



■ ■ ■ ADMINISTRATION GUIDE

DataFort FC-Series
Version 2.2.1

security

DataFort Administration Guide for FC-Series DataFort Appliance

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

Part number: 210-03954 A0 (011008_FC2.2.1)

Model Numbers: FC520/FC525/FC1020

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

LASER WARNING



WARNING: Class 1 Laser product.

ATTENTION: Produit laser de classe 1

WARNUNG: Laserprodukt der Klasse 1

POWER SUPPLY NOTICE

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



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

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

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

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

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

WARNUNG: Dieses Produkt ist darauf angewiesen, daß im Gebäude ein Kurzschluß- bzw. Überstromschutz installiert ist. Stellen Sie sicher, daß eine Sicherung oder ein Unterbrecher von nicht mehr als 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: Apparatet må kun tilkoples jordet stikkontakt.

DUAL POWER SUPPLY NOTICE



WARNING: This unit has more than one power supply connection; all connections must be removed to remove all power from the unit.

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

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

LITHIUM BATTERY NOTICE FOR SERVICE PERSONNEL

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



CAUTION: Danger of explosion if battery is replaced with incorrect type. Replace only with the same type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

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

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

RACK MOUNTING

Appropriate hardware is provided with the appliance in order 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 appliance, and attach the rail mounts to the rack. Then slide the appliance into the rack on the rails and secure the appliance in place using the provided screws.



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

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

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

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

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

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

CONTENTS

Chapter 1 Introduction	15
About the Decru DataFort Security Appliance	16
Encryption	16
Common Criteria Compliance	16
Hardened Architecture	17
CryptoShred Feature	17
Compartmentalization of Functions	17
Key Management	17
Lifetime Key Management Solutions	18
Configuration Database	18
Authentication Layers	18
DataFort Users	19
Security Domain	19
Installation Requirements	20
Conventions Used in this Manual	21
Chapter 2 Planning the Network Configuration	22
Decru DataFort Capacity	23
DataFort Capacity Limits and Mapping Methods	24
Installation Considerations	25
Planning the Security Domain	25
Updating Devices	25
DataFort Appliance Clusters	26
Failover Support in a Cluster	26
IPsec in a Cluster	26
Switch Connections in a Cluster	26
Secure Network Practices	27
Maintaining Configuration Database Backups	27
Sending Recovery Cards to Escrow	27
Planning Remote Security Logging	27
Removing the System Card	28
Preparing for Manual Security Responses	28
Recommended Network Configurations	29
Fabric Attached Cluster Configuration	30
In-line Cluster Configuration	30
Tape Backup	31
Physical Separation of Network Zones	32
Planning Data Backup and Restoration	33
Backup Methods	33
Chapter 3 Preparing to Install DataFort	35
Collecting Network Information	36
Preparing the Management Station	37

Management Station Security	37
Running the Installer	38
Setting Up Lifetime Key Management	39
Chapter 4 DataFort Appliance Installation	40
Notices and Warnings	41
Laser Warning	41
Power Supply Notice	41
Power Cable Notice	41
Dual Power Supply Notice	41
Lithium Battery Notice for Service Personnel	41
Perchlorate Present	41
Rack Mounting the Appliance	42
Unpacking the Appliance	42
Selecting a Location	42
Rack Mounting	42
Connecting the Appliance	44
Inserting the System Card	44
Connecting the Rear Panel Ports	44
Connecting Power	47
Assigning the Appliance IP Address	48
Setting the IP Address Using the LCD	48
Setting the IP Address Using the Serial Console	49
Powering Up and Shutting Down	50
Chapter 5 Initializing Appliances	51
About the Setup Wizard	52
Setup Wizard Functions	52
Incomplete Setup Wizard	52
About Smart Cards and Readers	52
About Remote Authorization	53
Initializing a Standalone Appliance or Cluster	54
Connect to Head of Cluster	55
Sign License Agreement	55
Recover From Database	55
Create Administrator	55
Configure Cluster and Recovery Schema	56
Network Settings	57
Add Licenses	58
Network and Certificates	58
Insert Recovery Card	58
Apply Settings	60
Apply Settings	61
Adding a Member to a Cluster	62
Connect to Head of Cluster	63

Cluster and Recovery Schema	63
Network Settings	63
Add Licenses	63
Network and Certificates	63
Insert Recovery Card	64
Apply Settings	65
Apply Settings	66
Chapter 6 Appliance Management Interfaces	67
Management Interfaces Overview	68
SecureView	68
Security Policies	69
Online Help	69
Accessing the Decru Management Console	70
Using the DMC	70
Connecting via Standard DMC	70
Connecting via Secure DMC	71
Connecting via DMC using Dual Authorization	71
Connecting to the Command Line Interface	72
Using the CLI	72
Connecting via Standard CLI	72
Connecting via Secure CLI	72
Connecting via CLI using Dual Authorization	73
Connecting to CLI via DMC	74
Serial Console	75
Logging in to the Serial Console Port	75
Configuring IP Settings	75
Clearing IP Settings	75
Zeroizing the Appliance	75
Appliance Front Panel LCD	76
Touch Panel Onscreen Buttons	76
SNMP Settings	77
Chapter 7 DataFort Admin Roles and Account Administration	78
Administrator Roles	79
Account Administration	81
Adding an Administrator	81
Requiring Authorization for Login	82
Changing the Administrator Password	84
Removing an Administrator	84
Adding or Changing a Card Association	84
Chapter 8 Before Storage Administration	85
Verifying DataFort Configuration	86
Verifying System Version	86
Checking Cluster State	86
Creating Additional Administrators	86

Configuring Remote Logging	86
Determining the Defense Setting	86
Configuring Disk or Tape Mode	87
Chapter 9 Storage Administration	88
Creating Cryptainers	89
Open the Decru Management Console	89
Cryptainer Creation Using Collections	89
Cryptainer Creation Without Collections	93
Hosts and Devices Tab	95
DataFort DMC Icons	96
Managing Hosts	97
Host Pane Menu	97
Host Collection Menu	98
Host Menu	98
Edit Host	99
Managing Cryptainers	100
Cryptainer Pane Menu	100
Cryptainer Collection Menu	101
Cryptainer Menu	101
Managing Storage	102
Storage Pane Menu	102
Storage Collection Menu	103
Storage Device Menu	103
Edit Device	104
LUN Menu	104
Map Disk to Cryptainer	105
Replace Disk	105
Edit Disk	105
Managing Tape Pools	106
Pools Pane Menu	106
Add Pool Screen	107
Pool Collection Menu	107
Tape Pool Menu	108
Tape Menu	108
Edit Pool Screen	109
Managing Tape Settings	110
Pool Defaults	110
Tape Settings	111
Key Settings	112
Mixed-Tape Mode Rules	112
Managing SAN Storage Settings	113
Virtualization Settings	115
Restoring a Cryptainer	116
Restoring a Cryptainer via DMC	116
Chapter 10 Key Administration	117
Managing Trustees	118

Trustee Scenarios	118
Setting Up Trustees	118
Creating Trustees on a Local Network	119
Creating Trustees on a Remote Network	122
Importing and Exporting Keys	127
Chapter 11 Backup Administration	128
Saving Configurations to Lifetime Key Management	129
Best Practices for Secure Backups	129
Configuring Backups to LKM Appliance	129
Configuring Backups to LKM Software	129
Backing Up the Configuration to LKM	130
Key Purging	130
Backing Up Configurations to a Remote Location	132
Chapter 12 Managing Appliance Security	133
Managing Appliance Defense Responses	134
Defense Triggers and Responses	134
DataFort Defense Setting	135
Changing the Defense Setting	135
Clearing a Defense Alert	135
CryptoShred Button States	136
System Card CryptoShred	137
Configuring Management Security Settings	138
Managing Recovery Officers and Recovery Cards	139
Replacing a Recovery Officer	139
Changing a Recovery Card Password	140
Resetting Smart Cards	141
Setting Date and Time	142
Configuring and Viewing Logs	143
Appliance Log Storage Guidelines	143
Decru Signed Syslog (DSS)	143
Configuring Log Storage	144
Windows Event Logging	145
Setting Up Syslog	145
Viewing the Log	146
Verifying Signed Log Messages	147
Zeroizing Appliances	148
Before Zeroizing	148
Zeroizing Using the DMC	149
Zeroizing Using the CLI	149
Zeroizing Using the Serial Console	150
Emergency Serial Console Port Access	150
Setting Security Certificates	151
Setting a Self-Signed Security Certificate	151
Setting a Certificate Authority Signed Certificate	151

Chapter 13 Cluster Administration	153
Cluster Management	154
Maintaining the Cluster Quorum	154
Cluster-Wide Management via DMC	155
Checking the Status of the Cluster	155
Resolving a Cluster Conflict	156
Adding and Removing Cluster Members	157
Adding a Cluster Member	157
Removing a Cluster Member	157
Replacing a DataFort in a Cluster	158
Recovering a Cluster	159
Changing Network Properties of a Cluster Member	160
Changing the IPsec Secret of a Cluster	160
Changing the IP Address of a Clustered DataFort Appliance	161
Changing the Hostname of a Clustered DataFort Appliance	161
Changing the Hostname on an FC1020	162
Chapter 14 Machine Administration	163
Changing Network Settings	164
Upgrading Appliances	165
Verifying an Upgrade Package	165
Managing Licenses	166
Viewing Licenses	166
Adding Licenses	166
SNMP Settings	167
About SNMP Options	167
Setting SNMP Options	168
Additional Appliance Management Tasks	169
Adding an Appliance	169
Logging into Appliances	169
Creating Custom Appliance Groups	169
Removing an Appliance from a Custom Group	170
Removing a Custom Group	170
Chapter 15 Decru Management Console Functions	171
State Displays	172
About the Appliances Tab	173
Using Tab Table Columns	173
Appliance Menu	174
Edit Menu	175
View Menu	175
Configuration Menu	176
Keys Menu	177
Topology Menu	178
Utilities Menu	178
Security Menu	179
Trustee Menu	180

Diagnostics	181
Help Menu	181
Chapter 16 CLI Administration	182
Using the CLI	183
Connecting to the CLI	183
CLI Help	183
Administration Commands	184
Administrator Roles	184
Creating a New Administrator	184
Cluster Management	185
System Properties and Log Management	186
Verifying System Logs	187
Stack Trace Settings	188
Network Management	188
Backup Management	188
Storage Management Commands	189
Disk Commands	189
Host Commands	191
Cryptainer Commands	192
Fibre Channel Kernel Commands	194
Manual Key Generation	195
Creating Cryptainer Keys	195
Viewing Cryptainer Keys	195
Changing Appliance Network Port Settings	196
	196
Chapter 17 Troubleshooting	197
Restoring an Appliance	198
Front Panel LEDs	199
Power Supply LEDs	200
Network Connections and Management Interfaces	201
Clusters	203
Smart Cards	204
Hardware	205
Storage	206
Decru DataFort Operation with NetApp Filer	208
Cisco MDS 92XX series FC switch - NetApp Filer appears offline	208
Decru DataFort Operation with Fujitsu Siemens CentricStor	209
Decru DataFort Operation with EMC	210
Symmetrix	210
CLARiiON	210
Decru DataFort Operation with Solaris	211
Migrating MetaTool Volumes to a DataFort	211
Veritas Volume Manager	214
Decru DataFort Operation with Legacy Encrypted Tapes	215

Contents

Decru DataFort Operation with Tivoli and STK Drives	216
Decru DataFort Operation with LT02 Serialized Commands	217
Decru DataFort AIX Atape Failover Support	218
Atape Operation Limitations	218
Decru DataFort SCSI Reservation Handling Fixes	219
Appendix I Command Line Interface Quick Reference	220
Using the CLI	221
CLI Syntax	221
CLI Help	221
CLI Command Overview	222
Top Level Commands	222
Device Commands	222
Disk Commands	223
FC Site Commands	223
FCC Cryptainer Commands	223
Host Commands	224
KFC Commands	224
Pool Commands	224
Tape Commands	225
CLI Formatting Commands	225
Help Command	225
Quit Command	225
Active-Role Commands	225
Authorize Command	225
Password Command	225
Role Commands	226
User Commands	226
Whoami Command	226
Trustee Commands	226
Network Commands	226
Key Management Commands	226
LKM Management Commands	227
Cluster Commands	227
Database Commands	227
System Commands	227
Appendix II Logging Functions	229
Appliance Log Event and Priority Types	230
Log message parameters	230
Log Storage Locations	232
Log Presentation	233
Temporary Logs	233
Database Logs	233
Remote Logs	234
Log Purging	236

Contents

Appendix III Port IDs	237
Appendix IV Specifications	238
Supported Systems	239
DataFort Appliance Specifications	240
Appendix V Partial List of ISO Country Codes	242
Appendix VI Regulatory and Certifications	243
FCC B Declaration of Conformity	244
European Union	245
Canadian ICES-003	246
VCCI Class A Statement	247
CE Statement	248
Korea MIC	249
Taiwan BSMI	250
Appendix VII DataFort Serial Adapter	251
Appendix VIII Glossary	252
Index	256



■ ■ ■ ■ 1 INTRODUCTION

The Decru DataFort[®] security appliance encrypts network data in transit to storage, providing authentication, fine grain access controls and secure logging in the process. DataFort supports the creation of secured storage targets called Cryptainer vaults[®] in which encrypted data is stored. Data remains encrypted while stored in a Cryptainer vault, protected from unauthorized access. When requested by an authorized host, the DataFort appliance decrypts and then forwards the data to the appropriate destination.

The Decru DataFort appliance can provide managed, encrypted network storage for NAS, SAN, SCSI and IP networks. This guide describes the features and functions of the FC-Series DataFort appliances.

Decru DataFort models correspond to the main types of storage architecture:

- **Decru DataFort[®] E-Series** appliances secure file-based data in Network Attached Storage (NAS) systems, and can also be used on the file server side of a SAN (Storage Area Network) when file and user level control is desired for SAN encryption. These appliances support Network File System (NFS) and Common Internet File System (CIFS) protocols. They can also secure block- or sector-based data over IP networks that support the iSCSI protocol.
- **Decru DataFort[®] FC-Series** appliances secure block- or sector-based data in Fibre Channel networks, such as SCSI over Fibre Channel (usually referred to as a SAN). These appliances also secure block-based data in Fibre Channel tape backup environments.
- **Decru DataFort[®] S-Series** appliances secure data stored on SCSI-based tape systems.

This chapter includes the following topics:

- [About the Decru DataFort Security Appliance](#)
- [Installation Requirements](#)
- [Conventions Used in this Manual](#)

ABOUT THE DECRU DATAFORT SECURITY APPLIANCE

When installed between hosts and storage, DataFort encrypts data en route to storage and decrypts data as it is read from storage by hosts without impact on the existing network structure. DataFort also supports legacy cleartext tapes, ensuring a seamless transition to a secure environment. Standard installation places DataFort appliances in a clustered configuration on a single network, with all encryption key and access control information shared securely between the cluster members.

The DataFort administrator has direct access to essential network setup and maintenance tasks via DataFort management interfaces. All key security administration tasks, including those necessary to manage cluster members, can be accessed from a single workstation.

DataFort uses a layered approach to provide optimal security, combining hardware-based encryption, compartmentalization, secure hardware, key management, cryptographically signed logging and multi-layered authentication. The Decru security system includes the following components:

- [Encryption](#)
- [Common Criteria Compliance](#)
- [Hardened Architecture](#)
- [CryptoShred Feature](#)
- [Compartmentalization of Functions](#)
- [Key Management](#)
- [Lifetime Key Management Solutions](#)
- [Configuration Database](#)
- [Authentication Layers](#)
- [DataFort Users](#)
- [Security Domain](#)

ENCRYPTION

Using the AES (Advanced Encryption Standard) algorithm, the DataFort encryption system transforms cleartext (unencrypted data) generated by network hosts into ciphertext (encrypted data) intended for storage. DataFort uses a high-quality, hardware-based random number generator to produce encryption keys. A multi-key encryption process ensures no key is ever transported in cleartext form, offering the highest level of security against attacks.

In the SAN environment, DataFort does not change the size of data when encrypting data to disk. DataFort employs hardware-based compression before writing data to tape for encryption, which reduces the size of data by a ratio of 2:1. This is done in order to ensure the backup size is the same.

COMMON CRITERIA COMPLIANCE

DataFort design conforms to Common Criteria EAL 4+. Common Criteria is an international security standard that is the gold standard for high assurance, well-defined security features, and rigorous third party testing and validation. Common Criteria requires each vendor to comply with stringent best practices in developer security, configuration management and testing. Instructions for operating DataFort in a manner compliant with Common Criteria standards are available from Decru.

HARDENED ARCHITECTURE

DataFort hardware and software were designed from the ground up for optimal security. At the heart of the system is Decru's Storage Encryption Processor (SEP), a hardware engine which enables Gigabit-speed, full-duplex encryption. The SEP is fully protected within the DataFort chassis, which is equipped with tamper-resistant features to protect all sensitive key material stored inside the appliance.

CRYPTOSHRED FEATURE

The DataFort CryptoShred™ feature offers immediate secure protection for data in storage by automatically deleting or barring access to encryption keys that are needed to decrypt data. CryptoShred describes the key deletion process, which can be triggered by an event specified in the defense setting of DataFort, or by engaging the physical CryptoShred button on a DataFort appliance that is equipped with the button.

DataFort can be configured to respond to potential threats to the physical security of stored data, according to the needs of the organization. CryptoShred can render primary and secondary copies of data permanently unusable by securely deleting encryption keys. For data in harm's way, CryptoShred can make the data temporarily inaccessible while a security threat is being assessed.

COMPARTMENTALIZATION OF FUNCTIONS

DataFort simplifies the implementation of secure storage with the concept of a Cryptainer vault. In the SAN environment, a Cryptainer is identified and managed on the Fibre Channel network by its WWN (World Wide Name) and Logical Unit Number (LUN).

DataFort separates the ability to manage stored data from the ability to read data from a storage device. This means the administrator does not necessarily have access to the data. Data is secure no matter where it is stored, or who manages the storage.

KEY MANAGEMENT

DataFort uses an advanced, comprehensive key management system to ensure a high level of security. Data stored using DataFort can be backed up, moved and managed without decryption, or rekeyed by the administrator at any time for additional security.

Each 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. The Parent Key is encrypted by a Master Key, unique to each DataFort. This Master Key, generated at the time DataFort is initialized, is used to decrypt and encrypt key material for safe storage and backup.

Since keys are always encrypted, they can be backed up and restored securely, as well as shared over a secure channel between DataFort appliances in clustered environments. All keys are stored in DataFort hardware, and do not ever leave DataFort in unencrypted form.

LIFETIME KEY MANAGEMENT SOLUTIONS

Decru's Lifetime Key Management (LKM) solutions—the LKM appliance and LKM server software—store encryption keys used by multiple DataFort appliances. This consolidates all key information for the purpose of emergency data recovery. LKM retains all encryption keys, even if they are purged from DataFort or the source DataFort is decommissioned. This ensures encryption key availability for the life of secured data.

CONFIGURATION DATABASE

The configuration database stored inside DataFort hardware contains network, security and access control information, as well as encrypted key material. Cryptainer keys can be retained even when a Cryptainer is deactivated, meaning data from an old Cryptainer is still recoverable using a working DataFort. A configuration database can be saved and used to restore or clone an existing DataFort.

AUTHENTICATION LAYERS

DataFort incorporates smart cards into network management, backup and recovery procedures. This provides a second layer of authentication beyond username and password credentials. Decru supplies a smart card reader and software which convert a Windows PC into a Management Station. The reader provides a dock for the smart cards. Three types of smart cards are shipped with every DataFort: the System Card, Admin Card and Recovery Cards.

Note: Decru smart cards are programmed with very specific functions, they are not the same as smart cards from other vendors. DataFort only supports Decru smart cards.

System Card

Each DataFort has a unique System Card to handle key data. The System Card is required for DataFort to boot and provides physical security for the appliance. If the System Card is removed, encryption keys will be protected even if the DataFort appliance itself is compromised (stolen or tampered with).

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

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

Admin Cards

An Admin Card adds an additional optional authentication layer to the communication between administrator and DataFort. Admin Cards can be used for one or more appliances (including a cluster or separate appliances). 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

Recovery Cards are used in sets to restore encrypted data or disabled DataFort appliances, and to replace other smart cards. Each Recovery Card is associated with a Recovery Officer, who is a highly trusted individual in the organization. Officers must present cards and passwords before a recovery procedure that could threaten data security can be performed.

DATAFORT USERS

DataFort administrators are responsible for configuration and maintenance of DataFort on the network. Other users include the Recovery Officers who are issued Recovery Cards.

DataFort Administrators

DataFort can be managed by several types of administrators. A Full Administrator can complete all operations necessary to set up, manage and maintain the DataFort appliance. Other administrators are able to execute a more limited set of functions, targeting specific administration tasks. Every administrator is authenticated with a login name and password. Administrators can be authenticated additionally with physical possession of an Admin Card. Depending on the organization, it may be desirable to create administrators that require authorization by another administrator in order to manage DataFort.

Recovery Officers

Recovery Officers are trusted individuals responsible for retaining initialized Recovery Cards after DataFort setup is complete. Each Recovery Officer is authenticated by a Recovery Card and its associated password. A set minimum of Recovery Officers must provide their associated cards in order to complete sensitive operations such as data recovery. This can be done locally or remotely via Remote Authorization.

Physical Security Officer

The Physical Security Officer is an individual responsible for maintaining and checking the physical security of the DataFort appliance prior to insertion of the System Card into the chassis.

User Management Interfaces

DataFort Administrators manage DataFort appliances from a Management Station using the Decru Management Console (DMC) and DataFort Command Line Interface (CLI). SecureView™ licenses enable administration of multiple appliances at the same time via the DMC. See [Chapter 6](#) for more information.

SECURITY DOMAIN

Security Domains are defined by sets of Recovery Cards. The deployment of DataFort appliances and the allocation of Recovery Cards can be used to create and enforce distinct zones of data access. Dividing an enterprise into multiple Security Domains can provide superior security through compartmentalization. Since a quorum of Recovery Cards presented by the responsible Recovery Officers is required in order to allow recovery of encrypted data, no single administrator or employee can bypass the system's security.

