



ADMINISTRATION GUIDE

Lifetime Key Management
Appliance 3.1

security

LKM Appliance Administration Guide

Copyright © 2003-2008 Decru, Inc. All rights reserved.

Part number: 210-03856 A0 LKMA (011408_KM31)

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 même type ou d'un type équivalent recommandé par le constructeur. Mettre au rebut les batteries usagées conformément 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, take special precautions to ensure that the system remains stable. These guidelines are provided to ensure your safety:

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

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

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

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

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

CONTENTS

Chapter 1 Lifetime Key Management Appliance Overview	12
About the Lifetime Key Management Appliance	13
Features at a Glance	13
LKM Guide Terms and Conventions	14
LKM Terminology	14
Conventions Used in this Manual	15
Understanding the LKM Appliance	16
How the LKM Appliance Works	16
How Keys are Archived and Shared	17
How Key and Configuration Database Archives Work	18
Chapter 2 Deploying an LKM Appliance	19
Enterprise Key Management	20
Key Sharing Policy	21
Key Sharing Group Guidelines	21
Archive Policy	23
Manual Key Translation	23
Enterprise Key Limits	24
Key Generation Frequency	24
Secure Network Practices	25
Maintain Configuration Database Backups	25
Send Recovery Cards to Escrow	25
Plan Remote Security Logging	25
Remove the System Card	26
Prepare for Manual Security Responses	26
Chapter 3 Installing LKM Appliance	27
Notices and Warnings	28
Power Supply Notice	28
Power Cable Notice	28
Dual Power Supply Notice	28
Lithium Battery Notice for Service Personnel	28
Rack Mounting	28
Installation Requirements	29
Hardware Requirements	29
Network Requirements	30
Management Station Requirements	30
Installing Hard Disk Drives	31
Rack Mounting the LKM Appliance	32
Connecting the LKM Appliance	33
System Card Insertion	33
Rear Panel Network Connections	33

Powering On and Off	34
Running the Installer	36
Chapter 4 Accessing Management Interfaces	37
About Management Interfaces	38
Security Policies	39
Using SecureView	39
Using Remote Authorization	39
SNMP Settings	39
Online Help	39
Decru Management Console (DMC) Options	40
Using the DMC	40
Connecting via Standard DMC	40
Connecting via Secure DMC	41
Connecting via DMC Using Dual Authorization	41
Using the Command Line Interface	42
CLI Help	42
Connecting via Standard CLI	42
Connecting via Secure CLI	43
Connecting via CLI Using Dual Authorization	44
Connecting to DMC CLI	44
Accessing the Appliance Serial Console	45
Logging into the Serial Console Port	45
Configuring IP Settings	45
Clearing IP Settings	45
Using the Appliance Front Panel LCD	46
Touch Panel On-screen Buttons	46
Chapter 5 Setting up an Appliance	47
Assigning IP Address	48
Setting IP Address Using the Serial Console	48
Setting IP Address Using the LCD	49
Initializing an Appliance via the Setup Wizard	50
About the Setup Wizard	50
Adding Appliances to DMC to Initialize	50
Using the Setup Wizard	51
Logging in to Appliances Using DMC	54
Exiting DMC	54
Chapter 6 Using DMC Menus and Displays	55
State Displays	56
About the Appliances Tab	57
Adjusting Table Columns	57
Appliance Menu	58
Edit Menu	59
View Menu	59
Configuration Menu	60

Keys Menu	61
Topology Menu	61
Utilities Menu	62
Security Menu	63
Trustee Menu	63
Diagnostics	64
Help Menu	64
Chapter 7 Managing Administrators and Smart Cards	65
Managing Administrators	66
About Administrator Roles	66
About Administrator Authentication	68
Protecting Against Insider Attacks	68
Viewing Administrators	69
Adding an Administrator	69
Modifying Administrators	70
Authorizing an Administrator Log In	71
Managing Smart Cards	72
About Smart Cards	72
Viewing Recovery Cards	73
Viewing Recovery Cards from LKM	74
Replacing a Recovery Officer	74
Adding an Admin Card to an Administrator	75
Sharing an Admin Card	76
Changing a Recovery Card Password	76
Resetting Smart Cards	76
Chapter 8 Managing Appliance Security	77
Configuring Management Security Settings	78
Setting Appliance Defense Responses	78
About Defense Response Triggers and Settings	78
About Defense Alerts	80
Changing the Defense Setting	80
Manual Security Response	80
Setting Security Certificates	81
About Security Certificates	81
Setting a Local Security Certificate	82
Setting a Certificate Authority Signed Certificate	82
Clearing Intrusion Alerts	83
Chapter 9 Sharing Keys	84
Creating Trustee Relationships	85
Creating Trustees on a Local Network	85
Creating Trustees on a Remote Network	89
Creating Link Policies	92
Creating a Key Sharing Policy	92
Creating an Archive Policy	93

Contents

Creating an OpenKey Policy	94
Managing Link Policies	95
Viewing Link Report	95
Adding Linked Appliances to DMC	95
Viewing an OpenKey Client	95
Changing Key Sharing Groups	96
Changing Key Sharing Groups for OpenKey Clients	96
Changing Key Sharing Groups for DataFort Appliances	96
Changing a Key Sharing Group for Keys	97
Moving Unshared Keys into a Key Sharing Group	97
Chapter 10 Managing Keys	98
Viewing Keys	99
Viewing Parent Keys	99
Viewing Parent Keys from LKM	99
Viewing Data Encryption Keys	99
Archiving DataFort Parent Keys	100
About Archiving Parent Keys	100
Creating Archives of Parent Keys	101
Backing Up Keys to External Storage	103
About Exporting and Importing Keys	103
Exporting and Importing Keys	103
Using Manual Key Translation	104
About Key Translation	104
Translating Cryptainer Keys	104
Chapter 11 Managing Appliances	107
Adding Appliances to DMC	108
Adding Appliances to DMC	108
Adding DataFort Cluster Members to DMC	108
Removing Appliances from DMC	108
Creating Custom Appliance Groups	109
Removing an Appliance from a Custom Group	109
Removing a Custom Group	109
Upgrading an Appliance	110
Setting Login and Refresh Preferences	110
Verifying an Upgrade Package	110
Managing Licenses	111
Viewing Licenses	111
Adding a License	111
View OpenKey License Usage	111
Backing Up Appliances Manually	112
Best Practices for Secure Backups	112
Backing Up an Appliance	112
Backing Up Appliances to LKM	113
Backing Up Appliances from LKM	113

Contents

Configuring SNMP Options	114
About SNMP Options	114
Setting SNMP Options	115
Updating Network Settings	116
Updating Date and Time Settings	116
Configuring and Viewing Logs	117
About Log Options	117
Appliance Log Storage Guidelines	118
About Decru Signed Syslogd (DSS)	118
Setting Log Options	119
Setting Windows Event Logging	120
Setting Up Syslog	120
Viewing the Appliance Log	121
Verifying Signed Log Messages	122
Adding Time Zone Information to Syslog Timestamp	122
Zeroizing an Appliance	123
About Zeroizing the Appliance	123
Zeroizing the Appliance	124
Zeroizing via the Serial Console	124
Zeroizing via the CLI	125
Emergency Serial Console Port Access	125
Rebooting an Appliance	126
Chapter 12 Using Advanced CLI Commands	127
Maintaining the Appliance	128
Changing Backup Intervals	128
Assigning Names to Data Encryption Keys	128
Checking the Status of an LKM Appliance	129
Checking the Connectivity Status Between Appliances	129
Setting System Properties	129
Viewing System Properties and Log Messages	130
Verifying System Logs	131
Setting Stack Trace	132
Chapter 13 Troubleshooting	133
Maintaining the Appliance Status	134
Viewing Appliance Details	134
Collecting Tech Support Info	134
Responding to a Bad Connection Error	134
Recovering LKM Appliances	135
About Recovering LKM Appliances	135
Recovering Linked LKM Appliances	135
Recovering Standalone LKM Appliance	136
Recovering Physically Damaged LKM Appliances	136
Recovering LKM Appliances Due to Hard Drive or Boot Failure	136
Recovering LKM Appliance Keys	139

Contents

About Key Recovery	139
Recovering Keys	139
Replacing Hardware	140
Replacing Hard Disk Drives	140
Replacing Fans and Power Supplies	141
Viewing LED Displays	142
Front Panel LEDs	142
Back Panel LEDs	142
Checking Network Connections and Management Interfaces	143
Checking Smart Cards	145
Appendix I Migrating from LKM Server to LKM Appliance	146
Migration Requirements	147
Halting LKM Server Operations	147
Installing the Key Transfer Tool	148
Using the Key Transfer Tool	148
Appendix II Port IDs	149
Appendix III Log Functions	150
About Logs	151
Appliance Log Types	151
Log Message Parameters	152
Log Storage Locations	154
Log Presentation	155
Temporary Logs	155
Database Logs	155
Remote Logs	156
Log Purging	158
Temporary Storage Log Messages	158
Database Storage Log Messages	158
LKM Appliance Log Messages	159
Appliance Management Messages	160
Appendix IV Partial List of ISO Country Codes	161
Appendix V Specifications	162
Appendix VI Regulatory and Certifications	163
FCC B Declaration of Conformity	164
European Union	164
Canadian ICES-003	164
VCCI Class B Statement	165
CE Statement	165
Appendix VII Glossary	166
Index	170

1 LIFETIME KEY MANAGEMENT APPLIANCE OVERVIEW

Key management is a critical component of any encryption system, especially when that system is intended to encrypt data at rest. Enterprise data is sometimes stored for months or years, so encryption keys must be archived securely and recovered transparently, without adding complexity for administrators or users. The Decru Lifetime Key Management™ appliance (LKM appliance) securely automates the archiving and recovery of encryption keys across the enterprise, so data is always secure and available.

The Lifetime Key Management™ appliance (LKM appliance) is Decru's third generation key management platform and enables centralized key management for large, distributed encryption environments. The LKM appliance delivers enterprise-class scalability, availability, and security, along with Decru OpenKey™ API's to support third-party encryption platforms.

This chapter contains the following topics:

- [About the Lifetime Key Management Appliance](#)
- [LKM Guide Terms and Conventions](#)
- [Understanding the LKM Appliance](#)

ABOUT THE LIFETIME KEY MANAGEMENT APPLIANCE

The LKM appliance stores and manages encryption keys and configurations for each Decru DataFort® appliance across an enterprise. Each LKM appliance is designed for enterprise-class availability, incorporating redundant hard drives and power supplies, and supporting automated key replication to other LKM appliances.

FEATURES AT A GLANCE

The LKM appliance offers the following features:

- Supports LKM clients across the enterprise LAN or WAN
- Supports 100 DataFort appliances and 10 million keys per LKM appliance
- Up to 16 LKM appliances can be linked to support large deployments of 1000 or more DataFort appliances
- Provides high availability of data through key encryption and replication
- Provides centralized management for multiple DataFort and LKM appliances
- Provides key management services to heterogeneous clients through OpenKey API
- Supports up to 14 user-defined key attributes for OpenKey client keys
- Provides global distributed backup, replication, and recovery of heterogeneous encryption keys
- Provides automated key distribution for information sharing
- Uses Decru's FIPS 140-2 Level 3-certified Storage Encryption Processor (SEP) for encryption
- Provides role-based administration controls for tiered management
- Provides tamper-evident logging and auditing

LKM GUIDE TERMS AND CONVENTIONS

This section contains the following topics:

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

LKM TERMINOLOGY

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 a Speciality Administrator may execute a limited set of specific functions. See About Administrator Roles on page 66.
Archive Policy	The LKM appliance archives all encryption keys for its clients and the most recent configuration database for any DataFort appliance. The LKM appliance uses automatic and manual backup methods to archive keys and configuration data. See How Keys are Archived and Shared on page 17.
Configuration Database	The database stored inside an appliance and contains network and security information, ACLs and (on DataFort) encrypted key material. The LKM appliance automatically stores the most recent configuration database for any linked DataFort or LKM appliance. See How Key and Configuration Database Archives Work on page 18.
Cryptainer Key	Each DataFort Cryptainer is associated with its own encryption key, which is required to encrypt and decrypt the stored data. Each encryption key used for a Cryptainer is in turn encrypted by a Parent Key, shared by the members of a DataFort cluster.
Data Encryption Key	LKM appliances automatically stores Data Encryption Keys for all LKM clients in the enterprise. See How Key and Configuration Database Archives Work on page 18.
Decru Management Console (DMC)	The Decru Management Console (DMC) is an application that is installed on a secure Management Station. It provides a centralized management interface for all LKM clients and appliances in a network. See Running the Installer on page 36.
Key Sharing Group	LKM clients form key sharing groups and automatically share keys between group members when creating a key sharing policy. Clients in a key sharing group with an LKM appliance pass encryption keys to that LKM appliance. The LKM appliance also passes keys to clients. See Key Sharing Group Guidelines on page 21.
Key Sharing Policy	LKM clients may use a key sharing policy when linking to an LKM appliance. This allows them to form a key sharing group and automatically share keys. The LKM appliance continues to archive all encryption keys for its clients and the most recent configuration database for any DataFort appliance. See How Keys are Archived and Shared on page 17.
LKM Client	Decru appliances or OpenKey clients that are linked to an LKM appliance.
LKM Software	The LKM Software utility securely automates the archiving of encryption keys across the enterprise, so data is always readily available. DataFort supports either the LKM software or the LKM appliance but not both. See the DataFort Administration Guide .

Opaque Key	This is a wrapped Data Encryption Key that the LKM appliance simply archives. To unwrap these keys, either a Recovery Card quorum or a Key Archive file for each Decru appliance is required. See How Keys are Archived and Shared on page 17.
OpenKey™	OpenKey is a Secure Key Management Network Protocol and API. The OpenKey API is used to create OpenKey clients which can securely communicate with the LKM appliance.
Parent Key	The Parent Key is encrypted by a master key, unique to each appliance. This master key, generated at the time an appliance is initialized, is used to decrypt and encrypt key material for safe storage and backup.
Recovery Officer	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 appliance. A quorum of Recovery Officers is required for other sensitive options such as data recovery, cluster authentication, and Recovery Card replacement. See About Smart Cards on page 72.
Remote Authorization	Remote Authorization allows an administrator to initiate and verify Recovery Card operations for DMC Setup and Trustee wizards from a remote location. Using Remote Authorization on page 39.
SecureView™	SecureView is a licensed feature which enables enterprise class appliance management. This feature is enabled on a per-appliance basis. See Using SecureView on page 39.
Smart Card	Credit card-sized devices with embedded microchips used by appliances for authentication procedures. Appliances incorporate smart cards into network management, backup and recovery procedures. This provides a second layer of authentication beyond username and password credentials. 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 72.
Trusted Key	The LKM appliance stores these unwrapped Data Encryption Keys on the LKM appliance and wraps them in its own Parent Keys. This allows unrelated Decru appliances to share keys using an LKM appliance without manually importing and exporting keys or going through the key translation process. A trustee relationship with an LKM appliance, and a key sharing group membership is required. See How Keys are Archived and Shared on page 17.
Trustee Relationship	Decru appliances must form a trust or trustee relationship with an LKM appliance before creating a key sharing group. This allows them to share keys without manually importing and exporting keys or going through the key translation process. See Creating Trustee Relationships on page 85.

CONVENTIONS USED IN THIS MANUAL

This guide uses the following typographic conventions:

- Keyboard commands appear in mono-spaced font in **blue**.
- PDF links appear as [underlined purple](#) text.
- Buttons that can be clicked in the interface are identified by name, with no change in font

UNDERSTANDING THE LKM APPLIANCE

The LKM appliance manages encryption keys for multiple DataFort appliances and OpenKey clients (LKM clients) ensuring encryption key availability for the life of the secured data. The LKM provides a central location to distribute keys between clients based on key sharing policies or by manually transferring keys.

This section contains the following topics:

- [How the LKM Appliance Works](#)
- [How Keys are Archived and Shared](#)
- [How Key and Configuration Database Archives Work](#)

HOW THE LKM APPLIANCE WORKS

The LKM resides on the Ethernet portion of the network along with the LKM clients. Linking LKM appliances and clients provides a secure channel for key backup and replication and allows clients to automatically share key data. See [How Keys are Archived and Shared](#) on page 17.

Note: Each LKM client must be connected to at least two LKM appliances, making connections across sites redundant. Each LKM appliance must link with another LKM appliance to ensure the availability of all keys.

The LKM appliance automatically archives all encryption keys for its clients and the most recent configuration database for any appliance on its hard disk drives (RAID). See [Figure 1-1](#).

The LKM appliance also maintains its own key and configuration databases which can be backed up to external storage and is automatically backed up to another LKM appliance. See [How Key and Configuration Database Archives Work](#) on page 18.

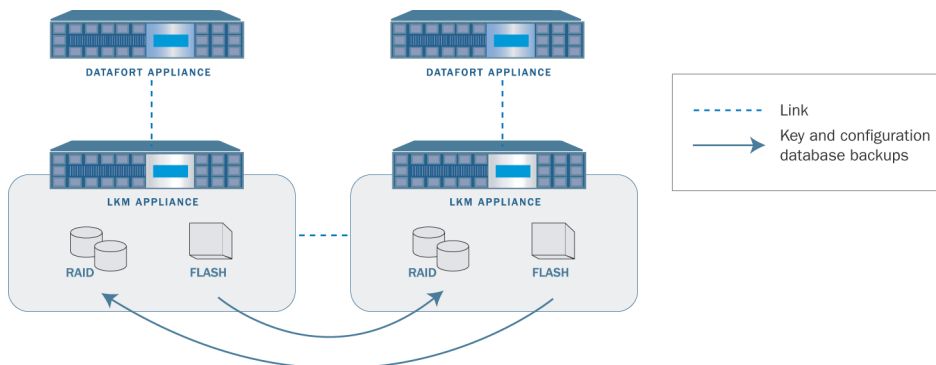


Figure 1-1: Key and Configuration Database Backups

HOW KEYS ARE ARCHIVED AND SHARED

Keys are archived on the LKM appliance and shared between LKM clients based on link policies including key sharing, archive and OpenKey policies. See [Creating Link Policies](#) on page 92.

Note: All links formed between appliances use a SSL (Secure Socket Layer) connection.

TABLE 1: LINK POLICIES

Link Policy	Details	Requirements
Decru Key Sharing Policy	• Allows Decru appliances to store keys wrapped with LKM appliance Parent Keys on the LKM appliance. • Allows unrelated Decru appliances to share keys through an LKM appliance without manually importing and exporting keys or going through the key translation process. • Allows Decru appliances to archive configuration data on the LKM appliance.	• A trustee relationship with an LKM appliance. See Creating Trustee Relationships on page 85. • A key sharing group membership. • A Recovery Card quorum for each Decru appliance is required to create trustee relationship. • A System Card must be present in the LKM appliance in order to execute this cryptographically sensitive operation.
Decru Archive Policy	• Not intended to enable key sharing. • Allows Decru appliances to store keys on the LKM appliance wrapped with the source Decru appliance Parent Keys. • Allows Decru appliances to archive configuration data on the LKM appliance.	• Manual key translation using the Decru Management Console (DMC). • Either a Recovery Card quorum or a Key Archive file for each Decru appliance is required to translate keys via DMC. See Using Manual Key Translation on page 104.
OpenKey Policy	• Enables OpenKey clients to store keys on the LKM appliance. • Allows OpenKey key sharing group members to securely distribute keys. • OpenKey clients are not yet able to share keys with DataFort appliances.	• A certificate package for each OpenKey client. • Optional—key sharing group membership.

HOW KEY AND CONFIGURATION DATABASE ARCHIVES WORK

The LKM appliance automates the global backup, replication and recovery of encryption keys, ensuring that keys are always available. DataFort appliances can automatically share keys with other DataFort appliances in a cluster for availability, and they can back up their configurations and keys to up to four distributed LKM appliances. If a required key is unavailable locally, DataFort appliances can then automatically retrieve the appropriate key from an LKM appliance. See [Enterprise Key Limits](#) on page 24.

TABLE 2: KEY AND CONFIGURATION DATABASE BACKUP METHODS

Backup Method	Key Backup	Configuration Database Backup
Automatic Backups to LKM appliance	- Decru appliances are queried for new keys every five seconds by an LKM appliance. If a Decru appliance returns a key, the LKM appliance asks for the new key immediately. If there is no new key, the LKM appliance waits five more seconds before sending another request. The LKM appliance does this for every Decru appliance it is linked with, so that almost as soon as a new key is created on an appliance, the key is synced to the LKM appliance. - OpenKey clients are responsible for sending updated keys to the LKM appliance. The LKM appliance does not query OpenKey clients for new keys.	- The LKM appliance retains only the most recent backup of the configuration database for Decru appliances. Decru appliances initiate a backup of the configuration database to an LKM appliance approximately every two hours. The backup interval can be changed. See Changing Backup Intervals on page 128. - The configuration database can also be backed up remotely from the Decru appliance. See Backing Up Appliances Manually on page 112.
Manual Backups to External Storage	In the unlikely event that an LKM appliance and its peers are down, backing up the LKM key database to external storage makes recovery possible. See Backing Up Keys to External Storage on page 103.	- Backing up the LKM appliance configuration database to external storage is useful in restoring key sharing group data. - 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 made obsolete. See Backing Up Appliances Manually on page 112.

■ ■ ■ ■ 2 DEPLOYING AN LKM APPLIANCE

LKM appliances provide key replication and archival for single network installations, and they can also be deployed to offer key management across multiple sites, multiple DataFort appliance clusters and OpenKey client locations.

This chapter contains the following topics:

- [Enterprise Key Management](#)
- [Key Sharing Policy](#)
- [Archive Policy](#)
- [Enterprise Key Limits](#)
- [Secure Network Practices](#)

ENTERPRISE KEY MANAGEMENT

Multiple LKM appliances can share keys across a large configuration which includes DataFort clusters and OpenKey clients. LKM appliances store encryption keys for the entire enterprise, and can share them between remote sites. Once LKM appliances are linked, the appliances provide seamless key management across the entire enterprise. A single instance of the Decru Management Console running on the Management Station manages all appliances in use.

When choosing how to link appliances consider how keys are archived to an LKM appliance and shared between LKM clients. See [How Keys are Archived and Shared](#) on page 17.

Note: Each LKM client must be connected to at least two LKM appliances, making connections across sites redundant. Each LKM appliance must link with another LKM appliance to ensure availability of all keys.

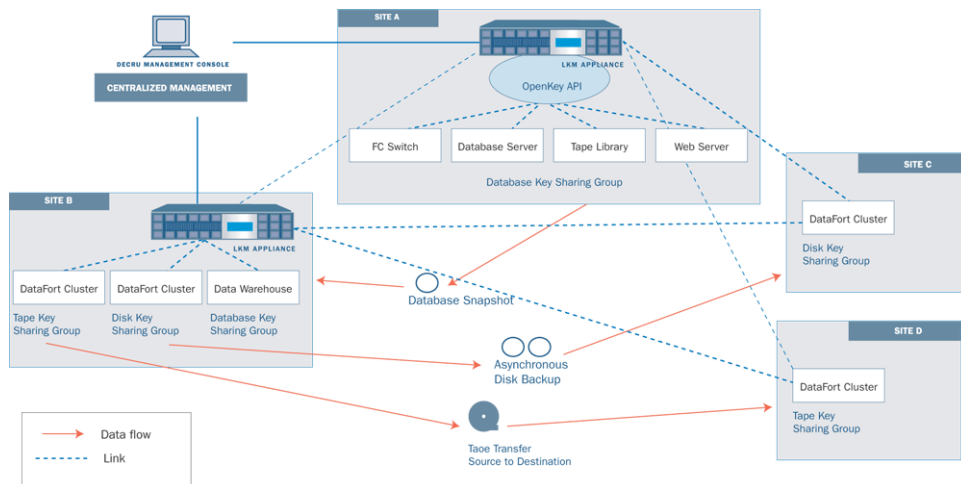


Figure 2-2: Enterprise Key Management

KEY SHARING POLICY

A key sharing policy allows LKM clients to form key sharing groups and automatically share keys between group members. Clients in a key sharing group with an LKM appliance may pass encryption keys to that LKM appliance, and LKM appliances pass keys to clients.

Key sharing group memberships are maintained on the LKM appliance. Therefore, the LKM administrator must ensure that each LKM client is registered into the same key sharing group on every LKM appliance it is linked to, otherwise key replication problems may occur.

Note: Use a Decru Key Sharing Policy or an OpenKey Policy when automatic key sharing is desired. See [Creating Link Policies](#) on page 92.

KEY SHARING GROUP GUIDELINES

When creating automatic key sharing groups the following guidelines apply:

- Key sharing group memberships are maintained on the LKM appliance. Therefore, the LKM administrator must ensure that each client is registered into the same key sharing group on every LKM appliance it is linked to, otherwise key replication problems may occur.
- Key sharing groups support hierarchies which include a top level or Root group, and may include additional Parent and Child groups up to two levels excluding the Root group.
- LKM appliances are always in the top level Root group ('/') and cannot be changed. Appliances in the Root group can receive keys from all other groups.
- Appliances in the same Child group may freely share keys with each other and with any Parent groups. For example, appliances in '/x/' may share keys with each other, and may also share keys with '/'.
 - Appliances in different Child groups may not share keys with each other. For example, appliances in '/x/' may share keys with each other, but they may not share keys with '/y/'.
- In scenarios that include a data recovery site, groups may be created such that one particular group of appliances may receive keys from all other appliances in a one-way fashion from Child to Parent group. For example, appliances in '/world/' may receive keys from both '/world/x/' and '/world/y/', but appliances in '/world/' may not share keys with '/world/x/' or '/world/y/'. See [Figure 2-4](#) on page 22.

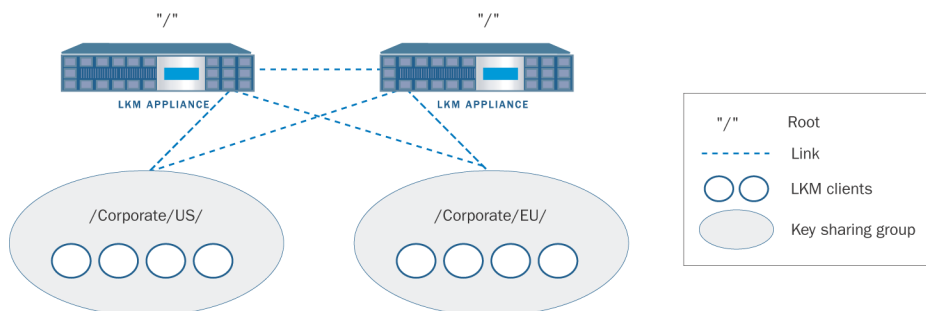


Figure 2-3: Sample 1: Key Sharing Groups

In [Figure 2-4](#) remote recovery sites decrypt data with encryption keys retrieved from either LKM appliance.

