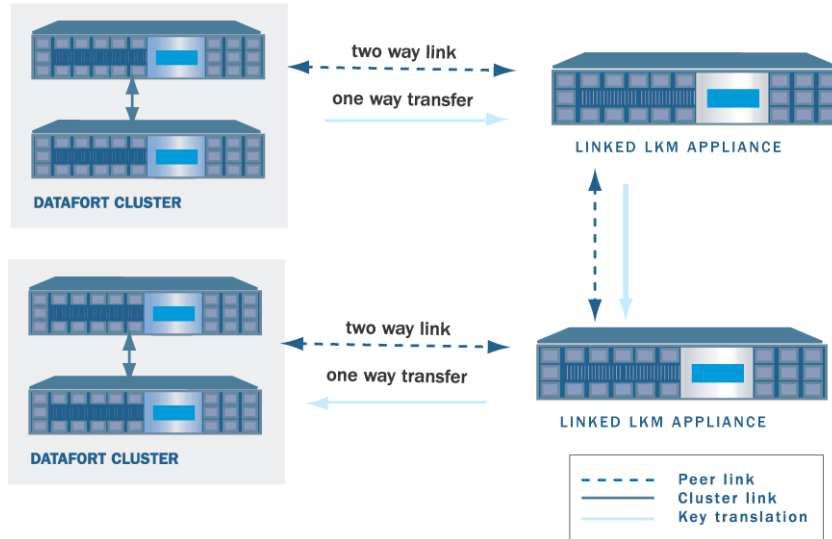


Figure 2-11: Linked LKM Appliances with Clustered DataFort Appliances



■ ■ ■ ■ 3 **INSTALLATION**

Ethernet connectivity is required between LKM appliances and all DataFort appliances 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 the RAID 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.

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, YOU MUST 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 THE RAID DISK DRIVES

The LKM appliance automatically stores all encryption keys and the most recent configuration database for any linked appliance on the RAID disk drives. See [About Configuration and Key Database Backups](#) on page 13.

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

To install the RAID:

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

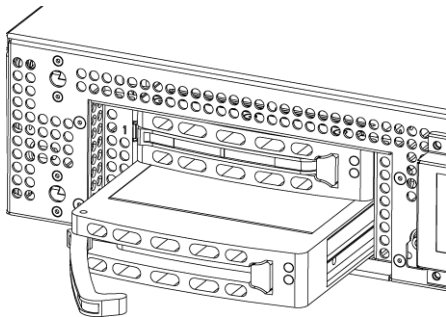


Figure 3-12: Front panel slots (with bezel removed) housing two RAID drives

6. Repeat the process for the RAID drive 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: A failed RAID drive can be replaced (hot-swap only) but working drives are not interchangeable. Contact Decru for service instructions if a RAID drive needs to be replaced.

RACK MOUNTING THE LKM APPLIANCE

LKM appliance design allows for easy installation in an EIA standard 19" rack or on a desktop. 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, and make sure you have 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. To insert the System Card:

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](#)

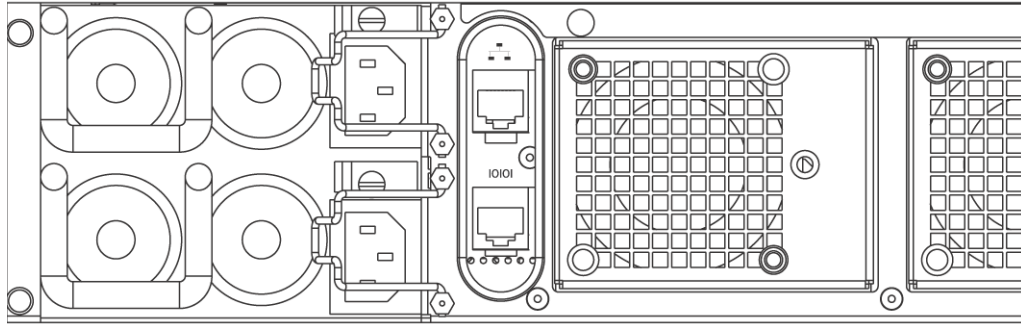


Figure 3-13: Rear panel connections

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 32.

Wait two to three minutes. When the LCD messages are complete you can 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 31.
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.

CAUTION: 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 [Backing Up the Configuration Database Manually](#) on page 63.
2. Choose from the following:
 - If using the CLI, see [Shutting Down an LKM Appliance](#) on page 93.
 - 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.

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

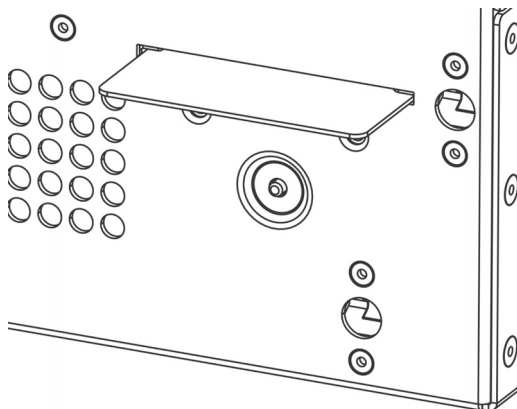


Figure 3-14: Front panel power button (bezel removed)

■ ■ ■ ■ 4 SETTING UP LIFETIME KEY MANAGEMENT

Use the Decru Management Console (DMC) interface to run the Setup Wizard and initialize new appliances. Because it is used to perform functions on both DataFort and LKM appliances, DMC provides a centralized management tool for the enterprise.

If SecureView is enabled, setup and management functions can be performed on several appliances simultaneously. See [SecureView](#) on page 15.

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 35.
2. Install the Decru Management Console on the Management Station.
See [Installing the Management Console](#) on page 37.
3. Initialize an appliance by adding it and running the Setup Wizard.
See [Initializing an Appliance via the Setup Wizard](#) on page 38.
4. Log into and link the initialized appliances that are added to DMC.
See [Logging into Appliances](#) on page 43 and [Linking Appliances to LKM](#) on page 44.

ASSIGNING THE IP ADDRESS

You must assign an IP address for the LKM appliance so that other devices on the network can send keys to the LKM appliance for storage, and 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.

See the following sections for details:

- [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 you finish entering the Management Port address, 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 31.
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: **MTKNMTKN**

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 LKM appliance
S. Shutdown LKM appliance
Z. Zeroize LKM 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 you finish and save your configuration, log in again. Settings are not saved until the Save and Exit commands are complete.

INSTALLING THE MANAGEMENT CONSOLE

The Decru Management Console runs on a dedicated PC (the Management Station). This console provides the management interface for the LKM appliance. It also offers some management functions for DataFort appliances in a given installation.

See the sections below for details:

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

MANAGEMENT STATION REQUIREMENTS

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

TABLE 5: MANAGEMENT STATION REQUIREMENTS

Software Requirements (choose 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. Key material is exposed during LKM operations—be sure the Management Station is a secure machine.

RUNNING THE INSTALLER

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

1. Insert the LKM CD in a drive on the Management Station.
The CD will run automatically if autorun is on.
2. Click the installer link.
The File Download screen prompts you to open or run the file.
3. 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 your 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

Use the Decru Management Console on the Management Station to run the Setup Wizard and initialize an appliance, including DataFort appliances. See the [DataFort Administration Guide](#) for information about using the wizard to add a DataFort appliance.

When you run the Decru Management Console for the first time, no appliances appear in the interface. To use the Setup Wizard, first add LKM appliance(s) to the console, then use the Setup Wizard to set up uninitialized appliances. Afterward, you can log into appliances for further management.

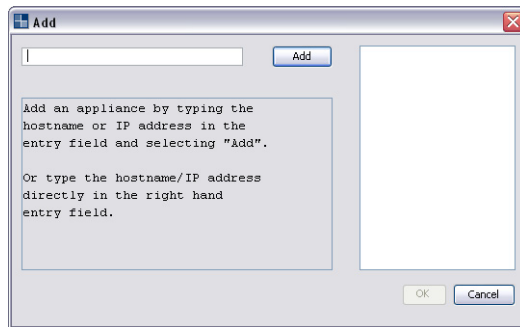
See the sections below for details:

- [Adding Appliances for the First Time](#)
- [Running the Setup Wizard](#)

ADDING APPLIANCES FOR THE FIRST TIME

Before running the Setup Wizard to initialize an LKM 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, choose from the following:
 - If no appliances are added, the Add screen appears automatically.
 - If appliances are added, from the Appliance menu, select Add.



3. On the Add screen, choose from the following:
 - In the single-entry text box, enter the IP address or hostname of the appliance and click Add.
 - In the multi-entry text box, enter all of the IP addresses or hostnames and click OK.
4. On the Certificates screen, choose whether to trust the certificate validating the connection between the appliance and the Management Console once or always.

RUNNING THE SETUP WIZARD

Before running the Setup Wizard, add an LKM appliance to the Decru Management Console. See [Adding Appliances for the First Time](#) on page 38.

To run the Setup Wizard:

1. In the Decru Management Console, in the Resources pane, highlight the appliance you will configure.
2. From the Appliance menu, select Setup.
3. On the Connect to Head of the Cluster screen, enter the hostname or IP address of the LKM appliance and click Next.
This is the same hostname or IP address you configured using the LCD or serial console during installation.
4. On the Certificates screen, choose whether to trust the certificate validating the connection between the appliance and the Management Console once or always.
5. On the Sign the License Agreement screen, read the license agreement and click Accept.
6. To skip the optional Recover from Database screen, click Next.
7. On the Create Administrator screen, enter a username and password for the administrator and click Next. 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 LKM 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. See [About Management Interfaces](#) on page 14.