INSTALLATION REQUIREMENTS

In order to install and configure a DataFort appliance, items included in the shipping package as well as those included in a separately-ordered Admin Kit are required. In addition, some information should be gathered before beginning installation. Installation requirements include:

- Decru DataFort security appliance.
- DataFort user CD. The CD contains software necessary for DataFort operation, such as the smart card reader driver and Decru Management Console installer.
- Serial adapter. Custom RJ45 to DB9 adapter and Category 5 cable for a serial connection.
- AC power cord or cords appropriate for the appliance model and location.
- DataFort smart cards, including System, Admin and Recovery Cards.
- Smart card reader. Connects via USB to the Management Station.
- Decru product licenses. Each appliance requires appropriate licenses to use its features.
- Slide rail mounting kit including hardware and instructions (included in the DataFort package)
- Fibre channel cables. Have the requisite number of fibre channel cables, of appropriate lengths, available for use during the installation. The connections on the DataFort are LC connectors.
- Fibre channel switch ports. Determine which fibre channel switch ports DataFort will use to connect to the fabric. Each FC-Series DataFort HBA board has two fibre channel connections, so two switch ports per board are needed unless cabled directly in-line to a device.
- Network cables. Obtain the requisite number of network cables, of appropriate lengths. Each DataFort requires one standard RJ-45 Ethernet cable.
- Network switch ports. Determine which Ethernet switch ports will connect the DataFort appliances to the network.
- IP address, Subnet mask and Default Gateway. Each DataFort requires one dedicated IP address. Know what the appropriate subnet mask and appropriate default gateway will be for each dedicated IP address to be used during installation.
- DataFort name. Establish what resolvable system name will be assigned to each DataFort being installed. Enter the specific IP addresses in the network's DNS to enable hostname/IP resolution prior to installation to simplify 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 (optional). Have the appropriate NTP time server information for each dedicated IP address to be used during installation.
- Recovery schema. Determine the recovery schema 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.

CONVENTIONS USED IN THIS MANUAL

The following typographic conventions are used in this manual:

- Commands entered from the keyboard are shown in monospaced font in `blue`.
- Active links in the PDF version of this guide are indicated by underlined purple text.
- Buttons that can be clicked in the interface are identified by name, with no change in font.
- Navigation in DMC menus is described from the top level down, using bold type, for example:
Select **Configuration > View Administrators**.



■ ■ ■ ■ 2 PLANNING THE NETWORK CONFIGURATION

Basic installation places DataFort in the SAN environment so that data passes through DataFort as it is written to storage. In the process DataFort applies an encryption algorithm to the data. When data is read, the process occurs in reverse, with DataFort decrypting the data before it reaches the host.

A network configuration that separates storage from hosts, using separate FC switches or FC switches capable of zoning, is necessary. It is recommended that a cluster be set up across separate fabrics to avoid compromising the availability of the cluster due to common fabric events.

Complete installation in the enterprise adds a Management Station (for initial DataFort configuration and for ongoing administration tasks) and a Lifetime Key Management server or appliance to the Ethernet portion of the network. This chapter summarizes topics to consider when planning DataFort network installation.

- [Decru DataFort Capacity](#)
- [Installation Considerations](#)
- [DataFort Appliance Clusters](#)
- [Secure Network Practices](#)
- [Secure Network Practices](#)
- [Recommended Network Configurations](#)
- [Planning Data Backup and Restoration](#)

DECURU DATAFORT CAPACITY

Before installing DataFort, review capacity needs and divide network storage traffic across multiple DataFort appliances accordingly. Keep the following limitations in mind.

TABLE 1: DATAFORT CAPACITY

Device	Number	Explanation
Number of FC-Series DataFort appliances in a cluster	8	A DataFort cluster can support up to 8 DataFort appliances, no more than 4 of which can be 10-port DataFort appliances.
Virtual devices	7	Each DataFort supports 7 virtual devices per DataFort port. The number of virtual devices a cluster can support is equal to 7 times the number of DataFort appliance ports in the cluster. 2-port DataFort supports 7 virtual devices and 7 virtual hosts, 10-port DataFort supports 35 virtual devices and 35 virtual hosts.
Virtual hosts	7	Each DataFort supports 7 virtual hosts per DataFort port. The number of virtual hosts a cluster can support is equal to 7 times the number of DataFort appliance ports in the cluster. 2-port DataFort supports 7 virtual devices and 7 virtual hosts, 10-port DataFort supports 35 virtual devices and 35 virtual hosts.
Tape drives	7	A maximum of seven tape drives should be accessible through any given DataFort storage port.
Non-virtualized hosts	32	32 non-virtualized hosts are supported per DataFort. For 10-port appliances, the number of hosts is limited to 32 for each port on the DataFort. The total number of hosts for cluster can be 32 times the number of DataFort appliances in the cluster.
LUNs on a single device	256	Port Mapping (one Cryptainer per LUN): 256 Cryptainers supported per virtualized storage device. The number of LUNs allowed across all devices seen by a single DataFort is also 256. For example, DataFort can support one device with 256 LUNs or four devices with 64 LUNs each. See DataFort Capacity Limits and Mapping Methods .
Cryptainers on the primary port	255	LUN Mapping (LUN 0 is reserved): 255 Cryptainers supported per DataFort cluster, regardless of the number of DataFort appliances in the cluster. When LUN Mapping, it is not possible to map Cryptainers to LUN 0 (the Decru Secure LUN). Creating a Cryptainer for LUN 0 will create a VLUN 1 and LUN 1 will be presented to the host instead of LUN 0. See DataFort Capacity Limits and Mapping Methods .
Cryptainer or tape keys	8000	Once more than 8000 keys have been generated for a cluster by creating or rekeying Cryptainers or tapes, keys should be purged from the system upon backup.
Active I/Os on single DataFort	512	DataFort should be installed so that no more than 512 I/Os are active at any time through one DataFort appliance.

DATAFORT CAPACITY LIMITS AND MAPPING METHODS

DataFort supports up to 256 disks, where a disk is defined as a unique path to a LUN. If DataFort is zoned to a single array controller port, it can manage 256 LUNs. If DataFort is zoned to four different arrays, it can manage an average of 64 LUNs per array. If a single DataFort is zoned to two controllers on the same array it sees each LUN twice, so the limit is to present 128 LUNs to that DataFort.

When planning a cluster configuration, consider whether any given DataFort in the cluster is above the limit. If each member of the cluster is zoned to a different array, each can manage 256 LUNs. If all DataFort appliances in the cluster are zoned to different controller ports on the same array and all DataFort appliances see all of the LUNs, the limit is 256 LUNs total.

Best practice is generally to use port-mapped Cryptainer vaults in disk environments. This requires the use of a separate virtual port on the fabric for each device being virtualized by DataFort. This configuration does not work for switches that do not support FL logins, which means LUN-mapped Cryptainer vaults are required. Because LUN 0 is reserved for Decru internal use, this results in a slightly lower limit of 254 Cryptainer vaults in the cluster.

INSTALLATION CONSIDERATIONS

In order to encrypt data moving to storage, DataFort separates the network into cleartext and ciphertext portions. Hosts are connected to the cleartext portion, while storage devices are connected to the ciphertext portion. Separate HBA ports are available on DataFort to make these connections. Host HBA ports are dedicated to cleartext traffic, while Storage HBA ports are dedicated to ciphertext traffic. DataFort is compatible with a variety of network hardware, network operating systems and network management systems. Contact Decru for detailed compatibility information.

PLANNING THE SECURITY DOMAIN

Dividing an enterprise into separate Security Domains enhances security. The Security Domain is a portion of the enterprise network that is protected by one or more DataFort appliances sharing user access and administrative oversight. Each Security Domain is associated with a set of Recovery Officers and Recovery Cards. Because each Security Domain is defined by a set of Recovery Cards and associated Recovery Officers, no single administrator can decrypt data outside of DataFort. Note that several Security Domains might physically reside on the same storage array, and a single Security Domain might include multiple heterogeneous storage devices.

UPDATING DEVICES

Hosts in a Microsoft operating system environment that were previously able to access storage devices through the fabric may not be able to when those devices are moved behind DataFort. This is because the WWN names and possibly the SCSI paths of the devices are changed, causing them to appear to the operating system as new devices. To reestablish access to the storage devices, the host's administrator must open Device Manager and install the appropriate driver for the new device.

DATAFORT APPLIANCE CLUSTERS

Clustered DataFort appliances share information across a peer link. If one fails, the other can continue providing service. By clustering DataFort appliances, total system redundancy is increased, decreasing the probability of downtime. Clustered DataFort appliances share critical configuration information to provide failover and load balancing support for the network.

To ensure proper behavior between clustered DataFort appliances, the cluster connection should utilize a low-latency local network infrastructure. DataFort appliances should not be clustered over WAN or high-latency local connections.

FAILOVER SUPPORT IN A CLUSTER

DataFort appliances should be installed as members of a cluster, with separate FC switches or zoned switches. Redundant paths and a DataFort cluster provide the best failover support in a SAN. It is recommended that the cluster be set up across two separate fabrics to avoid compromising the availability of the cluster due to common fabric events.

IPSEC IN A CLUSTER

Configuration changes are synchronized across a cluster. To protect communication between DataFort cluster members, inter-DataFort traffic is routed through an IPsec tunnel. In order for the cluster members to negotiate the secure IPsec tunnel, a shared secret must be created. This shared secret is the IPsec password, which the administrator enters when setting up a DataFort cluster. The password should be chosen in advance of setting up the cluster.

SWITCH CONNECTIONS IN A CLUSTER

Connect each DataFort in a cluster to a separate FC switch if at all possible. Separating cluster members on different switches ensures that upgrades, replacements or outages of an individual switch do not interrupt data access through the cluster. The other members of the DataFort cluster take over service during any switch outages. If all cluster members are connected to a single director, attempt to connect each DataFort to a separate blade.

Zone switches before connecting DataFort appliances to the fabric. If the switch combines devices not in any zone into a common zone make sure to create zones before attaching DataFort appliances. The goal is to separate out the host and storage sides of DataFort. This is particularly important for 10-port DataFort appliances. Storage and host ports should not be zoned together and multiple ports of the same type should not be zoned together.

SECURE NETWORK PRACTICES

Determine the desired level of security for the environment before installing DataFort. For a high-security environment, plan an installation that includes not only DataFort appliances and a Management Station, but also a Lifetime Key Management server or appliance, 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.

- [Maintaining Configuration Database Backups](#)
- [Sending Recovery Cards to Escrow](#)
- [Planning Remote Security Logging](#)
- [Removing the System Card](#)
- [Preparing for Manual Security Responses](#)

MAINTAINING CONFIGURATION DATABASE BACKUPS

For maximum security and recoverability, keep database backups up to date, and use Decru's Lifetime Key Management software or appliance to store encryption keys. Configure DataFort to send the latest configuration database backup to Decru's Lifetime Key Management (LKM) software automatically, or use an LKM appliance.

SENDING RECOVERY CARDS TO ESCROW

Each DataFort or DataFort cluster is configured with a data recovery schema setting 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. It is possible to use a different set of Recovery Cards for each DataFort cluster, or a single set of Recovery Cards for all DataFort appliances in the company.

An organization may choose to use a key escrow service to store Recovery Cards, configuration database backups and Key Archives (created using Decru's Lifetime Key Management solutions). Procedures for key escrow should be established as part of the organization's security policy. The recommended procedure is to send the escrow service both the encrypted backup of a configuration database for each DataFort or cluster and a quorum of Recovery Cards for each Security Domain.

When using an escrow service, configure DataFort 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 DataFort 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.

PLANNING REMOTE SECURITY LOGGING

DataFort provides detailed local and remote logging to help track events that occur in the Security Domain. Use the logging configuration features of DataFort to redirect all logs to a remote syslog server, logging critical operations locally as well as remotely.

REMOVING THE SYSTEM CARD

If the physical security of the DataFort appliance is a concern, it may be advisable to remove the System Card from the DataFort chassis after startup and store it in a safe location. This prevents DataFort 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 and reinserted in the DataFort prior to resumption of service. Consider this security/reliability trade-off when determining whether to leave the System Card inserted in a running DataFort.

PREPARING FOR MANUAL SECURITY RESPONSES

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

The defense setting determines the DataFort appliance's automatic response to physical intrusion. See [Defense Triggers and Responses](#) on page 134 for details. In an emergency, there are also manual steps that can be taken to suspend DataFort encryption and decryption operations.

TABLE 2: MANUAL SECURITY RESPONSES

Security Action	Result	Action to Return to Operation
Press the CryptoShred button (available on some DataFort models).	Basic Setting: Suspends encryption and decryption immediately.	The CryptoShred button must be released before the administrator can complete the reset. See CryptoShred Button States .
		A Full Administrator can reset DataFort. See Clearing a Defense Alert .
Press the CryptoShred button (available on some DataFort models).	Medium or High Setting: Suspends encryption and decryption immediately and deletes encryption keys.	The CryptoShred button must be released before the administrator can complete the reset. See CryptoShred Button States .
		With Medium and High Level defense, DataFort must be zeroized and then restored using the Setup Wizard, Recovery Officers, and a saved configuration database. See Restoring an Appliance .
Removing the System Card followed by shutdown and/or reboot (Removing the System Card alone does not stop DataFort operation).	Stops encryption and decryption immediately.	If the System Card is available, re-insert it and reboot the DataFort appliance.
		If the System Card was destroyed or lost, DataFort must be zeroized and then restored using the Setup Wizard, Recovery Officers, and a saved configuration database. See Restoring an Appliance .

RECOMMENDED NETWORK CONFIGURATIONS

The following section provides examples of ways to introduce DataFort into the existing storage network environment. No re-configuration is necessary for the devices on the SAN; DataFort can be added to the existing infrastructure of the network without impact on network functions. Fibre Channel restrictions apply for maximum number of WWNs, LUNs, loop initiators etc. on a given network. For more information about network configurations, contact Decru.

Note that DataFort supports legacy cleartext tapes, ensuring a seamless transition to a secure environment. Any tape read through DataFort is evaluated as encrypted or cleartext based on presence or absence of DataFort metadata. If no metadata is present, the read is passed through without encryption, transparently.

Connecting each DataFort to a switch provides a flexible, high-availability path for data. Data can be routed through DataFort for encryption, or passed through as cleartext data. In the following diagrams failover paths between clustered DataFort appliances are indicated, as well as ciphertext and cleartext data flow.

Once the physical connections are made, these configurations are supported by creating storage- and host-side zones on each switch and creating Cryptainers on the storage devices using the DataFort DMC. Host HBAs are granted access to the Cryptainers via DataFort.

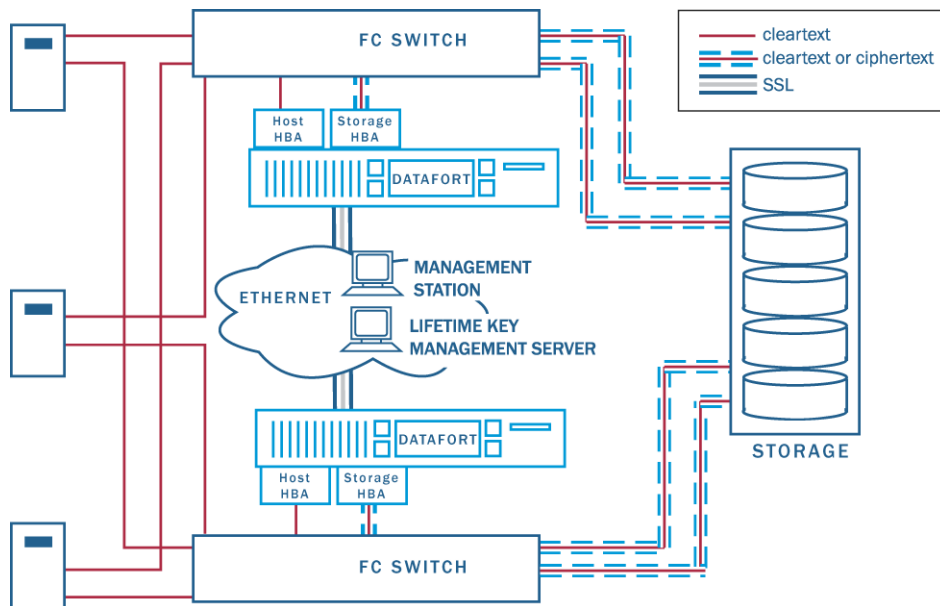


Figure 2-1: A DataFort cluster with two FC switches showing redundant paths

FABRIC ATTACHED CLUSTER CONFIGURATION

One possible implementation of a secure, high-availability installation provides a server with four data paths—two through each DataFort in the cluster. Each DataFort presents the server HBA with two virtual devices that are mapped by DataFort.

In the following example of such a configuration, HBAs 0 and 1 would be grouped together as the cleartext zone, while HBAs 2, 3 and 4 would form the ciphertext zone. Note that DataFort supports port or WWN zoning.

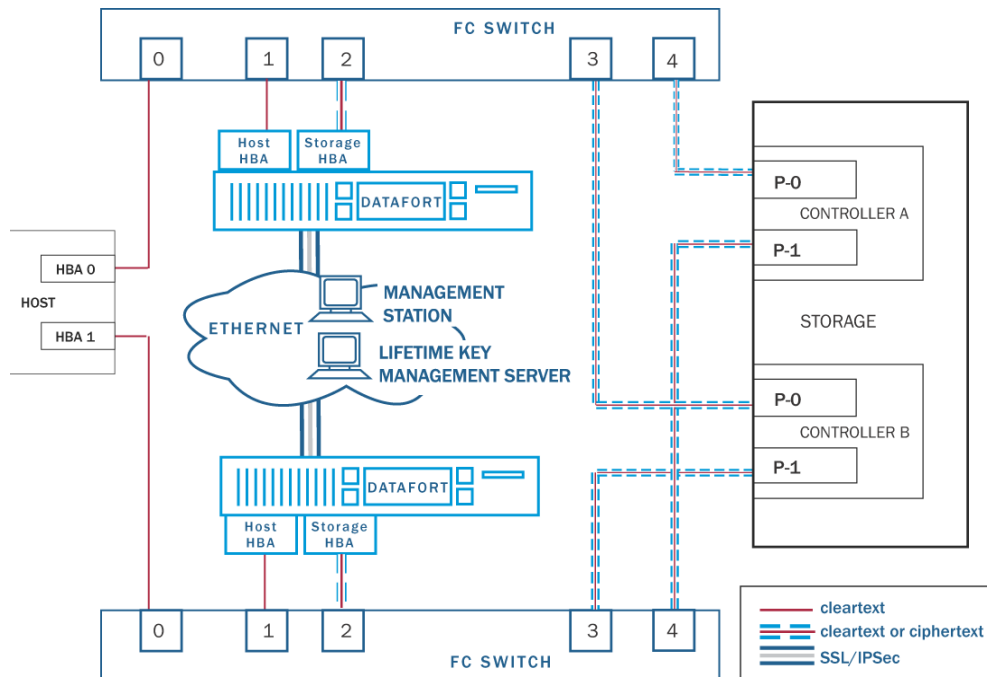


Figure 2-2: Fabric attached configuration

IN-LINE CLUSTER CONFIGURATION

An in-line configuration provides the server with two data paths—one through each DataFort. This is a hardened security option, as the data sent to storage must pass through DataFort, and cannot be accidentally (or maliciously) rezoned to pass through a port on a switch designated for cleartext data.

Note that an enterprise might include both in-line and fabric attached configurations, such as one where the hosts are connected to the fabric, but a specified storage device is accessible only through DataFort.

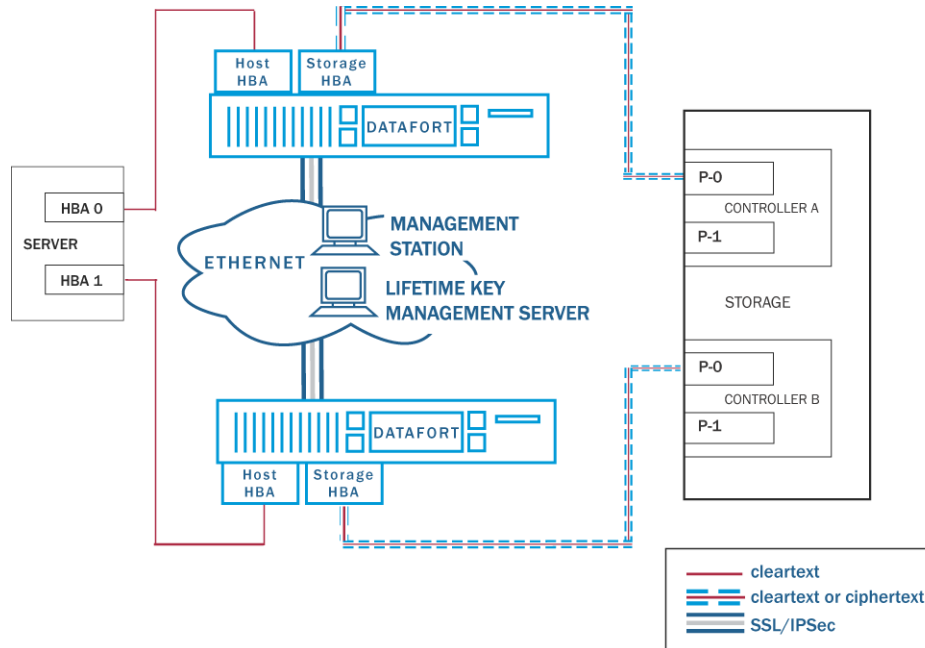


Figure 2-3: In-line configuration

TAPE BACKUP

DataFort fully supports data backup to tape in cleartext or encrypted form. Any tape read through DataFort is evaluated as encrypted or cleartext based on presence or absence of DataFort metadata. If no metadata is present, the read is passed through without encryption. If metadata is present the data is then encrypted.

In the following example, HBAs 0-3 would be grouped together as the cleartext zone, while HBAs 4 and 5 would be designated as the ciphertext zone. Note that some vendors recommend creating a zone per initiator, which would require zoning each initiator with the host-side HBA of a separate DataFort.

Mixed-Mode Tapes

As a general rule, DataFort does not support mixed-mode tapes, therefore tapes written through DataFort are either all cleartext or all encrypted. See [Mixed-Tape Mode Rules](#) on page 112 for more information about DataFort behavior in a mixed-tape mode environment.