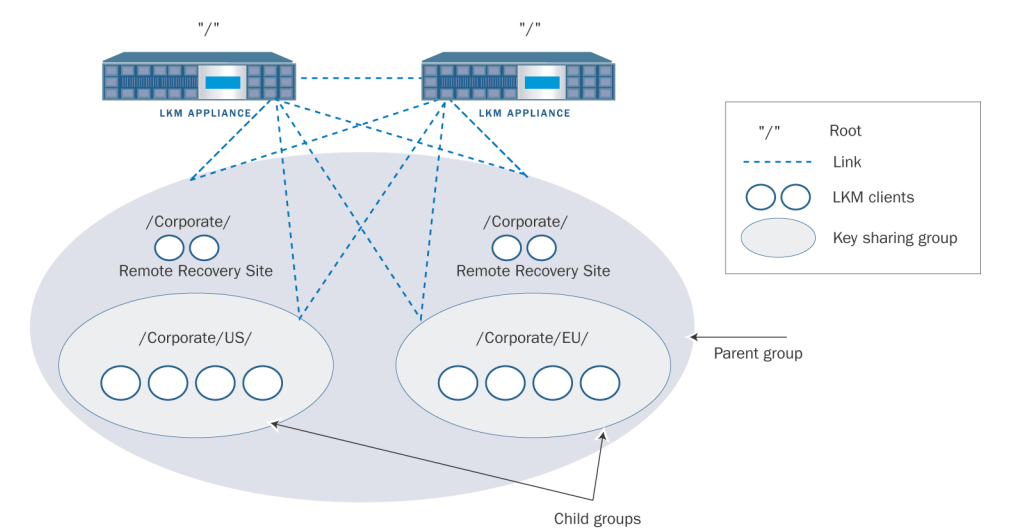


Figure 2-4: Sample 2: Key Sharing Groups

[Table 3](#) shows the key sharing group relationships that may be formed when using the configuration in [Figure 2-4](#).

TABLE 3: EXAMPLE OF KEY SHARING GROUP RELATIONSHIPS

Key Sharing Groups		To Destination: Data Read			
		/Corporate/EU/	/Corporate/US/	/Corporate/	/
From Source: Data Encrypted	/				✓
	/Corporate/			✓	✓
	/Corporate/US/		✓	✓	✓
	/Corporate/EU/	✓		✓	✓

ARCHIVE POLICY

The Decru Archive Policy is used to store Opaque Keys wrapped with the source Decru appliance Parent Keys, and to archive configuration data on the LKM appliance. When using an archive policy, [Manual Key Translation](#) is required to translate keys for DataFort appliances via DMC.

Note: Use a Decru Key Sharing Policy or an OpenKey Policy when automatic key sharing is desired. See [Creating Link Policies](#) on page 92.

MANUAL KEY TRANSLATION

When using a Decru Archive Policy, unrelated DataFort appliances that are linked to a shared LKM appliance may share keys by initiating a one-way key transfer. The LKM appliance enables the DataFort appliance receiving the keys to decrypt data encrypted by the DataFort appliance sending the keys. See [Using Manual Key Translation](#) on page 104.

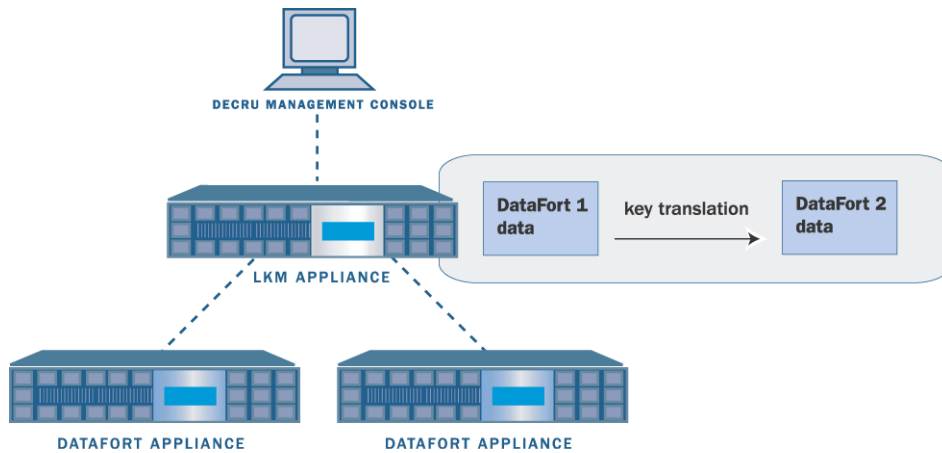


Figure 2-5: Key Translation

ENTERPRISE KEY LIMITS

LKM appliances provide encryption key backup, management, and replication across the entire enterprise. The number of LKM appliances and clients required across the entire installation is determined by the aggregate data throughput required by LKM clients, the frequency of key generation, and redundancy requirements.

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

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

TABLE 4: APPLIANCE KEY LIMITS

Appliance Type	Item	Limit
Lifetime Key Management appliance	Number of LKM clients per LKM appliance	100
	Keys per LKM appliance	10 million
	Number of LKM appliances that can be linked together	16
DataFort appliance	Keys per DataFort appliance. The DataFort appliance purges keys from the configuration database when the limit is reached.	4500 for E-Series 8000 for FC-Series
	Number of DataFort appliance connections to LKM appliance or LKM software. See DataFort Administration Guide .	4

KEY GENERATION FREQUENCY

For DataFort appliances, keys are generated when a Cryptainer is created, rekeyed or translated from one DataFort to another. In some organizations, such as those where new backup tapes are created each day, key generation may be high.

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

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

SECURE NETWORK PRACTICES

Determine the desired level of security for your organization before installing the LKM appliance. For a high-security organization, plan an installation that includes a location for storing remote logs and database backups, and the use of an escrow service for smart card and password storage. Consider the following recommended procedures for a highly-secure network installation.

- [Maintain Configuration Database Backups](#)
- [Send Recovery Cards to Escrow](#)
- [Plan Remote Security Logging](#)
- [Remove the System Card](#)
- [Prepare for Manual Security Responses](#)

MAINTAIN CONFIGURATION DATABASE BACKUPS

For maximum security and recoverability, keep configuration database backups up to date. See [Backing Up Appliances Manually](#) on page 112.

SEND RECOVERY CARDS TO ESCROW

Each LKM appliance is configured with a data recovery schema that determines the minimum number of Recovery Cards required for data recovery to take place. There are several ways in which Recovery Cards can be configured, depending on the security policy of the enterprise.

Your organization may choose to use a key escrow service to store Recovery Cards, configuration database backups and Key Archives. Procedures for key escrow should be established as part of your organization's security policy. The recommended procedure is to send the escrow service both the encrypted backup of a configuration database for each LKM appliance and a quorum of Recovery Cards for each Security Domain.

Note: With Remote Authorization, it is possible to store cards in escrow while still managing a global network of appliances. See [Using Remote Authorization](#) on page 39.

When using an escrow service, configure an LKM appliance to use 2 out of 5 Recovery Cards for recovery procedures. Two of the Recovery Cards should be sent to the key escrow service. Whenever changes are made to the LKM configuration, the configuration database should be backed up and a new copy sent to escrow. A predetermined set of rules for authorized retrieval should be in place before these items can be removed from storage with an escrow service.

PLAN REMOTE SECURITY LOGGING

LKM appliances provide detailed local and remote logging to help track events that occur in the Security Domain. Use the logging configuration features to redirect all logs to a remote syslog server, logging critical operations remotely and locally. See [Configuring and Viewing Logs](#) on page 117.

REMOVE THE SYSTEM CARD

If the physical security of the LKM appliance is a concern, it may be advisable to remove the System Card from the LKM chassis after startup and store it in a safe location. This prevents LKM from resuming encryption services if it is powered off, tampered with and rebooted. This provides greater security, but can also create a service interruption in the event of a power disruption or accidental tamper event. The System Card must be retrieved from storage, reinserted in the LKM appliance and the appliance must be rebooted in order to resume cryptographic services. Consider this security/reliability trade-off when determining whether to leave the System Card inserted in a running LKM appliance.

PREPARE FOR MANUAL SECURITY RESPONSES

Administrators can prepare for emergencies by maintaining configuration database backups and understanding the steps to recover an LKM appliance if necessary. If these practices are followed, complete recovery is possible after a threat that suspends LKM operation, weakens security, or disables LKM entirely.

The defense setting determines the appliance's automatic response to physical intrusion. See [About Defense Response Triggers and Settings](#) on page 78. In an emergency, suspend LKM encryption and decryption operations by removing the System Card and shutting down or rebooting the LKM appliance.

■ ■ ■ ■ 3 INSTALLING LKM APPLIANCE

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

This chapter contains the following topics:

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

NOTICES AND WARNINGS

POWER SUPPLY NOTICE

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



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

POWER CABLE NOTICE



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

DUAL POWER SUPPLY NOTICE



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

LITHIUM BATTERY NOTICE FOR SERVICE PERSONNEL

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



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

RACK MOUNTING



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

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



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

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

INSTALLATION REQUIREMENTS

This section contains the following topics:

- [Hardware Requirements](#)
- [Network Requirements](#)
- [Management Station Requirements](#)

HARDWARE REQUIREMENTS

Install the LKM appliance using items included in the shipping package and the separately-ordered Admin Kit.

The following are required for installation:

- LKM appliance
- LKM Documentation and Software CD-ROM. The documentation and software CD contains software necessary for LKM operation, such as the smart card reader driver and Decru Management Console installer.
- Custom RJ45 to DB9 adapter and standard straight through ethernet cable for a serial connection
- Two AC power cords
- Smart cards, including System, Admin and Recovery Cards
- USB smart card reader
- Decru product licenses
- Slide rail mounting kit including hardware and instructions (included in the LKM package)
- Network cables. Have the requisite number of network cables, of appropriate lengths. Each LKM requires one standard RJ-45 Ethernet cable.
- Network switch ports. Determine which Ethernet switch ports connect the LKM appliance to your network. Set the switch ports to auto-negotiate both speed and duplex settings. The use of any other setting can affect management performance.

NETWORK REQUIREMENTS

Gather the following network information before beginning installation:

- IP address, Subnet mask and Default Gateway. Each LKM requires one dedicated IP address. Know what the appropriate subnet mask and default gateway is for each dedicated IP address to be used during installation.
- LKM name. Establish what system name to assign each LKM appliance. Associating the specific IP addresses with their associated system names in your DNS configuration prior to installation simplifies IP resolution.
- DNS information. Have the appropriate DNS information (DNS suffix, primary DNS server IP address, secondary DNS server IP address) for each IP address to be used during installation.
- NTP address. If a network time server is in use on the network, have the appropriate NTP time server information.
- Recovery schema. Determine what the recovery schema is for the DataFort appliance or DataFort cluster. The recovery schema determines how many Recovery Cards and their associated owners must be present for sensitive data recovery operations.

MANAGEMENT STATION REQUIREMENTS

Select a computer that meets the requirements outlined in [Table 6](#) to serve as the Management Station.

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

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

TABLE 6: MANAGEMENT STATION REQUIREMENTS

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

INSTALLING HARD DISK DRIVES

The LKM appliance automatically stores all encryption keys and the most recent configuration database for any linked appliance on the hard disk drives. See [How the LKM Appliance Works](#) on page 16.

The hard disk drive is not interchangeable within an LKM appliance or between LKM appliances. However, hard disk drive are replaceable. When replacing a hard disk drive hot-swap it. To replace a hard drive, see See [Replacing Hardware](#) on page 140.

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

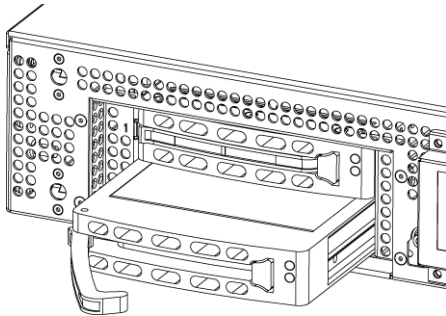


Figure 3-6: Front panel slots (with bezel removed) housing two drive slots for hard disk drive

6. Repeat the process for the hard disk 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.

RACK MOUNTING THE LKM APPLIANCE

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

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

CONNECTING THE LKM APPLIANCE

The following sections describe inserting the System Card and connecting the appliance to the network:

- [System Card Insertion](#)
- [Rear Panel Network Connections](#)
- [Powering On and Off](#)

SYSTEM CARD INSERTION

Note: Insert the System Card before powering on the appliance.

1. Insert the System Card into the smart card slot on the front panel of the LKM appliance.
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. See [Remove the System Card](#) on page 26.

REAR PANEL NETWORK CONNECTIONS

Complete the following procedures to connect the appliance to the network:

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

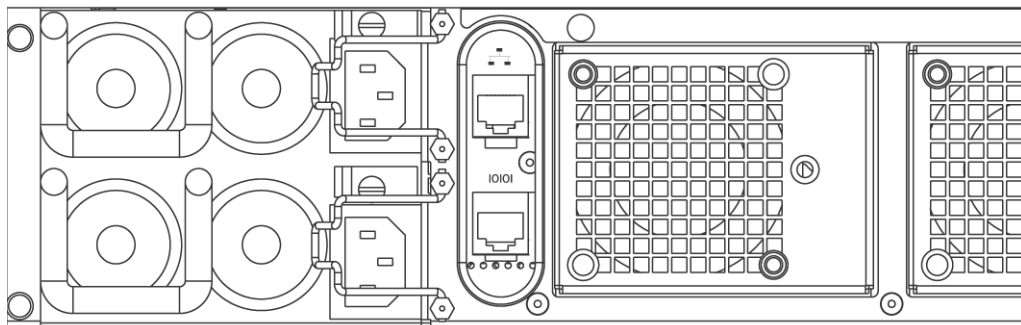


Figure 3-7: Rear panel connections

Ethernet Connection

Use a standard straight through ethernet cable to connect the Management Port (the Ethernet port marked with the network icon) to the Ethernet network shared by the Management Station.

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 standard straight through ethernet 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.

POWERING ON AND OFF

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

1. Connect each provided power cord to a LKM power port. Then connect the cord to an AC power source. See [Powering On and Off](#) on page 34.
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

1. Back up the configuration database before shutting down the LKM appliance. See [Backing Up an Appliance](#) on page 112.
2. Shut down using either the LKM appliance CLI shutdown command or the LCD. See [Powering Off via the CLI](#) on page 35 or [Powering Off via the LCD](#) on page 35.
3. After shutting down, power the LKM on again using the power button.

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

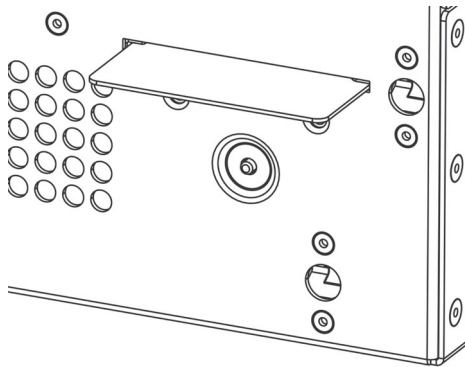


Figure 3-8: Front panel power button (bezel removed)

Powering Off via the CLI

See [Using the Command Line Interface](#) on page 42.

- At the CLI, run the following command:

```
system shutdown
```

Powering Off via the LCD

- 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 system.

Note: Touching Cancel also shuts down the system.

RUNNING THE INSTALLER

Run the installer on the Management Station before configuring an appliance. This installer places the Decru Management Console (DMC) and smart card reader driver on the Management Station. Both the smart card reader and DMC are required for initial setup of appliances.

Note: Administrator privileges are required to install and use DMC.

WARNING: THE DMC MUST BE INSTALLED ON A SECURE AND DEDICATED MANAGEMENT STATION PC. THE MANAGEMENT STATION MUST BE REGULARLY PATCHED AND PROTECTED FROM ACCESS FROM THE GENERAL NETWORK.

1. Insert the Decru installation CD into the Management Station drive.

Note: If autorun is off, browse to the CD manually and run the installer.

2. Click the installer link.
3. On the File Download screen, click the button to open or run the file.
4. Follow the prompts to start the installer.
5. Read and accept the terms of the license agreement.
6. Select the model number of the card reader.

The model number can be found on the underside of the card reader (i.e. GemPC USB-SL).

7. Click "Yes, I want to restart my computer now" and click Finish to complete installation



■ ■ ■ ■ 4 ACCESSING MANAGEMENT INTERFACES

Use management interfaces to log in to appliances and perform administrative tasks.

This chapter contains the following topics:

- [About Management Interfaces](#)
- [Decru Management Console \(DMC\) Options](#)
- [Using the Command Line Interface](#)
- [Accessing the Appliance Serial Console](#)
- [Using the Appliance Front Panel LCD](#)

ABOUT MANAGEMENT INTERFACES

After initial setup is complete use the management interfaces to configure and manage the appliance. The available management interfaces are summarized in [Table 7](#).

TABLE 7: MANAGEMENT INTERFACES

Interface	Description	Usage
Decru Management Console (DMC)	Perform management functions on all Decru appliances within your storage network. Installing a SecureView license enables additional enterprise class appliance management features. See Decru Management Console (DMC) Options on page 40.	Manage all LKM and DataFort appliances in an installation. Includes some management functions for OpenKey clients.
Secure Shell (SSH)	Allows a secure shell connection to the appliance CLI (command line interface) via secure shell client. Can require smart card authentication in addition to password. See Connecting via Secure CLI on page 43.	Manage Decru appliances, including some advanced configuration settings.
Serial Console	Enter network settings for uninitialized appliances. See Assigning IP Address on page 48.	Set, clear, or reset IP address, gateway and subnet mask. Zeroize when other interfaces are not available.
LCD	Display touch panel functions and interactive messages. See Using the Appliance Front Panel LCD on page 46.	View the Number of Keys (0-10M) and the CPU Load % (0-100) at a glance. Enter initial IP settings.
SNMP	Allows an SNMP tool (such as HP OpenView) to get read-only status information from the appliance. The standard MIB-II MIBs are exposed, as well as Decru's proprietary MIB. See Configuring SNMP Options on page 114.	View appliance status via SNMP tool. No secure information is permitted over this protocol (read only, no set commands).

SECURITY POLICIES

Security policy settings determine whether an Admin Card is required for logging in to the DMC or CLI of an appliance. By default, the appliance is set not to require an Admin Card for DMC or CLI access. To enable Secure DMC or Secure CLI (which require the presence of an Admin Card to log into the appliance), customize the security policy as described in [Configuring Management Security Settings](#) on page 78.

All administrators can log in to the DMC and the CLI. After logging in, specialized administrators are only able to perform the specialized administrative tasks authorized for their administrator type. For more about administrator types, see [Managing Administrators](#) on page 66.

USING SECUREVIEW

SecureView is a licensed feature that enables enterprise class appliance management in the Decru Management Console. This feature is enabled on a per-appliance basis. If an appliance is licensed for SecureView, it can be managed with other similarly licensed appliances from the Decru Management Console with a single step. The administrator multi-selects the requested appliances and is able to execute management functions on them simultaneously.

When managing multiple appliances using SecureView, it is helpful to add the same administrator (with the same name and password) to all appliances. This makes it possible to select, log into and manage all appliances simultaneously.

USING REMOTE AUTHORIZATION

A SecureView license is required to use Remote Authorization.

Remote Authorization allows an administrator to initiate and verify Recovery Card operations for DMC Setup and Trustee wizards from a remote location. See [Initializing an Appliance via the Setup Wizard](#) on page 50 and [Creating Trustee Relationships](#) on page 85.

SNMP SETTINGS

The appliance supports both MIB II and the read-only private Decru MIB. The Decru MIB is included on the appliance CD. It provides standard MIB-II as well as Decru MIB messages. All Decru MIBs are read-only for security reasons. See [Configuring SNMP Options](#) on page 114. A separate DataFort Appliance SNMP Alarms Guide is available from Decru for reference.

ONLINE HELP

Use the Decru Management Console to access online help for the appliance. Selecting an appliance in DMC and selecting the Help menu opens an online version of the administrative guide for the selected appliance. See [Using DMC Menus and Displays](#) on page 55 for details about the DMC Help menu.

DECRU MANAGEMENT CONSOLE (DMC) OPTIONS

The Decru Management Console (DMC) is an application installed on a Management Station PC. It provides a centralized management interface for all Decru appliances in a network. See [Using DMC Menus and Displays](#) on page 55 for a description of the menu options.

Management options for DMC include:

- [Using the DMC](#)
- [Connecting via Standard DMC](#)
- [Connecting via Secure DMC](#)
- [Connecting via DMC Using Dual Authorization](#)

USING THE DMC

- If equipped with SecureView licenses, more than one appliance can be selected at once, and a menu selection applied to all selected appliances.
- Some menu options initiate operations which are described only in the [DataFort Administration Guide](#).
- As a security measure, the DMC times out after 30 minutes of inactivity. To change this behavior, log in to an appliance, then select **Edit > Preferences**, select Stay logged in, and click OK.
- Hover the cursor over key on-screen elements for more information.
- If Secure DMC access is turned on, appliances cannot be managed by accessing the DMC through Windows Terminal Services or Remote Desktop.
- It is only possible to have one DMC instance open at a time on any given Management Station.
- Only one management interface should be open for a given cluster at any one time.
- The screen resolution on the Management Station should be set to at least 1024 x 768 pixels.

CONNECTING VIA STANDARD DMC

By default, the appliance is set for standard DMC, which allows login without requiring an Admin Card.

1. Select **Start > Programs > Decru > Decru Management Console** from the Management Station. Any appliance which has been added to DMC appears.
2. Right-click an appliance in the appliance tree and select Log in.
3. Enter the administrator login name and password.

CONNECTING VIA SECURE DMC

Secure DMC requires that an administrator present an Admin Card as well as a username and password in order to manage appliances.

A Full Administrator or Key Administrator can enable the smart card requirement (Secure DMC) by connecting to the DMC and accessing the Security Policy settings screen, as described in [Configuring Management Security Settings](#) on page 78.

1. Insert the Admin Card of a valid administrator into the Management Station smart card reader.
2. Access the DMC from the Management Station as described in [Connecting via Standard DMC](#) on page 40.
3. Log into an appliance. See [Logging in to Appliances Using DMC](#) on page 54.

CONNECTING VIA DMC USING DUAL AUTHORIZATION

By default, all administrators created using the DMC can log in to the DMC without additional authorization. By default, administrators created using the CLI require prior authentication before they can log in to the DMC or CLI. In addition, if the login privilege is revoked for a given administrator, that administrator requires the presence of an authorizing administrator in order to log in to the DMC or CLI. See [Authorizing an Administrator Log In](#) on page 71. The authorizing administrator can be any administrator who does not require authorization.

1. First the administrator with authorization privileges must log in. Access the DMC from the Management Station as described in [Connecting via Standard DMC](#) on page 40.
2. Log into an appliance. See [Logging in to Appliances Using DMC](#) on page 54.
3. From the Configuration menu, click View Administrators.
4. Right-click the Administrator to be authorized and click Authorize Login.
5. The administrator with authorization privileges should now log out.
6. The authorized administrator now has one minute to log in to the appliance.

USING THE COMMAND LINE INTERFACE

By default, the standard CLI setting is in effect, allowing an administrator created using DMC to log in to the CLI without an Admin Card. The standard CLI can be accessed from any workstation with an SSH client, by entering the administrator username and password.

Note: As a security measure, the CLI times out after 10 minutes of inactivity.

- [CLI Help](#)
- [Connecting via Standard CLI](#)
- [Connecting via Secure CLI](#)
- [Connecting via CLI Using Dual Authorization](#)
- [Connecting to DMC CLI](#)

CLI HELP

- Typing a partial command phrase (not word) and pressing enter results in a listing of the possible next words in a phrase to complete the command.
- Pressing tab after a command auto fills what has already been entered.
- Using partial commands is allowed. Typing the shortened version of a command like `sys ver` returns the same output as the complete command `system version`.
- Typing a command with too few arguments displays the full help listing for that command.
- Typing a command and a `?` with too few arguments displays a short description of the next argument required.
- Typing a command preceded by `help` displays a full description: purpose, usage, parameters and options, if any.
- Typing `cli documentation` displays the CLI documentation.

CONNECTING VIA STANDARD CLI

By default, the appliance is set for standard CLI, which allows login without first obtaining a temporary password from the DMC.

1. Open an SSH client on a workstation connected to the same network as the appliance.
2. Enter the IP address or hostname assigned to the appliance.
3. On the terminal window, enter the administrator login name and password.

CONNECTING VIA SECURE CLI

Secure CLI requires that an administrator present an Admin Card as well as a username and password. The smart card authentication requires log in to the DMC via the Management Station. A temporary CLI login password is generated, use this password to log in to CLI from an SSH client. See [Configuring Management Security Settings](#) on page 78.

Note: A Full Administrator or Key Administrator can enable the smart card requirement (Secure CLI). Secure CLI requires that a session-specific password be furnished via the DMC before the administrator can log in.

1. Insert the Admin Card of a valid administrator into the Management Station smart card reader.
2. Access the DMC Login screen from the Management Station.
3. Check One Time Password.

This button is present if the following conditions are met:

- Secure CLI is in effect
 - Smart card reader is connected to the Management Station
 - Admin Card is inserted into the smart card reader
4. Enter the username and password for an administrator associated with the Admin Card that is inserted in the Management Station smart card reader.
 5. Click OK.

A one-time login password (in hexadecimal format) appears on the screen.

6. Copy the password that is provided.
7. Log out of the appliance.

Note: Log in to the CLI immediately after retrieving the password from the DMC. Do not log in to the appliance via DMC after generating the Secure CLI password, as it invalidates CLI access.

8. Open an SSH client on a workstation connected to the same IP network as the appliance.
9. Enter the IP address or hostname assigned to the appliance.
10. At the prompt, enter the same administrator login name.
11. When prompted for the administrator password, paste or type the Secure CLI password into the command line.