8. On the 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.

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.

The screenshot shows a window titled "Decru Appliance Setup Wizard Step 7 of 12". The window has a "Network" header. Below the header, it says "Specify network information for each cluster member." and "Click Next after the Crypto Module is done initializing." There are four input fields: "Hostname 1" (empty), "Client NIC IP Address 1" (10.101.22.226), "Client NIC Netmask 1" (255.255.0.0), and "Client NIC Gateway 1" (10.101.20.1). At the bottom, there are "Cancel", "< Back", and "Next >" buttons.

9. On the Network screen, enter hostname of the appliance, the IP address of the appliance, and the netmask and gateway settings and click Next.
10. On the 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. Alternatively, you can paste multiple licenses in that are on consecutive but individual lines.
11. On the Network and Certificate screen, enter DNS information if you are using DNS and click Next.

Note: The next steps require that 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.

12. When prompted, insert the first Recovery Card into the Management Station's card reader.
Smart cards must be fully inserted into the reader. If a card is not recognized, re-insert it for better contact.

Decru Appliance Setup Wizard - Step 10 of 12

Initialize Recovery Card

Ask the Recovery Officer to pick a label and password for this new Recovery Card.
Use the Security Domain field to help you group related cards.

Card ID: 0900000053152511b8cfe69fb8fba2fa44402ac

Card Label:

Security Domain:

New Password:

Confirm Card Password:

Cancel < Back Next >

13. On the Initialize Recovery Card screen, enter a Card Label, security domain and password.
Confirm the password and click Next.

Note: Strong passwords are an important part of the overall security of the system. Passwords may be composed of upper and lower case characters, numbers and punctuation marks. Please select a password consisting of at least 8 valid, randomly chosen characters.

- 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.

When prompted, remove the Recovery Card and insert the next card, repeating for all Recovery Cards.

14. On the Apply Settings screen, click Next to complete setup of all the appliances.
15. On the Wizard Completed Successfully screen, click Finish.

You may now log into and link the initialized appliances that are added to DMC. See [Logging into Appliances](#) on page 43 and [Linking Appliances to LKM](#) on page 44.

■ ■ ■ ■ 5 GETTING STARTED

Add appliances to the Decru Management Console for centralized management. After adding appliances, log into and link them to LKM to automate backups and manage keys. See [About Configuration and Key Database Backups](#) on page 13, and [About Sharing Keys Between Appliances](#) on page 70.

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

This chapter includes the following topics:

- [Adding Appliances](#)
- [Logging into Appliances](#)
- [Linking Appliances to LKM](#)
- [Using Menus and Displays](#)

ADDING APPLIANCES

If you are adding an appliance for the first time, see [Adding Appliances for the First Time](#) on page 38.

To add an appliance:

1. In the Decru Management Console, from the Appliance menu, select Add.
2. On the Add screen, choose from the following:
 - In the single-entry text box, enter the IP address or hostname of the appliance and click Add.
 - In the multi-entry text box, enter all of the IP addresses or hostnames and click OK.
3. On the Certificates screen, choose 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 you log into them using the console.

LOGGING INTO APPLIANCES

Log into initialized appliances that are added to DMC. See [Initializing an Appliance via the Setup Wizard](#) on page 38.

To log into an appliance:

1. In the Decru Management Console, in the Resources pane, select an appliance.
 - Shift-click to select multiple appliances.
2. From the Appliance menu, select Log in.
 - You can also 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 46.

For the LKM appliance to manage keys it must be connected to the DataFort appliances that it will serve in the enterprise. See [Linking Appliances to LKM](#) on page 44.

LINKING APPLIANCES TO LKM

To support key management, create a communication channel between DataFort and LKM appliances. Once all appliances have been added to the console, and the relationship between appliances is created, appliance keys can be sent to LKM.

There are two methods to link appliances. See the following sections for details:

- [Using Drag and Drop](#)
- [Using the LKM Menu](#)

USING DRAG AND DROP

To link to an LKM appliance with drag and drop:

1. In the Decru Management Console, in the Resources pane, select an appliance.
 - Shift-click to select multiple appliances.
2. Drag the DataFort appliance icon(s) to the LKM appliance icon to send information from DataFort to LKM.
 - Drag one LKM appliance icon to the other to share information between LKM appliances.
3. On the Appliance Link screen, click OK.

USING THE LKM MENU

To link to an LKM appliance via the LKM menu:

1. In the Decru Management Console, in the Resources pane, select a DataFort or an LKM appliance.
2. From the LKM menu, select Link Appliances.
3. On the Select Appliance to Link screen, select the LKM appliance and click OK.
4. Repeat for all appliances that must be linked.

USING MENUS AND DISPLAYS

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

Note: If SecureView is enabled, you may select more than one appliance at once, and menu selections apply to selected appliances.

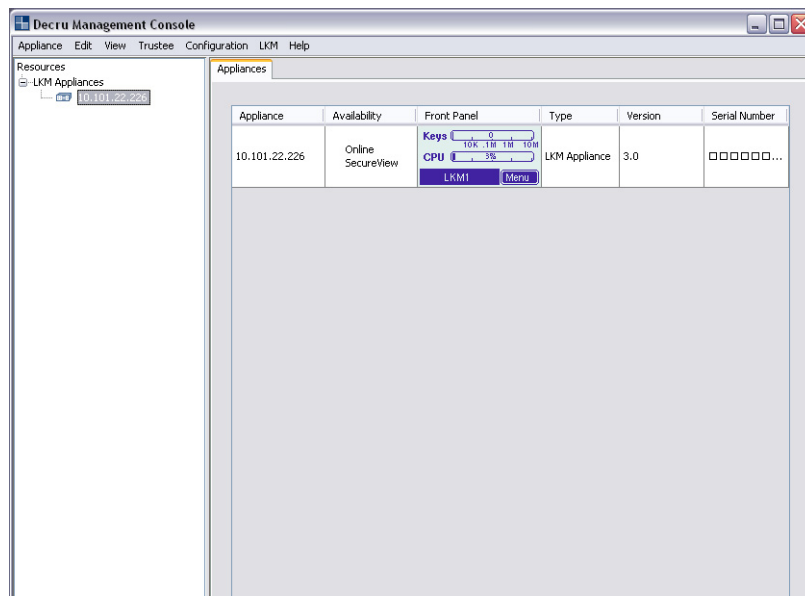
Some menu options initiate operations which are described in more detail in the [Appliance Management](#) and [Key Management](#) chapters of this guide.

The Decru Management Console provides the following options:

- [Appliance Tab](#)
- [State Displays](#)
- [Appliance Menu](#)
- [Edit Menu](#)
- [View Menu](#)
- [Trustee Menu](#)
- [Configuration Menu](#)
- [LKM Menu](#)
- [Help Menu](#)

APPLIANCE TAB

The DMC Appliance tab displays basic information about added appliances including name, status, and front panel LCD display. In addition, the Appliance tab displays the appliance type, software version and serial number. To display appliance information on the Appliance tab, select the appliance in the Resources pane.



LCD Display

The LKM appliance's front panel LCD is replicated on the Appliance tab. The front panel LCD shows name and status of the appliance, as well as any error messages about the condition of the appliance. It will also display the Number of Keys (0-10M) contained in the appliance and the CPU Load % (0-100).

STATE DISPLAYS

The condition of each appliance is indicated in the DMC with an icon in the Resources pane of the DMC screen. [Table 6](#) shows possible state displays for appliances in the Management Console.

TABLE 6: APPLIANCE STATUS INDICATORS

Icon	Icon Appearance	Appliance State
	Yellow with open icon	Uninitialized—IP address is set, but setup wizard not completed.
	Gray with exclamation	Incorrect login—Administrator name and/or password is incorrect, or log in is timed out (this occurs after 30 minutes if inactive).
	Blue	Online with no errors
	Blue with yellow alert	Online with error—See Appliance Tab for status details.
	Red	Offline
	Gray	Not logged in

APPLIANCE MENU

Appliance Menu options are available from the Appliance Menu or by right-clicking one or more appliances in the Resources pane.

Add	Add an LKM or DataFort appliance. See Adding Appliances for the First Time on page 38.
Remove	Remove an appliance in the Management Console. See Removing an Appliance on page 61.
Log in	Log in to an appliance as an administrator. See Logging into Appliances on page 43.
Log out	Log out of an appliance.
Set up	Set up an LKM or DataFort appliance by running the Setup Wizard. See Running the Setup Wizard on page 39.
Upgrade	Upgrade an appliance. Perform upgrades only after consulting Decru support. See Upgrading an Appliance on page 62.
Verify	Verify the validity of an upgrade package before upgrading. See Verifying an Upgrade Package on page 62.
Back up	Back up the configuration database of an appliance to a specified location. See Backing Up an Appliance on page 63.
Details	Show the system version for the selected appliance. See Viewing Appliance Details on page 61.
WebUI	Open the WebUI of the selected appliance (DataFort only). See Accessing the DataFort WebUI on page 52.
Command Line	Open the CLI. Whatever command you run executes on all selected appliances. See Accessing the Command Line Interface on page 52.
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 62.
Reboot	Reboot the selected appliance. See Rebooting an Appliances on page 61.
Zeroize	Zeroize the selected appliance. See Zeroizing an Appliance on page 61.
Smart Card Utilities	Reset a smart card and display card information. See Resetting Smart Cards on page 67.
Exit	Exit the Management Console. See Exiting the Console on page 52.