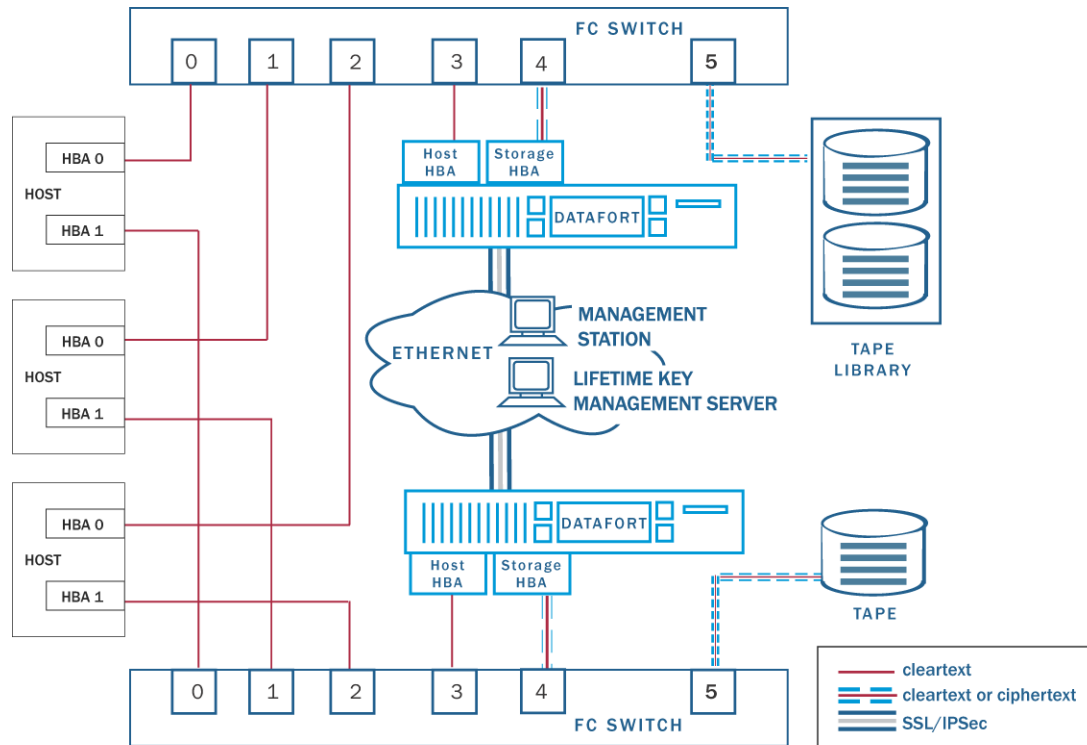


Figure 2-4: A DataFort cluster with two FC switches sending encrypted and cleartext data to tape

PHYSICAL SEPARATION OF NETWORK ZONES

Multiple switches can be used to separate the host and storage zones. This type of configuration has an application in environments which include the services of a security storage service provider. In a configuration with offsite storage, data is encrypted as it passes out of the enterprise to the remote storage location. This allows a configuration where only encrypted data is stored at the offsite location, if that is called for in the security needs of the enterprise.

In this configuration, DataFort serves as a storage firewall, protecting data at rest in the offsite locale. The physical separation also eliminates the risk of data being leaked due to a zoning error.

PLANNING DATA BACKUP AND RESTORATION

DataFort delivers secure backup and restore capabilities in the SAN environment. The backup and restore server's Fibre Channel connections should be placed in the DataFort's host zone while the tape library's Fibre Channel connections should be placed in the DataFort's storage zone. This channels the data path of every backup and restore through the DataFort. DataFort passes cleartext data through as well as encrypting data designated for encryption in a Cryptainer.

BACKUP METHODS

The FC-Series DataFort supports four main SAN backup topologies: LAN-based, LAN-free, Client-free, and Server-free.

TABLE 3: BACKUP METHODS

Backup Method	DataFort Solution
LAN-based — The data flows from the application server to the backup server by LAN. The backup server writes data to tape.	To encrypt backups, configure the network so that data flows from the backup server through DataFort to tape.
LAN-free by Client — The bulk of the data flow occurs between the application server and the tape library.	DataFort encrypts data as it is sent to tape.
Client-free — The bulk of the data flow is between the back-end disk array through the backup server and to the tape library. In this case the data server is freed from performing the backup.	• If the primary data is not encrypted or there is no reason to prevent the backup server from reading cleartext, place DataFort between the backup server and tape. Data is encrypted as it is sent to tape for storage. • If all data should be encrypted and the backup server should not read cleartext, place the backup server, storage, and tape libraries behind DataFort. In this design the data to be backed up is already encrypted by DataFort, allowing for completely secure backup and restore operations. DataFort encrypts data in blocks rather than files, so all blocks seen by the backup server are encrypted, and backup/restore operations must be at the block level. Methods that can be used for Client-free backup and restores must be either full backup/restores at a device or logical volume level, or incremental backup/restores at a block level.
Server-free — The bulk of the data flow goes directly from the disk array to the tape library. This topology is supported through the use of the SCSI extended copy command, or in some cases vendor proprietary features.	Server-free backup/restore technology is currently immature. This topology is supported through the use of the SCSI extended copy (xcopy) command, or similar vendor proprietary features. Currently DataFort does not support the xcopy SCSI command for Server-free environments. However, a backup server operating <i>behind</i> the DataFort can use xcopy to copy encrypted data from disk to tape. In this case too, the backup/restore operations are done at the block level.

SAN Mirroring

DataFort can operate in mirrored environments (disk-licensed DataFort). As the data is already encrypted on the storage arrays, the mirrored data is also encrypted. This mirrored copy can be transferred to tape, or in the event of a system failure can be configured as the primary storage array. The administrator of the DataFort can associate the Cryptainer keys from the primary volume to the secondary array, allowing for transparent failover.

3 PREPARING TO INSTALL DATAFORT

Collect the necessary information about the environment before beginning DataFort installation. Make key decisions about administration, data recovery and defense settings in advance, according to the organization's security policy.

Key operations necessary in order to get DataFort up and running include:

- [Collecting Network Information](#)
- [Preparing the Management Station](#)
- [Setting Up Lifetime Key Management](#)

Once DataFort is installed, manage the appliance using the DataFort management interfaces. See the [Management Interfaces Overview](#) on page 68 for a list of interfaces and their uses.

Keep in mind the following simplified task overview when planning DataFort installation:

Set up Management Station	Set up Lifetime Key Management solution	Set up DataFort appliance standalone or cluster
		
1 Connect PC that will serve as station to network Install smart card reader and Decru Management Console (DMC) Access management interfaces from the management station	2 Connect LKM appliance OR LKM server to network LKM server—Install LKM software LKM appliance—Assemble Recovery Cards and Recovery Officers and run Setup Wizard from Decru Management Console Complete setup of LKM appliances from Decru Management Console	3 Connect DataFort appliances to network Determine security settings and administrative roles Assemble Recovery Cards and Recovery Officers Run Setup Wizard from Decru Management Console Complete setup of DataFort appliances from Decru Management Console

COLLECTING NETWORK INFORMATION

The DataFort administrator may need to gather information from other individuals before installing DataFort appliances. The following information is required:

DataFort Network Information

- Resolvable hostname for DataFort appliance. DataFort hostnames can be up to 64 alphanumeric characters, including dashes, underscores and periods.
- DNS suffix and DNS server IP address (if DNS is used).
- DataFort Management IP address, Subnet Mask and Gateway

Cluster Member Information

- IP addresses or resolvable domain names of all DataFort cluster members
- User-defined IPsec secret to support [IPsec in a Cluster](#)
- Quorum of Recovery Cards and associated user names and passwords
- Purchased Decru licenses for all cluster members
- Remote syslog server IP address
- Lifetime Key Management solution (EITHER of the following):
 - LKM Server Software with fixed IP address
 - LKM Appliance

PREPARING THE MANAGEMENT STATION

Appliance configuration requires running the Setup Wizard from the Decru Management Console, which is installed on the Management Station.

Smart cards from the provided set must be inserted into the smart card reader connected to the Management Station while running the wizard. After completing the wizard, use the Management Station to access management interfaces for the appliance.

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

TABLE 4: MANAGEMENT STATION REQUIREMENTS

Management Station Requirements	
Windows operating system (one from list)	Windows XP Service Pack 2
	Windows 2000 Pro/Server Service Pack 4
	Windows 2003 Service Pack 1
Hardware requirements	2Ghz
	1GB RAM
	4GB free hard drive space
	An available USB port for the smart card reader from Decru
	A CD drive for installing software

MANAGEMENT STATION SECURITY

The Management Station should be current on security patches and have unnecessary services disabled or removed. The Management Station should not be used to browse untrusted web sites or run unverified code. Limit logons to authorized administrators and disable remote management.

Since initial appliance setup from the Management Station is a security-sensitive operation, it is recommended that the appliance and the Management Station be on the same subnet. After initial setup is completed, the appliance can be managed remotely from any Management Station.

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.

1. Insert the CD provided by Decru into the Management Station.
The CD runs automatically if autorun is enabled.
2. Click the installer link.
3. When prompted by the File Download screen to open or save the file, click Open.
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 smart card reader. The model number can be found on the underside of the smart card reader (i.e. GemPCUSB-SL).
7. Select "Yes, I want to restart my computer now" and click Finish to complete installation.

SETTING UP LIFETIME KEY MANAGEMENT

Decru provides two solutions for key management: the Lifetime Key Management server software and the Lifetime Key Management appliance. LKM solutions manage encryption keys for multiple DataFort appliances, ensuring encryption key availability for the life of the secured data. Either LKM solution maintains updates of encryption key data automatically. Before configuring DataFort, set up the LKM management solution.

Note: DataFort supports either the LKM software or the LKM appliance but not both.

Lifetime Key Management Appliance

The LKM appliance offers a central location for the administrator to load, view, manage, share and save all keys generated by all DataFort appliances in an installation.

When using an LKM appliance, set up the appliance using the Decru Management Console as described in the [LKM Appliance Administration Guide](#).

Lifetime Key Management Server Software

LKM software is designed to run on a network server, providing a solution for managing and archiving key information for multiple DataFort appliances.

When using LKM software, install the software on a designated server as described in the [LKM Server Software Administration Guide](#). Ensure the server is up and its IP address is reachable from the Ethernet network before configuring DataFort appliances. Instructions for enabling automatic updates to LKM servers are provided in [Chapter 11](#).

■ ■ ■ ■ 4 DATAFORT APPLIANCE INSTALLATION

Install the DataFort appliance on the network by completing the following procedures. Ethernet connectivity is required between the Management Station and all appliances for management purposes. Installation steps include:

- [Rack Mounting the Appliance](#)
- [Connecting the Appliance](#)
- [Assigning the Appliance IP Address](#)
- [Powering Up and Shutting Down](#)

Consider the [Notices and Warnings](#) when installing the appliance.

NOTICES AND WARNINGS

LASER WARNING



WARNING: CLASS 1 LASER PRODUCT.

POWER SUPPLY NOTICE

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



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

POWER CABLE NOTICE



CAUTION: 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:



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.

PERCHLORATE PRESENT

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

RACK MOUNTING THE APPLIANCE

Perform the following steps to install the appliance in a rack:

- [Unpacking the Appliance](#)
- [Selecting a Location](#)
- [Rack Mounting](#)

UNPACKING THE APPLIANCE

When unpacking the appliance, the [Physical Security Officer](#) should inspect the cardboard shipping box for any signs of tampering. The box is sent sealed with tamper-evident tape. Once cut, the tape is difficult to reseal as the diagonal lines will not match up. When removed, this tape damages the cardboard packaging. If the appliance is equipped with a Medeco lock, a tamper evident label is also applied to the key hole of the lock. Inspect this label for signs of tampering. If an appliance has been tampered with, return it to Decru.

Note: These instructions apply only to shipping within the U.S. and to those countries in which government customs inspections do not unpack and inspect merchandise.

SELECTING A LOCATION

Decru 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:

- Make sure 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)
- Make sure there is sufficient air flow around the unit. Do not block air flow to fans.
- Make sure electrical circuits are not overloaded - consider the nameplate rating of all the connected equipment, and make sure you have overcurrent protection.
- Make sure the equipment is properly grounded.
- Make sure no objects are placed 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 and power supplies.
- Avoid dusty or damp locations.



CAUTION: 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 WEIGHT.

RACK MOUNTING

Appropriate hardware is provided with the appliance in order 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 appliance, and attach the rail mounts to the rack. Then slide the appliance into the rack on the rails and secure the appliance in place using the provided screws.



WARNING: TO PREVENT BODILY INJURY WHEN MOUNTING OR SERVICING THIS UNIT IN A RACK, YOU MUST TAKE 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.
- Install any provided rack stabilizers before mounting or servicing the unit in the rack.

CONNECTING THE APPLIANCE

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

- [Inserting the System Card](#)
- [Connecting the Rear Panel Ports](#)
- [Connecting Power](#)

INSERTING THE SYSTEM CARD

The System Card is required to authenticate cryptographic operations during appliance boot-up and certain procedures. Insert the System Card BEFORE powering on the appliance.

1. Insert the System Card into the smart card slot on the appliance front panel.

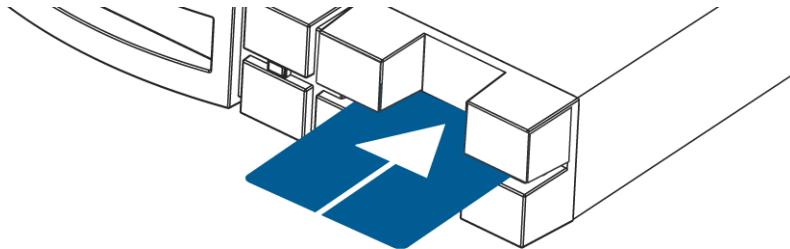


Figure 4-5: The front panel slot housing the System Card on a 1U DataFort

2. Slide the card into the slot firmly, with the gold contacts facing up and towards the back of the appliance. Push the card straight back into the slot. The card should fit snugly all the way into the slot, flush with the DataFort front bezel. The card must be fully inserted into the slot. Occasionally a smart card will need to be re-inserted in order to make proper contact.
3. Leave the System Card inserted until after the appliance boots up.

Note: For normal operation, leave the System Card in place after boot-up. Optionally, remove the System Card for higher security. See [Removing the System Card](#) on page 28 for details.

CONNECTING THE REAR PANEL PORTS

Connect appliance rear panel ports as described in the following sections:

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

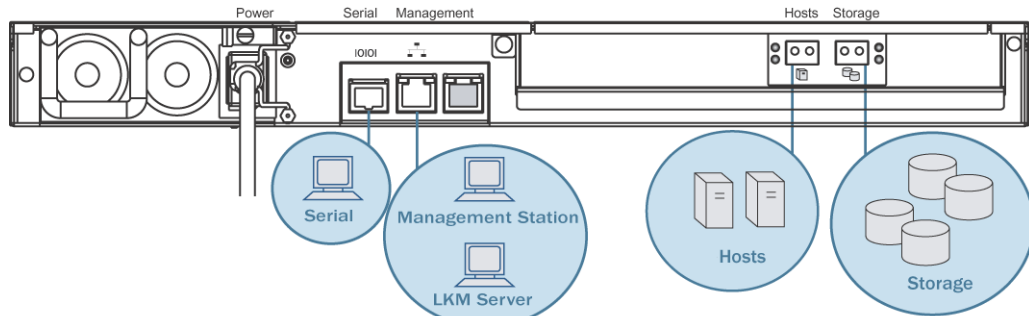


Figure 4-6: Rear panel connections 1U DataFort

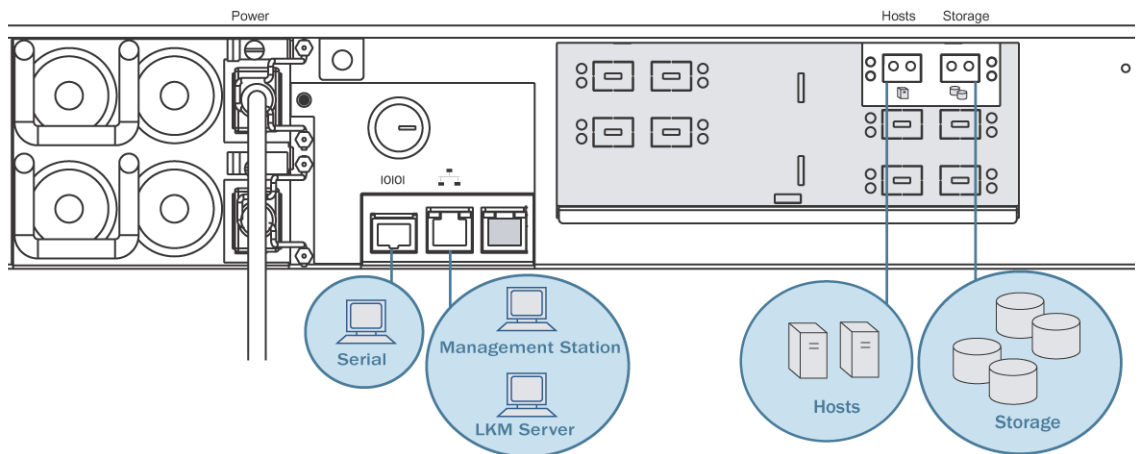


Figure 4-7: Rear panel connections 2U DataFort

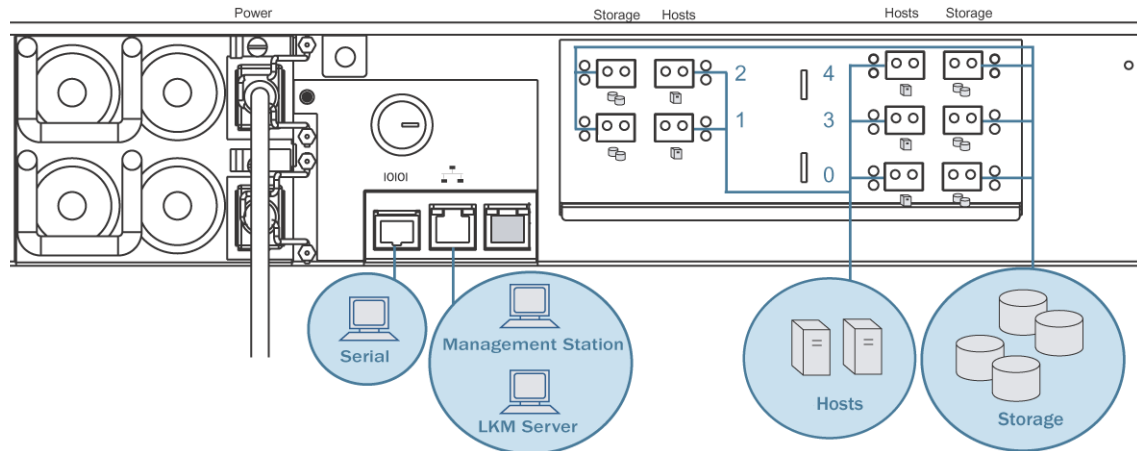


Figure 4-8: Rear panel connections 2U ten-port DataFort

Ethernet Connection

Use a Category 5 Ethernet cable to connect the appliance Management Port (the Ethernet port marked with the network icon) to the Ethernet network shared by the Management Station.

Fibre Channel Connection

DataFort features distinct interfaces for connecting to the network. Host-side ports provide interfaces for unencrypted data sent from hosts, and Storage-side ports provide interfaces for encrypted data being sent to storage devices. Icons on the DataFort indicate port types. Port label coloration indicates black for encrypted data flow, and silver for cleartext data.

1. Use a FC cable to connect each Host-side port to an FC fabric including network hosts.
2. Use a FC cable to connect each Storage-side port to an FC fabric including network storage devices.

Connecting DataFort to a Fibre Channel switch that has pre-configured zones is recommended. The following methods can be employed to avoid a loopback condition where DataFort Storage-side ports attempt to login to DataFort Host-side ports:

- Create separate host and storage zones
- Use separate switches to divide the host and storage zones
- If the switch supports it, use virtual SANs to separate host and storage devices

Each pair of ports (HBAs) on a 10-port DataFort functions as a standalone appliance, so in effect there are five DataFort appliances in the 10-port chassis. Keep this in mind when zoning and do not mix the zoning between ports on a 10-port DataFort appliance.

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 appliance's rear panel.

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

CONNECTING POWER

The appliance is equipped with one or two replaceable power supply/fan modules depending on the model.

1. Use the provided cords to connect each power port on the rear panel to a separate grounded power supply and secure the power plug using the wire retaining clamp.

Note: The 2U appliance operates with only one power cord, but the second cord provides failover protection if connected to a different circuit.

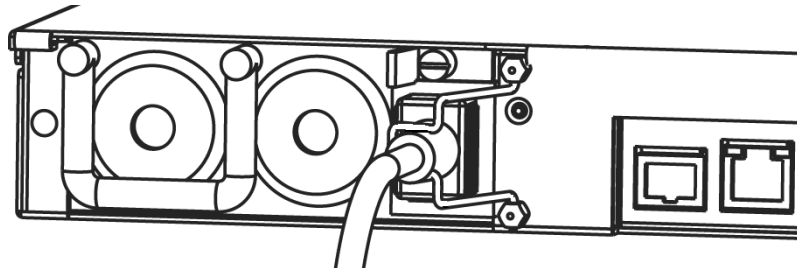


Figure 4-9: Power cord secured by the wire retaining clamp

2. When connected, the appliance powers on automatically. Wait several minutes while the appliance powers up.

When power up is complete, the LCD shows “DataFort” in place of a hostname, and an error message indicating that the Setup Wizard has not been completed.

3. Proceed to the step of [Assigning the Appliance IP Address](#).

Note: Leave the appliance powered on for normal operation. See [Powering Up and Shutting Down](#) on page 50 for instructions on powering off the appliance.

ASSIGNING THE APPLIANCE IP ADDRESS

Assigning an IP address for the appliance is required so that setup can be completed from the Management Station. Follow instructions for the appliance model:

2U appliance

Assign the appliance IP settings using the touch-sensitive buttons on the front panel LCD as described in [Setting the IP Address Using the LCD](#), or the serial console port, as described in [Setting the IP Address Using the Serial Console](#).