CONNECTING VIA CLI USING DUAL AUTHORIZATION

By default, administrators created using the CLI always requires prior authentication before they can log into DMC. In addition, if the login privilege is specifically revoked for a given administrator, that administrator requires the presence of an authorizing administrator in order to log in to DMC or CLI. Any Full Administrator who can log in without authorization can grant any administrator the right to log in.

A Full Administrator or an Accounts Administrator can create administrators that require login authorization.

Note: Full Administrators and Key Administrators (when using speciality administrator roles) must be authenticated by another administrator, preferably a Read Only administrator. See [About Administrator Authentication](#) on page 68.

To log into the CLI when dual authentication is required:

1. First the administrator with authorization privileges must log in. Open an SSH client on a workstation connected to the same network as the appliance.
2. Enter the IP address or hostname assigned to the appliance.
3. On the terminal window, enter the administrator login name and password.
4. At the prompt, enter:

```
authorize <username>[@<domain>]
```

The username is the login name of the administrator to be authorized. Enter the domain only if it is different from LKM_ADMIN.

5. Log out of the CLI by entering **quit** at the prompt.
6. The authorized administrator can now log in to the appliance.

When login is successful, the authorized administrator can enter CLI commands at the prompt.

CONNECTING TO DMC CLI

The DMC offers a direct link to a simplified version of the CLI. Note that it does not support all features of the true appliance CLI.

Note: The DMC CLI does not support the following features: command line editing and completion, output paging and context-sensitive help.

1. In the DMC, in the appliance tree, select an appliance.
2. From the Utilities menu, click Command Line.
3. On the Command Line tab, enter the command into the Command field.
 - Click Execute to execute the command. The command runs 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 runs 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 output to a .zip file.
 - Click Clear to clear the command output.

ACCESSING THE APPLIANCE SERIAL CONSOLE

Use the appliance serial console port to assign IP settings, and to temporarily or permanently clear the settings of an initialized appliance.

Use only the supplied crossover RJ45 to DB9 adapter and standard straight through Ethernet cable to connect to the serial console port on the appliance's rear panel. See [Serial Console Port](#) on page 34 for details.

This section contains the following topics:

- [Logging into the Serial Console Port](#)
- [Configuring IP Settings](#)
- [Clearing IP Settings](#)

LOGGING INTO THE SERIAL CONSOLE PORT

Log in to an uninitialized appliance with the default login name and password. Log in to an initialized appliance with an administrator username and password that is valid for that appliance.

Note: Appliance serial sessions time out after 90 seconds of inactivity. If a session times out before finishing and saving the configuration, log in again. Settings are not saved until the Save and Exit command are completed.

CONFIGURING IP SETTINGS

1. At the shell prompt, log into uninitialized appliances using the default administrator name and password.

Note: Entries are space and case sensitive.

- Login: **user**
 - Password: **MTKNMTKN**
2. From the menu, select option **1** to set an IP address, subnet mask and default gateway for the management network interface.
 3. Select option **3** to save the settings and exit the terminal window.

CLEARING IP SETTINGS

The serial console is used to temporarily set a new IP address for the appliance in order to manage it from a new network. After a reboot, the original settings are restored. This feature is useful when the appliance is being moved to a different network but zeroization is not required. When the appliance is moved to a different network that does not recognize the appliance's IP address, the administrator can temporarily clear the settings so that access via DMC and CLI are possible. To change the IP settings permanently, see [Updating Network Settings](#) on page 116.

1. At the shell prompt, log in using the administrator name and password assigned to the administrator (note that these entries are space and case sensitive).
2. From the menu, select option **C**.
3. Select option **3** to save the settings, and exit the terminal window.

USING THE APPLIANCE FRONT PANEL LCD

After setup, the appliance front panel LCD displays messages and a bar graph showing number of keys and CPU load. The on-screen buttons provide more options. The top bar indicates the number of keys stored in the appliance. The bottom bar indicates the CPU load.

TOUCH PANEL ON-SCREEN BUTTONS

Menu	The Menu button opens a scrollable menu with access to network settings and appliance information (including software version and serial number). Use the up and down arrows to navigate the menu options, touching the Select button to access more information about the selected topic, and the Return button to return to the previous screen.
Network	Touching the Network Settings and Select buttons on an uninitialized appliance allows use of the Edit button to set the IP address, subnet mask and gateway for the appliance.
Details	When an error message appears, the Details button becomes visible on the LCD. Touching the button displays more information about the current error, and suggested steps to take to correct the error.



■ ■ ■ ■ 5 SETTING UP AN APPLIANCE

Setup the appliance by assigning the IP address and initializing the appliance using the Setup Wizard.

This chapter contains the following topics:

- [Assigning IP Address](#)
- [Initializing an Appliance via the Setup Wizard](#)
- [Logging in to Appliances Using DMC](#)

ASSIGNING IP ADDRESS

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

This section contains the following topics:

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

SETTING IP ADDRESS USING THE SERIAL CONSOLE

See [Accessing the Appliance Serial Console](#) on page 45.

1. Open a serial console (such as HyperTerminal) on the workstation connected to the serial port.
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: The default login only works for uninitialized appliances. Additionally, 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**

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

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

SETTING IP ADDRESS USING THE LCD

See [Using the Appliance Front Panel LCD](#) on page 46.

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

INITIALIZING AN APPLIANCE VIA THE SETUP WIZARD

To initialize an appliance, add one or more appliance to the DMC console and run the Setup Wizard on each appliance.

See the sections below for details:

- [About the Setup Wizard](#)
- [Adding Appliances to DMC to Initialize](#)
- [Using the Setup Wizard](#)

ABOUT THE SETUP WIZARD

Consider the following when running the wizard:

- Initialization of a new LKM appliance creates the first Full Administrator for that appliance.
- Security settings established during this procedure require the full team of Recovery Officers. Be sure to have all smart cards and Recovery Officers available for initialization.
- To expedite setup, collect information described in [Network Requirements](#) on page 30 before beginning the wizard.
- If canceled before completion, the Setup Wizard retains data entered for the appliance before the cancellation. When the wizard starts again, it automatically fills in saved data and skips completed steps. This is by design, and eliminates the need to reenter data when re-running the wizard. The retained wizard entries can be cleared if necessary. See [Checking Network Connections and Management Interfaces](#) on page 143.
- When using Remote Authorization, some default passwords may be used throughout the initialization process. This creates a network security risk for the appliance being authorized remotely. To avoid this, complete the Remote Authorization process promptly, and check the configuration of the appliance to ensure that it conforms to the security policy of the organization. To do this, review the logs issued during the Remote Authorization process, or log into the appliance and verify that administrative accounts, users, and permissions are correct.

ADDING APPLIANCES TO DMC TO INITIALIZE

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

1. Click **Start > Programs > Decru > Decru Management Console** to view the console.
2. In the DMC, the Add screen appears automatically.
3. On the Add screen, select from the following:
 - To add appliances by IP address or hostname, enter the IP address(es) or hostname(s) of the appliance(s) in the text box and click OK.
 - To add appliances by IP range, enter the start and end addresses of the IP range and click OK.
4. On the Certificates screen, select whether to trust the certificate validating the connection between the appliance and the Management Console. See [About Security Certificates](#) on page 81.

USING THE SETUP WIZARD

Before using the Setup Wizard, add an appliance to the Decru Management Console. See [Adding Appliances to DMC to Initialize](#) on page 50.

1. In the DMC, in the appliance tree, select an appliance.
2. From the Appliance menu, click Set up.
3. On the Welcome to the Decru Setup Wizard screen, click Start.
4. On the Connect to Head of Cluster screen, follow the instructions to enter the hostname or IP address of the appliance and click Next.

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

5. On the Certificates screen, select whether to trust the certificate validating the connection between the appliance and the Management Console once or always.
6. On the Sign License Agreement screen, read the license agreement and click Accept.
7. On the Recover from Database - Optional screen, click Next to skip.

Note: Use when the appliance replaces a previously existing appliance and a configuration database from that previous appliance is being used to configure the new appliance. See [Recovering LKM Appliances](#) on page 135.

8. On the Create Administrator screen, enter a username and password for the administrator and record this information for future reference, then 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 is used every time the administrator logs in to the appliance. Note that double quotes and back slashes are not permitted.

Note: When using SecureView licenses, create the same administrator on multiple appliances. This allows one administrator to log into and manage multiple appliances at one time.

9. On the Configure Cluster and Recovery Schema screen, select the desired data recovery schema. LKM appliances cannot be clustered, however they can be linked using key sharing policies. For deployment scenarios, see [Deploying an LKM Appliance](#) on page 19.

Note: Use at least 2 of the 5 Recovery Cards 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.

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

10. Click Next.
11. On the Network screen, enter hostname of the appliance, the IP address of the appliance, and the netmask and gateway settings and click Next.
12. 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. Each license must be on a consecutive and individual line.

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

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

Authorizing Setup Locally

1. On the Introduce Recovery Cards screen, insert a Recovery Card into the card reader, enter the password and click Start.

Note: When a card is inserted into the reader, the Card Label/Security Domain fields are populated automatically. A card appears selected (green) once it has been processed and added.

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.

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

2. On the Apply Settings screen, click Next.
3. On the Wizard Completed Successfully screen, click Finish.

Initiating Remote Authorization for Setup

1. On the Introduce Recovery Cards screen, select a quorum of cards from the Recovery Officers list to use throughout the authorization process and click Enable Remote Authorization.

Note: If the administrator initiating the remote authorization process is a Recovery Officer, the administrator must be the last Recovery Officer to supply a card. This allows the administrator to verify the wizard data and complete the approval process. If the administrator is not a Recovery Officer, the administrator must still verify the wizard data and complete the approval process.

2. When the Remote Authorization Enabled message appears, close the Introduce Recovery Cards screen and notify Recovery Officer(s) that it is safe to continue the Setup Wizard approval and introduce Recovery Cards remotely. See [Authorizing Setup Remotely](#) on page 53.

Note: Only one Recovery Officer at a time can open the appropriate UI screen and continue the remote authorization process, otherwise Recovery Officers may overwrite each other's approvals.

Authorizing Setup Remotely

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

Note: When a card is inserted into the reader, the Card Label/Security Domain fields are populated automatically. A card appears selected (green) once it has been processed and added.

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

8. After the cards are added, close the Introduce Recovery Cards screen and notify the remaining Recovery Officer(s) that it is safe to continue the Setup Wizard approval.

Note: When the last card is introduced either the Recovery Officer or another administrator must verify that the information entered is correct before proceeding.

9. On the Apply Settings screen, click Next.
10. On the Wizard Completed Successfully screen, click Finish.

LOGGING IN TO APPLIANCES USING DMC

Log into initialized appliances that are added to DMC.

1. In the DMC, in the appliance tree, select an appliance.
 - To log into more than one appliance at once Shift- or Ctrl-click all desired appliances. The appliances must have an administrator in common.
2. From the Appliance menu, click Log in.
 - Alternatively, 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 56.

For the LKM appliance to manage keys it must share keys with the appliance(s) that it serves. See [Sharing Keys](#) on page 84.

As a security measure, the DMC connection to an appliance times out after 30 minutes of inactivity. See [Setting Login and Refresh Preferences](#) on page 110.

EXITING DMC

To exit DMC, select from the following methods:

- In the DMC, from the Appliance menu, click Exit.
- Click the Close box at the upper right-hand corner of DMC.
- Double-click the DMC icon at upper left-hand corner of DMC.

■ ■ ■ ■ 6 USING DMC MENUS AND DISPLAYS

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

This chapter contains the following topics:

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

STATE DISPLAYS

The condition of each appliance is indicated in the DMC with an icon in the tree view (appliance tree) of the DMC screen. [Table 8](#) shows possible state displays for appliances in the Management Console.

TABLE 8: APPLIANCE STATUS INDICATORS

Icon	Icon Appearance	Appliance State
	Blue	Online—The online states change the appearance of the appliance text to Online (black) and Linked (black bold).
	Blue with yellow alert	Online with error. See Availability on the Appliance tab. See About the Appliances Tab on page 57.
	Gray with exclamation	Logged off. Administrator name and/or password is incorrect, or login is timed out (this occurs after 30 minutes if inactive).
	Yellow with open icon	Not initialized. IP address is set, but Setup Wizard is not completed.
	Red	Offline. Is not available on the network.
	Gray	Not logged in.

ABOUT THE APPLIANCES TAB

The Appliances tab contains the following default columns:

- Appliance—Displays the appliance by name.
- Availability—Displays the appliance state.
- Front Panel LCD—Shows the LCD display from the front panel of the appliance. Includes the appliance name, status or error messages, number of keys, and CPU load.
- Type—Displays the appliance type, such as KM-Series for the LKM appliance.
- Version—Displays the appliance operating system version.
- Serial Number—Displays the appliance serial number.

Note: Most of the tab views in DMC display information in a table format. After events are processed, a status bar at the bottom of the Appliance table displays status messages.

ADJUSTING TABLE COLUMNS

When information in a tab is displayed in a table, the table can be customized.

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

APPLIANCE MENU

Log in	Log in to an appliance as an administrator. See Logging in to Appliances Using DMC on page 54.
Log out	Log out of an appliance.
Add	Add an appliance. See Adding Appliances to DMC on page 108.
Add Cluster Members	Add a cluster member to DMC. See Adding DataFort Cluster Members to DMC on page 108.
Add Linked Appliances	Add appliances linked to an LKM appliance to DMC. See Adding Linked Appliances to DMC on page 95.
Remove	Remove an appliance from the Management Console. See Removing Appliances from DMC on page 108.
Link	Select a link policy to archive or share keys between two appliances, one of which must be an LKM appliance. See Creating Link Policies on page 92.
Link LKM Software	DataFort supports either the LKM software or the LKM appliance but not both.
View Link Report	View details about appliance links, including key sharing group, on the View Link Report tab. See Viewing Link Report on page 95.
View Cluster Members	See the DataFort Administration Guide .
Set up	Set up an appliance by using the Setup Wizard. See Using the Setup Wizard on page 51.
Reboot	Reboot the selected appliance. See Rebooting an Appliance on page 126.
Zeroize	Zeroize the selected appliance. See Zeroizing an Appliance on page 123.
Exit	Exit the Management Console. See Exiting DMC on page 54.

EDIT MENU

Cut	Cut a text entry.
Copy	Copy a text entry.
Paste	Paste a text entry.
Find	Search for text in the active pane of the Management Console. The search is not case sensitive.
Find Again	Find next result in the same search.
Preferences	Check the stay logged in button and select a refresh duration for the session. See Setting Login and Refresh Preferences on page 110.

VIEW MENU

The View setting determines how appliances are displayed in the appliance tree. More than one option can be selected simultaneously. Appliances appears once in each sorted list.

All	List all appliances in the appliance tree.
Type (default)	Display appliances sorted by type, including LKM appliance, FC-Series appliance, E-Series appliance and S-Series appliance.
Subnet	Display appliances sorted by subnet.
Custom Groups	Display custom appliance groups.
Add Custom Groups	Add a custom appliance group to monitor appliances based on organizational hierarchies. See Creating Custom Appliance Groups on page 109.
Remove Custom Group(s)	Remove a custom appliance group. See Removing a Custom Group on page 109.
Remove from Custom Group	Remove an appliance from a custom appliance group. See Removing an Appliance from a Custom Group on page 109.
Refresh	Refresh the view of appliances.

CONFIGURATION MENU

View Administrators	View and manage administrators. See Viewing Administrators on page 69.
Add Admin	Add an administrator. See Adding an Administrator on page 69.
View License	View licenses. See Viewing Licenses on page 111.
Add License	Add licenses. See Adding a License on page 111.
View OpenKey Clients	View OpenKey clients linked to an LKM appliance. See Viewing an OpenKey Client on page 95.
View OpenKey License Usage	View OpenKey license usage. See View OpenKey License Usage on page 111.
Network	Update the hostname of the appliance, the IP address, and the netmask and gateway settings of an appliance. See Updating Network Settings on page 116.
SNMP Agent	Set SNMP agent options. See Configuring SNMP Options on page 114.
Date/Time	Update the date, time and time zone settings of an appliance. See Updating Date and Time Settings on page 116.
Log Configuration	Select a log configuration. See Configuring and Viewing Logs on page 117.
Set Cluster IPsec Shared Secret	See the <i>DataFort Administration Guide</i> .
View Cluster Failover	See the <i>DataFort Administration Guide</i> .

KEYS MENU

View Parent Keys	View all Parent Keys of an appliance. See Viewing Parent Keys on page 99.
View Parent Keys from LKM	View all Parent Keys stored on an LKM appliance. See Viewing Parent Keys from LKM on page 99.
View Data Encryption Keys	Use a search tool to locate specific Data Encryption Keys stored in LKM. See Viewing Data Encryption Keys on page 99.
Translate Keys	Translate Cryptainer Keys created on one DataFort appliance to another DataFort appliance, so that both DataFort appliances can access the Cryptainer. See Using Manual Key Translation on page 104.
Change Key Sharing Group for Appliance	Change a policy based key sharing group for DataFort appliances that are trustees of an LKM appliance. See Changing Key Sharing Groups on page 96.
Change Key Sharing Group for Key(s)	Change a key sharing group for any individual key. See Changing a Key Sharing Group for Keys on page 97.
Move Unshared Keys into Key Sharing Group	Move unshared keys into a key sharing group. See Moving Unshared Keys into a Key Sharing Group on page 97.
Make Key Archive	Create a archive of Parent Keys for a DataFort appliance. See About Archiving Parent Keys on page 100.
Make Cryptainer Key Archive	Create an archive of Parent Keys for a DataFort Cryptainer. See About Archiving Parent Keys on page 100.
Export Keys	Export key files to a local hard drive. The files can then be deleted from the LKM appliance, or imported back into the LKM appliance. Only key information is shared. See Exporting and Importing Keys on page 103.
Import Keys	Import key files that are exported from an LKM appliance. See Exporting and Importing Keys on page 103.
Key Recovery	Recovers key files in the rare event the LKM appliance and its peers are down. See Recovering LKM Appliance Keys on page 139.
Purge Unused Keys	See the DataFort Administration Guide .

TOPOLOGY MENU

Use these menus to manage secure storage. See the [DataFort Administration Guide](#) for more information.

UTILITIES MENU

Command Line	Open the CLI to run commands on selected appliances. See Using the Command Line Interface on page 42.
Back up	Back up the configuration database of a DataFort or LKM appliance. See Backing Up an Appliance on page 112.
Back up appliances to LKM	Back up configuration databases of all appliances linked to an LKM appliance to that LKM appliance. See Backing Up Appliances to LKM on page 113.
Back up appliances from LKM	Back up the most recent configuration database of all appliances backed up to an LKM appliance to a secondary location. See Backing Up Appliances from LKM on page 113.
Verify	Verify the validity of an upgrade package before upgrading. See Verifying an Upgrade Package on page 110.
Upgrade/Downgrade	Upgrade or downgrade an appliance. Perform upgrades and downgrades only after consulting Decru support. See Upgrading an Appliance on page 110.
Revert System	See the DataFort Administration Guide .

SECURITY MENU

View Recovery Cards	View Recovery Cards for individual appliances or groups of appliances. See Viewing Recovery Cards on page 73.
View Recovery Cards from LKM	View all Recovery Cards associated with appliances connected to an LKM appliance. See Viewing Recovery Cards from LKM on page 74.
Replace Recovery Officer	Replace Recovery Officers. See Replacing a Recovery Officer on page 74.
Change Recovery Card Password	Change a password for a Recovery Card. See Changing a Recovery Card Password on page 76.
Smart Card Utilities	Reset a smart card and display card information. See Resetting Smart Cards on page 76.
Management Security	Configure security levels for appliance management interfaces. See Configuring Management Security Settings on page 78.
Defense	Specify the automatic appliance response to evidence of threat or intrusion. See Setting Appliance Defense Responses on page 78.
Certificates	Configure appliance security certificates. See Setting Security Certificates on page 81.
Clear Intrusion	Reset the tamper alert and reboot the system if an intrusion alert appears. See Clearing Intrusion Alerts on page 83.

TRUSTEE MENU

Create Trustee Link	Create trustees when appliances are in the same local network. See Create Trustee Link on page 85.
Start Trustee Creation	Create trustees when appliances are on different remote networks. See Start Trustee Creation (Create TEP) on page 89.
Receive TEP	Allow selected appliance to receive a Trustee Establishment Package. See Receive TEP on page 90.
Receive TAP	Allow selected appliance to receive a Trustee Acceptance Package. See Receive TAP on page 91.
View Unapproved Trustees	Display a list of trustees not yet approved (waiting to accept a TAP). See Delete Unapproved TAP Trustee on page 91.
View Trustees	Display a list of trustees.
Export Trustee Keys	See the <i>DataFort Administration Guide</i> .
Import Trustee Keys	See the <i>DataFort Administration Guide</i> .

DIAGNOSTICS

View System Information	View system version information for the selected appliance.
View System Log	View the appliance log file. See Configuring and Viewing Logs on page 117.
Run Crypto Self Test	Run a self-test on the appliance's Storage Encryption Processor to check the state of its cryptographic system.
View Storage Details	See the DataFort Administration Guide .
Check Appliance Sensors	View the status of the hardware including Temperature Sensors, Fan Sensors, Voltage Sensors and Power Supply Sensors. This information is used by Decru Technical Support to diagnose problems with the appliance hardware.
Collect Tech Support Info	Create a file containing information useful to Decru Technical Support when troubleshooting for the selected appliance. See Collecting Tech Support Info on page 134.
AutoSupport	See the DataFort Administration Guide .
Performance Monitoring Setup	See the DataFort Administration Guide .
Export Performance Data	See the DataFort Administration Guide .

HELP MENU

Help Contents	To open online help as a .pdf administration guide for the selected appliance type..
About	Show information about this version of the Management Console.

7 MANAGING ADMINISTRATORS AND SMART CARDS

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

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.

Each Recovery Card belongs to a Recovery Officer, who is a highly trusted individual in the organization. Use Recovery Cards in sets to restore encrypted data or appliances, and to replace other smart cards.

This chapter contains the following topics:

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

MANAGING ADMINISTRATORS

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

Note: Only a Full Administrator or an Accounts Administrator can add, delete and manage administrators.

This chapter contains the following topics:

- [About Administrator Roles](#)
- [About Administrator Authentication](#)
- [Protecting Against Insider Attacks](#)
- [Viewing Administrators](#)
- [Adding an Administrator](#)
- [Modifying Administrators](#)
- [Authorizing an Administrator Log In](#)

ABOUT ADMINISTRATOR ROLES

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

Read-Only

A Read-Only Administrator can view all appliance settings and can view status and logs, but cannot modify settings.

Specialty

A Specialty Administrator is used to create an administrator with limited permissions. See [Table 9](#) on page 67.

Full Admin

The Full Administrator sets up each appliance for the first time by running a setup wizard. The Full Administrator can perform all administrative tasks.

About Specialty Administrators

A Full Administrator can assign select permissions to a Specialty Administrator. While they can be created for LKM appliances, Specialty Administrators are mainly used for management, supporting task specialization for increased security. See [Table 9](#).

TABLE 9: SPECIAL ADMIN TYPES

Admin Type	Privileges
Key Admin	A Key Administrator is responsible for applying security-related settings to appliances. Key Administrator tasks include: • Creating Trustee Relationships as well as importing and exporting exportable keys • Purging DataFort keys upon backup to LKM • Setting Appliance Defense Responses • Setting Security Certificates • Replacing a Recovery Officer
Security Admin	A Security Administrator is responsible for applying physical security-related settings to appliances. Security Administrator tasks include: • Configuring Management Security Settings • Zeroizing an Appliance
Accounts Admin	Only a Full Administrator or an Accounts Administrator can add, delete and manage administrators. Accounts Administrator tasks include: • Adding an Administrator • Create Specialty Administrator • Modifying Administrators • Adding an Admin Card to an Administrator • Authorizing an Administrator Log In • Adding an Admin Card to an Administrator
Backup Admin	A Backup Administrator is responsible for managing backups of the configuration database. Backup Administrator tasks include: • Backing Up Appliances Manually
Machine Admin	A Machine Administrator is responsible for managing system properties and non-security sensitive operations. This administrator can change local network settings. Machine Administrator tasks include: • Updating Network Settings • Managing Licenses • Configuring SNMP Options

ABOUT ADMINISTRATOR AUTHENTICATION

Administrative logins must be authenticated by the presence of a smart card. In addition, administrators with permission to modify appliance settings must require authentication by another administrator. This administrator should be created as an authorizing administrator with no other privileges: able to authorize other administrators, but not to manage an appliance.

- A Full Administrator is created during the setup wizard. After the wizard is complete, associate this administrator with an Admin Card.
- Create any additional administrators (Full or Specialty) and associate those administrators with Admin Cards.
- Create a Read Only Administrator and associate that administrator with an Admin Card. Do not modify the Read Only administrator to require prior authentication from another administrator.
- Once the Read Only Administrator is created, modify all other administrators to require prior authentication before log in. This means that the Read Only Administrator must also be present in order for the other administrators to log in to manage the appliance.

PROTECTING AGAINST INSIDER ATTACKS

The administration management options can help protect against insider attacks. One method of attack prevention would be to create three administrator accounts corresponding to three Admin Cards as follows:

- The first administrator account belongs to a Full Administrator, and is used when completing the Setup Wizard. An Admin Card should be associated with this administrator, then stored in a safe place and not used for routine administration.
- After the Setup Wizard, the Full Administrator should create an authorizing administrator and a limited administrator who requires the authorizer in order to log into the DMC.
- The administrator must be sure that the appliance is configured to require an Admin Card for authentication of DMC and CLI access.
- In subsequent logins, both the authorizing administrator and the limited administrator must log in in order to access the DMC or CLI.
- Other than requiring the authorizer in order to log in, the limited administrator has permission to complete all management tasks, including the creation of new limited and authorizing administrators and making backups. The authorizing administrator must also be present until the limited administrator logs out of the DMC or CLI.