EDIT MENU

The Edit menu allows you to search for items in the console.

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.

VIEW MENU

The View setting determines how appliances display in the Resources pane. The default setting organizes appliances by type. You can 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.
Refresh	Refresh the view of appliances.

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 Trustee Links with SecureView on page 79.
Start Trustee Creation	Create trustee relationship. See Manually Creating Trustee Links on page 81.
Receive TEP	Allow selected appliance(s) to receive a Trustee Establishment Package. See Manually Creating Trustee Links on page 81.
Receive TAP	Allow selected appliance(s) to receive a Trustee Acceptance Package. See Manually Creating Trustee Links on page 81.
Unapproved Trustee List	Display list of trustees not yet approved (waiting to accept a TAP). See Delete Unapproved TAP Trustee on page 85.
Trustee List	Display list of trustees.

CONFIGURATION MENU

Select an appliance in the Resources pane. Choose Configuration and select from menu options.

License	View licenses. See Viewing Licenses on page 53.
Add License	Add licenses. See Adding a License on page 53.
Administrators	View and manage administrators. See Viewing Administrators on page 58.
Add Admin	Add an administrator. See Adding an Administrator on page 55.
Log Configuration	Select a log configuration. See Setting Log Options on page 59.
Replace Recovery Officer	Replace Recovery Officers. See Replacing a Recovery Card on page 65.

LKM MENU

Select an LKM appliance in the Resources pane. Choose LKM and select a menu item, or right-click an appliance and select from the right-click menu.

Link Appliances	Create a link between appliances. This is used for two purposes: link a DataFort and LKM appliance so that LKM can manage keys for that DataFort appliance, or link LKM appliances so that they share key information. Select both appliances to create a link. See Linking Appliances to LKM on page 44.
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 72.
Parent Keys	View all Parent Keys known to LKM appliance. See Viewing Parent Keys on page 71.
Recovery Cards	View all Recovery Cards associated with appliances known to LKM.
Make Key Archive	Create an archive of Parent Keys. This does not archive the keys from a single Cryptainer, but from a DataFort or series of DataFort appliances. See Generating a Parent Key Archive on page 73.
Make Cryptainer Key Archive	Create an archive of Cryptainer Keys. See Generating a Cryptainer Key Archive on page 75.
Translate Key(s)	Translate keys from one DataFort to another. See Transferring Cryptainer Keys on page 76.
Next	View next 300 keys in list.
Previous	View previous 300 keys in list.

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 86.

Import Keys

Imports key files that have been exported from another LKM appliance. See [Exporting and Importing Keys](#) on page 86.

Recover Keys

Recovers key files in the rare event the LKM appliance and its peers are down. See [Recovering Keys](#) on page 97.

Back Up DataFort Appliances

Sends a backup of the configuration databases of all DataFort appliances known to an LKM appliance. See [Backing Up All DataFort Appliances Linked to LKM](#) on page 63.

Make Cryptainer Key Archive File From

Makes a Cryptainer Key Archive from a recovered Key File to use with Decru Data Decryption Software (DDS). See [Making a Cryptainer Key Archive From a Key File](#) on page 87.

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 APPLIANCE MANAGEMENT

Use the Decru Management Console to add and manage LKM and DataFort appliances as well as administrators and licenses for all appliances.

Note: If SecureView licenses are in use, management functions can be applied to several appliances simultaneously. See [SecureView](#) on page 15.

The chapter includes the following topics:

- [Using Management Interfaces](#)
- [Managing Licenses](#)
- [Managing Administrators](#)
- [Setting Log Options](#)
- [Maintaining Appliances](#)
- [Upgrading Appliances](#)
- [Backing Up the Configuration Database Manually](#)
- [Managing Smart Cards](#)

USING MANAGEMENT INTERFACES

This section includes the following topics:

- [Accessing the Decru Management Console](#)
- [Accessing the DataFort WebUI](#)
- [Accessing the Command Line Interface](#)

ACCESSING THE DECRU MANAGEMENT CONSOLE

Before initializing an LKM appliance, you must add it to the Decru Management Console. See [Adding Appliances for the First Time](#) on page 38.

To open the Decru Management Console:

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

Exiting the Console

To exit the console choose 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 at the DMC icon at upper left-hand corner of the console screen.

ACCESSING THE DATAFORT WEBUI

See the [DataFort Administration Guide](#) for instructions on using the WebUI to manage DataFort appliances.

To open the WebUI for a DataFort appliance:

1. In the Decru Management Console, in the Resources pane, select the DataFort appliance.
2. From the Appliance menu, select WebUI.

ACCESSING THE COMMAND LINE INTERFACE

See the [DataFort Administration Guide](#) for instructions on using the Command Line Interface (CLI) to manage DataFort appliances. See [CLI Commands](#) on page 89.

To open the CLI for an appliance:

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 Appliance 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 LICENSES

This section includes the following topics:

- [Adding a License](#)
- [Viewing Licenses](#)

ADDING A LICENSE

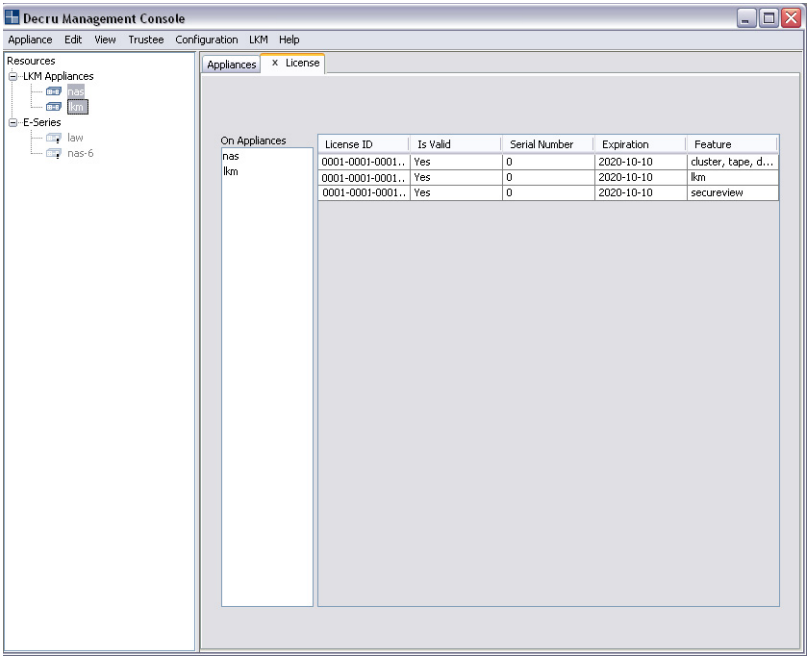
To add licenses to selected appliances:

1. In the Decru Management Console, in the Resources pane, select an appliance.
 - Shift-click to select multiple appliances.
2. From the Configuration menu, select Add License.
3. In the License ID field, enter the license and click Apply.

VIEWING LICENSES

To view the licenses on selected appliances:

1. In the Decru Management Console, in the Resources pane, select an appliance.
 - Shift-click to select multiple appliances.
 2. From the Configuration menu, select License.
- On the License tab, all known licenses for the selected appliance(s) appear.



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](#)
- [Adding an Administrator](#)
- [Viewing Administrators](#)

ABOUT ADMINISTRATORS AND RECOVERY OFFICERS

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

LKM 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 LKM 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.

Note: Decru recommends creating administrators with full permissions until appliance administration is well understood in the context of your organization.

Read-Only	Allows read-only permissions.
Specialty	Allows you to create an administrator with limited permissions.
Full Admin	Allows 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 7: SPECIAL ADMIN TYPES

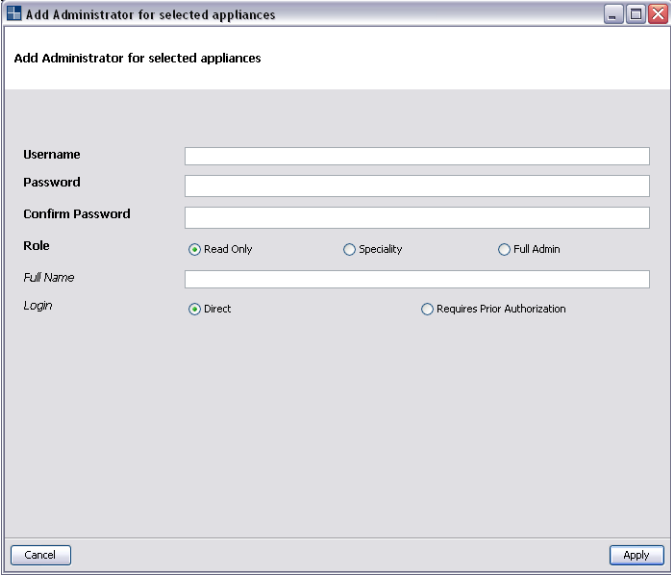
Admin Type	Responsibility	Appliance Type
Key Admin	Applying security-related settings to appliances.	DataFort only
Security Admin	Applying physical security-related settings to appliances.	DataFort and LKM
Accounts Admin	Adding, deleting and managing administrators.	DataFort and LKM
Storage Admin	Managing hosts/clients and storage to create Cryptainers.	DataFort only
Backup Admin	Managing backups of the configuration database.	DataFort only
Machine Admin	Managing system properties and non-security sensitive cluster operations. Changing local network settings.	DataFort and LKM

ADDING AN ADMINISTRATOR

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

To add an administrator to selected appliances:

1. In the Decru Management Console, in the Resources pane, select an appliance.
 - Shift-click to select multiple appliances.
2. From the Configuration menu, select Add Admin.