The LCD can only be used to configure IP settings for an uninitialized appliance.

1U appliance

Assign the appliance IP settings using the serial console port, as described in [Setting the IP Address Using the Serial Console](#).

SETTING THE IP ADDRESS USING THE LCD

1. Touch the Details button.
2. Touch the Menu button.

The Network Setting option is displayed by default.



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. Touching the decimal point button moves the focus to the next octet.



6. When finished entering the Management Port address, touch Next. The touch panel screen displays a keypad of numbers, and selectable fields for the Management Port netmask. A default entry of 255 is in place for the first field.
7. Touch the entry field to highlight it, and then touch the keypad buttons to enter each number.

8. Touch Next. The touch panel screen displays a keypad of numbers and fields for the gateway.
9. Touch the entry field to highlight it, and then touch the keypad buttons to enter each number. Use the decimal point to tab to the next field automatically.
10. Touch Next. Review the DataFort IP settings.



- If settings are correct, touch Return to exit the menu.
- If settings are incorrect, touch Edit and enter the settings again. When finished, touch Return to exit the menu.

SETTING THE IP ADDRESS USING THE SERIAL CONSOLE

1. Open a serial console (such as HyperTerminal) connected to the [Serial Console 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 that these entries are space and case sensitive):
 - Login: **user**
 - Password: **MTKNMTKN**

The main menu appears.

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

Note: Appliance serial sessions time out after 90 seconds of inactivity. If this happens before configuration is finished and saved, log in again. Settings are not saved until the Save and Exit command has been completed.

POWERING UP AND SHUTTING DOWN

The 1U appliance has one power cord and the 2U appliance has two power cords. On the 2U appliance, the second power cord should be plugged into a separate AC circuit to provide AC power redundancy. This enables the appliance to remain functional should one circuit fail.

Power supplies can be removed and replaced: the 1U power supply is cold-swappable, the 2U power supplies are hot-swappable. For instructions on replacing fans and power supplies, contact Decru.

Note: For normal operation, leave the appliance powered on, with the System Card in the card slot.

Power appliance on Connect each provided power cord to an appliance power port. Then connect the cord to an AC power source. The appliance powers on automatically.

Power appliance off temporarily Use the power button located on the rear panel next to the power supply. To temporarily power off the appliance, depress the recessed power button until the system turns off. This may take up to five seconds. To repower the appliance after shutdown, depress the power switch once more.

Power appliance off Unplug all power cords from the AC power source. Always back up the configuration database before powering off the appliance (as described in the administrative chapters of this guide).

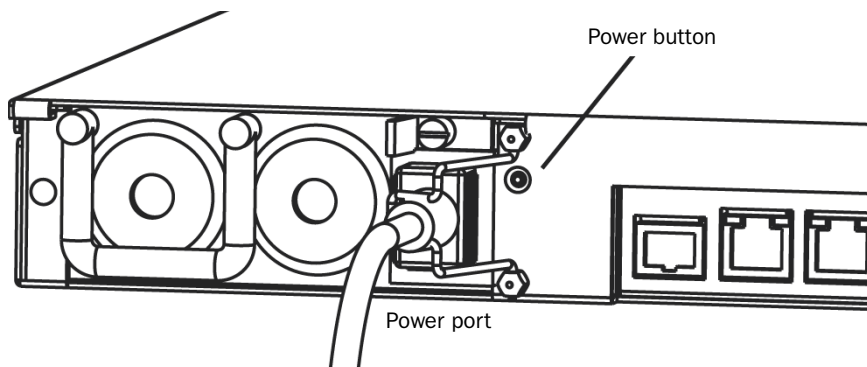


Figure 4-10: Rear panel power port and button on 1U appliance

5 INITIALIZING APPLIANCES

Run the Decru Management Console (DMC) from the Management Station to initialize appliances using the Setup Wizard.

Note: Only the Decru Management Console Setup Wizard can set up new appliances. Once appliances have been set up, they can be managed using the Decru Management Console and the appliance CLI. For more information about appliance management interfaces, see [Chapter 6](#).

Complete the procedures outlined in this chapter to initialize an appliance. See:

- [About the Setup Wizard](#)
- [Initializing a Standalone Appliance or Cluster](#)
- [Adding a Member to a Cluster](#)

ABOUT THE SETUP WIZARD

Consider the following when running the wizard:

- Initialization of a new appliance or cluster creates the first Full Administrator for that appliance or appliance cluster.
- 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 [Collecting Network Information](#) on page 36 before beginning the wizard.

SETUP WIZARD FUNCTIONS

The Setup Wizard allows an administrator to complete the procedures described in [Table 5](#).

TABLE 5: WIZARD FUNCTIONS

Procedure	Description
Set up a new standalone appliance	The new appliance must be initialized and connected to the network. See Initializing a Standalone Appliance or Cluster on page 54.
Set up a new cluster	All cluster members must be initialized and connected to the network. See Initializing a Standalone Appliance or Cluster on page 54.
Add a new member to an existing cluster	A configured standalone appliance must already be set up. The new appliance to be added must be initialized and connected to the network. See Adding a Member to a Cluster on page 62.
Set up a new appliance with an existing saved configuration (restore a configuration)	A saved prior configuration must be accessible to the new appliance. The new appliance must be initialized and connected to the network. This procedure requires only a quorum of Recovery Officers. See Restoring an Appliance on page 198.

INCOMPLETE SETUP WIZARD

If canceled before completion, the DataFort Setup Wizard retains data entered for the appliance before the cancellation. When the wizard starts again, it automatically fills in saved data and skips certain 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. For steps to clear wizard entries, see troubleshooting [Network Connections and Management Interfaces](#) on page 201.

ABOUT SMART CARDS AND READERS

When setting up a new standalone appliance or a new cluster, the setup process requires Recovery Cards and the Recovery Officers responsible for those cards. When initially introducing recovery cards during setup, the cards must be inserted sequentially into the smart card reader connected to the Management Station.

When setting up a new cluster, adding a member to a cluster, or restoring an appliance, it is possible to connect multiple smart card readers to the Management Station. Multiple readers allow authorization during Recovery Officer Quorum Selection without having to switch cards. For example, if 2 out of 5 cards are required to initialize a cluster and two card readers are connected, both required Recovery Cards can be inserted at once and cards do not need to be switched.

ABOUT REMOTE AUTHORIZATION

Remote authorization allows an administrator to initiate and verify Recovery Card operations for some DMC operations from a remote location. See [Initializing a Standalone Appliance or Cluster](#) on page 54 and [Setting Up Trustees](#) on page 118.

- If the administrator initiating the remote authorization process is also a Recovery Officer, Decru recommends the administrator be the last Recovery Officer to supply a card to verify that data is entered correctly and complete the approval process.
- If the administrator initiating the remote authorization process is not a Recovery Officer, Decru recommends that the last Recovery Officer to supply a card notify the administrator so that the administrator may verify that data is entered correctly and complete the approval process.

INITIALIZING A STANDALONE APPLIANCE OR CLUSTER

1. From the Windows Start Menu of the Management Station, select **Start > Programs > Decru > Decru Management Console**.

DMC starts.

- If no appliances have been added, the Add... pop-up screen appears automatically.
- If appliances have been added but not the one(s) to set up, select **Appliance > Add** to open the Add... pop-up screen.

2. Enter the IP address or hostname of all appliances to be set up.

More than one appliance can be added on this screen: enter the IP address or hostname for each appliance in the large text box provided. Separate multiple IP addresses or hostnames with a comma, a space, or by pressing Enter after each.

To add an IP address range for multiple appliances with consecutive IP addresses: enter the first IP address of the range in the IP range start field. Press Tab to move the cursor to the IP range end field and enter the end of the IP range.

3. Click OK.
4. A security certificate warning appears. Make the appropriate selection about trusting the certificate. 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.

The added appliances appear in the DMC.

5. From the appliance tree, right-click the first appliance to configure, and select Set up.
6. From the Welcome page, click Start.

CONNECT TO HEAD OF CLUSTER

Initialize a standalone appliance or connect to the cluster head (the first DataFort in a cluster).

1. Enter the hostname or IP address for the head of the cluster or standalone appliance.

If this is the first DataFort in a cluster, or will function as a standalone appliance, enter the IP address or resolvable hostname of the appliance (as configured during installation).

Note: If an appliance was selected in the resource pane prior to launching the setup wizard, its hostname or IP address appears in the field. If the wizard has been run before on this Management Station, previously entered IP information will appear in the field.

2. Click Next.
3. Agree to trust the certificate once or always.

SIGN LICENSE AGREEMENT

Agree to the license terms to continue the wizard.

1. Read the license agreement.
2. Click Accept to accept the terms and continue the wizard.

RECOVER FROM DATABASE

Use this page of the wizard **ONLY** if this appliance replaces a previously existing appliance and a configuration database from that previous appliance is used to configure this new appliance. For information about this feature, see [Restoring an Appliance](#) on page 198.

- Click Next to skip the Recover from Database screen.

CREATE ADMINISTRATOR

Create an administrator for this appliance. This administrator is a Full Administrator, and has management privileges for all members of a cluster.

This administrative name and password are used every time the administrator logs in to the appliance using any DataFort management interface.

The administrator can be associated with an Admin Card after the wizard is completed. Additional administrators can also be created after the wizard is completed.

1. Enter a username for the administrator.

Note: If SecureView licenses are in use, Decru recommends that the same administrator be created on multiple appliances. This allows multi-selecting appliances and logging into them as a group with one administrator profile.

2. Enter and confirm a password for the administrator and click Next.

Passwords may be composed of upper and lower case characters, numbers and special characters. Note that double quotes and backslashes are not permitted. Select a password consisting of at least 8 valid, randomly-chosen characters.

CAUTION:RECORD LOGIN INFORMATION CAREFULLY. THE ADMIN NAME AND PASSWORD ARE REQUIRED TO MANAGE THE APPLIANCE.

CONFIGURE CLUSTER AND RECOVERY SCHEMA

This step sets the recovery schema which determines how many Recovery Cards are required when performing sensitive procedures. This also determines if this wizard is configuring a standalone appliance or a DataFort cluster.

Note: The recovery schema is permanent. Plan the setting according to the security policy of your organization before completing the wizard.

- [Setting the Recovery Schema](#)
- [Setting the Cluster Size](#)

Setting the Recovery Schema

The recovery schema determines how many Recovery Cards must be present for sensitive data recovery operations. Recovery Cards work with passwords to create two-factor authentication for emergency data restoration or smart card replacement operations. The recovery schema is permanent for the entire cluster. Plan the setting according to the security policy of the organization.

2 out of 5 is the recommended data recovery setting, in which any 2 of the 5 Recovery Cards that are initialized during appliance setup are required to complete a recovery procedure. Each card should be given to a different individual, so that two people must be present for any data recovery to occur. In this scenario, two cards may be sent to escrow for safekeeping.

If needed, the number of people required for a recovery operation can be expanded by having one person in physical possession of a Recovery Card and another person know the password for the card. For more about options when managing smart cards, contact Decru.

- Select the desired data recovery schema. All appliances in a cluster use the same set of Recovery Cards and data recovery schema.

WARNING: DATA RECOVERY SETTINGS CANNOT BE CHANGED AFTER CONTINUING. ONCE THE NEXT BUTTON IS CLICKED ON THIS SCREEN, THIS SETTING WILL BECOME PERMANENT.

Setting the Cluster Size

1. Select the cluster size.

Select Standalone for a standalone appliance. Another DataFort can be added later to create a cluster.

Select the desired cluster size if forming a new cluster or adding a new cluster member.

2. Enter and confirm an IPsec secret for cluster members.

Note: This option is only available when a cluster size other than Standalone is selected in order to configure cluster members.

This password is shared by cluster members to ensure secure communication across the IPsec channel. The password can be composed of upper and lower case characters, numbers and special characters. Note that double quotes and backslashes are not permitted. Select a password consisting of at least 8 valid, randomly-chosen characters.

3. Click Next to proceed.

NETWORK SETTINGS

Enter the appropriate network settings.

- If Standalone was selected in the previous step, only one set of fields appears. See [Standalone Network Settings](#).
- If a Cluster Size was set in the previous step, a set of fields appears for each cluster member. See [Cluster Network Settings](#).
- There may be a delay of several minutes before the Next button becomes available in this screen.

Standalone Network Settings

For a standalone DataFort, one set of fields appears.

1. Enter a hostname for this appliance.
The IP address, Netmask and Gateway set for the Clients NIC appear. (These were set when [Assigning the Appliance IP Address](#) on page 48.)
2. The FC Site settings can be left at their default, or modified using the Customize option. Clicking Customize opens the Customize FC Sites window where the WWN settings for all Host and Storage Side HBAs in the cluster can be specified. Assign WWNs to override the default WWNs of the DataFort HBAs, and click Apply to preserve the settings. This function may be useful when cloning or replacing a DataFort.
3. Click Next.

Cluster Network Settings

For a DataFort cluster, one set of fields appears for each appliance.

1. Enter a hostname for the first appliance.
The IP Address, Netmask and Gateway set for the first appliance appear. (These were set when [Assigning the Appliance IP Address](#) on page 48.)
2. The FC Site settings can be left at their default, or modified using the Customize option. Clicking Customize opens the Customize FC Sites window where the WWN settings for all Host and Storage Side HBAs in the cluster can be specified. Assign WWNs to override the default WWNs of the DataFort HBAs, and click Apply to preserve the settings. This function may be useful when cloning or replacing a DataFort.
3. Enter a hostname for additional cluster members.
4. Enter IP Address, Netmask and Gateway information for additional cluster members.
5. Click Next.
6. Agree to trust the certificate once or always.

ADD LICENSES

Ensure that each appliance in the cluster has a license that supports the same features.

The FC-Series DataFort is licensed for use in environments with disk or tape storage. Disk features are not available to customers with DataFort appliances licensed only for tape and vice versa.

1. Enter the license key provided by Decru for each feature.
 - 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.
2. Click Next.

NETWORK AND CERTIFICATES

Enter optional DNS information and provide information for the self-signed security certificate for the appliance. While not required, DNS makes it easier to add servers and virtual servers to an appliance configuration.

DNS

1. If DNS is used, enter the DNS suffix for the network and at least one DNS server for the network.
2. Enter alternate domains, separated by a space, in the DNS Search Path(s) field (optional).

Certificate

Configure the appliance to create a self-signed security certificate to improve security for the SSL communication between the Management Station and the appliance.

1. Enter the country code for the appliance's location. The country code is limited to two characters in length. For the United States, enter **us**. Other codes are listed in [Partial List of ISO Country Codes](#) on page 242.
2. Enter the rest of the required information about the location of the appliance.
3. Click Next.

INSERT RECOVERY CARD

Recovery Officers responsible for Recovery Cards should be prepared to enter the existing password when prompted.

If the Recovery Cards are not initialized yet, the wizard prompts for a card label, security domain, and new password.

Password and Label Limitations

Keep the following in mind when selecting a password, label and domain for a smart card. Strong passwords are an important part of the overall security of the system.

Note: It is recommended to use the same Security Domain for all Recovery Cards in the set.

TABLE 6: CARD PASSWORD AND LABEL LIMITATIONS

Card Field	Character Limit	Restrictions
Password	At least 8 and no more than 30	Use upper and lower case characters, numbers and punctuation marks. Leading or trailing whitespace is not supported.
Label	20 characters or less	
Security Domain	50 characters or less	

Required Fields

Depending on whether or not the card is initialized, some fields are pre-filled.

Uninitialized Card If the card is uninitialized, the Recovery Officer responsible for this card should enter the required settings.

Initialized Card If the card has already been initialized, the Card Label and Security Domain appear and the wizard prompts for the password. The Recovery Officer responsible for this card provides this information.

To continue, select a method to authorize the Setup Wizard:

- To set up the appliance locally, see [Authorizing Setup Locally](#) on page 59.
- To set up the appliance using Remote Authorization (RA), see [Initiating Remote Authorization for Setup](#) on page 60.

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

Authorizing Setup Locally

1. Insert the first Recovery Card into the Management Station's smart card reader. Smart cards must be fully inserted into the reader. If a card is not recognized, re-insert it for better contact.
2. Enter the password and click Next.

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

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

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

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

3. Click Next.
4. When prompted, remove the initialized card and insert a new one.
Security Domain information from the first card is entered automatically. Change it to group the card differently.
5. Repeat the previous steps for all the cards specified by the recovery schema.

APPLY SETTINGS

1. Click Next to apply the settings to all appliances that are being configured using the wizard.
If this is a cluster, a prompt appears to insert the quorum of Recovery Cards. If one smart card reader is in use, the cards need to be inserted and removed as indicated by the wizard.
Note: If multiple card readers are connected to the Management Station it is possible to complete the wizard without having to switch cards. For example, if the quorum is 2 out of 5 cards for the cluster and two card readers are connected, both required Recovery Cards can be inserted at once and cards do not need to be switched.
2. Click Finish when the wizard completes and the final screen appears.

When the wizard is complete, the appliance is ready to be managed by the Decru Management Console or Command Line Interface. See [Chapter 6](#) for a list of appliance management interfaces.

Initiating Remote Authorization for Setup

1. On the Introduce Recovery Cards screen, click Enable Remote Authorization.
Note: If the administrator beginning the RA process is also a Recovery Officer, then Decru recommends that the administrator be the last Recovery Officer to supply a card and verify that all data is entered correctly on the last Setup Wizard screen.
2. When the Remote Authorization enabled message appears, click Cancel to close the Setup Wizard.
3. Notify the remaining Recovery Officer(s) that it is safe to continue the Setup Wizard approval and introduce Recovery Cards remotely. See [Authorizing Setup Remotely](#).

Authorizing Setup Remotely

1. In the Decru Management Console, from the appliance tree, select an appliance.
2. From the Appliance menu, select 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 card into the card reader, enter the password and click Start.

Note: When a card is inserted into the reader, the Card Label/Security D0main 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. WAIT FOR THE NEXT BUTTON TO BECOME AVAILABLE BEFORE PROCEEDING TO THE NEXT STEP.

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.

APPLY SETTINGS

1. Click Next to apply the settings to all appliances that are being configured using the wizard.

If this is a cluster, a prompt appears to insert the quorum of Recovery Cards. If one smart card reader is in use, the cards need to be inserted and removed as indicated by the wizard.

Note: If multiple card readers are connected to the Management Station it is possible to complete the wizard without having to switch cards. For example, if the quorum is 2 out of 5 cards for the cluster and two card readers are connected, both required Recovery Cards can be inserted at once and cards do not need to be switched.

2. Click Finish when the wizard completes and the final screen appears.

When the wizard is complete, the appliance is ready to be managed by the Decru Management Console or Command Line Interface. See [Chapter 6](#) for a list of appliance management interfaces.

ADDING A MEMBER TO A CLUSTER

Use the Setup Wizard to add one or more uninitialized appliances to a standalone appliance to form a cluster or to add additional appliances to an existing cluster.

- This requires the cluster quorum of Recovery Officers with their cards, and the shared secret of the cluster, as well as all applicable licenses for the existing and additional cluster members.
1. From the Windows Start Menu of the Management Station, select **Start > Programs > Decru > Decru Management Console**.

DMC starts.

- If no appliances have been added, the Add... pop-up screen appears automatically.
- If appliances have been added but not the one(s) to set up, select **Appliance > Add** to open the Add... pop-up screen.

2. Enter the IP address or hostname of all appliances to be set up.

More than one appliance can be added on this screen: enter the IP address or hostname for each appliance in the large text box provided. Separate multiple IP addresses or hostnames with a comma, a space, or by pressing Enter after each.

To add an IP address range for multiple appliances with consecutive IP addresses: enter the first IP address of the range in the IP range start field. Press Tab to move the cursor to the IP range end field and enter the end of the IP range.

3. Click OK.
4. A security certificate warning appears. Make the appropriate selection about trusting the certificate. 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.

The added appliances appear in the DMC.

5. From the appliance tree, right-click an **existing** member of the cluster or a standalone appliance and select Set up.

Note: Do not select the new appliance to be added. Select the already-configured standalone appliance or an existing member of the cluster.

The Welcome page of the Wizard appears.

6. Click Start.

CONNECT TO HEAD OF CLUSTER

1. Click Next to log in to the existing member of the cluster or standalone appliance.
2. Accept the certificate once or always.
3. Enter the administrator name and password set for the existing member of the cluster or standalone appliance being joined by the new appliance to form the cluster and click OK.

CLUSTER AND RECOVERY SCHEMA

The Recovery Schema cannot be modified, as it has already been set for the cluster.

1. Select the cluster size.
2. Enter the shared secret for the cluster and click Next.

NETWORK SETTINGS

The settings for the existing cluster member or standalone appliance appear. Enter the network settings for the appliance to be added.

1. Enter a hostname for the new appliance.
2. Enter IP Address, Netmask and Gateway information for the new appliance.
3. The FC Site settings can be left at their default, or modified using the customize option. Clicking Customize opens the Customize FC Sites window where the WWN settings for all Host and Storage Side HBAs (nodes) in the cluster can be specified. Assign WWNs to override the default WWNs of the DataFort nodes, and click Apply to preserve the settings. This function may be useful when cloning or replacing a DataFort.

Note: When setting up a cluster there may be a delay while the first member is being set up. This can mean that the Next button will not be available for 30 seconds or more.

4. Click Next.
5. Accept the certificate once or always.

ADD LICENSES

1. Enter the license provided by Decru for each feature for each appliance 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.
If site licenses are in use, the same licenses should be entered for each appliance.

NETWORK AND CERTIFICATES

Enter optional DNS information and set the security certificate for the appliance.

DNS

1. If DNS is used, enter the DNS suffix for the network and at least one DNS server for the network.
2. Enter alternate domains, separated by a space, in the DNS Search Path(s) field (optional).

Certificate

Configure the appliance to create a self-signed security certificate to improve security for the SSL communication between the Management Station and the appliance.

1. Enter a name for the appliance.
2. Enter the two-character country code for the appliance's location. For the United States, enter **US**. Other codes are listed in [Partial List of ISO Country Codes](#) on page 242.
3. Enter the rest of the required information about the appliance's location and click Next.