VIEWING ADMINISTRATORS

1. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, click View Administrators.
3. On the Administrators tab, select an administrator and right-click to perform the following actions:
 - To add an Admin Card to an administrator, see [Adding an Admin Card to an Administrator](#) on page 75.
 - To remove an Admin Card from an administrator, see [Removing an Admin Card from an Administrator](#) on page 76.
 - To move an Admin Card to an administrator, see [Sharing an Admin Card](#) on page 76.
 - To edit administrator permissions, see [Editing Administrator Permissions](#) on page 70.
 - To change a password for an administrator, see [Changing an Administrator Password](#) on page 70.
 - To remove an administrator, see [Deleting an Administrator](#) on page 71.
 - To authorize a login, see [Authorizing an Administrator Log In](#) on page 71.

ADDING AN ADMINISTRATOR

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

1. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, click Add Admin.
3. On the Add Administrator screen, enter the username and password of the administrator.
4. Select from the following administrator roles:
 - Select Read-Only to create an administrator with Read-Only permissions.
 - Select Specialty and then check any of the Specialty Roles to create an administrator with limited permissions. See [About Administrator Roles](#) on page 66.
 - Select Full Admin to create an administrator with full permissions.
5. Select from the following Login options:
 - Select Direct to allow the administrator to log in without authorization.
 - Select Requires Prior Authorization to pre-authorize an administrator's log in.

Note: In highly secure organizations where dual authorization is required, a Read-Only Administrator with direct login privileges may be created whose role is to authorize more privileged Specialty Administrators that require prior authorization. For security purposes, note that full and Accounts Administrators who require prior authorization may grant themselves direct login privileges. See [Authorizing an Administrator Log In](#) on page 71.

6. Click Apply.

MODIFYING ADMINISTRATORS

Administrator options are available by right-clicking on an Administrator in the table view.

The section contains the following topics:

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

Editing Administrator Permissions

1. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, click View Administrators.
3. On the Administrators tab, select an administrator and right-click to select Edit.
4. On the Edit Administrator screen, select from the following administrator roles:
 - Select Read-Only to create an administrator with Read-Only permissions.
 - Select Specialty and then check any of the Specialty Roles to create an administrator with limited permissions. See [About Administrator Roles](#) on page 66.
 - Select Full Admin to create an administrator with full permissions.
5. Enter the Full name and select from the following Login options:
 - Select Direct to allow the administrator to log in without authorization.
 - Select Requires Prior Authorization to pre-authorize an administrator's log in.

Note: Any Full Admin who can log in without authorization can grant any administrator the right to log in. See [Authorizing an Administrator Log In](#) on page 71.
6. Click Apply.

Changing an Administrator Password

1. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, click View Administrators.
3. On the Administrators tab, select an administrator and right-click to select Change Password.
4. On the Change Password screen, enter the current password, new password and confirm the new password of the administrator.

Deleting an Administrator

1. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, click View Administrators.
3. On the Administrators tab, right-click an administrator and select Remove.
 - Shift-click and then right-click to multi-select.
4. Click Apply.

AUTHORIZING AN ADMINISTRATOR LOG IN

See also [Connecting via DMC Using Dual Authorization](#) on page 41 and [Connecting via CLI Using Dual Authorization](#) on page 44.

1. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, click View Administrators.
3. On the Administrators tab, right-click an administrator and select Authorize Login.
4. Select the appliances to authorize a login for the selected administrator and click Apply.

Require an authorized log in for key administrators when using key sharing policies. This helps to maintain a two-person rule for important key operations.

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

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

MANAGING SMART CARDS

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

Note: Only a Full Administrator or an Accounts Administrator can manage Smart Cards.

This section contains the following topics:

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

ABOUT SMART CARDS

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

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

System Card

Each appliance has a unique System Card that provides physical security for the appliance and is required for the appliance to boot. If the System Card is removed, encryption keys are protected even if the appliance is compromised (stolen or tampered with).

The System Card's presence allows cryptographic operations to begin. Once appliance boots and cryptographic operations begin, the System Card can be removed. Note that some operations, such as the establishment of trust relationships, can not performed unless the System Card is present.

The System Card is initialized by the Setup Wizard at the same time the appliance is initialized, and is unique to that appliance. If the System Card is lost, the appliance must be zeroized and restored. Restoration is authorized by a quorum of Recovery Officers and cards.

Admin Card

The Admin Card authenticates communication between the administrator and appliance. Use Admin Cards for one or more appliance.

Although administrators may elect to allow logins based on username and password, there are advantages to requiring smart card authentication:

Authentication strength—Passwords are typically susceptible to brute force dictionary attacks, since it is difficult for users to remember a truly random password. The Admin Card authenticates with public key technology providing stronger authentication than passwords.

Two factor authentication—In order to access reserved services, the user must possess a physical object (the card) as well as remember a password.

Recovery Cards

Each Recovery Card belongs to a Recovery Officer, who is a highly trusted individual in the organization. Use Recovery Cards in sets to restore encrypted data or appliances, and to replace other smart cards.

A Recovery Officer retains an initialized Recovery Card after appliance setup is complete. Each Recovery Officer is authenticated by a Recovery Card and its associated password. A set of officers must present cards and passwords before any sensitive procedures can be performed.

Lost Recovery Card Best Practice

If a Recovery Card is lost or stolen, it must be replaced. In addition, it is best practice to replace and destroy the remaining quorum. This eliminates the possibility of a security breach if another Recovery Card is lost or stolen.

When a Recovery Card is lost, replace all of the cards from the original set one by one, then reset the old cards using the smart card reset function. Be sure not to reset the old cards until the original set has been replaced on every DataFort cluster and appliance that uses them. For more information see [Replacing a Recovery Officer](#) and [Resetting Smart Cards](#) on page 76.

VIEWING RECOVERY CARDS

View Recovery Cards for individual appliances or groups of appliances. This is useful when comparing card usage when sharing cards between appliances and when redefining how a card is shared, or to locate and replace a Recovery Officer.

1. From the Security menu, click View Recovery Cards.
2. On the View Recovery Cards tab, right-click on a card to change the recovery officer.

See [Replacing a Recovery Officer](#) on page 74.

VIEWING RECOVERY CARDS FROM LKM

View all Recovery Cards associated with appliances connected to an LKM appliance. If a DataFort appliance is down this is useful in locating Recovery Cards. To replace Recovery Officer, see [Replacing a Recovery Officer](#).

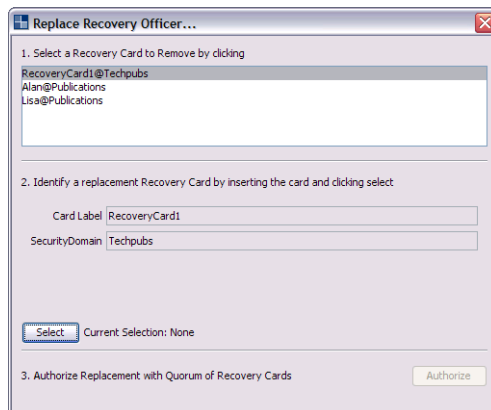
- From the Security menu, click View Recovery Cards from LKM.
The View Recovery Cards from LKM tab appears.

REPLACING A RECOVERY OFFICER

This option replaces the Recovery Card and its associated Recovery Officer. Before you begin, connect the smart card reader.

- In the DMC, in the appliance tree, select an appliance.
- From the Security menu, click Replace Recovery Officer.
- On the Replace Recovery Officer screen, click to select the card being replaced.
- Insert the card that replaces 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. If the card is uninitialized enter the Card Label, otherwise enter the password into the provided fields.



- On the Authorize Recovery Card Replacement screen, select from the following:
 - For multiple card readers, insert a quorum of cards into the readers, enter the passwords and click Start.
 - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the password and click Start.
- Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader it pre-populates the Card Label/Security Domain fields. A card appears selected (green) once it has been processed and added.

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.

7. 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 uninitialized enter the security domain, otherwise enter the password and click Add Card.
8. A message appears stating that the card has been replaced successfully, click OK.

ADDING AN ADMIN CARD TO AN ADMINISTRATOR

After adding an Admin Card to an administrator share it with one or more administrator. See [Sharing an Admin Card](#) on page 76.

1. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, click View Administrators.
3. On the Administrators tab, right-click an administrator and select Add Admin Card.
4. On the Add Admin Card screen, insert the Admin Card into the Management Station's card reader and click Apply.

Note: Smart cards must be fully inserted into the reader. If a card is not recognized, re-insert it for better contact.
5. On the Question screen, select to enable Secure Login or not.
 - To verify that the Admin Card is added to an administrator, on the Administrators tab, notice that the Card Associated column is set to y (yes).

Removing an Admin Card from an Administrator

1. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, click View Administrators.
3. On the Administrators tab, right-click an administrator and select Remove Admin Card.
4. On the Remove Admin Card screen, select an appliance and click Apply.

SHARING AN ADMIN CARD

1. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, click View Administrators.
3. On the Administrators tab, right-click an administrator and select Move Admin Card To.
4. On the Move Admin Card To screen, select an appliance and a user and click Apply.
 - To verify that the Admin Card is added to an administrator, on the Administrators tab, notice that the Card Associated column is set to y (yes).

CHANGING A RECOVERY CARD PASSWORD

1. In the DMC, from the Security menu click Change Recovery Card Password.
2. Insert the card for which the password is being changed into the Management Station smart card reader.

Note: Strong passwords are an important part of the overall security of the system. New passwords should be 8 or more characters, and include letters, digits and punctuation marks.
3. Enter the existing password.
4. Enter the new password twice and click Apply.

RESETTING SMART CARDS

Resetting smart cards, erases username and password settings.

Note: To enable this option, do not select any appliances.

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

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

■ ■ ■ ■ 8 **MANAGING APPLIANCE SECURITY**

This chapter contains the following topics:

- [Configuring Management Security Settings](#)
- [Setting Appliance Defense Responses](#)
- [Setting Security Certificates](#)
- [Clearing Intrusion Alerts](#)

CONFIGURING MANAGEMENT SECURITY SETTINGS

The appliance offers configurable levels of security for appliance management interfaces.

1. In the DMC, in the appliance tree, select an appliance.
2. From the Security menu, click Management Security.
3. From the Management Security screen, select the desired security level for each management interface.

Secure DMC - A valid Admin Card is required to access the DMC. See [Connecting via Secure DMC](#) on page 41.

Secure CLI - The administrator must access the DMC with a valid Admin Card to obtain a secure one-time password. See [Connecting via Secure CLI](#) on page 43.

4. Click Apply.

SETTING APPLIANCE DEFENSE RESPONSES

The defense setting specifies the automatic appliance response to evidence of threat or intrusion.

This sections contains the following topics:

- [About Defense Response Triggers and Settings](#)
- [About Defense Alerts](#)
- [Changing the Defense Setting](#)
- [Manual Security Response](#)

ABOUT DEFENSE RESPONSE TRIGGERS AND SETTINGS

A defense response can be triggered by the following:

Chassis Intrusion

If the appliance is opened, this causes an automatic defense response. If chassis intrusion has been detected, there should be physical evidence (such as scratches, a broken lock or a stolen chassis key).

Loss of Power

If the appliance is left without power for a long time (more than 3 weeks) a defense response can be triggered.

The appliance battery powers the intrusion-detection circuit even when the appliance is switched off. When this battery becomes low (because the appliance has been powered off for an extended period), it becomes possible for an intrusion to occur without appliance detection or notification. For this reason, a low battery triggers an intrusion alert.

The defense setting determines the extent of the response to the threats listed above and the requirements for recovery.

- **First response level**—disables the SEP (storage encryption processor) temporarily which immediately stops transparent key traffic in both directions. However, Opaque Key traffic and Opaque Key signing may continue for both DataFort appliance Cryptainer Keys being archived to, and restored from an LKM appliance. Also, it is still be possible to access management interfaces and view logs. Resume normal operation and key access perform an administrative reset. See [Clearing Intrusion Alerts](#) on page 83.
- **Second response level**—protects the data by deleting the SEP key hierarchy in the appliance. Recovery from this response requires zeroization and data recovery. When the SEP key hierarchy is deleted (Medium and High levels) all encrypted data becomes immediately unusable. Zeroization is required before the appliance configuration can be restored. See [Recovering LKM Appliances](#) on page 135.

WARNING: CHOOSE THE LOWEST LEVEL IF UNCERTAIN. THE DEFENSE LEVEL CAN BE INCREASED IN STRENGTH LATER BUT NOT DECREASED.

Defense levels are summarized in [Table 10](#). If in doubt, select the Basic level.

TABLE 10: APPLIANCE DEFENSE SETTINGS

Setting	When Used	Intrusion Trigger	Response	Operation Resumes
Basic	When it is sufficient to warn the administrator of an intrusion.	• Internal chassis intrusion detected. • Battery too low when system is powered on.	First response level	After administrator determines the cause of the intrusion and resets the appliance.
Medium	When it is necessary to delete the SEP key hierarchy in case of an intrusion but not if the battery is low.	Battery too low when system is powered on.	First response level	After administrator determines the cause of the intrusion and resets the appliance.
		Internal chassis intrusion detected.	Second response level	After appliance zeroization and restoration using Setup Wizard and Recovery Cards.
High	When it is necessary to delete the SEP key hierarchy immediately upon intrusion, whether a physical intrusion or low battery.	• Internal chassis intrusion detected. • Battery too low when system is powered on.	Second response level	After appliance zeroization and restoration using Setup Wizard and Recovery Cards.

ABOUT DEFENSE ALERTS

When an intrusion is detected, a defense alert is displayed. Depending on the defense setting, a Full Administrator may be able to clear a defense alert and allow the appliance to resume normal operations. For an appliance with a Basic level defense setting, alerts appear in the following places:

- On the front panel LCD
- From the Diagnostics menu, when selecting Details in DMC
- After CLI login
- In the appliance logs

After investigating the cause of the alert the administrator can reset the appliance from the CLI. See [Clearing Intrusion Alerts](#) on page 83.

Note: If the SEP key hierarchy is deleted under a High level defense setting, a simple reset is not possible. The appliance must be zeroized and recovered before normal operation can resume. Also, if there is a tamper intrusion under a Medium defense setting, the appliance must also be zeroized and recovered before normal operation can resume.

CHANGING THE DEFENSE SETTING

1. In the DMC, in the appliance tree, select an appliance.
2. From the Security menu, click Defense.
3. Select the desired defense level. See [Table 10](#).
4. Click Apply.

MANUAL SECURITY RESPONSE

Removing the System Card followed by shutdown or reboot stops encryption and decryption immediately.

Note: Removing the System Card alone does not stop LKM operation.

To return to normal operation:

- If the System Card is available, re-insert it and reboot the LKM appliance.
- If the System Card was destroyed or lost, LKM must be zeroized and then restored using the Setup Wizard, Recovery Officers, and a saved configuration database. See [Recovering LKM Appliances](#) on page 135.

SETTING SECURITY CERTIFICATES

This section contains the following topics:

- [About Security Certificates](#)
- [Setting a Local Security Certificate](#)
- [Setting a Certificate Authority Signed Certificate](#)

ABOUT SECURITY CERTIFICATES

A security certificate is a digital document used to confirm the identity of a person or website. During initial setup of the appliance, a self-signed certificate is created. When an administrator connects to the appliance from DMC, the appliance presents its security certificate in order to confirm its identity to the DMC. An alert appears in the DMC, prompting the administrator to review the security certificate and decide whether it is authentic and can be trusted.

Security certificate review options include:

All Always	Always accept connections from all appliances with their current security certificate for the remainder of the DMC session. After ending the session by closing and restarting DMC, certificate prompts appear again when required.
Always	Always accept connections from this particular appliance with its current security certificate. If the certificate of this appliance changes or expires, the certificate prompt appears again.
Once	Accept the connection from this appliance with its current security certificate only for this session. After ending the session by closing and restarting DMC, the certificate prompt appears again.
Never	Never accept a connection from this particular appliance with its current security certificate during this session. After ending the session by closing and restarting DMC, the certificate prompt appears again.

It may be desirable to install a certificate signed by a certificate authority as described in [Setting a Certificate Authority Signed Certificate](#) on page 82. Keep the following in mind:

- A certificate must be generated independently for each appliance in a cluster.
- Create the certificate and then use it until its expiration date.
- Only a Full Administrator can set the security certificate
- SSL private keys are cleared by zeroization, and may not be backed up or transferred to other appliances. If signed certificates are purchased, they have to be replaced for zeroized appliances. See [Zeroizing an Appliance](#) on page 123.

SETTING A LOCAL SECURITY CERTIFICATE

To create a self-signed security certificate for the appliance in DMC:

1. In the DMC, in the appliance tree, select an appliance.
2. From the Security menu, click Certificates.
3. From the Certificates screen, enter the information for the locally signed certificate. This information appears when certificate details are viewed.

The appliance hostname appears in the Common Name field. The Common Name must be the hostname or IP address of this appliance. If a hostname is used, it must be resolvable by DNS.

Note: Country codes are established by the International Organization for Standardization (ISO). See [Partial List of ISO Country Codes](#) on page 161.

4. To set the certificate, click Apply.
5. After a moment, the certificate prompt appears.
If it does not appear automatically, verify the appliance in question is still selected in the appliance tree, then select the Appliances tab.
6. Review the certificate, then click the appropriate button.

SETTING A CERTIFICATE AUTHORITY SIGNED CERTIFICATE

1. In the DMC, in the appliance tree, select an appliance.
2. From the Security menu, click Certificates.
3. From the Certificates screen, enter the required information into the fields provided and click Generate CA Request.
4. This generates a PEM-encoded request which can be submitted to a known certificate authority such as VeriSign or a local certificate authority.

Note: Country codes are established by the International Organization for Standardization (ISO). See [Partial List of ISO Country Codes](#) on page 161.

5. Submit the PEM-encoded file to a known certificate authority such as VeriSign or RSA and set the CA-signed certificate when it is received. See [Setting the CA-signed Certificate](#).

Note: Country codes are established by the International Organization for Standardization (ISO).

Setting the CA-signed Certificate

1. In the DMC, in the appliance tree, select an appliance.
2. From the Security menu, click Certificates.
3. From the Certificates screen, click Set CA Certificate.
4. Paste the certificate received from the certificate authority into the box provided. Cut and paste the entire contents of the certificate file, including the BEGIN and END lines.
5. Click OK and click Apply.
After a moment, the certificate prompt appears. If it does not appear automatically, verify the appliance in question is still selected in the appliance pane, then select the Appliances tab.
6. Review the certificate and accept it.

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.

Note: If the SEP key hierarchy is deleted under a Medium or High level defense setting, a simple reset is not possible. The appliance must be zeroized and recovered before normal operation can resume.

1. In the DMC, in the appliance tree, select an appliance.

WARNING: CLEARING AN INTRUSION ALERT AUTOMATICALLY REBOOTS THE SYSTEM.

2. From the Security menu, click Clear Intrusion.
3. From the Clear Intrusion screen, click Apply. The appliance reboots, clearing the alert.

■ ■ ■ ■ 9 SHARING KEYS

Keys are archived on the LKM appliance and shared between LKM clients based on link policies, including archive and key sharing policies. However, Decru appliances must form a trustee relationship with an LKM appliance before creating a link policy. See [How Keys are Archived and Shared](#) on page 17 for more information.

This chapter contains the following topics:

- [Creating Trustee Relationships](#)
- [Creating Link Policies](#)
- [Managing Link Policies](#)
- [Changing Key Sharing Groups](#)

CREATING TRUSTEE RELATIONSHIPS

Decru appliances must form a trustee relationship with an LKM appliance before creating a link policy for a key sharing group. This allows them to share keys without manually importing and exporting keys or going through the key translation process.

Note: A Recovery Card quorum for each appliance is required for setup. The System Card must be inserted into the DataFort appliance in order to fully authorize this cryptographically sensitive procedure.

DataFort appliances that do not reside in key sharing groups may continue to share keys by creating an archive policy. This requires a manually importing and exporting each key for each trustee. See the [DataFort Administration Guide](#).

Note: To abort the trustee setup at any point in the procedure, delete the unapproved trustee from both the View Trustees and Unapproved Trustees lists before reattempting trustee creation. See [Viewing Link Report](#) on page 95 and [Delete Unapproved TAP Trustee](#) on page 91.

This section contains the following topics:

- [Creating Trustees on a Local Network](#)
- [Creating Trustees on a Remote Network](#)

CREATING TRUSTEES ON A LOCAL NETWORK

Use this procedure to create a trustee relationship when appliances are in the same local network.

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

This section contains the following topics:

- [Create Trustee Link](#)
- [Authorizing Trustees Locally \(Approve TEP/TAP\)](#)
- [Initiating Remote Authorization to Approve TEP](#)
- [Initiating Remote Authorization to Approve TAP](#)

Create Trustee Link

1. In the DMC, in the appliance tree, Ctrl-click to select both appliances.
2. From the Trustee menu, click Create Trustee Link.

Note: By default the Trustee Label shows the hostname or IP address of the other appliance, though this can be changed.

3. On the Trustee Setup screen, notice that both appliances appear and click Create Link.
4. Select a method to authorize trustees:
 - To authorize trustees locally, see [Authorizing Trustees Locally \(Approve TEP/TAP\)](#) on page 86.
 - To authorize trustees using Remote Authorization, see [Initiating Remote Authorization to Approve TEP](#) on page 87.

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

Authorizing Trustees Locally (Approve TEP/TAP)

1. On the Approve TEP (Trustee Establishment Package) screen, select from the following:
 - For multiple card readers, insert a quorum of cards into the readers, enter the passwords, and click Start.
 - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the password for the first card, and click Start.
2. Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader, the Card Label/Security Domain fields are populated automatically. A card appears selected (green) once it has been processed and added.

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

3. On the Approve TAP (Trustee Acceptance Package) screen, select from the following:
 - For multiple card readers, insert a quorum of cards into the readers, enter the passwords, and click Start.
 - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the password for the first card, and click Start.
4. Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader, the Card Label/Security Domain fields are populated automatically. A card appears selected (green) once it has been processed and added.

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

Initiating Remote Authorization to Approve TEP

1. On the Approve TEP (Trustee Establishment Package) screen, select a quorum of cards from the Recovery Officers list to use throughout the authorization process and click Enable Remote Authorization.
Note: If the administrator initiating the remote authorization process is a Recovery Officer, the administrator must be the last Recovery Officer to supply a card. This allows the administrator to verify the wizard data and complete the approval process. If the administrator is not a Recovery Officer, the administrator must still verify the wizard data and complete the approval process.
2. When the Remote Authorization enabled message appears, close the Approve TEP screen and notify the Recovery Officer who will approve the TEP that it is safe to continue the TEP approval process and introduce Recovery Cards remotely. See [Authorizing TEP Approval Remotely](#) on page 87.
Note: Only one Recovery Officer at a time can open the appropriate UI screen and continue the remote authorization process, otherwise Recovery Officers may overwrite each other's approvals.

Authorizing TEP Approval Remotely

1. In the DMC, in the appliance tree, select both appliances.
2. From the Trustee menu, click Create Trustee Link.
3. On Approve TEP screen, select from the following:
 - For multiple card readers, insert a quorum of cards into the readers, enter the passwords, and click Start.
 - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the password for the first card, and click Start.
4. Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.
Note: When a card is inserted into the reader, the Card Label/Security Domain fields are populated automatically. A card appears selected (green) once it has been processed and added.

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. When the progress bar is complete, close the Approve TEP screen and notify the Recovery Officer(s) who will approve the TEP that it is safe to continue the TEP approval process.
Note: Do not close the Approve TEP screen if you are the last officer to Approve the TEP. Instead initiate the TAP approval process. See [Initiating Remote Authorization to Approve TAP](#) on page 88.

Initiating Remote Authorization to Approve TAP

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

Note: Only one Recovery Officer at a time can open the appropriate UI screen and continue the remote authorization process, otherwise Recovery Officers may overwrite each other's approvals.

Authorizing TAP Approval Remotely

1. In the DMC, in the appliance tree, select both appliances.
2. From the Trustee menu, click Create Trustee Link.
3. On the Approve TAP screen, select from the following:
 - For multiple card readers, insert a quorum of cards into the readers, enter the passwords, and click Start.
 - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the password for the first card, and click Start.
4. Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader, the Card Label/Security Domain fields are populated automatically. A card appears selected (green) once it has been processed and added.

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. When the progress bar is complete, close the Approve TAP screen and notify the Recovery Officer(s) who will approve the TAP that it is safe to continue the TAP approval process.
6. On the Trustee screen, a message appears indicating that the trustee is created, click OK.

CREATING TRUSTEES ON A REMOTE NETWORK

When appliances are on separate remote networks, follow the steps to create a trustee relationship.

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

This section contains the following topics:

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

Start Trustee Creation (Create TEP)

1. In the DMC, in the appliance tree, select an appliance.
 2. From the Trustee menu, select Start Trustee Creation.
 3. On the Start Trustee (Create TEP) screen, enter information in the following fields and click Create.
 - Enter a Trustee Label or hostname for the appliance.
 - Enter a Package Label or hostname for the package.
 4. On the Select File screen, verify the TEP file name and select a file location, then click Save.
 5. From the Trustee menu, select View Unapproved Trustees.
 6. On the View Unapproved Trustees tab, right-click the correct Trustee Label and select Copy Verifier.
 7. Paste the verifier into a text file and save it.
 8. Send the verifier file and the TEP file separately to the second appliance. See [Receive TEP](#).
- Note:** Communicate the verifier in a secure manner, by phone or direct contact rather than email. This is the only way to assure confidentiality when authenticating trustees for key sharing.

Receive TEP

To receive the TEP (Trustee Establishment Package), the second appliance needs the TEP file and verifier received from the first appliance. See [Start Trustee Creation \(Create TEP\)](#) on page 89.

Note: After receiving and approving the TEP, a TAP (Trustee Acceptance Package) is automatically created.

1. In the DMC, in the appliance tree, select the second appliance.
2. From the Trustee menu, select Receive TEP
3. On the Receive TEP screen enter the following and click Begin Approval.
 - Browse to the path of the TEP file to open it.
 - Paste the verifier text string from your saved text file.
 - Enter a Trustee Label or hostname for the appliance.
 - Enter a Package Label or hostname for the package.
4. On the Approve TEP (Trustee Establishment Package) screen, select from the following:
 - For multiple card readers, insert a quorum of cards into the readers, enter the passwords, and click Start.
 - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the password for the first card, and click Start.
5. Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader, the Card Label/Security Domain fields are populated automatically. A card appears selected (green) once it has been processed and added.

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, verify the TAP file name and select a location, then click Save.
7. From the Trustee menu, select View Unapproved Trustees.
8. On the View Unapproved Trustees 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 first appliance.