The screenshot shows a Windows-style dialog box titled "Add Administrator for selected appliances". The dialog has a title bar with standard minimize, maximize, and close buttons. The main content area is light gray and contains the following fields and options:

- Username:** A text input field.
- Password:** A text input field.
- Confirm Password:** A text input field.
- Role:** Three radio button options: ☒ Read Only, ☐ Specialty, and ☐ Full Admin.
- Full Name:** A text input field.
- Login:** Two radio button options: ☒ Direct and ☐ Requires Prior Authorization.

At the bottom of the dialog, there are two buttons: "Cancel" on the left and "Apply" on the right.

3. On the Add Administrator screen, enter the username and password of the administrator.
 4. Choose 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.
 - Select Full Admin to create an administrator with full permissions.
- Note:** Decru recommends creating administrators with full permissions until appliance administration is well understood in the context of your organization.

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

Cancel Apply

5. Enter the Full name and choose 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.

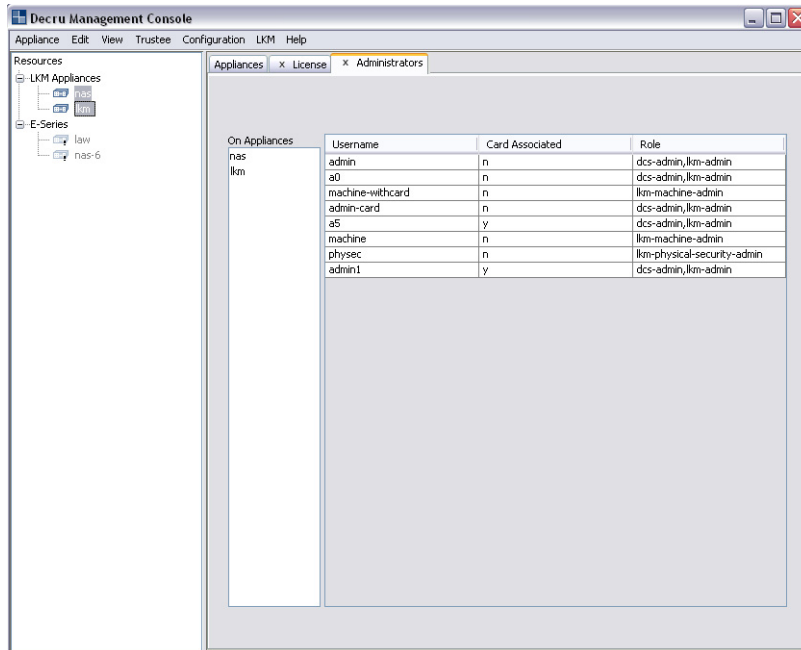
Note: Any Full Admin who can log in without authorization can grant any administrator the right to log in. See [Authorizing an Administrator Log In](#) on page 92.

6. Click Apply.

VIEWING ADMINISTRATORS

To view the administrator permissions for a selected appliance:

1. In the Decru Management Console, in the Resources pane, select an appliance.
 - Shift-click to select multiple appliances.
2. From the Configuration menu, select Administrators.



Deleting an Administrator

To delete an administrator:

- On the Administrators tab, right-click an administrator and select Delete.
- Shift-click and then right-click to multi-select.

SETTING LOG OPTIONS

This section includes the following topics:

- [About Log Options](#)
- [Setting the Logging Configuration](#)

ABOUT 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.

SETTING THE LOGGING CONFIGURATION

To set the log configuration:

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

Logging Configuration

Logging Configuration

Decru recommends storing critical logs in a permanent, remote location.

Windows Event Log User

Domain

Username

Password

Confirm Password

Modify Event Log User

☐

Security

	Temporary Database	Remote Logging Host	Event Log Host	Signed	
Low (6)	☐	☒			☐
High (4)	☐	☒			☐

Operations

Trace (7)	☒	☐			☐
Information (6)	☐	☒			☐
Warning (4)	☐	☒			☐
Error (1)	☐	☒			☐

Performance

Low (6)	☒	☐			☐
High (4)	☐	☒			☐

Cancel

Apply

The Logging Configuration screen appears

3. Select the desired settings and click Apply.

See [About Log Options](#) on page 59.

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

60

MAINTAINING APPLIANCES

This section includes the following topics:

- [Removing an Appliance](#)
- [Rebooting an Appliances](#)
- [Zeroizing an Appliance](#)
- [Viewing Appliance Details](#)
- [Collecting Tech Support Info](#)

REMOVING AN APPLIANCE

To remove an appliance from the Management Console:

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

REBOOTING AN APPLIANCES

To reboot selected appliances:

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

ZEROIZING AN APPLIANCE

Zeroizing an appliance erases and invalidates all encryption keys in the system and erases all configuration information. After zeroizing, run the Setup Wizard in the Management Console to assign a new configuration or restore a previous configuration. See [Running the Setup Wizard](#) on page 39 and [Disaster Recovery Scenarios](#) on page 95.

To zeroize an appliance:

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

VIEWING APPLIANCE DETAILS

To view the system version information for an appliance:

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.

COLLECTING TECH SUPPORT INFO

You can collect technical support information by running a script on the selected appliance. This is useful to technical support when evaluating a problem.

To run a script to collect technical support information:

1. In the Decru Management Console, in the Resources pane, select an appliance.
 - Shift-click to select multiple appliances.
2. From the Appliance menu, select Collect Tech Support Info.
3. Choose a location for the file and click Save.

UPGRADING APPLIANCES

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.

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.

This section includes the following topics:

- [Upgrading an Appliance](#)
- [Verifying an Upgrade Package](#)

UPGRADING AN APPLIANCE

To upgrade the appliance version with an upgrade package from Decru:

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Appliance menu, select Upgrade.
3. Browse to the upgrade file and click Apply.

VERIFYING AN UPGRADE PACKAGE

To verify an upgrade package before running it on the appliance:

1. In the Decru Management Console, in the Resources pane, select an appliance.
2. From the Appliance menu, select Verify.
3. Browse to the upgrade file and click Apply.

Note: After the package is verified, the hash will display in an alert box allowing you to verify the hash number with the known valid hash number.

BACKING UP THE CONFIGURATION DATABASE MANUALLY

This section includes the following topics:

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

BACKING UP AN APPLIANCE

To back up the configuration database of a DataFort or LKM appliance:

1. In the Decru Management Console, in the Resources pane, select an appliance.
 - Shift-click to select multiple appliances.
2. From the Appliance menu, select Back Up.
3. On the Select File screen, choose a location for the file and click Save.

BACKING UP ALL DATAFORT APPLIANCES LINKED TO LKM

An LKM appliance may access only the last backup of the configuration database for any DataFort appliance it is linked to.

To send a backup of the configuration databases of all DataFort appliances linked to an LKM appliance:

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

MANAGING SMART CARDS

Three types of smart cards are shipped with every LKM 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](#)
- [Resetting Smart Cards](#)

ABOUT SMART CARDS

The LKM 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 LKM appliance: the System Card, Admin Card and Recovery Cards.

System Card

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

Admin Card

The Admin Card authenticates communication between the administrator and LKM 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

To view Recovery Cards:

1. From the LKM menu, choose Recovery Cards.
2. On the Recovery Cards tab, 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

The Replace Recovery Officer option allows you to replace a Recovery Card in the set, thereby replacing the associated Recovery Officer as well.

To replace a Recovery Card or officer:

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

Replace Recovery Card

1. Select a Recovery Card to Remove

Jim@Finance
Alan@Finance
Bob@Finance
Cecilia@Legal
Warren@Legal

2. Identify replacement Recovery Card

Card Label

Security Domain

Select Current Selection: None

3. Authorize Replacement with Quorum of Recovery Cards

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.

Authorize Recovery Card Replacement

Replace Alan@Publications with new card with id 090000001f92d51742cfb6f5fadd98398a7ae216

Please select and/or insert a quorum of Recovery Cards.

Recovery Officers:

- Alan@Publications
- Lisa@Publications
- Jim@Publications

Card Label: Alan

Security Domain: Publications

Password:

Card Label: Jim

Security Domain: Publications

Password:

drCARD@ is not known to this DataFort

5. On the Authorize Recovery Card Replacement screen, choose 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.

Finish Replacement

new card with id 090000001f92d51742cfb6f5fadd98398a7ae216 has been authorized. Insert it now to finish the process.

Card Label:

Security Domain:

Password:

Confirm Password:

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 notifying you that the card has been replaced successfully.
7. Click OK.

ADDING AN ADMIN CARD TO AN ADMINISTRATOR

To add an administrator card to an administrator:

1. On the Administrators tab, right-click an administrator and select Add Admin Card.
2. 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.
3. On the Question screen, choose if you would like to turn on Secure Login.
4. To verify that your 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

To remove an administrator card from an administrator:

- On the Administrators tab, right-click an administrator and select Remove Admin Card.

RESETTING SMART CARDS

To reset smart cards, erasing username and password settings:

1. In the Decru Management Console, from the Appliance menu, choose 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.

Note: If you have multiple card readers, you can insert more than one card.
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.