INSERT RECOVERY CARD

Recovery Officers responsible for Recovery Cards should be prepared to enter their password when prompted.

To continue, select a method to authorize the Setup Wizard:

- To set up the appliance locally, see [Authorizing Setup Locally](#) on page 59.
- To set up the appliance using Remote Authorization (RA), see [Initiating Remote Authorization for Setup](#) on page 60.

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

Authorizing Setup Locally

1. Insert the first Recovery Card into the Management Station's smart card reader. Smart cards must be fully inserted into the reader. If a card is not recognized, re-insert it for better contact.
2. Enter the password and click Next.

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

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

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

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

3. Click Next.
4. When prompted, remove the initialized card and insert a new one.
5. Repeat the previous steps for all the cards specified by the recovery schema.

APPLY SETTINGS

1. Click Next to apply the settings to all appliances that are being configured.

A prompt appears to insert the quorum of Recovery Cards. If a single smart card reader is being used, the cards need to be inserted and removed as indicated by the wizard.

Note: If multiple card readers are connected to the Management Station it is possible to complete the wizard without having to switch cards. For example, if the quorum is 2 out of 5 cards for the cluster and two card readers are connected, both required Recovery Cards can be inserted at once and cards do not need to be switched.

2. Click Finish when the wizard completes and the final screen appears.

When the wizard is complete, the appliance is ready to be managed by the Decru Management Console or Command Line Interface. See [Chapter 6](#) for a list of appliance management interfaces.

Initiating Remote Authorization for Setup

1. On the Introduce Recovery Cards screen, click Enable Remote Authorization.

Note: If the administrator beginning the RA process is also a Recovery Officer, then Decru recommends that the administrator be the last Recovery Officer to supply a card and verify that all data is entered correctly on the last Setup Wizard screen.

2. When the Remote Authorization enabled message appears, click Cancel to close the wizard.
3. Notify the remaining Recovery Officer(s) that it is safe to continue the Setup Wizard approval and introduce Recovery Cards remotely. See [Authorizing Setup Remotely](#).

Authorizing Setup Remotely

1. In the Decru Management Console, from the appliance tree, select an appliance.
2. From the Appliance menu, select 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 card into the card reader, enter the password and click Start.

Note: When a card is inserted into the reader, the Card Label/Security D0main 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. WAIT FOR THE NEXT BUTTON TO BECOME AVAILABLE BEFORE PROCEEDING TO THE NEXT STEP.

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.

APPLY SETTINGS

1. Click Next to apply the settings to all appliances that are being configured using the wizard.

A prompt appears to insert the quorum of Recovery Cards. If a single smart card reader is being used, the cards need to be inserted and removed as indicated by the wizard.

Note: If multiple card readers are connected to the Management Station it is possible to complete the wizard without having to switch cards. For example, if the quorum is 2 out of 5 cards for the cluster and two card readers are connected, both required Recovery Cards can be inserted at once and cards do not need to be switched.

2. Click Finish when the wizard completes and the final screen appears.

When the wizard is complete, the appliance is ready to be managed by the Decru Management Console or Command Line Interface. See [Chapter 6](#) for a list of appliance management interfaces.



■ ■ ■ ■ 6 **APPLIANCE MANAGEMENT INTERFACES**

This chapter provides information about connecting to the DataFort management interfaces that are used for administrative tasks. It includes the following topics:

- [Management Interfaces Overview](#)
- [Accessing the Decru Management Console](#)
- [Connecting to the Command Line Interface](#)
- [Serial Console](#)
- [Appliance Front Panel LCD](#)
- [SNMP Settings](#)

MANAGEMENT INTERFACES OVERVIEW

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)	An application used for setup and management of Decru appliances. DMC provides a centralized management interface for all appliances in an installation. See Accessing the Decru Management Console .	The only way to set up an appliance. Primary method for administrators to configure appliance settings, create and manage Cryptainers, etc. SecureView enables many-at-once control of appliances. A SecureView license is required on all appliances that are managed simultaneously.
Secure Shell (SSH)	A secure shell connection to the Command Line Interface (CLI) via secure shell client. Can require smart card authentication in addition to password. See Connecting to the Command Line Interface .	Alternative method for creating and managing Cryptainers, appliance settings, users, etc. Also used for some advanced configuration.
Serial	A serial connection to the appliance can be used to enter network settings for an uninitialized appliance. See Serial Console .	Set, clear, or reset appliance IP settings. Zeroize an appliance when other interfaces are not available.
LCD	The appliance front panel displays messages. The 2U appliance front panel also functions as a touch screen. See Appliance Front Panel LCD .	View status and throughput information. Use 2U appliance touch panel buttons to enter IP settings for an uninitialized appliance and get information about errors and status.
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 SNMP Settings .	View appliance status via SNMP tool. No secure information is permitted over this protocol (read only, no set commands).

SECUREVIEW

SecureView™ is a licensed feature that allows the Decru Management Console to manage many appliances at once. This feature is enabled on a per-appliance basis. If an appliance is licensed for SecureView, it can be managed along with other licensed appliances from the Decru Management Console with a single step. The administrator multi-selects the appliances and performs management functions on them simultaneously.

To manage multiple appliances using SecureView, 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 at once.

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 turn on 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 138.

Note: All administrator types 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 [Chapter 7](#).

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 [Decru Management Console Functions](#) on page 171 for details about the DMC Help menu.

ACCESSING THE DECRU MANAGEMENT CONSOLE

Use the console to manage appliances from a central location.

By default, the administrator logs in to the DMC without an Admin Card.

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

USING THE DMC

- See [Decru Management Console Functions](#) on page 171 for a description of the menu options.
- 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 *Lifetime Key Management 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 appliances which have been added to DMC will appear.
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.

A Full Administrator or Key Administrator can turn on 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 138.

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 [Accessing the Decru Management Console](#) on page 70.
3. Right-click an appliance and select Log in.

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 [Requiring Authorization for Login](#) on page 82 for details. The authorizing administrator can be any administrator who does not require authorization.

To log in to DMC when dual authentication is required:

1. First the administrator with authorization privileges must log in. Access the DMC from the Management Station as described in [Accessing the Decru Management Console](#) on page 70.
2. Right-click an appliance and select Log in.
3. Select **Configuration > View Administrators**.
4. Right-click the Administrator to be authorized and select 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.

CONNECTING TO THE COMMAND LINE INTERFACE

By default, the standard CLI setting is in effect, allowing the administrator to log in to the appliance 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.

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

USING THE CLI

- See [Using the CLI](#) on page 183 for information about CLI online help.
- As a security measure, the CLI times out after 10 minutes of inactivity.

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. In 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, which can be used to log in to CLI from an SSH client.

A Full Administrator or Key Administrator can turn on the smart card requirement (Secure CLI) by connecting to the DMC and accessing the Security Policy settings page, as described in [Configuring Management Security Settings](#) on page 138. 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 from the Management Station as described in [Accessing the Decru Management Console](#) on page 70.
3. Right-click an appliance and select Log in.
4. Check One Time Password.

Note: This button is present only if

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

6. Click OK.
A one-time login password (in hexadecimal format) will appear on the screen.
7. Copy the password that is provided.
8. 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 will invalidate CLI access.
9. Open an SSH client on a workstation connected to the same network as the appliance.
10. Enter the IP address or hostname assigned to the appliance.
11. At the prompt, enter the same administrator login name.
12. When prompted for the administrator password, paste or type the Secure CLI password from step 7 into the command line. The CLI prompt is ready for commands.

CONNECTING VIA CLI 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. For more details about dual authorization see [Requiring Authorization for Login](#) on page 82. The authorizing administrator can be any administrator who does not require authorization.

To log in to 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. In 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 DATAFORT_ADMIN.
5. The administrator with authorization privileges should exit the CLI by typing `quit`.
6. The authorized administrator now has one minute to log in to the appliance from an SSH client, entering the IP address or hostname assigned to the appliance, and entering the username and password in the terminal window.

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

CONNECTING TO CLI VIA DMC

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

Note: DMC CLI does not support the following features:

- Command line editing and completion
 - Output paging
 - Context-sensitive help
1. Select an appliance from the appliance tree and select **Appliance > Command Line**.
The CLI tab opens. For commonly used CLI commands see [CLI Administration](#) on page 182.
 2. Enter the command into the field provided.
 - Click Execute to execute the command. The command is run on all selected appliances and the output returned on the screen.
 - Click File to open a command file to run on the selected appliances. The commands are run when the file is opened. Note that the file must be an XML-formatted file.
 - To save the output of a command that has been executed, click Save and save the file in a designated location.

SERIAL CONSOLE

The appliance serial console port can be used 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 47 for details.

LOGGING IN TO 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.

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

CONFIGURING IP SETTINGS

1. At the shell prompt, log in using the default administrator name and password (note that these entries are space and case sensitive):
 - Login: **user**
 - Password: **MTKNMTKN**The main menu appears.
2. Select option **1** to set an IP address, subnet mask and default gateway for the Network Interface.
3. Select option **3** to save the settings and exit the terminal window.

CLEARING IP SETTINGS

The serial console can be 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 meant to be used when the appliance is being moved to a different network but zeroization is not required. When an 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 [Changing Network Settings](#) on page 164.

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).
The main menu appears.
2. Select option **C**.
The IP settings are cleared.
3. Select option **3** to save the settings, and exit the terminal window.

ZEROIZING THE APPLIANCE

Enter the zeroize command from the serial console to return the appliance to an uninitialized state. See [Zeroizing Using the Serial Console](#) on page 150 for details.

APPLIANCE FRONT PANEL LCD

After setup, the front panel LCD displays messages and a bar graph showing data read and write rates. If the appliance is equipped with a touch-sensitive panel, onscreen buttons provide more options. The left side of the graph shows the rate (in bytes per second) at which the appliance reads data, or decrypts encrypted data. The right side of the graph shows the rate at which the appliance writes, or encrypts data. The read/write display differs according to the type of appliance LCD:

- [Read/Write Rate Display on 2U DataFort Appliances](#)
- [Read/Write Rate Display on 1U DataFort Appliances](#)

TABLE 8: READ/WRITE RATE DISPLAY ON 2U DATAFORT APPLIANCES

Bar Display	Rate (per second)
1 bar	1 - 10K
2 bars	10 - 100K
3 bars	100K - 1MB
4 bars	1 - 10MB
5 bars	10 - 100MB
6 bars	100MB and up

TABLE 9: READ/WRITE RATE DISPLAY ON 1U DATAFORT APPLIANCES

Bar Display	Rate (per second)
1 bar	1 - 5MB
2 bars	5 - 10MB
3 bars	10 - 100MB
4 bars	100M and up

TOUCH PANEL ONSCREEN BUTTONS

If the appliance is equipped with a touch-sensitive LCD on the front panel, the onscreen buttons can be used to navigate the LCD menu options.

- 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

View network settings including IP address, subnet mask, and gateway for the appliance. On an uninitialized appliance, touch the Edit button to configure these settings.
- 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.

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 [SNMP Settings](#) on page 167 for details. A separate [DataFort Appliance SNMP Alarms Guide](#) is available from Decru for reference.



■ ■ ■ ■ 7 DATAFORT ADMIN ROLES AND ACCOUNT ADMINISTRATION

This chapter provides an overview of the various administrative types that can be created to manage DataFort appliances, and provides instructions for adding and managing administrators. It includes general information about the following topics:

- [Administrator Roles](#)
- [Account Administration](#)

ADMINISTRATOR ROLES

All DataFort administration tasks can be carried out by a Full Administrator, who completes installation of each DataFort or DataFort cluster by running the Setup Wizard, and thereafter is the primary administrator. For many organizations, one or two Full Administrators can handle all DataFort administrative tasks. Having two Full Administrators for each cluster is highly recommended.

DataFort also supports the creation of specialized administrators. At any time after DataFort has been set up, a Full Administrator or an Accounts Administrator can designate additional administrators to whom distinct duties can be delegated. The administrative types defined for DataFort are:

- [Full Administrator](#)
- [Accounts Administrator](#)
- [Storage Administrator](#)
- [Key Administrator](#)
- [Security Administrator](#)
- [Backup Administrator](#)
- [Machine Administrator](#)
- [Read-Only Administrator](#)

Specialty administrators can be used to separate tasks for increased security. Because the roles have separately defined permissions, using them can ensure that certain administrators only have permission to execute designated commands. In some cases, more than one administrator may be required to complete a given procedure if it overlaps different areas of defined administrative ability.

If desired, compound administrators possessing the characteristics of more than one specialty administrator can also be created. It may be useful for example to have several combined Machine, Storage and Key Administrators, but leave the Security and Account roles for a few highly-trusted individuals. See [Table 10](#) for details.

TABLE 10: ADMINISTRATOR ROLES AND PRIVILEGES

Role Name	Privileges
Full Administrator	The Full Administrator sets up each DataFort or DataFort cluster for the first time by running a setup wizard as described in Initializing Appliances . The Full Administrator can complete all administrative tasks including: • Initializing Appliances • Account Administration • Storage Administration • Key Administration • Backup Administration • Managing Appliance Security • Cluster Administration • Machine Administration

TABLE 10: ADMINISTRATOR ROLES AND PRIVILEGES (CONTINUED)

Role Name	Privileges
Accounts Administrator	Only a Full Administrator or an Accounts Administrator can add, delete and manage administrators. An Accounts Administrator is capable of carrying out the following tasks as described in Account Administration: • Add and delete administrators • Create specialty administrators • Change administrator roles • Associate administrators with smart cards • Specify that an administrator requires login authorization
Storage Administrator	A Storage Administrator specializes in adding and deleting hosts and targets which are required in order to create Cryptainers. Storage Administrator tasks are described in Storage Administration.
Key Administrator	A Key Administrator is responsible for applying security-related settings to DataFort appliances as described in Key Administration. Key Administrator tasks include: • Managing Trustees as well as importing and exporting keys • Purging keys upon backup to LKM as described in Key Purging • Configuring Management Security Settings • Managing Recovery Officers and Recovery Cards
Security Administrator	A Security Administrator is responsible for applying physical security-related settings to DataFort appliances as described in Managing Appliance Security. Security Administrator tasks include: • Managing Appliance Defense Responses • Configuring Management Security Settings • Managing Recovery Officers and Recovery Cards • Resetting Smart Cards • Setting Date and Time • Configuring and Viewing Logs • Zeroizing Appliances • Setting Security Certificates
Backup Administrator	A Backup Administrator is responsible for managing backups of the configuration database, including those to LKM. Backup Administrator tasks described in Backup Administration include: • Saving Configurations to Lifetime Key Management • Backing Up Configurations to a Remote Location
Machine Administrator	A Machine Administrator is responsible for managing system properties and non-security sensitive cluster operations. This administrator can change local network settings. Machine Administrator tasks described in Machine Administration include: • Changing Network Settings • Upgrading Appliances • Managing Licenses • SNMP Settings • The Machine Administrator can also add cluster members as described in Cluster Administration.
Read-Only Administrator	A Read-Only Administrator can view all DataFort settings (see DataFort Appliance Settings and Status) and can view status and logs, but cannot modify settings.

ACCOUNT ADMINISTRATION

The appliance stores a profile that associates each administrator username with an administrator type and password. Optionally, the DMC can be used to associate administrators with specific Admin Cards. Observe the following guidelines with respect to DataFort administrators:

- It is recommend to associate at least two Full Administrators with each appliance or DataFort cluster. Each administrator should have an individual Admin Card associated. See [Adding or Changing a Card Association](#) on page 84.
- Appliance administrators should be highly trusted individuals in the organization.
- Administrators should remove the Admin Card from the smart card reader when they are logged out of the DMC.

The appliance offers considerable flexibility in assigning roles and smart cards to administrators. One or more administrators can be associated with a single Admin Card; administrators can also be added without an association to an Admin Card. A Full or Accounts Administrator can add administrators and delegate responsibility for certain functions by creating administrator types with specialized permissions. Administrative options include:

- [Adding an Administrator](#)
- [Requiring Authorization for Login](#)
- [Changing the Administrator Password](#)
- [Removing an Administrator](#)
- [Adding or Changing a Card Association](#)

ADDING AN ADMINISTRATOR

1. Log in to the appliance via DMC as a Full Administrator or an Accounts Administrator.
2. Select **Configuration > Add Admin**.
3. Enter the name of the new administrator, and a password for that administrator. Strong passwords are an important part of the overall security of the system. Select a password consisting of at least 8 valid, randomly chosen characters.

Passwords may be composed of upper and lower case characters, numbers and special characters. Note that double quotes and backslashes are not permitted.

4. Confirm the password.
5. Select the administrator role. The default selection is Read Only. See [Administrator Roles](#) on page 79 for details.

Note: Full Administrators have all privileges and can complete any administrative task. It's a good practice to create only Full Administrators until appliance administration is well understood in the context of the staff and workflow of the organization.

- Select **Read-only** to create an administrator who can view appliance settings, but cannot modify them.
- Select **Specialty** to create specialized administrators. When selecting Specialty, specialty administrator roles become available. Multiple roles may be selected for one administrator.
- Select **Full Admin** to create a Full Administrator role.

6. Enter a full name for the administrator.
7. As an additional security option, require that an administrator be authenticated before being able to log in to the appliance. See [Requiring Authorization for Login](#) on page 82 for more information.
8. Click Apply.
9. Select the newly created administrator from the list.
10. To associate this administrator with an Admin Card for additional security, see [Adding or Changing a Card Association](#) on page 84.

REQUIRING AUTHORIZATION FOR LOGIN

A Full Administrator or an Accounts Administrator can create appliance administrators that require login authorization in order to access the DMC.

Note: There must be at least one Full Administrator not requiring prior authorization at all times.

For instructions on creating an administrator requiring prior authentication see:

- [Requiring Authorization to Access the DMC](#)
- [Creating a New Administrator](#)

Protecting Against Insider Attacks

The administration management options DataFort offers 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 DataFort 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.

Requiring Authorization to Access the DMC

1. Log in to the appliance via DMC
2. Select **Configuration > View Administrators**.
3. Right-click an existing administrator and select Edit.
4. Select Requires Prior Authorization and click Apply.

Now this administrator requires authorization to log in to the appliance. See [Connecting via DMC using Dual Authorization](#) on page 71 for authorizing DMC login, and [Connecting via CLI using Dual Authorization](#) on page 73 for authorizing CLI login.

Note: To remove the requirement for login authorization, access the same page, select Direct login and click Apply.

CHANGING THE ADMINISTRATOR PASSWORD

Administrator passwords can be changed periodically if desired as a security measure. The administrator who is logged in can change only his own password. Full and Account Administrators can change other administrators' passwords provided they know their current password,

1. Log in to an appliance via DMC.
2. Select **Configuration > View Administrators**.
3. Right-click the administrator whose password will be changed and select Change Password.
4. Enter the current password for the administrator.

Note: If the current password is lost, remove the administrator account, then add it again with a new password.

5. Enter the new password and confirm the entry.

Passwords may be composed of upper and lower case characters, numbers and special characters. Note that double quotes and backslashes are not permitted. Select a password consisting of at least 8 valid, randomly-chosen characters.

6. Click Apply.

The password will be changed.

REMOVING AN ADMINISTRATOR

It may be desirable to delete an administrator profile. After an administrator has been deleted from an appliance's list of known administrators, the appliance or cluster no longer authenticates that administrator. A Full Administrator or an Accounts Administrator can delete an administrator.

1. Log in to an appliance via DMC.
2. Select **Configuration > View Administrators**.
3. Right-click the administrator to be removed and select Remove.

ADDING OR CHANGING A CARD ASSOCIATION

A Full or Accounts Administrator must be logged in to the DMC to change an administrator profile.

1. Log in to an appliance via DMC.
2. Select **Configuration > View Administrators**.
3. Insert an Admin Card.
 - To add a listed administrator to those who are authorized to use the inserted Admin Card, right-click the administrator and select Add Admin Card.
 - To remove an administrator's association with an Admin Card, right-click the administrator and select Remove Admin Card.
 - To change an administrator's association with a different Admin Card for the appliance or cluster, first remove the current Admin Card, then insert the other card, right-click the administrator, and select Add Admin Card.

■ ■ ■ ■ 8 BEFORE STORAGE ADMINISTRATION

DataFort is ready to create Cryptainers after the Setup Wizard is complete, but additional preparatory steps are recommended to prepare for Cryptainer creation and DataFort operation.

These operations are performed using the DMC. For login instructions see [Accessing the Decru Management Console](#) on page 70. For a complete DMC menu options overview see [Chapter 15](#).

The following should be completed after running the Setup Wizard and before creating Cryptainers:

- [Verifying DataFort Configuration](#)

These procedures should be completed after setup and before creating Cryptainers. Procedures completed on one member of the cluster are applied to the entire cluster.

VERIFYING DATAFORT CONFIGURATION

VERIFYING SYSTEM VERSION

For security purposes, it is recommended that the DataFort appliance product version be verified.

1. From the DMC, select **Diagnostics > View System Information**.
2. Check the Platform Firmware Build ID. It should end with an underscore and the word **secure**. If it does not, take the DataFort appliance offline and notify Decru support.

CHECKING CLUSTER STATE

A cluster must be in a committed/online state for proper operation.

1. From the DMC, select **Appliance > View Cluster Members**.
2. Check the cluster member status.

For information about cluster states see [Checking the Status of the Cluster](#) on page 155.

CREATING ADDITIONAL ADMINISTRATORS

Add another Full Administrator in order to ensure that there is always an administrator with complete access to DataFort. Associate administrators to Admin Cards for additional security.

It may be desirable to create distinct administrators responsible for certain tasks, as outlined in [Chapter 7](#).

1. From the DMC, select **Configuration > Add Admin**.
2. Create an additional administrator. If desired, associate one or both administrators with an Admin Card. See [Adding an Administrator](#) on page 81 for instructions.

CONFIGURING REMOTE LOGGING

It is recommended that DataFort be configured to use remote signed logging.

1. From the DMC, select **Configuration > Log Configuration**.
2. Determine which log messages should be sent to a remote syslog server on the network. See [Appliance Log Storage Guidelines](#) on page 143 for details.