Note: Communicate the verifier in a secure manner, by phone or direct contact rather than email. This is the only way to assure confidentiality when authenticating trustees for key sharing.

Receive TAP

To receive the TAP (Trustee Acceptance Package), the first appliance needs the TAP file and verifier received from the second appliance. See [Receive TEP](#) on page 90.

1. In the DMC, in the appliance tree, select the first appliance.
2. From the Trustee menu, select Receive TAP
3. On the Receive TAP screen, browse to the TAP file and copy the verifier into the provided field.
4. Click Begin Approval.
5. On the Approve TAP screen, select from the following:
 - For multiple card readers, insert a quorum of cards into the readers, enter the passwords, and click Start.
 - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the password for the first card, and click Start.
6. Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader, the Card Label/Security Domain fields are populated automatically. A card appears selected (green) once it has been processed and added.

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.

7. On the Trustee screen, a message appears indicating that the trustee is created, click OK.
- Note:** When the Administrator of the first appliance approves the TAP, it is recommended they notify the Administrator of the second appliance so that they can delete the unapproved TAP trustee. See [Delete Unapproved TAP Trustee](#) on page 91.

Delete Unapproved TAP Trustee

The first appliance must approve the TAP before the second appliance deletes the unapproved TAP trustee. This retains a backup TAP trustee file until the process is complete.

1. In the DMC, in the appliance tree, select the second appliance.
2. From the Trustee menu, click View Unapproved Trustees.
3. On the View Unapproved Trustees tab, right-click the trustee and select Delete.
4. On the Question screen, click Yes.

Note: If the trustee setup process was aborted at any point, use these steps to first remove unapproved trustees before attempting trustee setup again.

CREATING LINK POLICIES

There are three types of link policies: a Decru Key Sharing Policy, a Decru Archive Policy and an OpenKey Policy. Use a Decru Key Sharing Policy or an OpenKey Policy when automatic key sharing is desired. The Decru Archive Policy is used only to store keys wrapped with the source Decru appliance Parent Keys, and to archive configuration data on the LKM appliance.

This section contains the following topics:

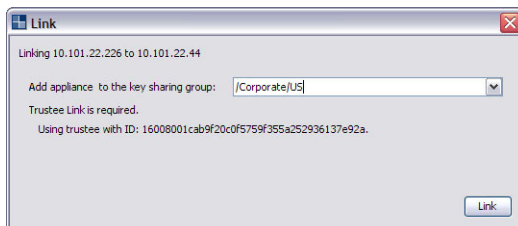
- [Creating a Key Sharing Policy](#)
- [Creating an Archive Policy](#)
- [Creating an OpenKey Policy](#)

CREATING A KEY SHARING POLICY

Decru appliances must form a trustee relationship with an LKM appliance before creating a key sharing group. This allows them to share keys without manually importing and exporting keys or going through the key translation process. See [Creating Trustee Relationships](#) on page 85.

1. In the DMC, in the appliance tree, select an LKM appliance.
2. From the Appliance menu, click Link.
3. From the Link screen, click Decru Key Sharing Policy and click Apply.
4. On the Select appliance to link screen, select an LKM trustee and click OK.

Note: When linking a DataFort cluster member other cluster members are automatically linked. However, when removing a link between DataFort cluster member and an LKM appliance, DMC does not automatically remove links with the cluster members. See [Removing Appliance Links](#) on page 95.



5. On the Link screen, from the Add appliance to the key sharing group combo box, type or select a group name. See [Key Sharing Group Guidelines](#) on page 21.
6. Click Link.
7. When the Appliance Link screen appears, verify that a connection is established between the selected appliances by clicking OK.

CREATING AN ARCHIVE POLICY

Use a Decru Key Sharing Policy or an OpenKey Policy when automatic key sharing is desired. The Decru Archive Policy is used only to store keys wrapped with the source Decru appliance Parent Keys, and to archive configuration data on the LKM appliance.

Note: When using an archive policy, manual key translation is required to translate keys for DataFort appliances via DMC. See [Using Manual Key Translation](#) on page 104.

1. In the DMC, in the appliance tree, select an LKM appliance.
 2. From the Appliance menu, click Link.
 3. From the Link screen, click Decru Archive Policy and click Apply.
 4. On the Select appliance to link screen, select an appliance and click OK.
- Note:** When linking a DataFort cluster member other cluster members are automatically linked.
5. When the Appliance Link screen appears, verify that a connection is established between the selected appliances by clicking OK.

CREATING AN OPENKEY POLICY

Linking an OpenKey client to an LKM appliance allows third-party clients to use the LKM as a secure key management service. To add an OpenKey client to a key sharing group on an LKM appliance, a certificate package and an OpenKey license are required. See [Adding a License](#) on page 111.

Note: OpenKey clients are not viewable in the appliance tree since they are added to an LKM appliance only and not to DMC. To view an OpenKey client, see [Viewing Link Report](#) on page 95.

1. In the DMC, in the appliance tree, select an LKM appliance.
2. From the Appliance menu, click Link.
3. From the Link screen, click OpenKey Policy and click Apply.

Add OpenKey clients

Paste the certificate in the text field or browse to the certificate to load the certificate in the text field.

IP Address: 10.101.22.226

Key Sharing Groups: /Corporate/ASIA/

Path to Certificate: 10.101.22.226

Browse...

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC3cCAccCAQAwgZkxFjAUBghNBAMTDTEwLjEwMS4yM4yMjYxZjA2BghVBAYT
AN/MTQwCgYDVQQLZwJlZDQTEVMBMGA1UEBxMMUjVkdz9vZCBOaXRSMRQwEgYDVQQL
EwE2ZWVudSwgSW5lJESMBAGA1UECzMVGVjaCBQdWJ3dMSQwIgY3KozThvcnAqK8
FHNkbc102WNocHic6RkZWMyYyY5dS5kZmVwagEjRABGCSySIB3DQEBAQUAA4IBDwAw
ggEKAAIBAQCLUGdcrcW/8N8doy3dDQKwfcw3S2YfymnPHCSWiaJPMv6h7ZIS
vz2ePqZAWBkdLVAxVkuQIBSJVH6X1JSHX8f8xwLFRM+C+1N#HDZOKU/NZ35/
LkEOQpRu483L47IkW2uVvTJPLUFO79Y2dchokPZWngEyoA0oesp/luG7dInUJLw
+kevnHBQ4y5uLC3+3JO739bUuqykYfCB5y8JG9C+rr7J6CC5myNHF5RpPF
boKBDWWH5fcpHXGNIeG47d7gWmWmDMYDDC3935gk30KStmuuo3PDCULMU
8bivNkldxd+742Ek8MBgcQuT+VGSgDAGMBAAAGADANBgkqhkiG9w0BAQUFAAOC
AQEAIm0ybhhQ0ty56X8u52DYfCbunIZW68E0nPEWgagncr6PZLa25oEzy0Pxx
v0MIT5yRpk8cvkHwQzy6JaBMGnatCa7Edp9divyETSDVgeUjYXN4Nuz2+JfK0RS
kaB3dogSpRl+K4775r73XUp3Mf93ALF5Vlx4W4wJLQRKQYpkr1HJURcVAp
CPRJYd+cp8d8w8vnuuFKZ2Z5yp7ivBTJ3m7gQH5upaAQCY1Gp8AwewidQwqY
DqBTraoDM5567P4ujg5evba+ZtoBQeCrydqB+9THPE7BvlpLLEo4pOj5nvbA
THvBW+8vzAzQzI3AGdFO/s9vw==
-----END CERTIFICATE REQUEST-----
```

Items in **bold** are required.

Cancel Apply

4. On the Add OpenKey clients screen, enter the client IP address of the client.
5. In the Key Sharing Groups combo box, type or select a group name. See [Key Sharing Group Guidelines](#) on page 21.
6. In the Path to Certificate text box, browse to or copy and paste the certificate package and click Apply.

MANAGING LINK POLICIES

Once Decru appliances and OpenKey clients are linked to an LKM appliance they are viewable in the link report. The link report shows appliance links and policies including key sharing group affiliations and key synchronization data.

This section contains the following topics:

- [Viewing Link Report](#)
- [Adding Linked Appliances to DMC](#)
- [Viewing an OpenKey Client](#)

VIEWING LINK REPORT

1. In the DMC, in the appliance tree click to select an appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Appliance menu, click View Link Report.

Note: When viewing DataFort cluster members, each cluster member appears linked to an LKM appliance and vice-versa since links are per appliance. However, since trustees are per cluster (not per appliance), when viewing trustees for the LKM appliance, only the cluster coordinator appears.

Removing Appliance Links

1. In the DMC, in the appliance tree click to select an appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Appliance menu, click View Link Report.
3. On the View Link Report tab, right-click a linked appliance and select Remove.
 - Shift- or Ctrl-click to select multiple appliances.
4. On the Remove Link screen, in the Link(s) box, verify that the appliance links selected are highlighted and click Apply.

ADDING LINKED APPLIANCES TO DMC

Any appliance that has been once added to DMC and that has been previously linked to an LKM appliance may be re-added to the DMC without having to re-link it.

1. In the DMC, select an appliance.
2. From the Appliance menu, click Add Linked Appliances.

Note: Once added, appliances appear in the appliance tree as either KM-Series, E-Series, FC-Series or S-Series. Appliances appear as Unknown until logged into.

VIEWING AN OPENKEY CLIENT

To view OpenKey Client license usage, see [View OpenKey License Usage](#) on page 111.

1. In the DMC, in the appliance tree click to select an LKM appliance.
2. From the Configuration menu, click View OpenKey Clients.

CHANGING KEY SHARING GROUPS

When managing key sharing groups, it is helpful to view details about appliance links and key sharing group affiliations in the link report. See [Viewing Link Report](#) on page 95.

This section contains the following topics:

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

CHANGING KEY SHARING GROUPS FOR OPENKEY CLIENTS

To change a key sharing group for OpenKey clients, use the same procedure used to create an OpenKey policy. See [Creating an OpenKey Policy](#) on page 94.

CHANGING KEY SHARING GROUPS FOR DATAFORT APPLIANCES

1. In the DMC, in the appliance tree click to select a DataFort appliance.
2. From the Keys menu, click Change Key Sharing Group for Appliance.
3. On the Change Key Sharing Group for Appliance screen, in the Key Sharing Groups combo box, type or select a group name. See [Key Sharing Group Guidelines](#) on page 21.
4. Click Apply.

CHANGING A KEY SHARING GROUP FOR KEYS

Change a key sharing group for an individual key. This is useful, for example, when a key is temporarily needed by another group to restore a DataFort Cryptainer.

Note: OpenKey clients cannot change a key sharing group for an individual key.

The Key Sharing Group column is not shown by default on the View Data Encryption Keys table. To view key sharing groups for keys, add this column to the View Data Encryption Keys table. See [Adjusting Table Columns](#) on page 57.

1. In the DMC, in the appliance tree, select an LKM appliance.
2. From the Keys menu, click View Data Encryption Keys.
3. On the View Data Encryption Keys screen, from the drop-down box, select the search criteria to use in locating keys and click Add.
 - Click Remove to delete search criteria.
 - Click the Remember Form Values to reuse selected search criteria.
4. To initiate a search using all of the selected criteria, click Find.
5. On the View Data Encryption Keys tab, select a key and right-click to select Change Key Sharing Group for Key(s).
6. On the Change Key Sharing Group for Key(s) screen, in the Key Sharing Groups combo box, type or select a group name. See [Key Sharing Group Guidelines](#) on page 21.
7. Click Apply.

MOVING UNSHARED KEYS INTO A KEY SHARING GROUP

Use this option when keys are purged from a DataFort at the time it is being upgraded from an archive link to a key sharing group link. Otherwise the LKM appliance is not able to share the purged keys.

1. In the DMC, in the appliance tree, select both a DataFort and an LKM appliance.
2. From the Keys menu, click Move Unshared Keys into a Key Sharing Group.
3. On the Move Unshared Keys into a Key Sharing Group screen, click Apply.

Note: Keys are moved from LKM to the key sharing group for the DataFort appliance.



■ ■ ■ ■ 10 MANAGING KEYS

The LKM appliance and the Management Console provide tools to manage, view, archive and translate keys in the enterprise.

The chapter contains the following topics:

- [Viewing Keys](#)
- [Archiving DataFort Parent Keys](#)
- [Backing Up Keys to External Storage](#)
- [Using Manual Key Translation](#)

VIEWING KEYS

Reports of all key policy attributes, including those that are set by the client, are available when viewing keys. Additionally, a log shows a record of each client access to a key. See [Configuring and Viewing Logs](#) on page 117.

This section contains the following topics:

- [Viewing Parent Keys](#)
- [Viewing Parent Keys from LKM](#)
- [Viewing Data Encryption Keys](#)

VIEWING PARENT KEYS

View all Parent Keys of an appliance.

1. In the DMC, in the appliance tree, select an appliance.
2. From the Keys menu, click View Parent Keys.

VIEWING PARENT KEYS FROM LKM

View all Parent Keys stored on the LKM appliance.

1. In the DMC, in the appliance tree, select an LKM appliance.
2. From the Keys menu, click View Parent Keys from LKM.
 - Right-click on a key to make a key archive from a Parent Key. See [Archiving DataFort Parent Keys](#) on page 100.

VIEWING DATA ENCRYPTION KEYS

Use a search tool to locate specific Data Encryption Keys stored in LKM.

1. In the DMC, in the appliance tree, select an LKM appliance.
2. From the Keys menu, click View Data Encryption Keys.
3. On the View Data Encryption Keys screen, from the drop-down box, select the search criteria to use in locating Cryptainer Keys and click Add.
 - Click Remove to delete search criteria.
 - Click the Remember Form Values check box to reuse selected search criteria.
4. To initiate a search using all of the selected criteria, click Find.

Keys appear on the View Data Encryption Keys tab.

Note: To assign names to DataFort Cryptainer Keys, see [Assigning Names to Data Encryption Keys](#) on page 128.

ARCHIVING DATAFORT PARENT KEYS

In the event that a DataFort appliance is unavailable, the LKM appliance uses an archive of Parent Keys to supply the keys needed to decrypt data. Selecting any of the Parent Keys for an DataFort appliance archives all of the Parent Keys for that appliance. Selecting a Cryptainer Key archives all of the Parent Keys for a Cryptainer Key.

Because archives of Parent Keys compromise the distributed security design of the system and DataFort Recovery Cards, create and use a Key Archive for only two purposes:

- immediate data recovery if an LKM client is no longer functioning
- Placement in key escrow or another form of trusted long-term storage, for use in an emergency

Note: Delete key archives immediately after use or upon submission to escrow.

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

This section contains the following topics:

- [About Archiving Parent Keys](#)
- [Creating Archives of Parent Keys](#)

ABOUT ARCHIVING PARENT KEYS

There are two types of archives for Parent Keys: an archive of Parent Keys for a DataFort appliance, and an archive of Parent Keys for a Cryptainer.

TABLE 11: ARCHIVING PARENT KEYS

Type	Details	Requirements
Archive of Parent Keys for a DataFort appliance	Selecting any of the Parent Keys for a DataFort appliance archives all of the Parent Keys for that DataFort appliance.	One of the following is required: • A quorum of Recovery Officers and Recovery Cards for each DataFort. Each Recovery Officer is required to present a Recovery Card and its password. • An existing Key Archive and its passphrase, supplied by the administrator during key archive generation.
Archive of Parent Keys for a Cryptainer	Selecting a Cryptainer Key archives all of the Parent Keys for a DataFort Cryptainer Key. This is useful when recovering data using Decru Data Decryption Software (DDS). See the Decru Data Decryption Software Administration Guide for details.	

CREATING ARCHIVES OF PARENT KEYS

1. In the DMC, in the appliance tree, select an LKM appliance.
Note: The LKM appliance must be linked to a DataFort appliance. See [Creating Link Policies](#) on page 92.
2. From the Keys menu, select from the following:
 - View Parent Keys from LKM
 - View Data Encryption Keys (See [Viewing Keys](#) on page 99.)
3. Select from the following:
 - On the View Parent Keys from LKM tab, right-click the key to archive and select Make Key Archive.
 - On the View Data Encryption Keys tab, right-click the key to archive and select Make Key Archive or Make Cryptainer Key Archive.
Note: Selecting any of the Parent Keys for a client archives all of the Parent Keys for that appliance. Selecting a Data Encryption Key archives all of the Parent Keys for a DataFort Cryptainer Key.
4. Select a method to create a key archive:
 - To use a Key Archive file, see [Using a Key Archive File to Create an Archive of Parent Keys](#).
 - To use Recovery Cards, see [Using Recovery Cards to Create an Archive of Parent Keys](#) on page 102.

Using a Key Archive File to Create an Archive of Parent Keys

Use a Key Archive file generated on an LKM appliance (.ka file) or a Master Key Archive file generated by LKM server software (.mka file) to make an archive of Parent Keys.

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

Note: Move the Key Archive file to escrow or secure long-term storage and store the passphrase.

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

Using Recovery Cards to Create an Archive of Parent Keys

1. On the Key Recovery screen, select Recovery Cards and click Recover.
2. On the Recover Secret Shares screen, select from the following:
 - For multiple card readers, insert a quorum of cards into the readers, enter the passwords and click Start.
 - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the password and click Start.
3. Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader it pre-populates the Card Label/Security Domain fields. A card appears selected (green) once it has been processed and added.

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

4. When prompted, select a name and location to save the Key Archive file.
5. Enter a password for the archive and click Save.

Note: Move the Key Archive file to escrow or secure long-term storage, and store the pass-phrase.

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

BACKING UP KEYS TO EXTERNAL STORAGE

This section contains the following topics:

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

ABOUT EXPORTING AND IMPORTING KEYS

Export keys to back them up from the LKM appliance to external storage. This is useful for non-redundant topologies that rely on manually exporting keys to external storage to regularly back them up.

Starting with LKM appliance 3.1, exported keys can only be imported into the LKM appliance from which they were exported. This is because exported keys are signed and signed keys must be verified by the appliance from which they were signed.

In the rare event that the key database gets corrupted on the LKM appliance, it is not possible to manually back up keys from the LKM appliance to a key export file. In this case, the LKM appliance has a second database of keys on its hard drives containing the last 599,186 keys to use when recovering keys that have not been manually backed up. To insure a complete key recovery, Limit keys that have not been manually backed up to less than 600,000 (the limit is 599,186). See [Recovering LKM Appliance Keys](#) on page 139.

EXPORTING AND IMPORTING KEYS

Note: When importing keys with LKM Key Administrator permissions, request that LKM Full Administrator temporarily change the `lkm.appliance.key.allow_unsigned_add` property to `true`. See [Setting System Properties](#) on page 129.

1. In the DMC, in the appliance tree, select an LKM appliance.
2. From the Keys menu, select Export Keys or Import Keys.
 - For export, select Full or Incremental export.
3. On the Select Directory screen, select a folder location and click Select.

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

Note: Use a separate empty folder per LKM appliance.

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

Note: Resume this procedure 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 incrementally exporting and importing new keys only.

USING MANUAL KEY TRANSLATION

When using a Decru Archive Policy, unrelated DataFort appliances that are linked to a shared LKM appliance may share keys by initiating a one-way key translation via the DMC.

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

This section contains the following topics:

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

ABOUT KEY TRANSLATION

When translating keys between DataFort appliances linked to an LKM using an Archive Policy, the LKM appliance enables the DataFort appliance receiving the keys to decrypt data encrypted by the DataFort sending the keys. See [Archive Policy](#) on page 23 and [Creating an Archive Policy](#) on page 93.

LKM Key Administrators must request the LKM administrator temporarily change the `lkm.appliance.key.allow_unsigned_add_property` to `true` to translate Cryptainer Keys. See [Setting System Properties](#) on page 129.

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

TRANSLATING CRYPTAINER KEYS

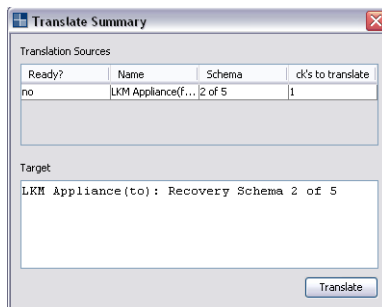
Translate Cryptainer Keys created on one DataFort appliance to another DataFort appliance, so that both DataFort appliances can access the Cryptainer.

WARNING: TRANSLATE 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, ANY KEY MATERIAL REMAINING IN THE PC'S RAM IS ZEROIZED.

1. In the DMC, in the appliance tree, select the LKM appliance.
2. From the Keys menu, click View Data Encryption Keys. See [Viewing Data Encryption Keys](#) on page 99.
3. On the View Data Encryption Keys tab, right-click the key to distribute (share), and select Translate Keys.
 - Ctrl-click to select more than one key,



- 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.
- Select a method to recover keys:
 - [Using an Key Archive File to Translate Cryptainer Keys](#)
 - [Using Recovery Cards to Translate Cryptainer Keys](#)

Using an Key Archive File to Translate Cryptainer Keys

Use a Key Archive file generated by a LKM appliance (.ka file) or a Master Key Archive file generated by LKM server software (.mka file) to distribute Cryptainer Keys.

1. On the Prepare Source DataFort <appliance_name> screen, select Key Archive or Master Key Archive file.
2. Click the Select ka or Select mka button to browse for the file, or enter the path and file name into the text box.
3. In the password text box, enter the password for the selected file, and click Recover.
4. On the Prepare Target DataFort screen, select a method to recover keys and click Recover.
5. A message appears indicating the number of keys successfully distributed, click OK.

Using Recovery Cards to Translate Cryptainer Keys

1. On the Prepare Source DataFort <appliance_name> screen, select Recovery Cards and click Recover.
2. On the Recover Secret Shares screen, select from the following:
 - For multiple card readers, insert a quorum of cards into the readers, enter the passwords and click Start.
 - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the password and click Start.
3. Follow the prompts, inserting the requested cards into the reader and clicking Start until all cards are processed.

Note: When a card is inserted into the reader it pre-populates the Card Label/Security Domain fields. A card appears selected (green) once it has been processed and added.

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

4. On the Prepare Target DataFort screen, select a method to recover keys and click Recover.
5. A message appears indicating the number of keys successfully distributed, click OK.

■ ■ ■ ■ 11 MANAGING APPLIANCES

Use the Decru Management Console to manage appliances.

The chapter contains the following topics:

- [Adding Appliances to DMC](#)
- [Creating Custom Appliance Groups](#)
- [Upgrading an Appliance](#)
- [Managing Licenses](#)
- [Backing Up Appliances Manually](#)
- [Configuring SNMP Options](#)
- [Updating Network Settings](#)
- [Updating Date and Time Settings](#)
- [Configuring and Viewing Logs](#)
- [Zeroizing an Appliance](#)
- [Rebooting an Appliance](#)

ADDING APPLIANCES TO DMC

This section contains instructions for adding appliances to DMC after they are initialized. To add an appliance to DMC for the first time, see [Adding Appliances to DMC to Initialize](#) on page 50.

This section contains the following topics:

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

ADDING APPLIANCES TO DMC

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

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

Once added, appliances appear in the appliance tree as either KM-Series, E-Series, FC-Series or S-Series. Appliances appear Unknown until logged into.

ADDING DATAFORT CLUSTER MEMBERS TO DMC

When adding a new DataFort cluster member to an existing DataFort appliance using DMC, archive links break for the existing DataFort and must be re-linked. To recreate an archive link, see [Creating an Archive Policy](#) on page 93.

Note: When re-linking DataFort cluster member links, do not delete and purge keys or keys may get purged before the re-linking occurs.

1. In the DMC, select a DataFort appliance.
2. From the Appliance menu, click Add Cluster Members.

Once added, appliances appear in the appliance tree as either KM-Series, E-Series, FC-Series or S-Series. Appliances appear Unknown until logged into.

REMOVING APPLIANCES FROM DMC

1. In the DMC, in the appliance tree, select an appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Appliance menu, click Remove.
3. On the Question screen, click Yes to remove the appliance from DMC.

CREATING CUSTOM APPLIANCE GROUPS

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

1. In the DMC, from the View menu, click Add Custom Group.
 - Add nested groups within custom groups.
2. On the Add Custom Group screen, type in a group name and click OK.
3. In the appliance tree, select an appliance.
 - Shift- or Ctrl-click to select multiple appliances.
4. Drag the appliance icon(s) into the group.

REMOVING AN APPLIANCE FROM A CUSTOM GROUP

1. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the View menu, click Remove from Custom Group.
3. On the Question screen, click Yes to remove the appliance from the custom group.

REMOVING A CUSTOM GROUP

1. In the DMC, in the appliance tree, select a custom group or nested group.
2. From the View menu, click Remove Custom Group(s).
3. On the Question screen, click Yes to remove the custom group.

UPGRADING AN APPLIANCE

Each upgrade package comes with its own set of instructions from Decru. Download the provided software package to the Management Station and complete the steps outlined in the upgrade instruction packet.

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.

WARNING: TO PREVENT UPGRADES FROM FAILING, SELECT THE STAY LOGIN OPTION IN DMC, OTHERWISE THE UPGRADE SESSION MAY EXPIRE BEFORE IT IS COMPLETE.

SETTING LOGIN AND REFRESH PREFERENCES

1. In the DMC, from the Edit menu, click Preferences.
 - Click the Stay Logged In check box to stay logged in until the DMC session is closed.
Note: As a security measure, the DMC connection to an appliance times out after 30 minutes of inactivity.
 - Select the interval to refresh the information on the Appliance tab (up to 20 minutes)
2. Click OK.

VERIFYING AN UPGRADE PACKAGE

Verify the package before performing the upgrade as described in the separate upgrade guide.

1. In the DMC, in the appliance tree, select an appliance.
2. From the Utilities menu, click Verify.
3. Browse to the upgrade file and click Apply.
Note: After the package is verified, the hash displays in a screen. Verify the displayed hash number with the known valid hash.
4. Copy and paste this number into a text editor and click OK to close the screen.

MANAGING LICENSES

This section contains the following topics:

- [Viewing Licenses](#)
- [Adding a License](#)
- [View OpenKey License Usage](#)

VIEWING LICENSES

1. In the DMC, in the appliance tree, select one or more appliance.
2. From the Configuration menu, click View Licenses.
3. On the View Licenses tab, all known licenses for the selected appliance(s) appear.
 - To remove a license, right-click the license and select Remove License.

ADDING A LICENSE

1. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Configuration menu, click Add License.
3. On the Add License screen, in the License ID field, enter the license and click Apply.

VIEW OPENKEY LICENSE USAGE

To view OpenKey Clients, see [Viewing an OpenKey Client](#) on page 95.

1. In the DMC, in the appliance tree, select an LKM appliance.
2. From the Configuration menu, click View OpenKey Key License Usage.

BACKING UP APPLIANCES MANUALLY

In the unlikely event that the LKM appliance and its peers are down, backing up the LKM appliance configuration database to external storage is useful in restoring key sharing group data. 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 made obsolete.

Note: An LKM appliance only stores the last backup of the configuration database for any appliance it is linked to.

This section contains the following topics:

- [Best Practices for Secure Backups](#)
- [Backing Up an Appliance](#)
- [Backing Up Appliances to LKM](#)
- [Backing Up Appliances from LKM](#)

BEST PRACTICES FOR SECURE BACKUPS

The backup should be retained and destroyed according to your organization's security policy.

- The system is designed to ensure that rollbacks to a prior state not possible.
- Only a single copy of the most recent LKM database must exist.
- This backup must be stored according to organizational retention guidelines.
- Old copies must be considered sensitive and must be shredded according to media shredding guidelines.
- Backups must not be transmitted over channels that retain data. Do not use Email, instead use SSH.
- When an LKM appliance's configuration database is backed up to only one location, back up the configuration database monthly.

BACKING UP AN APPLIANCE

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

1. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Utilities menu, click Back Up.
3. On the Select Directory screen, select a location for the file and click Save.

BACKING UP APPLIANCES TO LKM

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

1. In the DMC, in the appliance tree, select an DataFort appliance.
2. From the Utilities menu, click Back up Appliances to LKM.
3. On the Back up Appliances to LKM screen, click Apply.

BACKING UP APPLIANCES FROM LKM

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

1. In the DMC, in the appliance tree, select an LKM appliance.
2. From the Utilities menu, click Back up Appliances from LKM.
3. On the Select Directory screen, select a location for the folder and click Select.
4. Click Apply.

CONFIGURING SNMP OPTIONS

This section contains the following topics:

- [About SNMP Options](#)
- [Setting SNMP Options](#)

ABOUT SNMP OPTIONS

Decru appliances supports both MIB II and the read-only private Decru MIB. The Decru MIB is included on the appliance CD. It provides standard MIB-II as well as Decru MIB messages. All Decru MIBs are read-only for security reasons. A separate [Appliance SNMP Alarms Guide](#) is available from Decru for reference.

The LKM appliance support SNMP v1, v2c, v3 queries but sends only v1 traps.

Decru uses Net-SNMP agent with the following protocols:

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

Note: Decru does not support sending SNMPv3 traps.

For a complete list of Decru MIBs and SNMP alarms, contact Decru. Decru MIBs fall into the following categories:

Crypto Alerts	Useful for monitoring the status of the crypto subsystem for the DataFort appliance (crypto interrupts, crypto status, etc.).
Chassis Alerts	Useful for monitoring the physical status of the an appliance (fan speeds, temperatures, battery voltages, etc.).
System Alerts	Useful for monitoring the software running on an appliance (number of processes, file system usage, etc.).

SETTING SNMP OPTIONS

- 1. In the DMC, in the appliance tree, select an appliance.
- 2. From the Configuration menu, click SNMP Agent.
- 3. On the SNMP Agent screen, enable or disable SNMP for the appliance.
- 4. Enter information in the following fields and click Apply.

System	Enter the location of and contact person for the SNMP agent.
Trap	Host and Community—Enter the destination host IP address and the SNMP community name to send with the trap.
Version:	
SNMPv1/v2c—Read Community	A single read-only community string may be configured for SNMPv1 and SNMPv2.
SNMPv3—Optional	Check to send queries using SNMPv3. Username and Password—A single user and password can be configured for SNMPv3.

UPDATING NETWORK SETTINGS

1. In the DMC, in the appliance tree, select an appliance.
2. From the Configuration menu, click Network.
3. On the Network screen, update the hostname of the appliance, the IP address of the appliance, the netmask and gateway settings and click Apply.

Note: When changing the IP address of the appliance, DMC experiences a connection loss and the appliance has to be re-added to the management console. See [Adding Appliances to DMC](#) on page 108.

UPDATING DATE AND TIME SETTINGS

Setting date and time is a security function, in part because time controls key expiration.

1. In the DMC, in the appliance tree, select an appliance.
2. From the Configuration menu, click Date/Time.
3. On the Date/Time screen, update the date, time, and time zone settings.
 - To use a time server, enter the requested information in the NTP Time Server fields. Up to three NTP servers can be entered. Enter full server names (such as pool.ntp.org) or IP addresses.
4. Click Apply.

CONFIGURING AND VIEWING LOGS

This section contains the following topics:

- [About Log Options](#)
- [Appliance Log Storage Guidelines](#)
- [About Decru Signed Syslog \(DSS\)](#)
- [Setting Log Options](#)
- [Setting Windows Event Logging](#)
- [Setting Up Syslog](#)
- [Viewing the Appliance Log](#)
- [Verifying Signed Log Messages](#)
- [Adding Time Zone Information to Syslog Timestamp](#)

ABOUT LOG OPTIONS

The appliance logs events in these categories:

- Security
- Operations
- Performance

Within each category, there are priority levels. Elect to store appliance log information (according to category and priority level) in one or more possible location:

- Temporary (RAM inside appliance)
- Database (Appliance configuration database)
- Remote Logging Host (remote syslog server)
- Windows Event log (from Windows Event Viewer)—See [Setting Windows Event Logging](#) on page 120.

Note: It is recommended that logs be stored in more than one location. See [Recommended Log Configuration](#) for an example of a secure logging configuration.

Recommended Log Configuration

Configure the appliance to send secure Decru Signed Syslog (DSS) logs to multiple locations. For high security installations, configure appliance logging as follows:

- Enable remote logging for all types of logging messages.
- Enable Decru Signed Syslog (DSS) for Security, Operations and Performance messages.
- Store High Security, High Performance and Error and Warning Operations log messages both locally in the configuration database, and remotely.

APPLIANCE LOG STORAGE GUIDELINES

Keep in mind the following when configuring appliance logging:

- Redirect all logs to a remote syslog server, and enabling the Decru Signed Syslog feature for remote logs. Remote log storage is supported for a system running a standard syslogd configured to accept log data from the appliance.
- Critical operations must be logged both locally and remotely.
- Remote logs should be verified using the remote log verification utility.
- Note that log information stored in the configuration database is encrypted by the appliance, while the remote syslog is not encrypted and is not secure.
- The appliance configuration database can retain up to 2,500 events at a time. When this number is exceeded, old log information is purged. Logs exported via syslog remains on the syslog host subject to its log rotation and storage policies.

ABOUT DECRO SIGNED SYSLOGD (DSS)

Log signatures can be enabled if remote logging is being used. Signed logs offer a way to authenticate log messages and verify that the log is complete. The logs are sortable for missing messages and can be verified using CLI commands. The feature is applicable only to remote syslogd. See [About Signed Log Messages](#) on page 118.

When Decru Signed Syslogd (DSS) is enabled, the appliance adds metadata and a signature to each log message sent to a remote syslog server. Use the metadata and the signature to:

- Verify that a given log message is authentic.
- Verify the source and timestamp of log messages.
- Verify that no messages are missing from the log.

Note that in a regular syslogd the source and timestamp are generated by the remote daemon and therefore cannot be trusted.

About Signed Log Messages

It is possible for log data to be changed at the server or missed during a network transmission. To verify the correctness of the log, ensure that log source and global sequence numbers appear in correct order (with no log messages missing).

Logs that are missing from the sequence could be caused by the following:

- Log messages were deleted intentionally from the remote server to hide activity.
- Messages were dropped across the UDP connection between the appliance and the remote server.
- syslogd died on the remote server.

If logs appear to be missing, compare the logs saved to separate remote locations (logs can be sent to up to four locations, as indicated in [Configuring and Viewing Logs](#) on page 117) to verify breaks in the log are replicated. Remote logs can also be compared to the internal appliance log. See [Verifying Signed Log Messages](#) on page 122.

SETTING LOG OPTIONS

1. In the DMC, in the appliance tree, select an appliance.
2. From the Configuration menu, click Log Configuration.

Log Configuration
Select log configuration settings

Windows Event Log User

Domain:
 Username:
 Password:

	Temp	Db	Remote Log Host	Event Log Host	Signed
Security					
Low (6)	☐	☒			☐
High (4)	☐	☒			☐
Operations					
Trace (7)	☒	☐			☐
Information (6)	☒	☒			☐
Warning (4)	☒	☒			☐
Error (1)	☒	☒			☐
Performance					
Low (6)	☒	☐			☐
High (4)	☐	☒			☐

Reset:

Items in **bold** are required.

3. On the Log Configuration screen, select the desired settings and click Apply. See [About Log Options](#) on page 117.
 - To set a remote storage address, see [Setting a Remote Storage Address](#) on page 120.
 - To allow logs to be sent from the appliance directly to Windows Event Viewer, see [Setting Windows Event Logging](#) on page 120.

Setting a Remote Storage Address

1. In the DMC, in the appliance tree, select an appliance.
2. From the Configuration menu, click Log Configuration.
3. Enter an IP address or hostname for the machine that stores appliance log information.
Enter up to four separate servers, separated by commas, to configure the appliance to send logs to multiple locations.
4. If desired, activate Decru Signed Syslog (DSS) by checking the Signed box next to each log message type.
5. Click Apply.
 - Click Factory Default to reset the log configuration to the original Decru default settings.
 - Click Current to reset any unsaved changes to the log configuration to the last saved configuration

SETTING WINDOWS EVENT LOGGING

This feature allows logs to be sent from the appliance directly to Windows Event Viewer.

1. In the DMC, in the appliance tree, select an appliance.
1. From the Configuration menu, click Log Configuration.
2. On the Log Configuration screen, enter the following information about the user logging into the Windows host to generate the events: The domain the user belongs to, the user name, and the password. This user must have permission to log events to that host.
3. In the Event Log Host column, enter the IP address of the Windows host in these boxes.
Note: It is good practice to enter the same IP address for all event log host fields. Enter different IP addresses only if the user login is the same for all entered IP addresses.
4. Click Apply.
Note: Once configured, events from the appliance can be viewed on the host at **Computer Management > Event Viewer > Application**.

SETTING UP SYSLOG

1. On a system running a syslog daemon configured to accept syslog messages from remote hosts (specifically the Decru appliance), create an empty file to store the system log. Use any name. In this example it is Appliance1.

Note: The configuration information from the appliance is consistent with the standard syslog.conf format supported on a majority of Unix systems, but is also applicable to syslogd implementations available for other systems.

2. Edit the syslog.conf file and add these lines:

```
local0.* /var/log/Appliance1
# local0 is for Security messages

local1.* /var/log/Appliance1
# local1 is for Operations messages
```

```
local2.* /var/log/Appliance1
```

local2 is for Performance messages

- Signal syslogd to start receiving messages from the appliance.

Syslogd Mapping

[Table 12](#) shows the Descriptive Name, System Property Name, Syslog Facility and Level mapping for appliance logs.

TABLE 12: LOG MAPPING

Descriptive Name	System Property Name	Syslog Facility and Level
security low	sys.proc.syslogd.conf.sec_minor	local0.info
security high	sys.proc.syslogd.conf.sec_major	local0.warning
operations information	sys.proc.syslogd.conf.op_info	local1.info
operations warning	sys.proc.syslogd.conf.op_warning	local1.warning
operations error	sys.proc.syslogd.conf.op_error	local1.alert
operations trace	sys.proc.syslogd.conf.op_trace	local1.debug
performance low	sys.proc.syslogd.conf.perf_minor	local2.warning
performance high	sys.proc.syslogd.conf.perf_major	local2.info

Temporary Files Mapping

[Table 13](#) describes the mapping for temporary logs.

TABLE 13: TEMPORARY LOG MAPPING

WebUI Name	Temp File
security	/var/log/security
operations	/var/log/operation
performance	/var/log/performance

VIEWING THE APPLIANCE LOG

- In the DMC, in the appliance tree, select an appliance.
- From the Diagnostics menu, click View System Log.

VERIFYING SIGNED LOG MESSAGES

It is possible for log data to be changed at the server or missed during a network transmission. To verify the correctness of the log, ensure that log source and global sequence numbers appear in correct order (with no log messages missing).

Logs that are missing from the sequence could be caused by the following:

- Log messages were deleted intentionally from the remote server to hide activity.
- Messages were dropped across the UDP connection between the appliance and the remote server.
- The syslog daemon died on the remote server.

If logs appear to be missing, compare the logs saved to separate remote locations. Logs can be sent to up to four locations. See [Recommended Log Configuration](#) on page 117.

To verify breaks in the log are replicated. Remote logs can also be compared to the internal appliance log. The administrator can use the CLI to verify the correctness of the log using the `system log verify` command. See [Verifying System Logs](#) on page 131.

ADDING TIME ZONE INFORMATION TO SYSLOG TIMESTAMP

By default, timestamps in appliance syslog messages reflect the local time for the appliance sending the message, and do not contain any time zone information.

Use the following CLI commands to send syslog messages with the timestamp expressed in UTC and add the time zone information to the timestamp.

Express time in UTC

To send appliance syslog messages with the timestamp expressed in UTC:

1. Log in to the CLI and run the following command:

```
system property set sys.syslogd.utc_timezone 1
```
2. Restart the system log daemon by running the following command:

```
system log restart
```

Include Time Zone

To add time zone information in the appliance syslog timestamp:

1. Log in to the CLI and run the following command:

```
system property set sys.syslogd.print_timezone 1
```
2. Restart the system log daemon by running the following command:

```
system log restart
```

ZEROIZING AN APPLIANCE

Zeroizing an appliance erases and invalidates all encryption keys and configuration data in the system except the IP address of the appliance.

This section contains the following topics:

- [About Zeroizing the Appliance](#)
- [Zeroizing the Appliance](#)
- [Zeroizing via the Serial Console](#)
- [Zeroizing via the CLI](#)
- [Emergency Serial Console Port Access](#)

ABOUT ZEROIZING THE APPLIANCE

When an appliance is zeroized, all key and configuration material is deleted from the appliance. Some material may be recovered by selecting the recovery option of the Setup Wizard using a recent backup of the configuration and key databases. See [Table 14](#).

TABLE 14: DATA RECOVERY

Data Type	Example	Data Recovery
Keys that protect user data	Cryptainer Keys Parent Keys	Keys may be recovered to ensure data decryption by the recovered appliance.
Keys that authenticate an appliance	SSL keys SSH keys IPsec keys	Keys may not be recovered, to prevent misidentification.
Secrets belonging to users	User passwords	Passwords may be recovered to allows users access without recreating passwords.

WARNING: SSL PRIVATE KEYS ARE CLEARED BY ZEROIZATION, AND MAY NOT BE BACKED UP OR TRANSFERRED TO OTHER APPLIANCES. IF SIGNED CERTIFICATES ARE PURCHASED, THEY HAVE TO BE REPLACED.

Depending on defense settings, zeroization and recovery may be required after the chassis has been opened or if another defense response is triggered. Zeroization and recovery are required after loss or destruction of the System Card.

ZEROIZING THE APPLIANCE

Zeroizing an appliance erases and invalidates all encryption keys and configuration data in the system except the IP address of the appliance. After zeroizing, run the Setup Wizard to restore an appliance. See [Using the Setup Wizard](#) on page 51 and [Recovering LKM Appliance Keys](#) on page 139.

WARNING: BEFORE ZEROIZING AN APPLIANCE, BACK UP THE CONFIGURATION DATABASE TO ENABLE DATA RECOVERY OPERATIONS.

1. Verify the System Card is inserted into the appliance.
2. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
3. From the Appliance menu, click Zeroize.
4. On the Zeroize screen, select whether to keep the appliance's IP Address.
5. Enter the confirmation code listed on the screen (**ZeroizeYes**) and click Apply. The appliance reboots.
 - If IP settings were not preserved by checking Keep IP address, assign the appliance IP settings. See [Assigning IP Address](#) on page 48.
6. Complete the configuration by running the Setup Wizard.

ZEROIZING VIA THE SERIAL CONSOLE

When it is not possible to complete the Setup Wizard, reset the appliance using the serial connection.

1. Be sure the System Card is inserted in the appliance.
2. Connect the appliance serial console port. See [Serial Console Port](#) on page 34.
3. Log in to the serial console with a valid administrator username and password.
4. To zeroize the appliance, enter option **z**.
5. Enter a confirmation code when prompted. The appliance reboots.
6. Assign the appliance IP settings. See [Assigning IP Address](#) on page 48.
7. After the appliance has been assigned IP settings, complete the configuration by running the Setup Wizard.

ZEROIZING VIA THE CLI

In some situations it is necessary to use the CLI to zeroize the appliance. If Secure CLI is enabled, a valid Admin Card is still required to access the CLI in order to zeroize the appliance. Never reset all Admin Cards before zeroization unless Secure CLI is off.

Note: Before zeroizing the appliance, back up the configuration database by running the command `db export`. Otherwise, zeroizing may fail.

1. Be sure the System Card is inserted in the appliance.
2. Log in to the CLI with a valid administrator username and password.
3. Execute the `system zeroize` command. To preserve the existing IP address, use the `system zeroize [-k, --keep_ip]` command. A prompt appears to enter a confirmation code.
4. Enter the command again, followed by the code: `system zeroize [confirmation-value]`
5. Wait while the System Card is reset, and the appliance reboots.
6. If they were not preserved, reassign the appliance IP settings. See [Assigning IP Address](#) on page 48.
7. Complete the configuration by running the Setup Wizard.

EMERGENCY SERIAL CONSOLE PORT ACCESS

If the Admin Card and password for an appliance are lost, logging into the DMC or CLI is not possible. Instead connect to the appliance using the serial console and zeroize the appliance using a valid Recovery Card (one of the cards used to initialize the appliance).

Once zeroized, the appliance is initialized using the Decru Setup Wizard. If a current backup of the configuration database is available, the configuration can be restored using the Recover from Database function of the wizard. See [Using the Setup Wizard](#) on page 51 and [Recovering LKM Appliance Keys](#) on page 139.

1. Connect a Management Station or other PC to the appliance serial console port.
2. Connect a smart card reader to the PC connected to the serial port.
3. Insert one of the Recovery Cards for the appliance into the smart card reader.
Make a note of the Recovery Card label (e.g. RecoveryCard1).
4. Remove the Recovery Card from the card reader.
5. Remove the System Card from the appliance front panel slot.
6. Insert the Recovery Card into the appliance front panel slot.
7. On the PC, launch a terminal client to connect to the appliance.
8. At the login prompt, enter the Recovery Card label as the username and enter the Recovery Card password.
If authentication succeeds, the console menu is displayed.
9. Enter option **Z** to zeroize the appliance.

REBOOTING AN APPLIANCE

1. In the DMC, in the appliance tree, select one or more appliance.
 - Shift- or Ctrl-click to select multiple appliances.
2. From the Appliance menu, click Reboot.
3. On the Question screen, click Yes to reboot the selected appliance(s).



■ ■ ■ ■ 12 USING ADVANCED CLI COMMANDS

This chapter contains CLI procedures that cannot be completed using the Decru Management Console menus. See the [DataFort Administration Guide](#) for instructions on using the Command Line Interface (CLI) to manage DataFort appliances. See also [Using the Command Line Interface](#) on page 42 of this guide.

The chapter contains the following topics:

- [Maintaining the Appliance](#)
- [Viewing System Properties and Log Messages](#)
- [Verifying System Logs](#)
- [Setting Stack Trace](#)

MAINTAINING THE APPLIANCE

The section contains the following topics:

- [Changing Backup Intervals](#)
- [Assigning Names to Data Encryption Keys](#)
- [Checking the Status of an LKM Appliance](#)
- [Checking the Connectivity Status Between Appliances](#)
- [Setting System Properties](#)

CHANGING BACKUP INTERVALS

By default, a linked DataFort appliance sends its configuration database to the LKM appliance approximately every two hours. To change the interval at which the DataFort appliance sends a backup of its configuration database to a linked LKM appliance:

- At the CLI, run the following command:

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

Note: This system property is hidden until it is set.

ASSIGNING NAMES TO DATA ENCRYPTION KEYS

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

- 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 new_cryptainerkey_name
```

CHECKING THE STATUS OF AN LKM APPLIANCE

If keys are not syncing due to a suspected 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:

- At the CLI, run the following command:

```
lkm status
```

Option:

```
-v
```

 Verbose status.

CHECKING THE CONNECTIVITY STATUS BETWEEN APPLIANCES

If there is an error, check the network connectivity status between appliances.

To check the connectivity status between appliances:

- At the CLI, run the following command for the appliance to connect to:

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

SETTING SYSTEM PROPERTIES

- At the CLI, run the following command:

```
system property set <property_name> <value>
```

VIEWING SYSTEM PROPERTIES AND LOG MESSAGES

Use the CLI to view system logs, search for messages, and to aid in [Verifying System Logs](#).

<code>system property get</code>	View the current values of system properties, and see permissions for the administrator currently logged in. To view the current values of system properties in a detailed view that shows permissions for the administrator logged in, and lists all the administrator roles permitted to change (set) those properties use: <code>system property get -d</code> Output is in the form: <code>security-admin RW global</code> <code>sys.security.web.usesmartcard: 0</code>
<code>system selftest</code>	Performs a series of tests on the appliance and configured servers. For more details during the self tests use: <code>system selftest -v</code>
<code>system util lcdmessages</code>	Displays text of any warnings currently on the LCD.
<code>system version</code>	Displays current system version, including Platform Serial Number, Platform Firmware Version, Platform Firmware Build ID, database version, HBA firmware information, SEP information and System Card information.
<code>system reboot</code>	Reboots appliance. Adding the <code>-p</code> flag to <code>system reboot</code> cycles power to the appliance. Power-cycling is necessary after an upgrade.
<code>system log list</code>	Lists system logs in the database. Various filtering options are available, for example: Search for messages of priority 1 and type SEC: <code>system log list -p 1 -t SEC</code> Search for messages starting from 2007/1/17 1pm to 2pm (the interval <code>i</code> is in seconds): <code>system log list -b '2007-01-17 13:00:00' -i 3600</code> To search for messages of the last 24 hours: <code>system log list -b now -i -86400</code> To search for the last 10 messages: <code>system log list -o -10</code>

VERIFYING SYSTEM LOGS

1. To verify a signed log message, use:

```
system log verify <mesg>
```

2. Single quotes, double quotes, and back slashes in the message must be preceded with a back slash and the entire message must be surrounded by double quotes. For example, to verify the following log message, execute the `system log verify` command followed by the log message:

```
2004-02-10 16:21:22 Local1.Info 10.20.21.163 Feb 10 16:21:22
syslogd: boxmanager: Executed: share virtual add --ip "his"
\\\\\\his\\\\chi "nas-hiro1" (sess id: 228933632)
[AAAAAEAAAAFAAAAgUpQA== 3NKQ18/5r3x6n+Rw]
system log verify "syslogd: boxmanager: Executed: share virtual add
--ip \\"his\\" \\\\\\\\\\\his\\\\\\chi \\"nas-hiro1\\" (sess id: 228933632)
[AAAAAEAAAAFAAAAgUpQA== 3NKQ18/5r3x6n+Rw]"
```

The log `<mesg>` parameter to verify, for example `"mesg-text [meta-data signature]"` is shown here:

```
system log verify "syslogd: boxmanager: Security property
sys.security.groupreview was set to 1 [AAAAAEAAAAHAAAnCruPg==
5uKW37o/jlF5t+VT]"
```

This returns:

```
Valid message
Source sequence number: 1
Global sequence number: 7
Source timestamp: Mon Jun 16 13:37:48 2003
```

Execute the verification procedure again to check sequence validity:

```
system log verify "syslogd: boxmanager: Security property
sys.security.localacl was set to 1 [AAAAAAIAAAAIAAAnCruPg== /
xluPgNyIsypvlnx]"
```

This returns:

```
Valid message
Source sequence number: 2
Global sequence number: 8
Source timestamp: Mon Jun 16 13:37:48 2003
```

The output indicates the validity of the message, and provides a trusted timestamp and counters to help verify that no messages are missing.

SETTING STACK TRACE

Appliances have the capability to dump a trace of the platform execution stack in the event of a kernel panic. This stack trace information is useful for debugging, but may expose state information. Decru does not believe that this information poses a security risk or leaks any user or critical data, as no function arguments are leaked in the trace. However, the administrator should determine whether or not stack trace dumps should be enabled.

Note: Stack trace is on by default.

To change the stack trace setting, log into the CLI and execute the appropriate `system property` command:

- To disable stack trace:
`system property set sys.stacktrace.enabled 0`
- To enable stack trace:
`system property set sys.stacktrace.enabled 1`
- To retrieve a stack trace:
`system util stacklog`



■ ■ ■ ■ 13 TROUBLESHOOTING

This chapter contains troubleshooting information specific to the LKM appliance.

The chapter contains the following topics:

- [Maintaining the Appliance Status](#)
- [Recovering LKM Appliances](#)
- [Recovering LKM Appliance Keys](#)
- [Replacing Hardware](#)
- [Viewing LED Displays](#)
- [Checking Network Connections and Management Interfaces](#)
- [Checking Smart Cards](#)

MAINTAINING THE APPLIANCE STATUS

This section contains the following topics:

- [Viewing Appliance Details](#)
- [Collecting Tech Support Info](#)
- [Responding to a Bad Connection Error](#)

VIEWING APPLIANCE DETAILS

1. In the DMC, in the appliance tree, select an appliance.
2. From the Diagnostics menu, click View System Information.
3. The system version command runs in the CLI and the output displays.

COLLECTING TECH SUPPORT INFO

To assist Decru Technical Support in evaluating a problem, collect information useful to support from the selected appliance.

1. In the DMC, in the appliance tree, select one or more appliance.
2. From the Diagnostics menu, click Collect Tech Support Info.
3. Select a location for the file and click Save.

RESPONDING TO A BAD CONNECTION ERROR

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

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

To respond to “ERROR: Bad connection to DB3”:

1. In the serial console, log into the appliance. See [Serial Console Port](#) on page 34.
2. From the menu, select “F. fsck RAID filesystems”.