7 KEY MANAGEMENT

The LKM appliance and the Management Console provide tools to manage keys in the enterprise. Encryption keys are required when data is decrypted. LKM and DataFort appliances will automatically decrypt data when online, but LKM also offers tools that make data recovery possible even if the DataFort or LKM appliance is offline. Use LKM menus in the console to create archive files of encryption keys to make data recovery possible if a DataFort or LKM appliance is made unavailable.

The chapter includes the following topics:

- [About Keys and Key Files](#)
- [About Sharing Keys Between Appliances](#)
- [Archiving Keys](#)
- [Transferring Cryptainer Keys](#)
- [Managing Trustees](#)
- [Backing Up Keys to External Storage](#)

ABOUT KEYS AND KEY FILES

The LKM appliance uses the following key types and files:

Key Types	Parent Keys	Parent Keys are used to encrypt all Cryptainer keys within a DataFort appliance. See Viewing Parent Keys on page 71.
	Cryptainer Keys	Cryptainer Keys are used to encrypt data within Cryptainers. See Viewing Cryptainer Keys on page 72.
	Translated Keys	Translated Keys are Cryptainer keys that have been decrypted from one DataFort appliance's Parent Key and encrypted with another DataFort's Parent Key, making it possible for both DataFort appliances to access the Cryptainer. See Translating Cryptainer Keys on page 76.
Key Files	Cryptainer Key Archive	This archive contains Cryptainer keys in a .cka file. To recover data, the LKM generates a Cryptainer Key Archive for a single Cryptainer or for all Cryptainers in a DataFort configuration to use with Decru Data Decryption Software (DDS). See Generating a Cryptainer Key Archive on page 75.
	Parent Key Archive	This archive contains Parent Key information in a .ka file. To recover data without Recovery Cards, you must generate a Parent Key Archive when a DataFort appliance is initialized. Use the archive to recover encrypted data if the original DataFort is unavailable. See Generating a Parent Key Archive on page 73.
	Key File	This file contains encryption keys exported from an LKM appliance in a .klf file. See Exporting and Importing Keys on page 86.

ABOUT SHARING KEYS BETWEEN APPLIANCES

There are several ways to share keys between appliances depending on the level of trust you want to create between appliances. The methods of key sharing and their requirements are listed below:

Cluster Link	Provides redundancy between DataFort appliances, by allowing key sharing and replication. Requirement: A Recovery Card quorum for each appliance is required for setup. See DataFort Administration Guide.
Peer Link	Provides automatic configuration database and data encryption key backups for any appliance linked to LKM. See Linking Appliances to LKM on page 44. Requirement: Appliances must be linked using DMC.
Trustee Link	Provides a link between any two non-clustered DataFort appliances, allowing appliances with no Recovery Cards in common, and that may not even be on the same network, to share data encryption keys. See Managing Trustees on page 78. Requirement: A Recovery Card quorum for each appliance is required for setup. Thereafter, you must import and export each key for each trustee. See Exporting and Importing Keys on page 86.
Key Translation	Transfers keys between DataFort appliances via LKM, allowing appliances with no Recovery Cards in common, and for which you do not wish to form a long term trustee relationship, to share data encryption keys. See Transferring Cryptainer Keys on page 76. Requirement: Either a Recovery Card quorum for each appliance or a Key Archive file for each appliance is required.

ARCHIVING KEYS

There are two types of key archives, a Parent Key Archive and a Cryptainer Key Archive. DataFort uses a Parent Key to encrypt Cryptainer Keys and a Cryptainer Key to encrypt data.

In the event that both a DataFort and its associated Recovery Cards are unavailable, LKM uses a Parent Key Archive to supply the keys needed to decrypt data. A Cryptainer Key Archive contains passphrase-encrypted Cryptainer or tape keys and allows the recovery of encrypted data under special circumstances without a DataFort appliance.

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:

- [Viewing Keys](#)
- [Generating a Parent Key Archive](#)
- [Generating a Cryptainer Key Archive](#)

VIEWING KEYS

View Parent and Cryptainer Keys from the Parent or Cryptainer Key tabs in the Decru Management Console. You may also change the view columns for both the Parent and Cryptainer Key tabs.

This section includes the following topics:

- [Viewing Parent Keys](#)
- [Viewing Cryptainer Keys](#)

Viewing Parent Keys

To view Parent Keys:

1. In the Decru Management Console, in the Resources pane, select an LKM appliance.
2. From the LKM menu, choose Parent Keys.
3. On the Parent Keys tab, click on a column to sort keys by that column.

To add and remove columns:

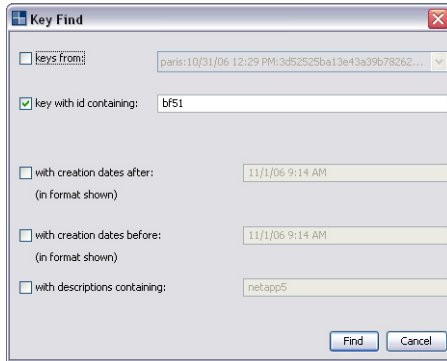
- Right click on a column title.
- From the Column Editor screen, select to add and remove columns and click OK.

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.

To view Cryptainer Keys:

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



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

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.
5. On the Cryptainer Keys tab, click on a column to sort 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.

GENERATING A PARENT KEY ARCHIVE

Create a Parent Key Archive after every DataFort is initialized in order to ensure key availability. The Key Archive is generally valid for the life of the DataFort. A new Key Archive is needed only if the DataFort is zeroized and subsequently reinitialized.

A Parent Key Archive requires the following:

- A quorum of Recovery Officers and Recovery Cards as configured during DataFort setup. 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.

To generate a Parent Key Archive:

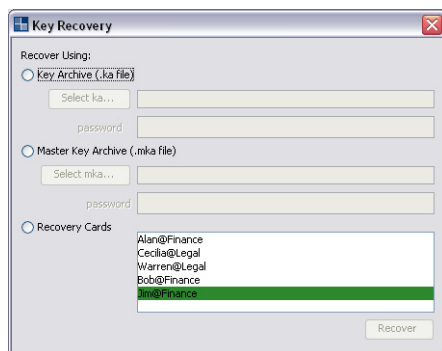
1. In the Decru Management Console, in the Resources pane, select an LKM appliance.

Note: The LKM appliance must be linked to a DataFort appliance. See [Linking Appliances to LKM](#) on page 44.

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

2. From the LKM menu, select from the following:
 - Cryptainer Keys. See [Viewing Cryptainer Keys](#) on page 72.
 - Parent Keys. See [Viewing Parent Keys](#) on page 71.
3. On the Cryptainer Keys or Parent Keys tab, right-click the key you would like to archive and choose Make Key Archive.

Note: Selecting any of the Parent Keys for a DataFort archives all of the Parent Keys for that DataFort. Selecting a Cryptainer Key archives all of the Parent Keys for that Cryptainer Key.



4. On the Key Recovery screen, choose a method to recover keys:

- [Using an Archive File to Generate Parent Key Archive](#)
- [Using Recovery Cards to Generate Parent Key Archive](#)

Using an Archive File to Generate 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. Select Key Archive or Master Key Archive file. Click the Select ka or Select mka button to browse for 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, choose 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 Generate Parent Key Archive

1. Select Recovery Cards and click Recover.
2. On the Recover Secret Shares screen, choose 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, choose 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.

GENERATING A CRYPTAINER KEY ARCHIVE

Use a Cryptainer Key Archive with separate Decru Data Decryption Software (DDS) to recover data. See the [Decru Data Decryption Software Administration Guide](#) for details.

A Cryptainer Key Archive requires **one** of the following:

- A quorum of Recovery Officers and Recovery Cards as configured during DataFort setup. 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.

To generate a Cryptainer Key Archive:

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 [Linking Appliances to LKM](#) on page 44.
2. From the LKM menu, choose Cryptainer Keys. See [Viewing Cryptainer Keys](#) on page 72.
3. On the Cryptainer Keys tab, right-click the key you would like to archive and choose Make Cryptainer Key Archive.
4. On the Key Recovery screen, choose a method to recover keys:
 - [Using an Archive File to Generate Cryptainer Key Archive](#)
 - [Using Recovery Cards to Generate Cryptainer Key Archive](#)

Using an Archive File to Generate Cryptainer 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 Cryptainer Key Archive.

1. Select Key Archive or Master Key Archive file. Click the Select ka or Select mka button to browse for 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, choose a name and location for the key archive file.
4. Enter a password for the archive and click Save.

Using Recovery Cards to Generate Cryptainer Key Archive

1. Select Recovery Cards and click Recover.
2. On the Recover Secret Shares screen, choose 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, choose a name and location for the key archive file.
4. Enter a password for the archive and click Save.

TRANSFERRING CRYPTAINER KEYS

Key Translation transfers Cryptainer Keys between DataFort appliances that are unrelated, that do not necessarily share Recovery Cards, and for which you do not wish to form a long term trustee relationship. See [Managing Trustees](#) on page 78.

This section includes the following topics:

- [About Translating Cryptainer Keys](#)
- [Translating Cryptainer Keys](#)

ABOUT TRANSLATING CRYPTAINER KEYS

Administrators may transfer (share) Cryptainer Keys from a source DataFort to a target DataFort. Key Translation does not disable Cryptainer Keys from the source DataFort.

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 TRANSLATION, CLEARTEXT KEYS ARE ZEROIZED IN RAM.