DETERMINING THE DEFENSE SETTING

Determine the level of defense necessary when an intrusion to the appliance is detected. In all cases, a warning is displayed and encryption and decryption are immediately disabled when an intrusion is detected. Whether encryption keys are also deleted is determined by the choice of defense setting. Selecting a defense setting appropriate for the organization involves deciding:

- The relative importance of the defense triggers.
- The need for an automatic response vs. a manual response at the appliance.
- The need for temporary data protection with quick and easy recovery (after assessing the triggering event) or complete data protection requiring secure recovery.

To configure the defense setting:

1. From the DMC, select **Security > Defense**.
2. Select the appropriate defense setting. See [Defense Triggers and Responses](#) on page 134.

CONFIGURING DISK OR TAPE MODE

While the FC-Series DataFort appliance supports encryption of data both on disk and tape, the appliance does not support simultaneous operation of disk and tape.

Proper configuration settings and features differ between disk and tape deployments. Use the FC-Series DataFort appliance either for disk or for tape, but not for both at the same time.

Using DataFort for tape No additional steps are needed.

Using DataFort for disk Disable tape support.

Disabling Tape Support

1. Log in to the DataFort CLI. See [Connecting to the Command Line Interface](#) on page 72 for detailed instructions.
2. Set the system properties to disable tape support by running the following CLI commands:

```
system property set dfc.disable_host_fc_tape true
system property set dfc.disable_storage_fc_tape true
```

Configuring Tape Settings

Set the tape settings to determine how DataFort interacts with tape devices. Note that these features are only available if a DataFort license controlling tape features is present.

1. From the DMC, select **Topology > Tape Settings**.
2. Select whether DataFort will encrypt, compress or encrypt and compress data as it is sent to tape devices for backup.



■ ■ ■ ■ 9 STORAGE ADMINISTRATION

This chapter includes instructions for using the Decru Management Console to manage Cryptainers, the backbone of a storage network secured by DataFort appliances. A Full Administrator is assumed to have completed installation and preparation of DataFort appliances. A Full Administrator as well as a Storage Administrator can perform all of the functions outlined in this chapter.

- [Creating Cryptainers](#)
- [Managing Hosts](#)
- [Managing Cryptainers](#)
- [Managing Storage](#)
- [Managing Tape Pools](#)
- [Managing Tape Settings](#)
- [Managing SAN Storage Settings](#)
- [Restoring a Cryptainer](#)

It is recommended that the DataFort administrator follow these procedures in the SAN environment:

- Maintain current information about the relationships between device port WWNs and target IDs.
- Use persistent binding to aid in the recovery of DataFort if necessary.

CREATING CRYPTAINERS

Use the Hosts and Devices tab of the Decru Management Console for Cryptainer creation and management. The Hosts and Devices tab shows all known hosts and storage devices, along with any Cryptainers that have been created. See [Hosts and Devices Tab](#) on page 95 for details about the tools each onscreen pane provides, including right-click menus, multiple device selection and the lower information pane.

Hosts and storage devices appear in the DMC listed by WWN. Cryptainer creation in a DataFort cluster is simplified with the use of the collection feature, which allows multiple instances of the same host or device on the network to be placed in a collection for management. For an overview of basic Cryptainer creation using the Decru Management Console, see:

- [Cryptainer Creation Using Collections](#) (recommended)
- [Cryptainer Creation Without Collections](#)

OPEN THE DECRU MANAGEMENT CONSOLE

1. From the Management Station, select **Start > Programs > Decru > Decru Management Console**.
2. Select an appliance in the appliance tree on the left.
3. From the Appliance menu, select Log in.

CRYPTAINER CREATION USING COLLECTIONS

To create Cryptainers using the collection features of DataFort, complete these steps:

- [Create a Host Collection](#)
 - [Create a Storage Collection](#)
 - [Create a Cryptainer](#)
 - [Assign Permissions to a Cryptainer](#)
 - [Encrypt Cryptainer Data](#)
1. A Full Administrator or Storage Administrator must log in to the DMC to create Cryptainers. See [Open the Decru Management Console](#) for login instructions.
 2. Access the Hosts and Devices tab by selecting **Topology > Hosts and Devices** from the DMC menu.

The Hosts and Devices tab is identified as a Cluster-wide display, meaning that the configuration visible on the tab applies to the entire cluster. Cryptainer creation and maintenance can be completed from any member of the cluster, as all cluster members see an identical Hosts and Devices tab.

All discovered hosts and targets appear on the Hosts and Devices tab. Click the tree to expand the view and see individual hosts and targets.

Create a Host Collection

In a standard highly available clustered configuration the same host appears more than once as each path from that host to storage is represented in the DMC. The number of appearances of the host is based on the number of connections it has to the fabric. For ease of management, group the instances of each host (or hosts that share access and configuration settings) into a collection.

1. Multiple-select host instances by Shift- or Ctrl-clicking them in the Host Management pane.
2. Right-click to view the [Host Collection Menu](#) and select **Move to > New collection...**
3. Enter a name for the collection and click Apply.

The new collection appears in the DMC.

Create a Storage Collection

1. Multiple-select storage device instances (use WWN information to identify paths to the same device) by Shift- or Ctrl-clicking them in the Storage Management pane.
2. Right-click to view the [Storage Collection Menu](#) and select **Move to > New collection...**
3. Enter a name for the collection and click Apply.

The new collection appears in the DMC.

Create a Cryptainer

1. Right-click the storage device collection and select Create Cryptainers. As long as the collection contains paths to the same device, a Cryptainer is created for each LUN in the collection.

The Create Cryptainer screen appears.

2. Select the settings for the Cryptainer on this device. For a list of options and their defaults see [Options When Creating a Cryptainer for a Storage Collection](#) on page 91.
3. Click Apply.

The Cryptainer appears listed in the Cryptainer Management pane. The default name automatically reflects the storage device where the Cryptainer was created.

4. To change the name of the Cryptainer, right-click it and select Edit.
5. Enter the new name in the Description field and click Apply.

About Port and LUN Mapping

A logical map must be established between the LUNs presented from the storage devices to DataFort and those presented from DataFort to the hosts. This mapping exists within the DataFort configuration and can be set at the port level or at the LUN level.

In situations where storage devices are virtualized to the hosts, Port Mapping maintains identical LUN addresses, thereby avoiding changes within host configurations. Port Mapping supports seven storage devices connected in Multi ID mode, and one in Single ID mode.

When mapped at the port level, DataFort establishes that any requests for a given WWN presented on its host-side relates to a particular WWN on its storage side. Note that in a virtualized environment, the WWN on the host side may be identical to the WWN mapped to it on the storage side. In a non-virtualized environment, these would be different. The specific LUN number within this WWN should be unchanged from what is seen on the storage side.

Mapping at the individual LUN level does not necessarily maintain LUN-to-port groupings from storage devices when presenting LUNs to hosts. LUN Mapping can be used to enable a larger number of storage devices to be connected behind DataFort.

Port Mapping, which presents the LUN of the storage device to the host, is recommended when creating Cryptainers on an enterprise storage target. This method of mapping preserves the LUN assignments of the target by creating a virtual port which DataFort maps to the actual storage port on the target. One virtual port can be assigned to each port in the device. The WWN of this virtual port is based on DataFort's WWN. The virtual LUN of this Cryptainer matches the real LUN of the disk for which the Cryptainer was created.

LUN Mapping is recommended if the storage is a multi-target device, as there is a limit on the number of virtual ports that can be created (the number of virtual ports available on DataFort is determined by HBA limitations). LUN Mapping allows DataFort to assign a virtual LUN number to each disk or tape drive in the device. The Cryptainer appears as a LUN on the target WWN of the DataFort. LUN mapped Cryptainers are assigned virtual LUNs by DataFort which may not match the real LUN of the disk for which the Cryptainer was created.

Note: The same mapping method must be used for all LUNs within a given device. The administrator can create either Port-mapped or LUN-mapped Cryptainers for a device but not both.

Options When Creating a Cryptainer for a Storage Collection

The following options are available when creating a Cryptainer. With the exception of assigning a key at creation time, these settings cannot be reversed after the Cryptainer has been created.

Map Type

Select how to map the Cryptainer: Port Mapped (off by default) or LUN Mapped (on by default). For more information about Port and LUN Mapping see [About Port and LUN Mapping](#) on page 90.

Host Collection Name (empty by default)

When creating a Cryptainer on a storage collection for a virtualized host, the administrator must specify the host collection name. Since the storage device presents LUNs to multiple hosts, this tells DataFort which specific instance of the storage device should have Cryptainers created. See [Managing Hosts](#) for more about virtualizing hosts.

Encryption (Cleartext by default)

If set to Encrypted, the contents of the new Cryptainer are automatically encrypted. Note that existing data on the target disk is not preserved.

If set to Cleartext, DataFort preserves the data on the Cryptainer's disk and does not encrypt/decrypt data being written or read from the disk automatically. The Cryptainer can then be manually rekeyed to enable encryption. Use this method to create an encrypted Cryptainer on a disk with existing data. See [Managing Cryptainers](#) for more about data encryption.

Port Forwarding (off by default)

If set to ON, the virtual port created for a port mapped Cryptainer has the same exact WWN as the disk's Cryptainer. If this feature is used, it is recommended that the host side and storage side HBAs of the DataFort be on separate fabrics, or that port zoning be used on the FC switch.

Assign Permissions to a Cryptainer

1. Right-click a Cryptainer and select Access Grant.
2. From the displayed host list, select the host WWN to grant access to.
3. Check Cross Mapping at the bottom right, then select a host, Cryptainer, or storage to view the results.

Bold text indicates the storage location of the Cryptainer and which host has access.

Encrypt Cryptainer Data

Cryptainers created on disk can be encrypted after creation. A Cryptainer is cleartext until rekeyed (unless Encrypted is selected at time of creation). Its icon indicates if encryption is on.

- When ready to encrypt the contents of the Cryptainer, right-click the Cryptainer.
 - To encrypt a Cryptainer with data for the first time, or to rekey an existing Cryptainer with data, select **Encryption > Encrypt/Resume Populated Disk**.
 - To encrypt a Cryptainer without data for the first time, or to rekey an existing Cryptainer without data, select **Encryption > Encrypt/Resume Empty Disk**. Any data on the disk is lost.

CRYPTAINER CREATION WITHOUT COLLECTIONS

Cryptainers can be created at the LUN, storage device or collection of storage devices level. Do not create more than one Cryptainer for a given volume.

Use this method only if there is a single path to the device where the Cryptainer will be created. If there is more than one path to the volume, see [Cryptainer Creation Using Collections](#).

1. Right-click a storage device or an individual LUN in the Storage Management pane.
 - Select the entire storage device to create a Cryptainer per LUN for the entire device.
 - Select an individual LUN to create a Cryptainer only on the selected LUN.
 - Shift- or Ctrl-click and select multiple LUNs to create Cryptainers on them.
2. Select Create Cryptainer.
3. Select the settings for the Cryptainer on this device. See [Options When Creating a Cryptainer](#).
For more information about Port and LUN Mapping see [About Port and LUN Mapping](#) on page 90.
4. Click Apply.
5. The Cryptainer is added to the Cryptainers Management pane. The default name automatically reflects the storage device where the Cryptainer was created.
6. Change the name of the Cryptainer by right-clicking it and selecting Edit.
7. Enter the new name in the Description field and click Apply.

Options When Creating a Cryptainer

The following options are available when creating a Cryptainer. With the exception of assigning a key at creation time, these settings cannot be reversed after the Cryptainer has been created.

Map Type	Select how to map the Cryptainer: Port Mapped (off by default) or LUN Mapped (on by default). For more information about Port and LUN Mapping see About Port and LUN Mapping on page 90.
Encryption (Cleartext by default)	If set to Encrypted, the contents of the new Cryptainer are automatically encrypted. Note that existing data on the target disk is not preserved. If set to Cleartext, DataFort preserves the data on the Cryptainer's disk and does not encrypt/decrypt data being written or read from the disk automatically. The Cryptainer can then be manually rekeyed to enable encryption. Use this method to create an encrypted Cryptainer on a disk with existing data. See Managing Cryptainers for more about data encryption.
Host Port WWN	When creating a Cryptainer on a storage device for a virtualized host, the administrator must specify the host port WWN. Since the storage device presents LUNs to multiple hosts, this tells DataFort which specific instance of the storage device should have Cryptainers created. See Managing Hosts for more about virtualizing hosts.
Port Forwarding (off by default)	If enabled, the virtual port created for a port mapped Cryptainer has the same WWN as the disk's Cryptainer. To avoid WWN conflicts, put the host side and storage side HBAs of the DataFort on separate fabrics, or use port zoning on the FC switch.

Assign Permissions to a Cryptainer

1. Right-click a Cryptainer and select **Access Grant**.
2. From the displayed host list, select the host WWN to grant access to.
3. Check Cross Mapping at the bottom right, then select a host, Cryptainer, or storage to view the results. Bold text indicates the storage location of the Cryptainer and which host has access.

Encrypt Cryptainer Data

Cryptainers created on disk can be encrypted after creation. A Cryptainer is cleartext until rekeyed (unless Encrypted is selected at time of creation). Its icon indicates whether or not data is encrypted.

- When ready to encrypt the contents of the Cryptainer, right-click the Cryptainer.
 - To encrypt a Cryptainer with data for the first time, or to rekey an existing Cryptainer with data, select **Encryption > Encrypt/Resume Populated Disk**.
 - To encrypt a Cryptainer without data for the first time, or to rekey an existing Cryptainer without data, select **Encryption > Encrypt/Resume Empty Disk**. Any data on the disk is lost.
- Note:** Encryption of tape devices is not necessary. Tape encryption keys are managed either per pool or per tape.

HOSTS AND DEVICES TAB

The Hosts and Devices tab of the DMC shows all known hosts and targets, along with any Cryptainers that have been created.

Access the Hosts and Devices tab by selecting **Topology > Hosts and Devices** from the DMC menu. Each onscreen pane provides the following tools for managing the storage network:

Right-click menus	Right-click each device or collection of devices for menu options.
Lower information pane	Detailed information about a selected device appears in the lower pane. Click an item onscreen to update its information in the details pane.
Collections	Collect onscreen objects for ease of management.
Multiple device select	Select multiple devices by Shift- or Ctrl-clicking them onscreen.
Filter	Change the view so that only items relevant to the selected filter object expand onscreen. Multiple filters can be set. They can be removed by clicking the onscreen buttons that appear after they have been set.
Cross Mapping	Check Cross Mapping at the bottom right, then select a host, Cryptainer, or storage. This displays access paths between host, Cryptainer, and storage.
Icons	Icons show the state of the device. Click the Icon Legend link at the bottom right on the Hosts and Devices tab for an overview of icons.

The following sections describe menu options on the Hosts and Devices tab:

- [Managing Hosts](#)
- [Managing Cryptainers](#)
- [Managing Storage](#)

DATAFORT DMC ICONS

Icons display status information about network devices including hosts, targets and Cryptainers. Images may be combined to describe multiple conditions. For example, an encrypted Cryptainer that is offline shows the icon for encrypted Cryptainer along with the yellow alert icon.

Use the following key to understand the icons display. Click the [Icon Legend](#) link at the bottom right on the Hosts and Devices tab for a complete overview of icons.

TABLE 11: SAMPLE ICONS

Device	Icon State	Meaning	Example
	Yellow !	Device or path to device has an error	
	Red X	Device or path to device is offline	
Host icon	Yellow !	One or more paths to initiator is offline	
Host path icon	No icon	Path is online	NA
	Red X	Path is down	
Target icon	Yellow !	One or more paths to a LUN on the target is offline	
LUN icon	Yellow !	One or more paths to the LUN is offline	
LUN path icon	No icon	Path is online	NA
	Yellow !	Path has an error	
	Red X	Path is down	
Cryptainer icon	Yellow !	Rekey error, or Cryptainer is offline	
	Lock	Cryptainer is encrypted	
	No lock	Cryptainer is cleartext	
	Arrows	Currently being rekeyed	
	Arrows + W	Waiting to be rekeyed	

MANAGING HOSTS

DataFort offers Port Locking to prevent unauthorized hosts from accessing data. The Host Management pane of the DMC features the following elements:

Host Pane Menu	Right-click in the Host pane to use the top level host menu. The menu offers options to modify or refresh the pane view and add a new host or collection of hosts. See Host Pane Menu on page 97.
Host Collection Menu	Right-click a host collection to use the menu to manage all host instances together. See Host Collection Menu on page 98.
Individual Host Menu	Right-click a host instance to view the host level menu. The Host Menu offers key tools for managing individual host paths.
Individual Host Icons	Icons indicate the condition of the host including whether a host has port locking on or is virtualized. A red X indicates offline status, a yellow alert indicates a problem. For more information click the Icon Legend link at the bottom right on the Hosts and Devices tab or see DataFort DMC Icons on page 96.

HOST PANE MENU

Right-click in the host pane to view the storage pane menu. Use this menu to manage storage tasks.

Refresh	Refresh the Host pane view.
Expand, Collapse	Expand or collapse the host tree.
New Collection	Create a new host collection.
New Host	Add a new host. See Add a Host on page 97.
Rescan, Cluster-wide Rescan	Rescan the fabric for hosts.
Purge Unused	Remove hosts that are offline from the host pane.
DataFort Filter	Display only hosts seen by the specified DataFort appliance.

Add a Host

Hosts can be added manually. Options to add a host include:

Host Node WWN	Enter the Host Node WWN.
Host Port WWN	Enter the Host Port WWN.
Hostname	Enter the host name.
Discovering FC Site Name	Select the FC site name of the DataFort HBA where the host was discovered.

HOST COLLECTION MENU

Right-click a host collection to view the host collection menu. Use this menu to manage a collected host or group of hosts with the same access and configuration.

Filter	Restrict the DMC view to show only the Cryptainers and storage devices the selected host collection can access.
Add Host	Add another host to the collection. Specify its host name, Node WWN, and Port WWN. See Add a Host on page 97.
Virtualize, Unvirtualize Collection	Some storage devices reserve space for a specific host as identified by its WWN. DataFort presents host HBAs to storage, so some devices require that DataFort virtualize the host in order to make it possible for storage devices to see it. Right-click the collection and select Virtualize Collection. The host is virtualized on available virtual ports. If the previously assigned Virtual Port Index is known, assign it again to use the same default WWN.
Set Default Pool	A typical backup environment includes backup pools to which hosts write backup tapes. If a host without access to any pool writes a backup tape, DataFort creates a default pool for that host (host_wwn_Default_pool). In order for other hosts to write to the default pool, permission must be granted using the Managing Tape Pools features.
Set Port Lock	Right-click the collection and select Set Port Lock > On to set the lock for the host. Port locking allows access to a Cryptainer only from the HBA of the selected host. The port lock locks the host to a port on a switch. It must be turned off if the host is moved, and reset at the new port. Individual Host Icons show whether port locking is enabled. The setting also appears in the lower pane. Note that port locking is only available on Brocade and McData switches.
Edit	Change the host collection name.
Delete	Right-click the collection and select Delete to remove it from the DMC. All hosts must be removed before the host collection can be deleted.

HOST MENU

Right-click a host to view the host menu. Use this menu to manage individual paths from host to storage.

Filter	Restrict the DMC view to only the Cryptainers and storage devices the selected host can access.
--------	---

Virtualize, Unvirtualize Host	Some storage devices reserve space for a specific host as identified by its WWN. DataFort presents host HBAs to storage, so some devices require that DataFort virtualize the host in order to make it possible for storage devices to see it. Right-click the host and select Virtualize Host. The host is virtualized on available virtual ports. If the previously assigned Virtual Port Index is known, assign it again to use the same default WWN.
Move To	Move the selected host instance to a specified collection.
Edit	Change host properties such as Name, Label of Default Pool, Discovering FC Site Name, Port Lock Mode, RAID admin mode and Host Authentication. See Edit Host on page 99.
Delete	Right-click the host and select Delete to remove it from the DMC. This option removes the host from the DMC. The host is not deleted from the fabric. If the host is still online and zoned with the DataFort, it reappears at the next rescan.

EDIT HOST

Options to edit a host include:

Hostname	Change the name of the host displayed in the DMC.
RAID Admin Mode (off by default)	Enable RAID Admin Mode to support device management software running a server (host) that needs direct access to the device through the Fibre Channel. When RAID Admin mode is enabled on a host, DataFort passes commands through from that host to the devices it has permission to access. DataFort recognizes standard commands and expected behavior. However there are some unspecified commands or vendor-unique commands which are not recognized and can be blocked by DataFort. Enabling RAID Admin Mode allows such vendor-unique commands to pass through DataFort.
Port Lock Mode (off by default)	Enable Port Lock Mode to permit access to a Cryptainer only from the HBA of the selected host. The port lock locks the host to a port on a switch. It must be disabled if the host is moved, and reset at the new port. Individual Host Icons show whether port locking is enabled. The setting also appears in the lower pane. Note that port locking is only available on Brocade and McData switches.
Label of Default Pool	A typical backup environment includes backup pools to which hosts write backup tapes. If a host without access to any pool writes a backup tape, DataFort creates a default pool for that host. Use this label to set the name of the default pool for this host.
Discovering FC Site Name	Displays the FC site name of the DataFort HBA where the host was discovered.

MANAGING CRYPTAINERS

The Cryptainer Management pane of the DMC features the following elements:

Cryptainer Pane Menu	Right-click in the Cryptainer pane to use the top level menu. The menu offers options to modify or refresh the pane view, or add a new collection.
Cryptainer Collection Menu	Right-click a collection of Cryptainers to use the collection menu. See Cryptainer Collection Menu .
Individual Cryptainer Menu	Right-click a Cryptainer to view the Cryptainer level menu. See Cryptainer Menu .
Individual Cryptainer Icons	Icons identify the condition of the Cryptainer. A red X indicates offline status, a yellow alert indicates a problem. Icons for Cryptainers created on disk show whether the Cryptainer has been encrypted or is in cleartext form, is in the process of being encrypted or is waiting for encryption, and whether the Cryptainer is healthy or not. An unhealthy Cryptainer is indicated if at least one device that maps to the Cryptainer is offline. For more information click the Icon Legend link at the bottom right on the Hosts and Devices tab or see DataFort DMC Icons on page 96.

CRYPTAINER PANE MENU

Right-click in the Cryptainer pane to view the Cryptainer pane menu. Use this menu to manage Cryptainer-related tasks.