RECOVERING LKM APPLIANCES

This section provides instructions to recover the LKM appliance in both linked or standalone deployment scenarios, including restoration for physically damaged appliances and appliances that encounter hard drive and/or boot failure.

This section contains the following topics:

- [About Recovering LKM Appliances](#)
- [Recovering Linked LKM Appliances](#)
- [Recovering Standalone LKM Appliance](#)
- [Recovering Physically Damaged LKM Appliances](#)
- [Recovering LKM Appliances Due to Hard Drive or Boot Failure](#)

ABOUT RECOVERING LKM APPLIANCES

When recovering an LKM appliance, use a saved configuration database from that appliance to configure a replacement. Use the Setup Wizard to assign a new appliance the configuration from a pre-existing appliance. The replacement retains 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
- A minimum set of Recovery Officers and Recovery Cards as determined by the recovery schema
- A manual back up of the LKM appliance configuration database.

Before beginning, connect the new or zeroized appliance to the network and assign it the IP settings of the old appliance. See [Assigning IP Address](#) on page 48.

After restoring the appliance, restore its keys by importing the last key backup of the old LKM appliance. See [Exporting and Importing Keys](#) on page 103.

Additionally, to recover keys, see [Recovering LKM Appliance Keys](#) on page 139.

RECOVERING LINKED LKM APPLIANCES

Use when several LKM appliances are linked, forming a reliable, redundant LKM appliance peer network. The linked LKM appliances automatically synchronize key and configuration databases.

1. Zeroize the failed LKM appliance or obtain a replacement LKM appliance.
2. Run the Setup Wizard on the LKM appliance to configure it, or restore a saved configuration database backup, and connect it to the LKM appliance peer network and clients (DataFort appliances, OpenKey clients).

The replacement LKM appliance automatically rebuilds its key and configuration databases using replication from the LKM appliance peer network.

Note: For deployments with a large number of keys (more than one million keys) in the LKM appliance peer network, a rebuild can take several days. For a faster recovery, follow one of the standalone LKM appliance procedures below, then connect it to the LKM appliance peer network.

RECOVERING STANDALONE LKM APPLIANCE

In deployments with a single standalone LKM appliance or where an LKM appliance is isolated from a LKM appliance peer network, the administrator is responsible for performing regular backups of the LKM appliance configuration and key databases. A failed standalone LKM appliance without backup may not be recoverable.

- To recover a failed standalone LKM appliance, see [Recovering LKM Appliances Due to Hard Drive or Boot Failure](#) on page 136.
- For more information about backing up the LKM appliance, see [Backing Up Appliances Manually](#) on page 112.

RECOVERING PHYSICALLY DAMAGED LKM APPLIANCES

Causes for physical damage to appliances include:

- Natural disasters (fires, earthquakes, floods, etc.) which affect the datacenter. The LKM appliance chassis and some hardware is damaged, but the hard drives are recovered.
- Hardware failures which require hardware replacement. The administrator retains the hard drives, the LKM appliance is replaced with a new one.

Use the following recovery method:

- Assign a new LKM appliance with new hard drives the configuration of the damaged LKM appliance by restoring key and configuration database backups. See [Using the Setup Wizard](#) on page 51.

Note: The procedure to move hard drives to recover an LKM appliance is not supported for LKM 3.1 and later.

RECOVERING LKM APPLIANCES DUE TO HARD DRIVE OR BOOT FAILURE

This section contains the following topics:

- [Recovering an LKM Appliance that Boots but One Hard Drive Fails](#)
- [Recovering an LKM Appliance that Boots but Both Hard Drives Fail](#)
- [Recovering an LKM Appliance that Does Not Boot After Improper Reassembly](#)
- [Recovering an LKM Appliance that Boots but Hard Drives Are In Incorrect Drive Bay](#)

Recovering an LKM Appliance that Boots but One Hard Drive Fails

If when the LKM appliance is powered on, one hard drive is non-operational due to physical failure, the LKM appliance is still fully functional with one working and one failed hard drive. However, the failed hard drive must be replaced in order to reestablish data storage redundancy. For more information, see [Replacing Hardware](#) on page 140.

Recovering an LKM Appliance that Boots but Both Hard Drives Fail

When the LKM appliance is powered on, but both hard drives are non-operational due to physical failure, the LKM appliance is alive but cannot access the key and configuration databases or communicate with other DataFort or LKM appliances. In this case, the LKM appliance reports alerts about software or file system errors.

Some examples of reported alerts are:

- LCD shows "Software problem found: PRC3 20"
- LCD shows "Major software problem found: FSS3 6"
- `lkm key statistics` CLI command shows "ERROR: Bad connection to DB3"

Before performing a recovery, attempt to recover keys that were changed or created after the most recent key backup:

- Follow the instructions for [Recovering LKM Appliance Keys](#) on page 139.

Next, attempt to repair the hard drive manually:

- Log in to the CLI and run the following command:

```
sys util cat /var/log/fsck.log
```

If there are indications to "RUN fsck MANUALLY," connect to the serial console and select the menu option "F. fsck RAID filesystems". See [Accessing the Appliance Serial Console](#) on page 45.

If the LKM appliance is now operational, no further action is required.

If the LKM appliance is not operational and both hard drives cannot be recovered, a full recovery of the LKM appliance is required:

- Follow the instructions for [Using the Setup Wizard](#) on page 51.
- Follow the instructions for [Exporting and Importing Keys](#) on page 103 to import the key backup file. If key recovery was successful, import the key recovery file, too.

Recovering an LKM Appliance that Does Not Boot After Improper Reassembly

Use when LKM appliance hard drives are switched.

For example:

- The top drives of LKM appliance #1 and LKM appliance #2 are switched.
- The top disk from LKM appliance #1 and the bottom disk from LKM appliance #2 are inserted into LKM appliance #3.

An LKM appliance with incorrect hard drives exhibits the following symptoms:

- Does not boot
- Does not respond to ping
- Does not proceed past the "-INITIALIZING-" screen on the LCD.

In this scenario, all the mismatched drives are unmodified and are still usable in their original LKM appliance.

To return all LKM appliances to their correct configuration:

1. Power off all LKM appliances that are in this state using the power button behind the bezel on the front panel.
2. Remove all hard drives and insert them into the correct LKM appliances.
To match each drive to the proper LKM appliance, verify the serial number on each drive.
3. Power on the LKM appliances.

Recovering an LKM Appliance that Boots but Hard Drives Are In Incorrect Drive Bay

When the LKM appliance drives are switched and inserted into the incorrect drive bays. The top drive (labeled Drive #1) is in the bottom bay, and the bottom drive (labeled Drive #2) is in the top bay. The LKM appliance powers on and appears to be fully functional.

To return the LKM appliance to a supported configuration:

1. Power off the LKM appliance.
2. Swap the hard drives.
3. Power on the LKM appliance.

RECOVERING LKM APPLIANCE KEYS

This section contains the following topics:

- [About Key Recovery](#)
- [Recovering Keys](#)

ABOUT KEY RECOVERY

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

- The administrator needs 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.

In the rare event that the key database gets corrupted on the LKM appliance, it is not possible to manually back up keys from the LKM appliance to a key export file. In this case, the LKM appliance has a second database of keys on its hard drives containing the last 599,186 keys to use when recovering keys that have not been manually backed up. To insure a complete key recovery, Limit keys that have not been manually backed up to less than 600,000 (the limit is 599,186). See [Recovering LKM Appliance Keys](#) on page 139.

Key recovery requires:

- The last key backup of the LKM appliance keys. See [Exporting and Importing Keys](#) on page 103.
- The recovery key backup. See [Recovering Keys](#).

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

RECOVERING KEYS

1. In the DMC, in the appliance tree, select the LKM appliance.
2. From the Keys menu, click Key Recovery.
3. A message appears asking to continue with key recovery, click Yes.
4. On the Select Directory screen, select a folder location and click Select.

A message prompt states 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, do not pause this procedure to incrementally export keys.

REPLACING HARDWARE

This section contains the following topics:

- [Replacing Hard Disk Drives](#)
- [Replacing Fans and Power Supplies](#)

REPLACING HARD DISK DRIVES

The hard disk drive is not interchangeable within an LKM appliance or between LKM appliances. However, hard disk drive are replaceable. When replacing a hard disk drive hot-swap it.

This section contains the following topics:

- [Cold Swap](#)
- [Hot Swap](#)

Cold Swap

Cold swapping describes the process of replacing a hard drive while the appliance is powered off. Cold swapping is currently not supported. If the administrator cold swaps a hard drive and powers on the LKM appliance, it does not rebuild the RAID configuration on the hard drive. Remove the replacement hard drive and perform a hot swap instead.

Hot Swap

Hot swapping describes the process of replacing a hard drive while the appliance is powered on.

1. Determine the hard drive status by logging in to the CLI and running the following command:

```
system raid status
```

The appliance reports one physical drive status as "FAILED" and the logical drive status as "DEGRADED":

```
Logical Drive - DEGRADED  
Physical Drive 1 (S/N: DA00P6100ANU) - Online  
Physical Drive 2 (S/N: DAA0P650192G) - FAILED  
Rebuild Progress - Not Rebuilding
```

2. If necessary, order a replacement hard drive.
3. Place the appropriate drive bay label (#1 or #2) on the replacement drive.
4. Power on the LKM appliance if it is not already running.
5. Pull out the failed drive. Leave the functional drive in its bay.

WARNING: WHEN REPLACING THE RAID, UNLATCH AND WAIT 30 SECONDS FOR DRIVE TO SPIN DOWN BEFORE REMOVAL

6. Insert the replacement drive.

The LKM appliance automatically starts rebuilding the RAID configuration. The Rebuild Progress meter increments from 0% to 100%. This may take several hours. To view the status, log in to the CLI and run the following command:

```
system raid status
Logical Drive - DEGRADED
Physical Drive 1 (S/N: DA00P6100ANU) - Online
Physical Drive 2 (S/N: DAA0P650192G) - REBUILDING
Rebuild Progress - 45%
```

7. Periodically check the progress of the RAID configuration rebuild process. When it is completed, the Physical Drive status changes to "Online" and the Logical Drive status changes to "Optimal":

Logical Drive - Optimal

Physical Drive 1 (S/N: DA00P6100ANU) - Online

Physical Drive 2 (S/N: DAA0P650192G) - Online

Rebuild Progress - Not Rebuilding

Note: The LKM appliance is still fully functional during the drive replacement process.

REPLACING FANS AND POWER SUPPLIES

The appliance has field-replaceable power supplies and fan modules. For instructions on replacing fans and power supplies, refer to the service documentation.

WARNING: THERE ARE NO SERVICEABLE PARTS INSIDE THE APPLIANCE. DO NOT OPEN THE CHASSIS.

VIEWING LED DISPLAYS

This section contains the following topics:

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

FRONT PANEL LEDs

There are two front panel LEDs. See [Table 15](#).

TABLE 15: 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 [Table 16](#).

TABLE 16: BACK PANEL LED

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

CHECKING NETWORK CONNECTIONS AND MANAGEMENT INTERFACES

[Table 17](#) contains troubleshooting tips for the network and management connections to DataFort.

TABLE 17: NETWORK CONNECTIONS AND MANAGEMENT INTERFACES

Problem	Possible Cause and Solution
No Ethernet network connection	• Check the LCD on the front panel for messages. • Appliance must have an IP address assigned. See Assigning IP Address on page 48.
Power not on	• The Power LED is solid green after the power switch is turned on. If the LED is not lit, the power source may be bad. • Check power cable and if necessary plug the cable into another power source. • If the front panel LED is not lit, use the power switch to power on.
There is no output on serial console	• Console should be set to: Speed 9600, Data bits 8, Stop bits 1, Parity None, Hardware or no Flow Control. Check settings on the terminal program. • Be sure the COM port connected to the serial cable is on and working correctly. Use a different workstation if the COM port is not functioning. • Check cabling. Use only the connector provided by Decru and a straight-through cable to connect to the serial port. Make sure the cable is connected to the port marked IOIOI.
Cannot log in via serial connection	• Log in only with a valid username and password. • Try logging in again using the defaults: User: user, Password: MTKNMTKN.
Cannot connect to IP address	• Check that IP settings were set and saved after initialization. See Assigning IP Address on page 48. • Be sure the Management Station can reach the IP address on the network.
Cannot connect to domain name of appliance	The domain name must be added to the domain by the administrator, and the name must be resolvable by DNS. If not, use the IP address instead.
LCD says Intrusion Detected	Intrusion detection occurs when the chassis of the appliance is opened. Log in to the DMC and reset the tamper detection alert. See Clearing Intrusion Alerts on page 83.
LCD asks for System Card or Status LED is red	• A System Card needs to be inserted before the appliance is powered on. Once the appliance is powered on, the System Card can be removed. Messages appear about this condition. • For an appliance that has not been configured, power the appliance off, and re-insert the System Card before powering the appliance back on. Be sure the System Card is inserted all the way into the front panel slot, with gold contacts facing up and to the back. • A configured appliance may have a security setting in place that halts operations if the appliance is rebooted without a System Card. See System Card Insertion on page 33.

TABLE 17: NETWORK CONNECTIONS AND MANAGEMENT INTERFACES (CONTINUED)

Problem	Possible Cause and Solution
Cannot log in to DMC	• Access the DMC from the from the Management Station. • The network switch port connected to the appliance should be set to auto-negotiate. • Be sure no firewall is turned on for the Windows Management Station, and be sure web traffic is not going through a proxy. • In Add/Remove Programs make sure the following programs are installed: Decru Smart Card Reader, and Gemplus Smart Card Reader Tools. • Some administrators are created requiring login authorization by another administrator. If dual authentication is required for the administrator attempting to log in, an authenticating administrator must log in first. See Configuring Management Security Settings on page 78.
Need to clear the saved entries from an incomplete wizard	• Zeroize the appliance. • Delete the setup file from the Management Station. The default location for the file is C:\Program Files\Decru\Decru Management Console\components\setup\prefs. • Run the wizard again.
Cannot log in to CLI	• Log in only with a valid username and password. • Try logging in again using the defaults: User: user, Password: MTKNMTKN. • Check that Secure CLI is not on. See Configuring Management Security Settings on page 78..
Lost login information for only administrator	Log in using a Recovery Card and zeroize the appliance. See Zeroizing via the Serial Console on page 124..
CLI sessions take a long time to establish	This can occur if the DNS servers are unavailable. Log in through WebUI and change the DNS servers, or wait for the SSH to connect and then change the DNS servers from the CLI.

CHECKING SMART CARDS

[Table 18](#) contains troubleshooting tips for working with smart cards.

TABLE 18: SMART CARDS

Problem	Possible Cause and Solution
Management Station doesn't detect Admin Card	• The installer places the necessary files on the Management Station. Reinstall the smart card reader software if necessary. • The Management Station must be running Windows 2000, Windows Server 2003 or Windows XP and IE 6.0 or greater. • Be sure the Admin Card is properly inserted in the smart card reader. Re-insert the card if necessary. The reader LED should flash and then light continuously.
Need to reset System Card	Appliance needs a new or reset System Card in order to complete the setup wizard. If the System Card was not inserted into the chassis during zeroization or if it was not properly reset during zeroization, manually reset it. See Resetting Smart Cards on page 76..
Lost System Card	• Zeroize, insert a new System Card and run the Setup Wizard.
WebUI does not recognize type of card inserted into Management Station smart card reader	• The reader may identify the type of smart card incorrectly. Pull out and re-insert the card. Wait a few seconds for the card reader to detect card insertion (indicated by the status light turning green) before clicking OK. • Disconnect and re-connect the smart card reader. • Do not open more than one DMC at a time on a single Management Station.
Lost Recovery Card	Assemble a quorum of Recovery Officers and replace the Recovery Card. See Replacing a Recovery Officer on page 74..
Wrong System Card found error appears on LCD or in logs.	Software versions require specific smart card versions. A complete compatibility matrix is available from Decru. The version of the smart card is indicated by a sticker on the back of each smart card, for example V147. Check the card version by entering the following command at the CLI: <code>system version</code>
Smart card errors appear	Use an eraser to clean the metal contact on the smart card.

■ ■ ■ ■ ■ **APPENDIX I 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 appliance. When transferring keys, do not connect the LKM Server and LKM appliance to the same DataFort.

Note: This process decommissions LKM Server. Do not transfer keys back to LKM Server from the LKM appliance.

This chapter contains the following topics:

- [Migration Requirements](#)
- [Installing the Key Transfer Tool](#)
- [Using the Key Transfer Tool](#)

MIGRATION REQUIREMENTS

The migration 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 into the LKM appliance.
- LKM Key Transfer tool
- A Full Administrator must set the system property:
`lkm.appliance.key.allow_unsigned_add` to `true` before importing the keys, and when the process is complete turn the property to `false`.
See [Setting System Properties](#) on page 129.

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 clicking **Start > Settings > Control Panel > Administrative Tools**.
2. Click Services.
3. Click Decru Lifetime Key Management Service and click 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 runs automatically if autorun is enabled on the PC.
2. Click the LKM Key Transfer installer link.
3. Follow the prompts to start the installer and accept the terms of the license agreement.
4. Specify the installation directory or use the default. Click Next.
5. Click Install to begin installation.
6. Click Finish when installation concludes.

USING THE KEY TRANSFER TOOL

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

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

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

Note: The transfer tool makes a parent.xml file and keys*.xml files with 300 keys each.

3. Click OK.

Note: Key files appear in the selected directory for import into the LKM appliance. Keys must be manually imported into the LKM appliance by their entire folder. However, it is also possible to import files one at a time, in any order. See [Exporting and Importing Keys](#) on page 103.

■ ■ ■ ■ APPENDIX II PORT IDS

The LKM appliance uses the following network ports and protocols. Ensure that communication on these ports is not blocked in the network environment by firewalls or other filtering mechanisms.

TABLE 19: PORT IDS

Port ID	Transport	Protocol	Appliance Interface	Communication Interface	Communicates over VIP	Programmable Port ID
22	TCP	SSH	Secure Shell	Mgmt/Client	no	no
53	UDP	DNS	DNS network client	Mgmt/Client	no	no
123	UDP	NTP	NTP network client	Mgmt/Client	no	no
161	UDP	SNMP	SNMP client	Mgmt/Client	no	no
443	TCP	HTTPs	DMC CLI, DMC	Mgmt/Client	no	no
1040	TCP	LKMa	LKM appliance config DB backup (SSL)	Mgmt/Client	no	yes
32579	TCP	LKMa	LKM appliance key sync (XML, SSL)	Mgmt/Client	no	yes



■ ■ ■ ■ **APPENDIX III LOG FUNCTIONS**

The appliance audit function logs security relevant operations, errors, and warnings and many non-security relevant operations, errors and warnings.

This chapter contains the following topics:

- [About Logs](#)
- [Appliance Log Types](#)
- [Log Storage Locations](#)
- [Log Presentation](#)
- [Log Purging](#)
- [LKM Appliance Log Messages](#)
- [Appliance Management Messages](#)

ABOUT LOGS

Log messages are stored in one of multiple appliance logs, depending on the reason and severity of the logged event. The appliance audit configuration supports multiple log storage options, configurable for each of the appliance logs. The supported options include temporary storage within the appliance, permanent storage within the appliance, and remote storage using an external syslog host. For remotely maintained logs, the appliance may also be configured to sign exported log messages. Verification may be requested of the appliance at a later time.

Log purging is defined independently for each of the log storage locations. Note that the same log message may be stored in more than one of the storage locations, or none of the storage locations (in which case the log message is not produced).

For more information about configuring logs, see [Configuring and Viewing Logs](#) on page 117.

APPLIANCE LOG TYPES

The appliance maintains multiple logs, which distinguish the reason and severity of the event being logged. The following logs are maintained:

TABLE 20: LOG TYPES

Type	Definition
Security Logs	• Security Log messages give information about access control, logins and appliance state changes. They include IFC logs, Auth logs, Security Management logs and Integrity logs. • IFC log messages are generated when Information Flow Control rules either deny an unauthorized information flow or allow an authorized information flow. • Auth logs record authentication requests and decisions made by the appliance. • Security Management logs record changes to authentication policies. • Integrity Logs record events that might modify the integrity of the appliance (for example clock or tamper settings).
Operational Logs	Operational Logs indicate the status of various processes and activities in the system.
Performance Logs	Performance Logs indicate utilization characteristics of the appliance.
Audit Logs	Audit logs are generated by the appliance audit function when modifications to its configuration or state are made.

LOG MESSAGE PARAMETERS

For each category, there are set parameters for what may appear in log messages for that category. Any log message parameters not described in the following table are described with the log message.

TABLE 21: PARAMETERS IN LOG MESSAGES

Parameter	Description
<action>	Action taken in response to event, may be: • DISABLE_SEP: The SEP was disabled as a result of the event. • ZEROIZE_SEP: The SEP was zeroized as a result of the event
<admin>	This parameter indicates an appliance administrator.
<code>	Error code returned by LKM appliance database upon exit.
<command>	Command the system attempted to execute.
<db_name>	Name of database that was removed.
<details>	Details of the error.
<domain>	Domain name of the user that changed the configuration parameter.
<duration>	Number of seconds it took for the message to be handled.
<errno>	Error code returned, if any.
<error>	Description of the error.
<error_string>	Description of returned error code, if any.
<event>	Name of event that occurred.
<info_int>	Miscellaneous additional information, if any.
<info_string>	Miscellaneous additional information, if any.
<interface>	Interface to which the user is attempting to authenticate, may be: • CLI—The user is authenticating to the CLI interface. Note that this interface is disabled in the CC evaluated configuration. • DMC—The user is authenticating to the DMC interface. Note that administrators may use the DMC CLI interface after authenticating to the DMC interface. • SERIAL—The user is authenticating to the appliance MenuShell interface.
<ip>	IP address of LKM peer.
<key_descriptor>	Value of key_class_name, key_format_name, id, and key_description of key.
<key_sharing_group>	Name of the key sharing group the peer belongs to.
<message>	Error message description.
<node>	Description of the node to which connection was established or terminated.
<peer>	LKM peer type.
<prop_name>	Name of a logging facility configuration property (see Table 4).
<query>	SQL query send to LKM database.
<reason>	The reason parameter indicates the rule that caused access denial. • port locking rule—the host is not connected via the required port number • authentication rule—the host is not authenticated • authorized flow rule— the host is requesting an unauthorized information flow Reason for authentication failure, may be: • USERPASS—The user entered an incorrect password. • SMARTCARD—The user attempted to authenticate using the wrong smart card.

TABLE 21: PARAMETERS IN LOG MESSAGES (CONTINUED)

<serial_number>	Serial number of the appliance that denied or allowed the information flow
<setcleared>	The certificate is either set or cleared.
<signal>	ID of signal, e.g. SIGPIPE, SIGTSTP
<src_db_name>	Name of source database.
<tgt_db_name>	Name of target database.
<user_session_id>	ID of the user session.
<user>	Name of user that changed configuration parameter or attempted to authenticate.
<username>	Administrator user name.
<usertype>	ADMIN or USER
<user_target>	This parameter is used for log messages indicating a modification of a user account. In these log messages, <user> is the user that performed the action, while <user_target> is the user that was modified.
<user_domain>	This parameter is used for log messages indicating a modification of a user account. In these log messages, <domain> is the domain of the user that performed the action, while <domain_target> is the domain of the user that was modified.

LOG STORAGE LOCATIONS

For each of the appliance logs, the administrator may select multiple storage locations. Whenever a new log message is generated, it is written to storage location(s) as configured for the log the message belongs to. The following storage options are available:

- Temporary storage

Logs stored in the temporary storage location are written to RAM within the appliance. Note that log messages of the same event type (but different severity) are aggregated in temporary storage (i.e. Security logs, Operations logs, Performance logs).
- Database storage

Logs stored in the database storage location are written to the appliance configuration database.
- Remote storage

The appliance forwards a log message to a remote syslog host whenever a generated log message is of an event and priority type for which the administrator has specified remote storage. For remotely stored logs, the administrator may also optionally specify log message signing, in which case the appliance appends a signature to the exported log message.

TABLE 22: DEFAULT LOG STORAGE LOCATIONS

Log	Default Location	Location when in CC mode
High priority security log	database storage	database storage
Low priority security log	database storage	database storage
Operations trace log	RAM storage: /var/log/operation	disabled
Operations warning log	database storage RAM storage: /var/log/operation	disabled
Operations informational log	database storage RAM storage: /var/log/operation	disabled
Operations error log	database storage RAM storage: /var/log/operation	disabled
High priority performance log	database storage	disabled
Low priority performance log	RAM storage: /var/log/performance	disabled

LOG PRESENTATION

- [Temporary Logs](#)
- [Database Logs](#)
- [Remote Logs](#)

TEMPORARY LOGS

The administrator may view log messages stored in RAM by issuing the CLI command `sys util cat`, with one of the following parameters:

```
/var/log/security
/var/log/operation
/var/log/performance
/var/log/audit
```

The logs shown for each selectable location are dependent on the configuration options the administrator has chosen for temporary storage locations.

All log messages include:

- time the event occurred
- event type and priority
- hostname of the appliance that generated the log
- log message

DATABASE LOGS

The administrator may view log messages stored in the database using either the CLI or the DMC.

- [Viewing Database Logs via CLI](#)
- [Viewing Database Logs via DMC](#)

Viewing Database Logs via CLI

The administrator may view log messages stored in the database by issuing the `sys log list` command. The command may be used with optional parameters to filter outputted log messages.

Log messages are listed in the following format:

```
<SEQ> <DATE> <CAT> <MSG>
```

<SEQ> is the unique number assigned to each log message.

<DATE> is the date the log message was generated.

<CAT> represents which log contains the message as follows:

- <16.[4,3,2,1,0]>: High priority Security Log
- <16.[7,6]>: Low priority Security Log
- <17.[1,0]>: Operations Error Log
- <17.4>: Operations Warning Log

- <17.6>: Operations Information Log
- <17.7>: Operations Trace Log
- <18.[4,3,2,1,0]>: High priority Performance Log
- <18.6>: Low priority Performance Log
- <19.[4,3,2,1,0]>: High priority Security Log
- <19.6>: Low priority Security Log

Note: <19.*> is different from <16.*> messages in that the <19.*> messages are also available in CC mode.

<MSG> is the log message.

Viewing Database Logs via DMC

The administrator may view log messages stored in the database by clicking **Diagnostics > View System Log** in the DMC.