Transfer the key(s) to the LKM appliance for both the source and target DataFort appliances. After transferring keys to the target DataFort, perform a Cryptainer Restore operation on each of the Cryptainers, in order to make them accessible from the target DataFort. See the [DataFort Administration Guide](#) for details.

Transferring Cryptainer Keys requires **one** of the following:

- A quorum of Recovery Officers and Recovery Cards for both the source DataFort and the target DataFort. Each Recovery Officer is required to present a Recovery Card and its password.
- A Cryptainer Key Archive file for both the source DataFort and the target DataFort.

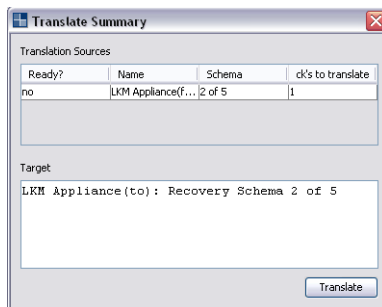
TRANSLATING CRYPTAINER KEYS

To transfer Cryptainer Keys:

1. In the Decru Management Console, in the Resources pane, select the LKM appliance.
2. From the LKM menu, choose Cryptainer Keys. See [Viewing Cryptainer Keys](#) on page 72.
3. On the Cryptainer Keys tab, right-click the key you would like to transfer, and choose Translate Key(s).
 - To select more than one key, Ctrl-click and then right-click.



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



- On the Translate Summary screen, review the translation activity and if correct, click Translate.
- On the Prepare Source DataFort Appliance (from) screen, choose a method to recover keys:
 - [Using an Archive File to Translate Cryptainer Keys](#)
 - [Using Recovery Cards to Translate Cryptainer Keys](#)

Using an Archive File to Translate 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 translate Cryptainer keys.

- Select Key Archive or Master Key Archive file. Click the Select ka or Select mka button to browse for the file, or enter the path and file name into the text box.
- In the password text box, enter the password for the selected file, and click Recover.
- When prompted, choose a name and location for the file.
- Enter a password for the archive and click Save.
- On the Prepare Target DataFort screen, choose a method to recover keys.
- A message appears indicating the number of keys successfully translated, click OK.

Using Recovery Cards to Translate Cryptainer Keys

1. Select Recovery Cards and click Recover.
2. On the Recover Secret Shares screen, choose 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, choose a name and location for the file.
4. Enter a password for the archive and click Save.
5. On the Prepare Target DataFort screen, choose a method to recover keys.
6. A message appears indicating the number of keys successfully translated, click OK.

MANAGING TRUSTEES

Creating trustees allows any two non-clustered DataFort appliances with no Recovery Cards in common, and that may not even be on the same network, to share data encryption keys. Once you establish a trustee relationship, it is possible to freely transfer keys between the two clusters by importing and exporting them. See [About Sharing Keys Between Appliances](#) on page 70.

Note: A trustee may export keys to or import keys from another trustee. Imported keys cannot be exported once they are imported. See [Sharing Keys between Trustees](#) on page 85.

Before sharing keys, trustees establish a relationship using two messages:

- The first message is the Trustee Establishment Package (TEP).
- The second message, a response to a TEP, is the Trustee Acceptance Package (TAP).

The establishment of trustees enables several enterprise scenarios:

- | | |
|-------------------------------|--|
| Disaster Recovery Site | Where there is an appliance off-site, and it is not desirable to form a cluster to share key data (either because there is no network connectivity between the main and off-site location, or because the topology is different at the remote site). |
| HQ with branches | Where there are many branch offices and it is desirable 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. |

This section includes the following topics:

- [Creating Trustee Links with SecureView](#)
- [Manually Creating Trustee Links](#)
- [Sharing Keys between Trustees](#)

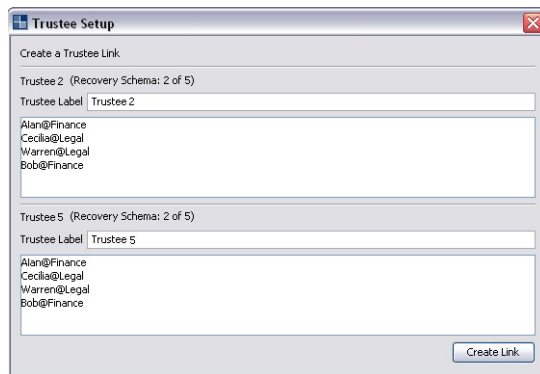
CREATING TRUSTEE LINKS WITH SECUREVIEW

You may create a trustee link if SecureView is enabled for multi-selection and both non-clustered DataFort appliances are in the same local network. See [About Management Interfaces](#) on page 14.

Note: Creating a trustee link requires a quorum of Recovery Officers and Recovery Cards for all appliances that will become trustees. Each Recovery Officer is required to present a Recovery Card and its password.

To create a trustee link using SecureView:

1. In the Decru Management Console, in the Resources pane, Ctrl-click to select both non-clustered DataFort 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.

You can edit the trustee label. By default it shows the hostname or IP address of the other appliance.

Note: The next step requires that you present smart cards to DMC. The number of cards required is established by the recovery schema set for each appliance at the time it was initialized.

Step 1: Approve TEP

Name | Trustee 2

Verifier | 19e5b2ec86d900328ce587b824d4832590fb4e6e6ad24afdec47388a1b5f820

Please select and/or insert a quorum of Recovery Cards.

Recovery Officers:

Alan@Finance
Cecilia@Legal
Warren@Legal
Bob@Finance

Card Label

Security Domain

Password

Card Label

Security Domain

Password

4. On the Approve TEP screen, choose 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.

5. A message appears indicating that a trustee link is created, click OK.

MANUALLY CREATING TRUSTEE LINKS

If the non-clustered DataFort appliances you wish to link are not on the same local network, you must follow the steps to manually create a trustee link for remote appliances. To create a trustee link if SecureView is enabled for multi-selection and both appliances are in network, see [Creating Trustee Links with SecureView](#) on page 79.

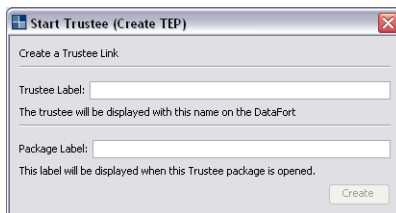
This section includes the following topics:

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

Start Trustee Creation

To create a trustee manually:

1. In the Decru Management Console, in the Resources pane, select a non-clustered DataFort appliance.
2. From the Trustee menu, select Start Trustee Creation.



3. On the Start Trustee (Create TEP) screen, do the following:
 - Enter a Trustee Label for the secondary trustee's appliance, for example the hostname of the appliance.
 - Enter a Package Label to identify the appliance (of the primary trustee) to the secondary trustee.
4. Click Create.
5. On the Select File screen, select a TEP file name and location and click Save.
6. From the Trustee menu, select Unapproved Trustee List.
7. On the Unapproved Trustee List tab, right-click the newly created trustee and select Copy Verifier.
8. Paste the verifier into a text file and save it.
9. Send the verifier file and the TEP file separately to the secondary trustee.

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 TEP

To receive the TEP (Trustee Establishment Package), the secondary trustee needs the TEP file and verifier received from the primary trustee. See [Start Trustee Creation](#) on page 81.

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

To receive the TEP:

1. In the Decru Management Console, in the Resources pane, select the secondary trustee non-clustered DataFort appliance.
2. From the Trustee menu, select Receive TEP

File:

Verifier:

Trustee Label:
The trustee will be displayed with this name on the DataFort

Package Label:
This label will be displayed when this Trustee package is opened.

3. On the Receive TEP screen do the following:
 - Browse to the TEP file.
 - Copy the verifier into the provided field.
 - Enter a Trustee Label for the primary trustee's appliance, for example the hostname of the appliance.
 - Enter a Package Label to identify the appliance (of the secondary trustee) to the primary trustee.
4. Click Begin Approval.

Note: The next step requires that you present smart cards to DMC. The number of cards required is established by the recovery schema set for each appliance at the time it was initialized.

Approve TEP

Name: TrusteeA

Verifier: db31e68d9b2de80229beccc76d6e47bcf8b5a365c5edb46d296dfe485ef4d276

Please select and/or insert a quorum of Recovery Cards.

Recovery Officers:

- dr3@sd
- dr2@sd
- dr1@sd

Card Label:

Security Domain:

Password:

Verify Password

Card Label:

Security Domain:

Password:

Verify Password

Start

5. On the Approve TEP screen, choose 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.

6. On the Select File screen, select a TAP file name and location and click Save.
7. From the Trustee menu, select Unapproved Trustee List.
8. On the Unapproved Trustee List tab, right-click the trustee and select Copy Verifier.
9. Paste the verifier into a text file and save it.
10. Send the verifier file and the TAP file separately to the primary trustee.

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 primary trustee needs the TAP file and verifier received from the secondary trustee. See [Receive TEP](#) on page 82.

To receive the TAP:

1. In the Decru Management Console, in the Resources pane, select the primary trustee non-clustered DataFort 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.

Note: The next step requires that you present smart cards to DMC. The number of cards required is established by the recovery schema set for each appliance at the time it was initialized.

5. On the Approve TAP screen, choose 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.

6. A message appears indicating that a trustee link is created, click OK.

Note: Once the primary trustee receives and approves the TAP, notify the secondary trustee so that they can delete the unapproved TAP trustee from their appliance.