Refresh	Refresh the Host pane view.
Expand, Collapse	Expand or collapse the host tree.
Add Collection	Create a new Cryptainer collection.

CRYPTAINER COLLECTION MENU

Right-click a Cryptainer collection to view the Cryptainer collection menu. Use this menu to manage collections of Cryptainers.

Encryption/ Decryption	Manage Cryptainer encryption. Cryptainer icons indicate whether a Cryptainer is already encrypted or if it is in cleartext, in the process of being encrypted or waiting to be encrypted. Select this option to encrypt/decrypt the data. For more information, see Encrypt Cryptainer Data on page 92. Select Pause or Cancel to halt the encryption process. Submenu options change depending on the Cryptainer encryption status.
Access	Grant or revoke Cryptainer access to hosts. Select a host or host collection in the host pane, then right-click a Cryptainer collection and choose Access Grant/Revoke Selected to grant/revoke access. Alternatively, without selecting a host in the host pane, grant/revoke access by selecting the desired hosts from the Access Grant/Revoke host lists.
Edit	Change the Cryptainer collection name.
Delete	Right-click the Cryptainer collection and select Delete to remove it from the DMC. All Cryptainers must be deleted before the collection can be removed.

CRYPTAINER MENU

Right-click a Cryptainer to view the Cryptainer level menu. Use this menu to manage individual Cryptainers.

Encryption/ Decryption	Manage Cryptainer encryption. Cryptainer icons indicate whether a Cryptainer is already encrypted or if it is in cleartext, in the process of being encrypted or waiting to be encrypted. Select to encrypt/decrypt the data. For more information, see Encrypt Cryptainer Data on page 92 Select Pause or Cancel to halt the encryption process. Submenu options change depending on the Cryptainer encryption status.
Access	Grant or revoke Cryptainer access to hosts. Select a host or host collection in the host pane, then right-click a Cryptainer collection and select Access Grant/Revoke Selected to grant/revoke access. Or, without selecting a host in the host pane, grant/revoke access by selecting the desired hosts from the Access Grant/Revoke host lists.
Move to	Move the selected Cryptainer to a specified collection.
Edit	Change the Cryptainer name.
Delete	Right-click the Cryptainer and select Delete to remove it from the DMC.

MANAGING STORAGE

The Storage Management pane features the following elements:

Storage Pane Menu	Right-click in the Storage pane to use the top level menu. See Storage Pane Menu on page 102.
Storage Collection Menu	Right-click a collection of Storage devices to use the collection menu. See Storage Collection Menu on page 103.
Individual Storage Device Menu	Right-click a storage device to view the storage device level menu. See Storage Device Menu on page 103.
Individual LUN Menu	Right-click a LUN to view the LUN level menu. See LUN Menu on page 104.
Individual Storage Icons	The icons in the DMC indicate the condition and type of storage device. A red X indicates offline status, a yellow alert indicates a problem. Distinct icons are displayed for direct access LUNs and sequential access LUNs (tape). The type of device is displayed in the Device Info field of the Storage Management lower pane. Icons will show whether a device is healthy or not. A device is shown as unhealthy if it is uninitialized, has a hardware error, or the login has failed. For more information click the Icon Legend link at the bottom right on the Hosts and Devices tab or see DataFort DMC Icons on page 96.

STORAGE PANE MENU

Right-click in the storage pane to view the storage pane menu. Use this menu to manage storage related tasks.

Refresh	Refreshes the list of storage devices.
Expand, Collapse	Expand or collapse the storage device tree.
Add Collection	Create a new storage collection.
Cryptainer Keys	List all Cryptainer keys.
Export/Import Trustee Keys	Export/import keys between Trustees. See Managing Trustees on page 118.
Rescan, Cluster-wide Rescan	Rescan the fabric for disks. This command may be needed to update recent changes to disks. Note that disk rescans are potentially disruptive to disk I/O.
Purge Unused	Remove disks that are offline and have no Cryptainers from the storage pane.
DataFort Filter	Display only storage seen by the specified DataFort appliance.

STORAGE COLLECTION MENU

Right-click a storage device collection to view the storage collection menu. Use this menu to manage collected storage devices.

Filter	Restrict the DMC view to only the Cryptainers and hosts associated with the selected storage collection.
Create Cryptainers	Create a Cryptainer on the device (a Cryptainer per LUN for the entire device). See Options When Creating a Cryptainer for a Storage Collection on page 91. Use Port Mapping if the LUN assignment structure must be consistent with the physical configuration of the device. Use LUN Mapping if the storage device is a multi-target device such as a JBOD.
Edit	Change the collection name.
Delete	Removes the collected storage device from the DMC. The device is not deleted from the fabric.

STORAGE DEVICE MENU

Right-click a storage device to view the storage menu. Use this menu to manage storage devices.

Filter	Restrict the DMC view to only the Cryptainers and hosts associated with the selected storage device.
Create Cryptainers	Create a Cryptainer on the device (a Cryptainer per LUN for the entire device). See Options When Creating a Cryptainer for a Storage Collection on page 91. Use Port Mapping if the LUN assignment structure must be consistent with the physical configuration of the device. Use LUN Mapping if the storage device is a multi-target device such as a JBOD.
Map, Unmap	Map/Unmap devices to add or remove a path from a Cryptainer to a storage device. Use this feature when a Cryptainer was created without using collections (a single path to a storage device) and a second path to that Cryptainer from the storage device needs to be created. Select the storage LUN that already has the Cryptainer, then Shift-click the LUN without the Cryptainer and select Map to associate the Cryptainer with that LUN. Select Unmap to remove this association.
Move to	Move the selected device to a specified collection.
Edit	Change the device name, and the FC site name of the DataFort HBA where the storage device was discovered. See Edit Device on page 104.

EDIT DEVICE

Options to edit a storage device include:

Device Name	Change the name of the storage device displayed in the DMC.
Discovering FC Site Name	Displays the FC site name of the DataFort HBA where the storage device was discovered.

LUN MENU

Expand a storage device view to see its LUNs. Right-click a LUN to view the LUN menu. Use this menu to manage individual LUNs.

Filter	Restrict the DMC view to only the Cryptainers and hosts associated with the selected LUN.
Show Alternate Paths	View all paths to the device.
Create Cryptainer	Create a Cryptainer on the LUN. See Options When Creating a Cryptainer for a Storage Collection on page 91.
Map, Unmap	Map a disk to a Cryptainer or remove a mapped disk. See Map Disk to Cryptainer on page 105.
LED	Blink the LED on the physical disk to help identify it in the rack. This is intended for disk use only.
Export Trustee Keys	Key export allows the Cryptainer key for this LUN to be exported to a trustee. See Managing Trustees on page 118.
Restore Cryptainer	Restore Cryptainer allows DataFort to restore a deleted Cryptainer. Obtain the port and LUN information for the Cryptainer to restore. Select the device onto which to restore the Cryptainer and select Restore Cryptainer. The Restore Cryptainer page appears. Select the key (using the Cryptainer Key ID information you have for the original Cryptainer). Select Port or LUN Mapping and click Restore. This feature is intended for disk use only.
Replace	Replace a disk with a new one. See Replace Disk on page 105.
Edit	Change the device name, the Host Port WWN, and the FC site name of the DataFort HBA where the storage device was discovered. See Edit Disk on page 105.
Delete	Remove the LUN from the DMC. The device is not deleted from the storage device.

MAP DISK TO CRYPTAINER

Right-click a LUN and select Map Disk. Alternatively, select a Cryptainer in the Cryptainer pane, then right-click a LUN and select Map Selected. Options to map a disk include:

Cryptainer Record ID	Specify the record ID of the Cryptainer to map to the disk. The Cryptainer Record ID can be obtained by selecting a Cryptainer in the Cryptainer pane. It is then displayed in the lower pane.
FC Site Name	Displays the FC site name of the DataFort HBA where the disk was discovered.
Host Port WWN	Specify which virtualized host port WWN can see the LUN.

REPLACE DISK

Options to replace a disk include:

Disk Port WWN	Enter the Port WWN of the new disk.
LUN	Enter the LUN of the new disk.
Host Port WWN	Specify which virtualized host port WWN can see the LUN.

EDIT DISK

Options to edit a disk include:

Disk Name	Change the name of the disk displayed in the DMC.
Host Port WWN	Specify which virtualized host port WWN can see the LUN.
Discovering FC Site Name	Displays the FC site name of the DataFort HBA where the disk was discovered.

MANAGING TAPE POOLS

Select **Topology > Hosts and Backup Pools** to view the Hosts and Backup Pools tab. This menu option is only available if a license controlling tape features is installed on DataFort. The Pool Management Pane features the following elements:

Pools Pane Menu	Right-click in the Pools pane to use the top level menu. See Pools Pane Menu on page 106.
Pool Collection Menu	Right-click a pool collection to use the collection menu. See Pool Collection Menu on page 107. A pool does not display the tapes it includes until encrypted data has been written to the tapes in that pool.
Individual Tape Pool Menu	Right-click a tape pool to view the tape pool level menu. See Tape Pool Menu on page 108.
Individual Tape Menu	Right-click a tape to view the tape level menu. See Tape Menu on page 108.
Individual Tape Device Icons	The icons in the DMC indicate the condition and type of tape device. A red X indicates offline status, a yellow alert indicates a problem. A problem may be caused because host authentication failed. For more information click the Icon Legend link at the bottom right on the Hosts and Devices tab or see DataFort DMC Icons on page 96.

POOLS PANE MENU

Right-click in the Pools pane to see the Pools pane menu. Use this menu to manage the Pools display.

Refresh	Refreshes the list of tape pools.
Expand, Collapse	Expand or collapse the tape pools tree.
Add Pool Collection	Create a new tape pool collection.
Add Pool	Create a new pool for tapes. See Add Pool Screen on page 107.
Export/Import Trustee Keys	Export/import keys between Trustees. See Importing and Exporting Keys on page 127.
Tape Settings	Configure pool and tape storage related settings. See Managing Tape Settings on page 110.

ADD POOL SCREEN

Right-click in the Pools pane and select Add Pool to see new tape pool options.

Label	Enter the label for the new pool.
Name	Enter the alias of the pool as it is displayed in the DMC.
Key Policy	Select whether the key policy used by this pool is the one set for tapes or for the pool. These policies are defined on the Tape Settings page of the DMC. See Managing Tape Settings on page 110.
Encryption	If enabled, data written to this pool is automatically encrypted. If disabled, data remains in cleartext. The pool can then be manually rekeyed to enable encryption.
Key Lifespan	Set the lifespan of the key assigned to tapes in the pool. Lifespan represents the span that the key may be used for reading. Lifespan can be specified in days, months, weeks or years. By default the lifespan of a key is infinite. Lifespan settings should be set only if key expiration is desired. This option is not available when keys are generated per pool.
Key Read/Write Span	Sets the read/write life span of the key used to encrypt tape contents. Read/write represents the span that the key may be used for writing. Lifespan can be specified in days, months, weeks or years. By default the lifespan of a key is infinite. Lifespan settings should be set only if key expiration is desired. This option is not available when keys are generated per pool.

POOL COLLECTION MENU

Right-click a tape pool collection to view the tape pool collection menu. Use this menu to manage collected tape pools. A pool will not display the tapes it includes until encrypted data has been written to the tapes in that pool. If a tape is moved from one pool to another by the application, only the current location of the tape is displayed in the DMC once encrypted data is written to the tape.

Add Pool	Add a new pool to the collection. See Add Pool Screen on page 107.
Access	Grant or revoke host access to the tape pool collection. Select a host in the Hosts pane, then right-click a pool collection and select Access Grant/Revoke Selected to grant/revoke access. Alternatively, without selecting a host, grant/revoke access by selecting the desired hosts from the Access Grant/Revoke host lists.
Edit	Change the pool collection name.
Delete	Remove the pool collection from the DMC. All pools must be deleted before the pool collection can be removed.

TAPE POOL MENU

Right-click a tape pool to view the tape pool menu. Use this menu to manage tape pools.

Access	Grant or revoke host access to the tape pool. Select a host in the Hosts pane, then right-click a pool and select Access Grant/Revoke Selected to grant/revoke access. Alternatively, without selecting a host, grant/revoke access by selecting the desired hosts from the Access Grant/Revoke host lists.
Set Pool Key	A key is assigned to each media pool discovered by or assigned to DataFort. For pools which encrypt per-pool, the key is used to encrypt any data assigned to the pool and is consistent throughout a single tape. For pools which encrypt per-tape, this key is not used for data encryption but rather as a placeholder to keep track of default key attributes for per-tape keys originating from this pool. Note that cleartext cannot be appended to ciphertext on an encrypted tape, nor can ciphertext be appended to a cleartext tape. See Mixed-Tape Mode Rules on page 112.
Move To	Move the selected pool to a specified collection.
Edit	Change the pool name, Key Policy, and key lifespan. See Edit Pool Screen on page 109.
Export Trustee Keys	Export the Cryptainer key for this LUN to a trustee. See Managing Trustees on page 118.
Delete Tapes	Right-click the pool and select Delete Tapes to remove the tapes associated with the pool from the DMC, but leave the pool.
Delete	Right-click the pool and select Delete to remove it from the DMC. All tapes must be deleted before the pool can be removed.

TAPE MENU

Right-click a tape to view the tape menu. Use this menu to manage individual tapes.

Export Trustee Keys	Export the Cryptainer key for this LUN to a trustee. See Managing Trustees on page 118.
Delete	Right-click the tape and select Delete to remove it from the DMC.

EDIT POOL SCREEN

Right-click a pool and select Edit to see Pool management options.

Name	Change the alias for the pool as it is displayed in the DMC. Note this does not change the actual pool label which DataFort uses to sync with the backup application.
Key Policy	Select whether the key policy used by this pool is the one set for tapes or for the pool. These policies are defined on the Tape Settings page of the DMC. See Managing Tape Settings on page 110.
Key Lifespan	Set the lifespan of the key assigned to tapes in the pool. Lifespan represents the span that the key may be used for reading. Lifespan can be specified in days, months, weeks or years. By default the lifespan of a key is infinite. Lifespan settings should be set only if key expiration is desired. This option is not available when keys are generated per pool.
Key Read/Write Span	Set the read/write life span of the key used to encrypt tape contents. Read/write represents the span that the key may be used for writing. Lifespan can be specified in days, months, weeks or years. By default the lifespan of a key is infinite. Lifespan settings should be set only if key expiration is desired. This option is not available when keys are generated per pool.

MANAGING TAPE SETTINGS

Access the **Tape Settings** screen to configure pool and tape storage related settings. A key is assigned to each media pool discovered by DataFort. DataFort pool and tape settings determine how auto-detected tapes and pools are managed by default. This menu option is only available if a license controlling tape features is installed on DataFort.

1. Access the Tape Settings page by selecting **Topology > Tape Settings**.
The page can also be accessed from the **Hosts and Backup Pools** tab of the DMC:
 - Right-click in the Pools pane and select Tape Settings.
2. Select the desired setting and click Apply to set the changes. Tape settings include:
 - [Pool Defaults](#)
 - [Tape Settings](#)
 - [Key Settings](#)

POOL DEFAULTS

DataFort allows access control for tapes to be set by pool, and supports pool types including auto-detected pools and host default pools.

Auto-detected pools are found during backups as data from tape block 0 is parsed for media and pool labels. The media and pool information is passed from kernel to management and stored in the database. Auto-detected pool labels match the application pool label.

Host Default Pools are used when DataFort cannot parse pool information from the tape block 0 data. If the media ID is detected, it is recorded in the tape history along with the host default pool label.

Cleartext	Determines whether pools that are automatically detected by DataFort are encrypted or not by default.
------------------	---

Global Default Pool

The global default pool allows a single pool to be set across all hosts for applications which do not support pools. To use this feature:

1. Log in to the DataFort CLI.
2. Override the application pools which are auto-detected in DataFort by running the following command:


```
system property set dfc.override_with_default_pool true
```
3. Create a default pool with the global pool properties:


```
system property set dfc.default_pool_name <pool-label>
```
4. Create a default pool by specifying pool properties:


```
pool add [--policy ] [-n, --nokey] [--aclstate ] [--days ] [--rw-days ]
```

5. Assign the new pool as the default pool:

```
system property set dfc.default_pool_name <pool-label>
```

- To change a default pool set the system property to another pool name.
- To roll the pool key for a global default pool:

```
pool key set [-n, --nokey] [-k, --pk-id ] [--days ] [--rw-days ]
global default pool name
```

The previous pool key is saved in the pool key history table (viewable by running the command: `pool key history`) and may be used for reads and appends to tapes created prior to the pool update.

- To return to normal pool mode:

```
system property set dfc.override_with_default_pool false
```

Using Global Default Pool and Exception Pools

It is possible to use both a global default pool as well as specific application pools. To create additional pools with application-specific pool names:

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

```
pool add [--policy ] [-n, --nokey] [--aclstate ] [--days ] [--rw-
days ] <pool-label>
```

A backup to a pool unrecognized by the DataFort appliance uses the global default pool. A backup to a specific pool recognized by the DataFort appliance uses this pool instead.

TAPE SETTINGS

The Tape settings section determines whether ACL learning and Compression are on or off by default.

ACL Learning

By default ACL learning mode is enabled, which allows DataFort to monitor backup activity on the network and record which devices have access to storage. When ACL learning is turned off, only the hosts which had access when learning mode was on is allowed to access storage.

Compression

If compression is enabled, DataFort compresses data sent to tape, depending on host settings to the tape drive. If the host sets the drive to compress, DataFort compresses data. If the host disables compression on a drive, DataFort does not compress data to that tape drive.

Compressed data takes up less tape space and is written faster than the original uncompressed data. Some tape systems automatically compress all data written to tape, however because encrypted data is not compressible, DataFort offers its own compression option.

Decru recommends to continue using the compression functions of the backup software and tape library. Both DataFort and application or tape library compression must be set ON if compression is desired.

KEY SETTINGS

DataFort allows access control for tapes to be set by pool, and supports pool types including auto-detected pools and host default pools.

Auto-detected pools are found during backups as data from tape block 0 is parsed for media and pool labels. The media and pool information is passed from kernel to management and stored in the database. Auto-detected pool labels match the application pool label.

Host Default Pools are used when DataFort cannot parse pool information from the tape block 0 data. If the media ID is detected, it is recorded in the tape history along with the host default pool label.

Key Policy

Determines whether keys are generated per tape or per pool by default. Select Keys Per Tape to manage key life spans.

Key Lifespan

Set the lifespan of the key assigned to tapes in the pool. Lifespan represents the span that the key may be used for reading. Lifespan can be specified in days, months, weeks or years. By default the lifespan of a key is infinite. Lifespan settings should be set only if key expiration is desired. This option is not available when keys are generated per pool.

Key Read/Write Span

Set the read/write life span of the key used to encrypt tape contents. Read/write represents the span that the key may be used for writing. Lifespan can be specified in days, months, weeks or years. By default the lifespan of a key is infinite. Lifespan settings should be set only if key expiration is desired. This option is not available when keys are generated per pool.

MIXED-TAPE MODE RULES

As a general rule, DataFort does not support mixed-mode tapes, therefore tapes written through DataFort are either all cleartext or all encrypted. Should a backup job violate these rules (for example attempt to append encrypted text to an existing cleartext tape), DataFort does not allow it and the backup fails. Depending on the state of a pool, the following rules apply:

TABLE 12: MIXED-MODE TAPE RULES

Pool state	Tape state	Cleartext append	Encrypted append
Cleartext	Cleartext	Allowed	Not allowed
Cleartext	Encrypted	Not allowed	Allowed
Encrypted	Cleartext	Not allowed	Not allowed
Encrypted	Encrypted	Not allowed	Allowed

MANAGING SAN STORAGE SETTINGS

To configure the way DataFort HBAs work on the SAN:

1. Access the SAN Storage Settings screen by selecting **Topology > SAN Settings**.
2. Select the desired SAN Storage Settings. See [About SAN Storage Settings](#) on page 114.
3. Click Apply.
Keep in mind the following:
 - Any paths set through DataFort virtual ports before changing the virtualization mode become inaccessible.
 - After changing virtualization settings DataFort prompts for a reboot.
 - When in Single ID mode, some unsupported settings in the DMC are greyed out.

About SAN Storage Settings

Host Virtualization

Enabled: Virtualize up to 7 storage devices on the DataFort host-side HBA and operate the HBA in Multi ID mode. This allows retaining the existing storage device LUN configuration by mapping the storage devices to the virtual WWNs (ports) presented on the DataFort host-side HBA (referred to as port mapping).

Optional: Port forwarding allows presenting the virtual storage devices on the host side with the same WWN as the original storage device. However, since duplicate WWNs are being used, the Fibre Channel switch must use port zoning, or the DataFort host and storage HBAs must be on different fabrics to avoid conflicts.

Disabled: The DataFort host-side HBA operates in Single ID mode. Multiple storage devices can be presented on the host-side HBA but all on the same DataFort target HBA WWN (port). With only one storage device, the LUNs can stay the same. With multiple storage devices the real LUNs must be mapped to non-matching virtual LUNs (referred to as LUN mapping).

Storage Virtualization

Enabled: Virtualize up to 7 host devices on the DataFort storage-side HBA and operate the HBA in Multi ID mode. This allows the storage to continue differentiating between hosts.

Optional: Port forwarding allows presenting the virtual hosts on the storage side with the same WWN as the original host. This means no changes are necessary to the storage device LUN masking configuration. However, since duplicate WWNs are being used, the Fibre Channel switch must use port zoning, or the DataFort host and storage HBAs must be on different fabrics to avoid conflicts.

Disabled: The DataFort storage-side HBA operates in Single ID mode. Multiple hosts are presented as one single host on the DataFort storage-side HBA.

For more information about Virtualization, see [Virtualization Settings](#) on page 115.

VIRTUALIZATION SETTINGS

Virtualization can be turned on or off for any DataFort port using the SAN Storage Settings screen of the DMC. Virtualization settings determine whether DataFort presents its own WWNs or those of another device. DataFort can virtualize storage devices to the hosts and/or host devices to the storage. The maximum number of devices that can be virtualized in either direction is seven.

The DataFort Host and Storage HBA ports are NL-Ports, allowing virtualization on the host and storage sides of the fabric. The SAN Storage Settings page allows virtualization to be turned on or off for DataFort HBAs, depending on the environment in which DataFort functions.