All log messages include:

- time the event occurred
- hostname of the appliance that generated the log
- event type
- priority
- log sequence number
- log message

To customize the log view, see [Configuring and Viewing Logs](#) on page 117.

REMOTE LOGS

The formatting for exported log messages corresponds to the syslog protocol as specified in the syslog RFC. The following represents the formatting for an exported log message:

```
<TIME> ' ' <MSG>
```

<TIME> contains a timestamp as specified in the syslog RFC.

<MSG> is the log message, as specified in section 3.

The following is an example log message, as forwarded to a remote syslog host (line breaks are added for readability):

```
Oct11 15:45:26 <17.7> qa-lkm9.nasqa.decru.com syslogd:<message>
```

TABLE 23: APPLIANCE EVENT AND PRIORITY CORRESPONDENCE TO SYSLOG FACILITY AND SEVERITY

Appliance Log	Syslog facility	Syslog priority
High Priority Security Log	LOG_LOCAL0 (16)	4,3,2,1,0
Low Priority Security Log	LOG_LOCAL0 (16)	6
Operations Error Log	LOG_LOCAL1 (17)	1,0
Operations Warning Log	LOG_LOCAL1 (17)	4
Operations Informational Log	LOG_LOCAL1 (17)	6
Operations Trace Log	LOG_LOCAL1 (17)	7
High Priority Performance Log	LOG_LOCAL2 (18)	4,3,2,1,0
Low Priority Performance Log	LOG_LOCAL2 (18)	6

The administrator may configure the appliance to sign log messages. See [Configuring and Viewing Logs](#) on page 117. The configuration option is available separately for each appliance log. If configured, metadata and signature fields are appended to the exported log message:

```
<TIME> ' ' <MSG> '[' <MDATA> ' ' <SIG> ' ']
```

The <MDATA> field includes the following base 64 encoded bytes:

```
0x0000000000 padding
4 bytes local sequence number
4 bytes global sequence number
4 bytes timestamp
```

The local sequence number is the message sequence number with respect to the specific appliance log. The global sequence number is the message sequence number with respect to all appliance generated logs. Note that the appliance maintains sequence numbers across power cycles.

The <MDATA> field is appended to the message before the signature is computed. The signature is computed across:

```
<MSG> ' ' <MDATA>
```

The computed signature is the first 12 bytes of a SHA_1 based HMAC. The 12 byte signature is then appended to the message. The following are example <MDATA> and <SIG> fields:

```
[AAAAAKxXAAC4FWAA6tgoQg== b/hPTEecqTCpD/Mk]
[AAAAAHAdAAC5FWAA69goQg== fN1evQzBytL/ulfz]
```

LOG PURGING

The appliance purges stored log messages depending on what type of storage location is selected for the log type. The purging operation is independent for the same message stored in multiple locations.

- [Temporary Storage Log Messages](#)
- [Database Storage Log Messages](#)

TEMPORARY STORAGE LOG MESSAGES

The appliance checks for maximum space requirements on log messages stored in RAM at 5 minute intervals. Separate checks are performed for each aggregation of log messages.

TABLE 24: SPACE ALLOWANCES FOR TEMPORARILY STORED APPLIANCE LOG MESSAGE

Appliance log	Meaning	Max size
High priority security log Low priority security log	combined size of high / low priority security logs	100kB
Operations error log Operations warning log Operations informational log Operations trace log	combined size of all operations logs	1000kB
High priority performance log Low priority performance log	combined size of both performance logs	500kB

If a large number of log messages are generated in a short period of time, the space allowances for each log type may be exceeded before the 5 minute timer expires. In this case, two events may trigger earlier purging:

- The total allocated space for all log messages stored in RAM reaches 70% capacity
- The total allocated space for all log messages stored in RAM reaches 90% capacity

Note: A 10 second timer checks for the previous conditions.

DATABASE STORAGE LOG MESSAGES

The log database has a saturation limit of 2500 events. When that limit is hit, the system should delete old events based on the following criteria.

Log messages should be deleted so that the last 925 high priority and 1330 low priority messages remain in the log database.

LKM APPLIANCE LOG 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 25: LKM PROCESS MESSAGES

Message	Details
LKM daemon started	lkmd process has started.
LKM daemon stopped	lkmd process has shut down.

The logs in [Table 26](#) 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. Messages concerning cleartext connections, SSL/cleartext mismatches or certificate mismatches 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 26: LKM APPLIANCE CONNECTION MESSAGES

Message	Details
LKM: SSL connection to X.X.X.X:Y succeeded	Outgoing SSL connection is established.
LKM: SSL connection to X.X.X.X:Y rejected	Outgoing SSL connection has failed.
LKM: SSL connection from X.X.X.X rejected (unknown peer)	Incoming SSL connection has failed, peer is unknown.
LKM: SSL connection from X.X.X.X:Y accepted	Incoming SSL connection is established
LKM: SSL connection from X.X.X.X rejected (no certificate stored for peer)	Incoming SSL connection has failed, certificate is not stored.
LKM: SSL connection from X.X.X.X rejected (unmatched certificate for peer)	Incoming SSL connection has failed, certificate is unmatched.
LKM: SSL connection to/from X.X.X.X:Y rejected attempting to use the certificate of Z.Z.Z.Z	Outgoing/Incoming SSL connection has failed; certificate matches one from another peer.

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 27: PROCESS MESSAGES

Log Message	Details
Deleting LKM key database: <msg>	All the keys are being deleted; appears when zeroizing.
Deleting LKM Configdbs: <msg>	All the stored remote configuration databases are being deleted; appears when zeroizing.
Deleting LKM key journal: <msg>	All the keys are being deleted; appears when zeroizing.

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 28: CONNECTION MESSAGES

Log Message	Details
Closing bad connection to LKMDB	Closing bad connection to the LKM database.
Opening connection to LKMDB	Opening connection to the LKM database.
Failed to connect to LKMDB	Failed to connect to the LKM database.
Failed to initialize LKMDB: <msg>	Fail to initialize the LKM database.
Closing connection to inconsistent LKMDB	Closing connection to inconsistent LKM database.
Closing connection to LKMDB	Closing connection to LKM database.
LKM Server X.X.X.X inserted DataFort X.X.X.X inserted	Added LKM peer: LKM appliance, LKM software, or DataFort.
LKM Server X.X.X.X updated: Port: Y -> Z DataFort X.X.X.X updated: Port: Y -> Z	Updated LKM peer: LKM appliance, LKM software, or DataFort.
LKM Server X.X.X.X deleted DataFort X.X.X.X deleted	Deleted LKM peer: LKM appliance, LKM software, or DataFort.

■ ■ ■ ■ APPENDIX IV PARTIAL LIST OF ISO COUNTRY CODES

The country codes that are used when setting SSL security certificates are established by the International Organization for Standardization (ISO). A full list of country codes can be found on their website. A partial list of codes is shown below.

TABLE 29: ISO COUNTRY CODES

Country	Code	Country	Code
AUSTRALIA	AU	MEXICO	MX
AUSTRIA	AT	NETHERLANDS	NL
BELGIUM	BE	NEW ZEALAND	NZ
CANADA	CA	NORWAY	NO
CHINA	CN	PANAMA	PA
DENMARK	DK	PHILIPPINES	PH
FINLAND	FI	POLAND	PL
FRANCE	FR	PORTUGAL	PT
GERMANY	DE	PUERTO RICO	PR
GREECE	GR	SINGAPORE	SG
HONG KONG	HK	SPAIN	ES
INDIA	IN	SWEDEN	SE
IRELAND	IE	SWITZERLAND	CH
ISRAEL	IL	TAIWAN	TW
ITALY	IT	THAILAND	TH
JAPAN	JP	UNITED KINGDOM	GB
KOREA	KR	UNITED STATES	US

APPENDIX V SPECIFICATIONS

TABLE 30: 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 8.9 cm (3.5") H x 79.5 cm (31.3") D
	Security	Chassis and SEP 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 ~ 47 - 63 Hz, SA 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 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	13,000ft at 30C
	Transportation	ISTA-2A
	RoHS	R5, EU, China 2007
	WEEE	EU
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, TUV2845 China CCC International CB: IEC 60950-1



■ ■ ■ ■ **APPENDIX VI REGULATORY AND CERTIFICATIONS**

The chapter contains 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 are applied:

- EN55022:1998 +A1:2000 and A2:2003, CISPR22:1997
- EN 61000-3-2 (2000) / IEC 61000-3-2 (2000) Harmonics
- EN 61000-3-3 +A1 (2001) / IEC 61000-3-3 (1994) Flicker
- EN55024: 1998 Plus A1: 2000 & A2: 2003, CISPR24:1997
- EN60950-1: 2001+A11: 2004
- UL60950-1:2003
- CAN1CSA-C22.2 No. 60950-1-03

■ ■ ■ ■ ■ APPENDIX VII GLOSSARY

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 a Speciality Administrator may execute a limited set of specific functions.
Admin Card	A smart card used to authenticate an administrator. An individual possessing the Admin Card and the username and password for that card has privileges of an administrator. Appliances detect 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.
Archive Policy	The LKM appliance archives all encryption keys for its clients and the most recent configuration database for any DataFort appliance. The LKM appliance uses automatic and manual backup methods to archive keys and configuration data.
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, appliances require both a username/password combination and a token to authenticate an administrator and Recovery Officers. Appliances 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. Appliances are 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 device. The CLI allows remote users to log in as an administrator 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. The LKM appliance automatically stores the most recent configuration database for any linked DataFort or LKM appliance.
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.
Data Encryption Key	LKM appliances automatically stores Data Encryption Keys for all LKM clients in the enterprise.
Decru Management Console (DMC)	The Decru Management Console (DMC) is an application that is installed on the Management Station. It provides a centralized management interface for all LKM clients and appliances in a network.
failover	The ability to withstand the failure of one or several system components by transferring access to data from a failed path to a healthy one. To provide redundancy in case of failure, the DataFort can be connected to the fabric via two ports, allowing the same LUN to be addressed via two or more WWNs or port addresses.
Fibre Channel	Fibre Channel is a physical layer (fabric) that connects servers, switches and hubs, storage devices and appliances (such as DataFort). Fibre Channel carries SCSI-3 traffic. Hosts in the fabric see storage devices as if they were locally attached storage.
IPsec	Internet Protocol Security. A standard for secure network communication. Communication between clustered DataFort devices occurs over IPsec; IPsec communication is a licensed option between DataFort and clients.
key	In cryptography, a key is a value applied to cleartext (using an algorithm) in order to generate ciphertext, or applied to ciphertext to generate cleartext. Each cipher requires a key in order to encrypt or decrypt data.
Lifetime Key Management™ appliance (LKM)	Decru's proprietary solution for encryption key management. LKM software and the LKM appliance both store key information.
LKM Client	Decru appliances or OpenKey clients that are linked to an LKM appliance.
LKM Software	The LKM Software utility securely automates the archiving of encryption keys across the enterprise, so data is always readily available. DataFort supports either the LKM software or the LKM appliance but not both. See the DataFort Administration Guide .
Key Sharing Group	LKM clients form key sharing groups and automatically share keys between group members when creating a key sharing policy. Clients in a key sharing group with an LKM appliance pass encryption keys to that LKM appliance. The LKM appliance also passes keys to clients.
Key Sharing Policy	LKM clients may use a key sharing policy when linking to an LKM appliance. This allows them to form a key sharing group and automatically share keys. The LKM appliance continues to archive all encryption keys for its clients and the most recent configuration database for any DataFort appliance.

Management Station	A Windows PC equipped with a smart card reader, from which an administrator can manage an appliance.
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.
Opaque Key	This is a wrapped Data Encryption Key that the LKM appliance simply archives. To unwrap these keys, either a Recovery Card quorum or a Key Archive file for each Decru appliance is required.
Parent Key	The Parent Key is encrypted by a master key, unique to each appliance. This master key, generated at the time an appliance is initialized, is used to decrypt and encrypt key material for safe storage and backup.
Parent Key, Archive of	The archive of Parent Keys for a DataFort appliance. Selecting any of the Parent Keys for a DataFort appliance archives all of the Parent Keys for that appliance. Selecting a Cryptainer Key archives all of the Parent Keys for a DataFort Cryptainer Key.
quorum	The minimum number of Recovery Officers required to complete sensitive management procedures.
RAID Disk Drives	The backup of the configuration database including synced keys (from any LKM client including 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 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 appliance. A quorum of Recovery Officers is required for other sensitive options such as data recovery, cluster authentication, and Recovery Card replacement.
Remote Authorization	Remote Authorization allows an administrator to initiate and verify Recovery Card operations for DMC Setup and Trustee wizards from a remote location.
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.
SecureView	SecureView™ is a licensed feature which enables enterprise class appliance management. This feature is enabled on a per-appliance basis.
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 appliances.
Smart Cards	Credit card-sized devices with embedded microchips used by appliances 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 the appliance for boot-up to enable encryption services. The System Card may be removed during normal operation to prevent unauthorized use of the appliance upon reboot.
Trusted Key	The LKM appliance stores these unwrapped Data Encryption Keys on the LKM appliance and wraps them in its own Parent Keys. This allows unrelated Decru appliances to share keys using an LKM appliance without manually importing and exporting keys or going through the key translation process. A trustee relationship with an LKM appliance, and a key sharing group membership is required.
Trustee Relationship	Decru appliances must form a trust or trustee relationship with an LKM appliance before creating a key sharing group. This allows them to share keys without manually importing and exporting keys or going through the key translation process.
Trustee Acceptance Package (TAP)	The second message between appliances when setting up a trustee relationship.
Trustee Establishment Package (TEP)	The first message sent between 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.

INDEX

A

- adaptor
 - RJ45 to DB9 34
- add
 - administrator 69
 - administrator card 75
 - appliance 108
 - cluster members 108
 - license 111
 - linked appliances, DMC 95
- Admin Card
 - about 166
- administrator
 - about roles 66
 - accounts 67
 - add 69
 - add card 75
 - authorize login 71
 - backup 67
 - change password 70
 - delete 71
 - edit permissions 70
 - full admin 66
 - key 67
 - machine 67
 - manage 65, 66
 - read only 66
 - remove card 76
 - security 67
 - speciality 66, 67
 - storage 67
 - view 69
- AES
 - about 166
- alert
 - clear, intrusion 83
- appliance
 - add 108
 - assign IP settings from LCD 49
 - back up 112
 - back up manually 112
 - defense response 78
 - menu 58

- reboot 126
- remove 108
- remove, custom group 109
- security 77
- upgrade 110
- verify upgrade package 110
- zeroize 124

- archive
 - create policy 93
 - keys 100
 - Parent Keys 100
 - policy 23
- archive Parent Keys
 - create via Key Archive file 101
 - create via Recovery Cards 102
- authentication
 - about 166
- authorize
 - login 44

B

- back panel
 - LED 142
- back up
 - appliance 112
 - appliances, manually 112
 - configuration database 25, 113
- backup
 - frequency, configuration database 128
 - secure 112
- battery iv, 28
- block cipher
 - about 166

C

- Canadian ICES-003
 - certification 164
- CE
 - certification 165
- certificate
 - about 81
 - lost after zeroize 123
 - set authority 82

- set local 82
 - certification
 - Canadian ICES-003 164
 - CE 165
 - declaration of conformity 164
 - European Union 164
 - VCCI Class A 165
 - change
 - key sharing group 96
 - key sharing group for DataFort appliance 96
 - key sharing group for keys 97
 - key sharing group, OpenKey client 96
 - Recovery Card password 76
 - chassis
 - about 166
 - intrusion 78
 - ciphertext
 - about 166
 - cleartext
 - about 166
 - CLI
 - administrator login 42
 - command help 42
 - commands 127
 - connect from SSH client 42
 - connect via DMC 44
 - connecting 42
 - documentation 42
 - dual authorization 44
 - help 42
 - login 42
 - login via DMC 44
 - login, dual authorization 44
 - secure 39
 - standard 42
 - system commands 130
 - system properties 130
 - client
 - about 166
 - cluster
 - about 166
 - add members 108
 - collect
 - tech support info 134
 - commands
 - CLI 127
 - configuration
 - menu 60
 - configuration database
 - about 167
 - back up 113
 - backup frequency 128
 - event log capacity 118
 - configure
 - management security settings 78
 - connection error
 - respond 134
 - conventions
 - LKM appliance guide 15
 - create
 - archive of Parent Keys 101
 - archive Parent Keys via Key Archive file 101
 - archive Parent Keys via Recovery Cards 102
 - archive policy 93
 - custom group 109
 - key sharing policy 92
 - OpenKey policy 94
 - Cryptainer
 - about 167
 - Cryptainer Keys
 - identification 128
 - transfer 104
 - translate via Key Archive file 106
 - translate via Recovery Cards 106
 - cryptography
 - about 167
 - custom group
 - create 109
 - remove 109
 - remove appliance 109
- D**
- daemon
 - Syslogd 118, 120
 - Data Encryption Key 99
 - identification 128
 - DataFort
 - change key sharing group 96
 - diagram, back panel 33
 - management interfaces 38
 - purge keys 24
 - restore 135
 - specifications 162
 - date
 - set 116
 - date and time settings

- update 116
- declaration of conformity
 - certification 164
- Decru Signed Syslogd (DSS) 118
- defense
 - alert, clearing 80
 - response settings 78
 - response, change setting 80
 - response, triggers 78
 - setting 78
- delete
 - administrator 71
- display
 - state 56
- DMC 40
 - dual authorization 41
 - secure 39
 - secure login 41
 - standard login 40
- dual authorization
 - connect via DMC 41
 - login 44
 - login, CLI 44

E

- edit
 - administrator permissions 70
 - menu 59
- Ethernet cable 29
- European Union
 - certification 164
- event log 117
- exit
 - management console 54
- export
 - keys 103
 - keys to external storage 103
- external
 - back up 113

F

- failover 169
 - about 167
- fibre channel
 - about 167
- front panel
 - assign IP address 49
 - LED 142

- System Card slot 33

H

- hard drive
 - replace 140
- hardware
 - replace 141

I

- import
 - keys 103
 - keys from external storage 103
- install
 - key transfer tool 148
 - management console 36
 - precautions iv, 29
 - rack mount 32
 - requirements 29
- International Organization for Standardization (ISO) 82, 161
- intrusion
 - clear alert 80, 83
 - defense setting 26
 - detection 78, 80
- IP address 30
- IP settings
 - assign from LCD 49
 - assign from serial console 48
 - assigning from serial console 45
 - configuring from CLI 45
- IPsec
 - about 167
- ISO 161
- IT power systems 28

K

- key sharing group
 - change 96
- key sharing policy
 - create 92
- key translation 104
- key, chassis 78
- keys
 - about 167
 - archive 100
 - change key sharing group 97
 - escrow 25
 - escrow service 25

- export to external storage 103
- export/import 103
- import from external storage 103
- install transfer tool 148
- limits 24
- manage 98
- move into key sharing groups 97
- quorum 25
- recover 139
- run transfer tool 148
- transfer, LKM 2.5 to 3.0 146

L

LCD

- assign appliance IP settings 49
- bar graph 46
- buttons 46
- front panel, display 46

LED

- back panel 142
- front panel 142
- power supply 143, 145
- view display 142

license

- add 111
- manage 111
- view 111
- view, OpenKey 111

Lifetime Key Management

- about 167

link

- add appliance links, DMC 95
- remove policy 95
- view report 95

link policy

- archive policy 23

lithium battery iv, 28

LKM appliance 135

- assign IP address 48
- assign IP settings from serial console 48
- boxmanager connection messages 160
- boxmanager process messages 160
- connect 33
- connectivity status 129
- deployment 19
- features overview 13
- guide conventions 15
- how it works 16

- link policies 17
- LKM connection messages 159
- LKM process messages 159
- log into 54
- menu 61
- overview 13
- recover 135, 136
- shut down via CLI 35
- shut down via LCD 35
- status 129
- troubleshooting 133

LKM server

- halt operations 147

lkmd 159

log 117, 118, 121, 152

- about 151
- appliance management, messages 160
- database 155
- database, storage messages 158
- LKM appliance 159
- options 117
- planning remote security 25
- purge 158
- remote 156
- set options 119
- set Windows event log 120
- signed messages 118
- storage 118
- storage locations 154
- Syslogd 118
- Syslogd map 121
- temporary 155
- temporary file map 121
- temporary, storage messages 158
- types 151
- verify messages 122
- verify, system 131
- view 121

login 45

- authorize 44
- authorize for administrator 71
- CLI 42
- LKM appliance 54

M

manage

- keys 98
- license 111

Index

- smart card 72
- management
 - console, exit 54
 - console, install 36
 - port 34
 - port, Ethernet 34
 - station 30
- management security setting
 - configure 78
- Management Station
 - about 168
 - requirements 30
- manual key translation 23
- map
 - Syslogd 121
 - temporary file 121
- menu
 - appliance 58
 - configuration 60
 - diagnostic 64
 - edit 59
 - help 64
 - keys 61
 - LKM appliance 61
 - security 63
 - topology 61
 - trustee 63
 - use 55
 - utilities 62
 - view 59
- message parameters 152
- messages 159
- metadata 118
- move
 - keys into key sharing group 97

N

- NAS
 - about 168
- network
 - switch ports 29
 - time servers 116
 - update settings 116
- NTP 116

O

- online help 39
- OpenKey client

- change key sharing group 96
- create policy 94
- view 95
- options 40

P

- panel
 - connections 33
- Parent Key
 - create archive 101
- Parent Keys 99
 - about archive 100
 - about archives 100
 - view via LKM 99
- password
 - change for administrator 70
 - one-time, CLI 43
 - Recovery Card, change password 76
- port
 - management 34
- power
 - LKM appliance on 34
 - on after shut down 34
 - precautions 28
 - supply notice 28
- power supply
 - LEDs 143, 145
- purge keys
 - DataFort appliance 24

Q

- quorum
 - about 168

R

- rack mount
 - DataFort 32
 - installation 32
 - kit 29
 - standard 32
- RAID
 - about 168
- reboot
 - appliance 126
- recommended configuration 117
- recover 135
 - keys 139
 - LKM appliance 135, 136

- Recovery Card
 - about 168
 - change password 76
 - lost 73
 - replace 73
- recovery officers
 - about 168
 - setup requirement 50
- Remote Authorization
 - DMC 39
 - via SecureView 39
- remove
 - administrator card 76
 - appliance 108
 - custom group 109
 - link policy 95
- replace
 - hard drive 140
 - hardware 141
- requirements
 - Management Station 30
- reset
 - smart card 76, 117
 - System Card 145
- restore
 - DataFort 135
- RJ45 to DB9 adapter 29
- run
 - key transfer tool 148
 - Setup Wizard 51

S

- SAN
 - about 168
- Secure CLI
 - login 43
- secure login
 - connect via DMC 41
- secure shell (SSH)
 - support 38
- SecureView 39
- security
 - appliance 77
 - certificate, local 82
 - certificate, self-signed 82
 - domain, about 168
 - menu 63
- security certificate

- certificate authority signed, installing 82
- SEP
 - about 169
- serial console
 - access 45
 - clearing IP Settings 45
 - connect serial port 34
 - connecting serial port 45
 - interface 38
 - LKM appliance settings 48
- server
 - halt operations 147
- set
 - certificate authority 82
 - date 116
 - defense response 78
 - log options 119
 - remote storage address 120
 - SNMP options 115
 - stack trace 132
 - system properties 129
 - time 116
- setup
 - Syslog 120
 - wizard 50
- Setup Wizard 50
 - run 51
- shut down
 - LKM appliance 34
 - LKM appliance via CLI 35
 - LKM appliance via LCD 35
- smart card
 - about 72, 168
 - admin 73
 - manage 65, 72
 - reader, USB 29
 - recovery 73
 - reset 76, 117
 - system 72
 - troubleshooting 145
- SNMP
 - about 38, 168
 - chassis alerts 114
 - configuration 114
 - crypto alerts 114
 - options 114
 - set options 115
 - settings 39

Index

- system alerts 114
- SSH 38
 - about 169
 - CLI access 42, 44
- SSL
 - about 169
- stack trace
 - set 132
- standard login
 - connect via DMC 40
- standard straight through ethernet cable 29, 34
- state displays 56
 - use 55
- storage
 - address, set remote 120
 - log 118
- Syslog
 - setup 120
- syslog mapping table 121
- Syslogd
 - about 118
 - daemon 118, 120
 - map 121
- System Card
 - about 169
 - insert 33
 - reset 145
- system details
 - view 134
- system properties
 - CLI 130
 - set 129

T

- tab
 - appliance 57
 - table columns 57
- TAP
 - about 169
- tech support info
 - collect 134
- temporary file mapping 121
- TEP
 - about 169
- time
 - set 116
- time servers 116
- time-out

- CLI 42
 - serial session 45
- transfer
 - Cryptainer Keys 104
 - keys, LKM 2.5 to 3.0 146
- translate
 - Cryptainer Keys via Key Archive file 106
 - Cryptainer Keys via Recovery Cards 106
- troubleshooting
 - LKM appliance 133
 - network connections 143
 - smart card 145
- Trustee Acceptance Package (TAP) 86
- Trustee Establishment Package (TEP) 86, 87, 88, 90
- trustee relationship
 - about 169
 - approve TAP, on local network 88
 - approve TEP, on local network 87
 - authorizing trustees locally to approve TEP/
TAP, on a local network 86
 - create 85
 - create TEP, on remote network 89
 - create trustee link, on local network 85
 - create, on local network 85
 - create, on remote network 89
 - delete, unapproved TAP trustee 91
 - initiating remote authorization to approve
TAP, on local network 88
 - initiating remote authorization to approve
TEP, on local network 87
 - receive TAP, on remote network 91
 - receive TEP, on remote network 90

U

- UDP
 - about 169
- update
 - date and time settings 116
 - network settings 116
- upgrade
 - appliance 110
 - verify upgrade package 110

V

- VCCI Class A
 - certification 165
- verify

Index

- log messages 122
- system log 131
- system logs 131
- via serial console
 - serial console 45
- view
 - LED 142
 - license 111
 - link report 95
 - log 121
 - OpenKey client 95
 - OpenKey license 111
 - Parent Keys via LKM 99
 - system details 134
 - view 99

W

- Windows
 - set event log 120
- Windows event logging 119, 120
- Windows Event Viewer 119, 120
- wizard
 - setup 50

Z

- zeroize
 - about 123
 - appliance 124
 - lost certificate 123