Delete Unapproved TAP Trustee

Decru recommends that the primary trustee approve the TAP before the secondary trustee deletes the unapproved TAP trustee. This retains a backup TAP trustee file. See [Receive TAP](#) on page 84.

To delete the unapproved TAP trustee from the secondary trustee appliance:

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

SHARING KEYS BETWEEN TRUSTEES

Cryptainer keys may be shared between non-clustered DataFort appliance trustees. To export or import a key for a specific Cryptainer from a trustee via the CLI follow the instructions below.

Note: To export (but not import) 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](#).

BACKING UP KEYS TO EXTERNAL STORAGE

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 a key export fails, LKM keeps a copy of the last one million keys on its drives 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 Keys](#) on page 97.

This section includes the following topics:

- [Exporting and Importing Keys](#)
- [Making a Cryptainer Key Archive From a Key File](#)

EXPORTING AND IMPORTING KEYS

To export and import keys:

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

MAKING A CRYPTAINER KEY ARCHIVE FROM A KEY FILE

You may make a Cryptainer Key Archive from a Key File for use with separate Decru Data Decryption Software (DDS) to recover data. See the [Decru Decryption Software Administration Guide](#) for details.

WARNING: PERFORM THIS OPERATION ONLY IN THE RARE EVENT THAT THE LKM AND ITS PEERS ARE DOWN.

To make a Cryptainer Key Archive from a Key File:

1. In the Decru Management Console, from the LKM menu, select Make Cryptainer Key Archive From File.
2. On the Select Directory screen, choose a folder location and click Select.
3. On the Input screen, enter a full or partial key description (usually the Cryptainer name).
4. On the Select Key to include in Key File screen, select a key file from the list.
5. On the Key Recovery screen, choose a method to recover keys:
 - [Using an Archive File to Make a Cryptainer Key Archive From a Key File](#)
 - [Using Recovery Cards to Make a Cryptainer Key Archive From a Key File](#)

Using an Archive File to Make a Cryptainer Key Archive From a Key File

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 Cryptainer Key Archive.

1. Select Key Archive or Master Key Archive file. Click the Select ka or Select mka button to browse for 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, choose a name and location for the file.
4. Enter a password for the archive and click Save.

Note: Move the archive key file 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 Make a Cryptainer Key Archive From a Key File

1. Select Recovery Cards and click Recover.
2. On the Recover Secret Shares screen, choose 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. **17**

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, choose a name and location for the file.
4. Enter a password for the archive and click Save.

Note: Move the archive key file 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.

■ ■ ■ ■ 8 CLI COMMANDS

This chapter contains CLI commands that cannot be completed using the Decru Management Console menus.

Issuing CLI commands requires logging into the CLI. See [Accessing the Command Line Interface](#) on page 52.

The chapter includes the following topics:

- [Managing DataFort Appliances Linked to LKM](#)
- [Managing SNMP](#)
- [Viewing System Properties](#)
- [Changing Backup Intervals](#)
- [Assigning Names to Cryptainer Keys](#)
- [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](#)

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 [Linking Appliances to LKM](#) on page 44.

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, use 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, use 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 Lifetime Key Management](#) on page 33.

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, enter the appropriate SNMP command:

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 running 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
```

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, choose from 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 32.



■ ■ ■ ■ **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:

- [Disaster Recovery Scenarios](#)
- [Restoring an Appliance](#)
- [Recovering Keys](#)
- [Responding to a Bad Connection Error](#)
- [Viewing LED Displays](#)

DISASTER RECOVERY SCENARIOS

Failed appliances can be restored from saved configurations using the following procedures.

Standalone or Clustered DataFort Appliances

Recovering a failed standalone DataFort appliance requires a backup of the configuration database and the quorum of Recovery Cards from the original DataFort appliance or cluster. See the *DataFort Administration Guide*.

Standalone LKM Appliance

Recovering a failed LKM appliance requires the configuration database and the quorum of Recovery Cards from the original appliance, and an LKM Key Database export file. See [Restoring an Appliance](#) on page 96.

LKM to LKM Peer Appliances

Creating a peer link between LKM appliances allows appliances to automatically replicate keys. If one LKM appliance fails, the other maintains the key data for both. A Recovery Card set (new or previously initiated) is required when appliances are first installed, but not to create the link between peers. To recover the peer link, restore any failed appliances and re-link them. See [Linking Appliances to LKM](#) on page 44.

LKM to LKM Trustee Appliances

Creating a trustee link between LKM appliances allows keys to be shared so that if one trustee fails the other maintains its keys. A failed trustee can be restored with a backup configuration database and a quorum of Recovery Cards from the original appliance. See [Managing Trustees](#) on page 78.

RESTORING AN APPLIANCE

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.

Note: 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 35.

To start the Setup Wizard:

1. In the Decru Management Console, in the Resources pane, highlight the appliance you will configure.
2. From the Appliance menu, select Setup.
3. On the Welcome to the Decru Appliance Setup Wizard screen, click Start.
4. On the Connect to Head of the Cluster screen, enter the hostname or IP address of the LKM appliance and click Next.

This is the same hostname or IP address you configured using the LCD or serial console during installation.

5. On the Certificates screen, choose whether to trust the certificate validating the connection between the appliance and the Management Console once or always.
6. On the Sign the License Agreement screen, read the license agreement and click Accept.
7. On the Recover from Database screen, browse to select the .xdf file and click Open, then click Next.
8. On the Create Administrator screen, click Next.
 - If you do not have the administrator password, click the New Admin check box and click Next.

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 LKM appliance.

9. On the Recovery Card Schema screen, click Next.
10. On the Network screen, wait until the progress bar completes and click Next.
11. On the Add Decru-provided Licenses screen, add licenses and click Next.
12. On the Network and Certificate screen, click Next.

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.

13. On the Recovery Card Authentication screen, enter a Recovery Card and password.
14. On the Apply Settings screen, reinsert the cards and when prompted click OK.
Note: Multiple readers allow you to move through this process quickly since you can insert multiple cards at once. Otherwise, insert one card at a time into the single reader.
15. The Wizard Completed Successfully screen, click Finish.
 After restoring the appliance, you may restore its keys.
16. To restore appliance keys, import the last key backup of the LKM appliance. See [Exporting and Importing Keys](#) on page 86.
Note: Additionally, you may need to recover keys.

RECOVERING KEYS

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: LKM keeps a copy of the last one million keys on its drives 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 86.
- The recovery key backup. See procedure below.

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

To recover keys:

1. In the Decru Management Console, in the Resources pane, select the LKM appliance.
2. From the LKM 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, choose 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 running 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 31.
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 8: 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 9: BACK PANEL LED

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

■ ■ ■ ■ APPENDIX II MIGRATING FROM LKM SERVER TO LKM APPLIANCE

Use this process to migrate keys from the Lifetime Key Management (LKM) Server software to the Lifetime Key Management (LKM) appliance. When transferring keys, do not connect the LKM software and LKM appliance to the same DataFort.

Note: This process will decommission LKM software. You cannot transfer keys back to LKM software from the LKM appliance.

This chapter includes the following topics:

- [Requirements](#)
- [Halting LKM Server Operations](#)
- [Installing the Key Transfer Tool](#)
- [Running the Key Transfer Tool](#)

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 choose 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.

RUNNING THE KEY TRANSFER TOOL

Before running 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, choose 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 86](#).



■ ■ ■ ■ **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 10: LKM PROCESS MESSAGES

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

The logs in [Table 11](#) 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 11: LKM APPLIANCE CONNECTION MESSAGES

Message	Description
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 12: PROCESS MESSAGES

Log Message	Description
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 13: CONNECTION MESSAGES

Log Message	Description
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 14: 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
	WEEE	Europe, China 2007
Regulatory Compliance	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



■ ■ ■ ■ **APPENDIX V REGULATORY AND CERTIFICATIONS**

The chapter includes the following topics:

- [FCC B Declaration of Conformity](#)
- [European Union](#)
- [Canadian ICES-003](#)
- [VCCI Class B Statement](#)
- [CE Statement](#)



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 Management™ 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 (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	The backup of the configuration database including synced keys (from either the DataFort or another LKM appliance) are stored on the RAID (redundant array of independent disks) disk drives in the LKM appliance.
Recovery Cards	Recovery Cards are special smart cards used in sets to store and recover DataFort and LKM encryption keys by sharing a secret. Recovery Cards are given to the Recovery Officers, who will have to present them in order to perform security-sensitive procedures.
Recovery Officers	Recovery Officers are entrusted with keeping Recovery Cards and their associated passwords safely. Recovery Officers must present their cards and passwords to initialize a new DataFort. A quorum of Recovery Officers is required for other sensitive options such as data recovery, cluster authentication, and Recovery Card replacement.
SAN	A Storage Area Network (SAN) is a high-performance network dedicated to the transmission of storage data. It is often (but not necessarily) implemented with Fibre Channel.
Security Domain	A Security Domain defines a distinct group of Recovery Cards. Multiple Security Domains can be used in the enterprise to compartmentalize access to deployed DataFort appliances.
Smart Cards	Credit card-sized devices with embedded microchips used by DataFort for authentication procedures.
SNMP	Simple Network Management Protocol. A protocol for network management and monitoring of network devices.
SSH	Secure Shell or Secure Socket Shell. A command interface and protocol used for remote access to a computer. SSH communication with the remote computer is encrypted.
SSL	Secure Sockets Layer. A protocol providing secure message transfer over the Internet. Used to secure transmission of data via web browsers.
Storage Encryption Processor (SEP)	DataFort's hardware encryption/decryption engine, that enables gigabit-speed, full duplex encryption.
System Card	A smart card provided by Decru that is inserted at the front panel of DataFort for boot-up to enable DataFort encryption services. The System Card may be removed during normal operation to prevent unauthorized use of DataFort upon reboot.
Trustee	A trustee is a remote DataFort with which a trust relationship has been formed, allowing exportable Cryptainer Keys to be shared. A trustee may import from or export to a trustee.
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

- about
 - cluster link 70
 - Cryptainer key archive file 69
 - Cryptainer keys 69
 - key translation 70
 - parent key archive file 69
 - parent keys 69
 - peer link 70
 - transfer of Cryptainer keys 76
 - translated keys 69
 - trustee link 70
- access
 - CLI 52
 - WebUI 52
- adaptor
 - RJ45 to DB9 31
- add
 - administrator 55
 - administrator card 67
 - license 53
 - LKM appliance to DMC 43
 - LKM appliance, first time 38, 52
- Admin Card
 - about 108
- administrator
 - about 108
 - add 55
 - add card 67
 - manage 58
 - permissions 55
 - remove card 67
 - types 55
- administrators
 - about 54
- AES
 - about 108
- appliance
 - back up 63
 - menu 47
 - remove 61
 - tab 45
 - upgrade 62

- verify upgrade package 62
- zeroize 61

- archive
 - Cryptainer keys 75
 - Cryptainer keys from file 87
 - keys 71
 - parent keys 73
- authentication
 - about 108

B

- back panel
 - LED 98
- back up
 - appliance 63
 - configuration database to external storage 14
 - DataFort appliance 63
 - keys to external storage 86
 - LKM appliance 63
 - LKM keys to external storage 14
- backup interval
 - configuration database 92
- backups
 - about 13
 - frequency of configuration database 13
 - frequency of keys to LKM 13
- battery iv, 28
- block cipher
 - about 108

C

- Canadian ICES-003
 - certification 106
- Category 5 cable 31
- CE
 - certification 107
- certification
 - Canadian ICES-003 106
 - CE 107
 - declaration of conformity 106
 - European Union 106
 - VCCI Class A 107
- chassis
 - about 108

- ciphertext
 - about 108
- cleartext
 - about 108
- CLI
 - access 52
 - commands 89
- client
 - about 109
- cluster
 - about 109
- collect
 - tech support info 62
- commands
 - CLI 89
 - intrusion alerts 93
 - SNMP 91
- configuration
 - menu 49
- configuration database
 - about 109
 - backup interval 92
 - frequency of automatic backups 13
 - manual back up 14
- conventions
 - LKM appliance guide 15
- create
 - trustee links manually 81
 - trustee links with SecureView 79
- Cryptainer
 - about 109
- Cryptainer keys
 - about 69
 - about archive file 69
 - about key transfer 76
 - archive 75
 - archive from file 87
 - assign names to 92
 - transfer 76
 - view 72
- cryptography
 - about 109

D

- DataFort
 - assign IP address 35
 - assign IP settings from LCD 35
 - assign IP settings from serial console 36

- back panel connections 31
- back up 63
- diagram, back panel 31
- link to LKM 44, 90
- purge keys 17
- restore 96
- specifications 104
- declaration of conformity
 - certification 106
- Decru Management Console 15
- deployment scenarios
 - multiple LKMs and clustered DataForts 25
 - multiple LKMs and non-clustered DataForts 24
 - single LKM and clustered DataFort 22
 - single LKM and DataFort 22
 - single LKM and multiple clustered DataForts 23
 - single LKM and non-clustered DataFort 23
 - single LKM appliance 22
- disaster recovery requirements
 - for LKM peers 95
 - for standalone DataFort 95
 - LKM trustee appliances 95
- display
 - LCD 46
 - state 46

E

- edit
 - menu 48
- encryption keys
 - transfer 76
- European Union
 - certification 106
- exit
 - management console 52
- export
 - keys to external storage 86
 - trustee keys 85

F

- failover 108
 - about 109
- fibre channel
 - about 109
- front panel
 - assign IP address 35
 - LED 98
 - System Card slot 30

H

- help
 - menu 50

I

- import
 - keys from external storage 86
 - trustee keys 85
- installation
 - key transfer tool 100
 - management console 37
 - precautions v, 28
 - rack mount 30
 - RAID 29
 - run installer 38
- intrusion alerts
 - clear 93
 - commands from CLI 93
- IP settings
 - assign from LCD 35
 - assign from serial console 36
- IPsec
 - about 109
- IT power systems 28

K

- keys
 - about 109
 - archive 71
 - back up to external storage 86
 - Cryptainer 69
 - Cryptainer key archive file 69
 - export to external storage 86
 - frequency of automatic backups 13
 - import from external storage 86
 - install transfer tool 100
 - key file 69
 - limits for enterprise 17
 - manage 68
 - manual back up 14
 - parent 69
 - parent key archive file 69
 - recover 97
 - run transfer tool 100
 - transfer from LKM 2.5 to 3.0 99
 - transfer of 70
 - translated 69
 - translation 76

- translation of 70
- view 71

L

- LCD
 - assign DataFort IP settings 35
 - display 46
- LED
 - back panel 98
 - front panel 98
- license
 - add 53
 - management 53
- Lifetime Key Management
 - about 109
- link
 - cluster 70
 - DataFort appliances to LKM 90
 - peer 70
 - to LKM via drag and drop 44
 - to LKM via the LKM menu 44
 - trustee 70
- lithium battery iv, 28
- LKM appliance
 - add to DMC 43
 - add to DMC, first time 38, 52
 - back up 63
 - backups 13
 - boxmanager connection messages 103
 - boxmanager process messages 103
 - check connectivity status of 93
 - check status of 93
 - connect 30
 - deployment of 16
 - features overview 11
 - guide conventions 15
 - link to DataFort appliance 44
 - LKM connection messages 102
 - LKM process messages 102
 - log into 43
 - menu 49
 - shut down 93
 - troubleshooting 94
 - understanding 12
- LKM server
 - halt operations 100
- lkmd 102
- log in

- authorizing administrator log in 92
- to LKM appliance 43

M

- manage

- administrator 53, 58
 - keys 68
 - licenses 53
 - Smart Cards 64
 - the LKM appliance 61
 - trustees 78

- management

- console, exit 52
 - console, install 37
 - from console 15
 - interface 14
 - port 31
 - SecureView 15
 - station 37

- management interface

- console 14
 - LCD 14
 - serial 14

- management port

- connect to Ethernet 31

- Management Station 15

- management station

- about 109
 - requirements 37
 - security 37

- menu

- appliance 47
 - configuration 49
 - edit 48
 - help 50
 - LKM appliance 49
 - trustee 48
 - use 45
 - view 48

N

- names

- assign to Cryptainer keys 92

- NAS

- about 109

O

- online help 50

- operations scenarios

- configuration database backups 21

- key translation 20

- key translation vs. Trustee Link 19

P

- parent keys

- about 69
 - about archive file 69
 - archive 73
 - view 71

- permissions

- administrator 55

- port

- management 31

- power

- cords 31
 - LKM appliance on 32
 - on after shut down 32
 - precautions 28
 - supply notice 28

- purge keys

- DataFort appliance 17

Q

- quorum

- about 109

R

- rack mount

- DataFort 30
 - installation 30
 - standard 30

- RAID

- about 110
 - installation 29

- recover

- keys 97

- Recovery Card

- about 110
 - replace 65

- recovery officers

- about 54, 110

- remove

- administrator card 67
 - appliance 61

- replace

- Recovery Card 65

- requirements
 - management station 37
- reset
 - Smart Cards 67
- restore
 - DataFort 96
- run
 - installer 38
 - key transfer tool 100
 - Setup Wizard 39

S

- SAN
 - about 110
- security
 - management station 37
- security domain
 - about 110
- SEP
 - about 110
- serial console
 - connect serial port 31
 - DataFort settings 36
- Setup Wizard
 - run 39
- shut down
 - LKM appliance 32, 93
- Smart Cards
 - about 64, 110
 - admin 64
 - manage 64
 - recovery 64
 - reset 67
 - system 64
- SNMP
 - about 110
 - commands 91
- SSH
 - about 110
- SSL
 - about 110
- state displays 46
 - use 45
- System Card
 - about 110
 - insert 30
- system details
 - view 61

- system properties
 - view 91

T

- tab
 - appliance 45
- TAP 78
 - about 110
- tech support info
 - collect 62
- TEP 78
 - about 111
- transfer
 - Cryptainer keys 76
 - encryption keys 76
- transfer keys
 - from LKM 2.5 to 3.0 99
- translated keys
 - about 69
- troubleshooting
 - LKM appliance 94
- trustee
 - about 110
 - create links manually 81
 - create links with SecureView 79
 - export keys 85
 - import keys 85
 - manage 78
 - menu 48
- Trustee Acceptance Package (TAP) 78
- Trustee Establishment Package (TEP) 78

U

- UDP
 - about 111
- upgrade
 - appliance 62

V

- VCCI Class A
 - certification 107
- verify
 - appliance upgrade package 62
- view
 - Cryptainer keys 72
 - keys 71
 - menu 48
 - parent keys 71

- system details 61
- system properties 91

W

- WebUI
 - about 111
 - access to 52
- wizard
 - use Setup Wizard 38

Z

- zeroize appliance 61