When using virtualization, the DataFort appliance port presenting the virtualized devices must be plugged into a port supporting FCAL (Fibre Channel Arbitrated Loop). Virtualization requires multiple devices to be presented on one physical port. When using virtualization, verify that the DataFort appliance has logged in as a Loop port.

A DataFort HBA with virtualization OFF operates in Single ID mode, while a DataFort HBA with virtualization ON operates in Multi ID mode. This setting defines the number of WWNs (IDs) presented by the DataFort port. If the Host Port is in Multi-ID mode, this allows DataFort to represent itself as multiple devices, each with a distinct WWN.

The suggested settings for different environments are:

Tape configurations It is recommended to enable virtualization for the Host HBA, and disable it for the Storage HBA on a DataFort in most tape configurations. This is the default setting for DataFort. This setting also supports the use of switch models which do not allow NL-port logins. When virtualization is disabled, the DataFort HBA logs in to a switch in fabric mode.

Disabling virtualization on the Storage HBA allows DataFort and tape drives to maintain connectivity if tape becomes busy for long periods of time.

Enabling virtualization for the Host HBA allows features such as Port Mapping to be used to create Cryptainers (see [Options When Creating a Cryptainer](#) on page 94).

Disk configurations It is recommended to enable virtualization for both the Host HBA and Storage HBA of a DataFort in most disk configurations. Enabling virtualization allows the full range of DataFort features to function.

When virtualization is enabled, DataFort logs in to a fabric switch as an NL-port. This allows DataFort to present virtual WWNs to the initiators connected to it. Only when virtualization is enabled can Port Mapping be used to create Cryptainers (see [Options When Creating a Cryptainer for a Storage Collection](#) on page 91).

Note: It may be necessary to disable virtualization on both HBAs if connecting to a switch that does not support loop logins, or in a situation where a specific hardware configuration problem needs to be addressed.

RESTORING A CRYPTAINER

Each Cryptainer is assigned an ID in the DataFort configuration database. This Cryptainer ID is the record ID for the Cryptainer object. A Cryptainer that has been deleted from the DataFort configuration database can be restored using the Cryptainer ID and DataFort's restore features (Cryptainers created on disk only).

Note: No more than one instance of a particular Cryptainer can exist simultaneously (it is not possible to restore the same Cryptainer to multiple places at once).

A Cryptainer restore requires the following:

- The original encrypted data and the port and LUN information of the original Cryptainer location.
- The Cryptainer ID.
- A DataFort that remembers the original Cryptainer. DataFort stores information about Cryptainers in the configuration database indefinitely, even if the Cryptainers are deleted (unless they are purged when backing up to LKM, in which case LKM recovers the Cryptainer information). Any DataFort using the configuration database that contains information about the original Cryptainer works.

RESTORING A CRYPTAINER VIA DMC

1. In the DMC, right-click the device LUN onto which to restore the Cryptainer. Select **Restore Cryptainer > LUN Mapped** or **Port Mapped** depending on the desired mapping method. For more information about Port and LUN Mapping see [About Port and LUN Mapping](#) on page 90.
2. Select the desired Cryptainer restoration options. See [Restore Cryptainer Options](#) on page 116.
3. Click Apply.

Restore Cryptainer Options

Cryptainer Key ID	Click Select to see a list of Cryptainer keys that can be assigned to the Cryptainer when it is restored. Select the correct Cryptainer key (using the Cryptainer ID information for the original Cryptainer) and click Apply.
Cryptainer Description	Enter an optional description.
Host Port WWN	Specify which virtualized host port WWN can see the LUN.
Port Forwarding (off by default)	If set to ON, the virtual port created for a port mapped Cryptainer has the same exact WWN as the disk's Cryptainer. If this feature is used, it is recommended that the host side and storage side HBAs of the DataFort be on separate fabrics, or that port zoning be used on the FC switch.

10 KEY ADMINISTRATION

The DataFort appliance can archive encryption keys to LKM appliances and share encryption keys with other appliances.

Archiving encryption keys to LKM appliances allows the DataFort appliance to back up keys as a safety precaution as well as purge unused keys from its key database. For details about archiving keys to LKM appliances see the [LKM Appliance Administration Guide](#).

Sharing keys with other appliances allows multiple DataFort appliances to use the same encryption key which is useful in certain scenarios. This is done by creating trustee relationships between appliances. For details about setting up and using trustees see the following topics in this chapter:

- [Managing Trustees](#)
- [Importing and Exporting Keys](#)

MANAGING TRUSTEES

A trustee is a remote DataFort with which a trust relationship has been formed, allowing encryption keys to be shared. Creating trustees allows encryption keys to be shared between DataFort appliances that have no Recovery Cards in common, and may not even be on the same network.

A trustee may import keys from or export keys to another trustee. Imported keys cannot be exported once they are imported. Trustees send messages to establish a relationship before key sharing. The first message in setting up a trustee relationship is the Trustee Establishment Package (TEP). The second message, a response to a TEP, is the Trustee Acceptance Package (TAP).

Once trustee setup is complete, encryption keys are shared via a Link Key, which is similar to a Domain Key. The Link Key lives only in hardware, and keys are moved by DataFort. Recovery Cards are only required during trustee setup.

TRUSTEE SCENARIOS

The establishment of trustees enables several enterprise scenarios:

- | | |
|-------------------------------|--|
| Disaster Recovery Site | Used in a situation where there is a DataFort appliance offsite, and it is not desirable to form a cluster to share key data (either because there is no network connectivity between the main and offsite location, or because the topology is different at the remote site). |
| HQ with branches | Used in a situation where there are many branch offices and it is desirable to share a different encryption key with each branch exclusively. |
| Vendors/Third parties | Used in a situation where a vendor and supplier both have DataFort appliances, but it is not desirable to share all keys. |

SETTING UP TRUSTEES

This example describes a trustee relationship between a main and a remote site. Setting up trustees requires:

- A Full Administrator for each appliance.
- The quorum of Recovery Officers and their Recovery Cards for each appliance. If the Security Setup requires 2 out of 5 cards, for example, two people have to be present to insert their cards and enter the label name and password for the card, in order to establish trustees.
- Each DataFort appliance that will become a trustee must have a valid System Card inserted during trustee setup.
- Files and information will need to be provided by the main site administrator so that the remote site administrator can import the trust package.

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 Decru Management Console, 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 119.
 - To authorize trustees using Remote Authorization, see [Initiating Remote Authorization to Approve TEP](#) on page 120.

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 the 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 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.

2. 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 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 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 Trustee screen, when 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, Decru recommends the administrator be the last Recovery Officer to supply a card.

2. When the Remote Authorization enabled message appears, close the Approve TEP screen. 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 120.

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

Authorizing TEP Approval Remotely

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

Note: When a card is inserted into the reader it 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 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 as the last officer to supply a card automatically initiates the TAP approval process. See [Initiating Remote Authorization to Approve TAP](#) on page 121.

Initiating Remote Authorization to Approve TAP

1. In the Decru Management Console, 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](#) on page 121.

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

Authorizing TAP Approval Remotely

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

Note: When a card is inserted into the reader 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.

4. 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.
5. 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 different 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 TEP](#)
- [Receive TAP](#)
- [Delete Unapproved TAP Trustee](#)

Start Trustee Creation (Create TEP)

1. In the Decru Management Console, in the appliance tree, select the first appliance.
2. From the Trustee menu, select Start Trustee Creation.
3. On the Start Trustee (Create TEP) screen, enter the following and click Create.
 - A Trustee Label or hostname for the appliance.
 - A Package Label or hostname for the package.
4. On the Select File screen, 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 method to securely authenticate trustees for key sharing.

Receive TEP

To receive the TEP (Trustee Establishment Package), the second appliance needs the TEP file and verifier received from the first appliance. See [Start Trustee Creation \(Create TEP\)](#) on page 122.

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

1. In the Decru Management Console, in the appliance tree, select the second appliance.
2. From the Trustee menu, select Receive TEP
 - If the administrator has previously initiated remote authorization, a prompt appears. Click yes to interrupt or no to quit the trustee link authorization.
3. On the Receive TEP screen enter the following:
 - Browse to the path of the TEP file to open it.
 - Paste the verifier text string from your saved text file.
 - A Trustee Label or hostname for the appliance.
 - A Package Label or hostname for the package.

4. Click Begin Approval.
5. Select a method to authorize trustees:
 - To authorize trustees locally, see [Authorizing TEP Approval Locally](#) on page 123.
 - To authorize trustees using Remote Authorization, see [Initiating Remote Authorization to Approve TEP](#) on page 124.

Authorizing TEP Approval Locally

1. On the Approve TEP (Trustee Establishment Package) screen, select from the following:
 - For multiple card readers, insert the 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.

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

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

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, Decru recommends the administrator be the last Recovery Officer to supply a card.

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 124.

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

Authorizing TEP Approval Remotely

1. In the Decru Management Console, in the appliance tree, select an appliance.
2. From the Trustee menu, select View Unapproved Trustees.
3. On the View Unapproved Trustees tab, right-click the trustee and select Approve TEP and Create TAP.
 - If the administrator has previously initiated remote authorization, a prompt appears. Click yes to interrupt or no to quit the trustee link authorization.
4. On the Approve TEP package screen, enter the package name and click Approve.
5. On the Approve TEP recovery card screen, insert a card into the card reader, enter the password and click Start.

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.

6. 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.
7. On the Select File screen, select a TAP file name and location and click Save.
8. While on the View Unapproved Trustees tab, select **View > Refresh** to update the trustee verifier.
9. Right-click the trustee and select Copy Verifier.
10. Paste the verifier into a text file and save it.
11. Send the verifier file and the TAP file separately to the first appliance. See [Receive TAP](#) on page 125.

Note: Communicate the verifier in a secure manner, by phone or direct contact rather than email. This is the only method to securely authenticate 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 122.

1. In the Decru Management Console, 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. Select a method to authorize trustees:
 - To authorize trustees locally, see [Authorizing TAP Approval Locally](#) on page 125.
 - To authorize trustees using Remote Authorization, see [Initiating Remote Authorization to Approve TAP](#) on page 125.

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

Authorizing TAP Approval Locally

1. On the Approve TAP screen, select from the following:
 - For multiple card readers, insert the 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 and selected (green), enter the password and click the Verify Password button. Cards remain selected after removal.

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

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

Note: When the first appliance approves the TAP, it is recommended they notify the second appliance so that they can delete the unapproved TAP trustee. See [Delete Unapproved TAP Trustee](#) on page 126.

Initiating Remote Authorization to Approve TAP

1. On the Approve TAP screen, select a quorum of cards from the Recovery Officers list and click Enable Remote Authorization.

Note: If the administrator initiating the remote authorization process is a Recovery Officer, Decru recommends the administrator be the last Recovery Officer to supply a card.

2. 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](#) on page 126.

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

Authorizing TAP Approval Remotely

1. In the Decru Management Console, in the appliance tree, select the first appliance.
2. From the Trustee menu, select View Unapproved Trustees.
3. Right-click a column title.
4. In the Column Editor screen, add the State column, then click OK.
5. On the View Unapproved Trustees tab, right-click the trustee with the state tap_received and select Approve TAP.
6. On the Approve TAP package screen, click Approve.
7. On the Approve TAP recovery card screen, insert a 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. 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.
9. 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 Unapproved TAP Trustee](#).

Delete Unapproved TAP Trustee

The first appliance should approve the TAP before the second appliance deletes the unapproved TAP trustee. This retains a backup TAP trustee file until the process is complete. See [Receive TAP](#) on page 125.

1. In the Decru Management Console, from the appliance tree, select the second appliance.
2. From the Trustee menu, select View Unapproved Trustee.
3. On the View Unapproved Trustee tab, right-click the trustee and select Delete.
4. When prompted, click Yes to confirm.

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

IMPORTING AND EXPORTING KEYS

Once a trustee relationship is established it is possible to transfer keys between the two DataFort appliances using the import and export key options of the DMC.

Exporting a Key

1. In the Decru Management Console, from the appliance tree, select the exporting DataFort appliance.
2. Select **Topology > Hosts and Devices or Hosts and Backup Pools**.
3. Select the LUN, pool, or tape which will have its key exported.
4. Select **Trustee > Export Trustee Keys**.
5. From the drop-down list, select the trustee that the key will be transferred to and click Apply.
6. When prompted, download a .kdf file.
7. Transfer the saved .kdf file via email, FTP, disk or other method to the other cluster location.

Importing a Key

1. At the importing DataFort, select any storage device or pool.
2. Select **Trustee > Import Trustee Keys**.
3. When prompted, upload the .kdf file. Once this file is uploaded the key is known to the DataFort appliance.

■ ■ ■ ■ 11 BACKUP ADMINISTRATION

The DataFort configuration database contains all relevant information about the secure network. This configuration database can be downloaded to a remote location at any time using the DMC. A downloaded configuration can be applied to a new or zeroized DataFort in order to restore the configuration. It is crucial to back up the configuration database any time a change is made to DataFort configuration. Failing to back up the database after making changes to the configuration can result in lost data.

A specified Backup Administrator or a Full Administrator can perform backups:

- [Saving Configurations to Lifetime Key Management](#)
- [Backing Up Configurations to a Remote Location](#)

Note that while a Backup Administrator can send backups to LKM, only a Key Administrator or a Full Administrator can configure backups to LKM.

Note: Do not use the LKM Settings page of the DMC to configure backups to an LKM appliance. Refer to the [LKM Appliance Administration Guide](#) for instructions.

SAVING CONFIGURATIONS TO LIFETIME KEY MANAGEMENT

The LKM appliance or LKM server software manages keys for one or more DataFort appliances, consolidating all encryption key information, for the purpose of emergency data recovery. LKM keeps all encryption keys even if the original keys are purged from DataFort or the source DataFort is decommissioned. LKM maintains an encrypted copy of all encryption keys, providing a single key management and data recovery solution for the cluster. See the [LKM Appliance Administration Guide](#) for more information.

In order to configure DataFort to back up the configuration database to LKM automatically, link DataFort to the LKM appliance or server. DataFort then backs up configuration changes automatically every hour. The configuration can also be backed up to LKM manually.

BEST PRACTICES FOR SECURE BACKUPS

Only a single copy of the most recent backup of a database should exist. The backup should be retained and destroyed per the organization's security policy.

- The system is designed to ensure that rollbacks to prior state is not possible.
- Only a single copy of the most recent LKM database must exist.
- Store this backup in conformance with organizational retention guidelines.
- Old copies must be considered sensitive and must be shredded in conformance with media shredding guidelines.
- Backups must not be transmitted over channels that retain data. Email must not be used but SSH can be used.
- DataFort should not back up keys in any other form other than sending them to LKM.
- DataFort can connect to a maximum of 4 LKM peers (software or appliance).

CONFIGURING BACKUPS TO LKM APPLIANCE

To back up the DataFort configuration to one or more LKM appliances, first establish a link by selecting a key sharing policy. For more details about linking DataFort to an LKM appliance and configuring backups, see the [LKM Appliance Administration Guide](#).

CONFIGURING BACKUPS TO LKM SOFTWARE

Use this procedure to set up regular automatic backups to LKM software.

DataFort supports up to four servers for the LKM system. Backups will be sent to all LKM servers at the same time. Enter the IP addresses for each LKM server as described below. DataFort supports automated configuration backups to four LKM servers.

Note: The following steps can be repeated four times to support up to four LKM servers

1. Log in to a DataFort appliance via DMC.
2. With the appliance selected from the appliance tree, select **Appliance > Link LKM Software**.
3. Enter the IP address of the server on which LKM software is running
4. Enter the port number that the LKM server is listening on. For more information about LKM software configuration, see the [Lifetime Key Management Server Software Administration Guide](#).
5. Enter the password for the LKM server.
6. Click Apply.

BACKING UP THE CONFIGURATION TO LKM

Use this procedure to perform a manual backup to LKM.

1. Select **Utilities > Back up Appliances to LKM**.
2. Click Apply.

The configuration is sent to the LKM server, connecting to the ports configured on the LKM Settings page, and using SSL if that option was selected. When backing up to LKM manually, unused keys can be purged from the DataFort appliance.

KEY PURGING

Keys are automatically backed up to LKM when LKM is in use. After backing up to LKM manually or automatically, the administrator has the option to purge keys by selecting **Keys > Purge Unused Keys**. This removes unused keys from the DataFort database, and stores them only in LKM.

Only keys that are no longer current (meaning they are not assigned to tapes, pools or Cryptainers) are allowed to be purged. The tape or storage device that originally used the key must have been removed from the configuration. If a tape is overwritten with a different encryption key, then the previous key can be purged. If there is more than one LKM server defined for a cluster, all servers must have the key present before the purge is allowed.

In a large installation, it is a good idea to check the size of the configuration database using the CLI command **db size**. This command returns a table of entries and a percent full number. Should the database be more than 75% full, consider purging keys. Use the **keyman purgekeys** command to specify which keys are purged at backup. Use the **keyman purgekeys start -a** command to define the age of the keys to be purged in days.

The tape settings policy in use affects the frequency with which keys may need to be purged. Table 13 on page 130 outlines the relationship between tape settings and key generation. See [Managing Tape Settings](#) on page 110 for information about tape settings.

TABLE 13: TAPE POLICY AND KEY PURGING

Tape Policy	Key Creation Rules	Purge Recommendations
Per-Pool Policy	Tapes are created using the same key as the pool key. LKM traffic should be minimal in this case since there will be very few keys generated over time. Normally the new pool keys will either be created in advance for each pool or auto-created as backups are run. Key expiration is not supported in this mode.	Purging may not be needed.
Per-Tape Policy	Tapes are created with a unique key. The main reason for this is to support key expiration and deletion. Expect much higher numbers of keys in the cluster in this mode. Given a backup window of 12 hours per day with an 8-node cluster, 3 LTO-2 drives each, running at full speed (70MB/s) assuming a tape capacity of 400GB at 2:1 compression this will yield about 1 key every 10 minutes within the cluster.	Based on the number of tapes in use, consider how many keys will be generated in a given time window, and plan to purge keys when the 8000 key limit is being approached.

TABLE 13: TAPE POLICY AND KEY PURGING

Tape Policy	Key Creation Rules	Purge Recommendations
Host Default Pools	In the case where the pool information is not detected in the tape volume header, DataFort uses host default pools. For best results, all media servers should be grouped into a single host group and assigned a common pool at the group level. This way all tapes will be encrypted with the same key. Key expiration and deletion are not supported. If this is not done, and the pools are auto-created, each host will be assigned by DataFort to a HOSTWWN_Pool which will be assigned a different key from the other hosts. If there are pre-existing host default pools they can be assigned the same key.	Purging may not be needed.

BACKING UP CONFIGURATIONS TO A REMOTE LOCATION

Use this procedure for a manual backup to a designated location. Download the DataFort configuration to a remote location any time a major change is made to the configuration. Save the configurations in a secure, accessible location in case recovery is needed.

1. Log in to a DataFort appliance via the DMC.
2. With the appliance selected from the appliance tree, select **Utilities > Backup**.
3. Determine a secure remote location for the backup copy of the configuration database.
4. Save the backup.

■ ■ ■ ■ 12 MANAGING APPLIANCE SECURITY

This chapter describes various security related functions after initial appliance setup. It contains the following topics:

- [Managing Appliance Defense Responses](#)
- [Configuring Management Security Settings](#)
- [Managing Recovery Officers and Recovery Cards](#)
- [Resetting Smart Cards](#)
- [Setting Date and Time](#)
- [Configuring and Viewing Logs](#)
- [Zeroizing Appliances](#)
- [Setting Security Certificates](#)

MANAGING APPLIANCE DEFENSE RESPONSES

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

DEFENSE TRIGGERS AND RESPONSES

A defense response can be triggered by the following:

- | | |
|---------------------------|---|
| Chassis Intrusion | If the appliance chassis 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 | <p>If the appliance is left without power for a long time (more than 3 weeks) a defense response can be triggered.</p> <p>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 detection or notification. For this reason, a low battery triggers an intrusion alert.</p> |
| CryptoShred Button | If the appliance is equipped with a CryptoShred button, pressing the button activates the defense response. |

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

- The first response level disables the SEP and makes the DataFort appliance unusable for cryptographic operations. It is still possible to access management interfaces and view logs, but encrypted data is inaccessible. To resume normal operation and data access perform an administrative reset (see [Clearing a Defense Alert](#) on page 135).
- The second response level protects the data by automatically clearing all encryption keys in the DataFort. Recovery from this response requires zeroization and data recovery. When encryption keys are cleared (Medium and High levels) all encrypted data becomes immediately unusable. Zeroization is required before DataFort configuration can be restored.

WARNING: SELECT THE LOWEST LEVEL IF UNCERTAIN. THE DEFENSE LEVEL CAN BE INCREASED IN STRENGTH LATER IF IT SEEMS ADVISABLE, BUT NOT DECREASED.

DATAFORT DEFENSE SETTING

Defense levels are summarized in [Table 14](#). If in doubt, select the Basic level.

TABLE 14: DATAFORT 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. • CryptoShred button pressed. • Battery too low when system is powered on.	Encryption and decryption disabled.	After administrator determines the cause of the intrusion and resets DataFort.
Medium	When it is necessary to clear encryption keys in case of an intrusion but not if the battery is low.	Battery too low when system is powered on.	Encryption and decryption disabled.	After administrator determines the cause of the intrusion and resets DataFort.
		Internal chassis intrusion detected or CryptoShred button pressed.	Encryption and decryption disabled and encryption keys cleared.	After DataFort zeroization and restoration using Setup Wizard and Recovery Cards.
High	When it is necessary to clear encryption keys immediately at the possibility of intrusion, whether a physical intrusion or low battery.	• Internal chassis intrusion detected. • CryptoShred button pressed. • Battery too low when system is powered on.	Encryption and decryption disabled and encryption keys cleared.	After DataFort zeroization and restoration using Setup Wizard and Recovery Cards.

CHANGING THE DEFENSE SETTING

1. Log in to the appliance via DMC as a Full Administrator and select **Security > Defense**.
2. Select the desired defense level and click Apply.

CLEARING A DEFENSE ALERT

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

- On the front panel LCD
- On the main tab of the DMC
- On the **Diagnostics > Details** tab in the DMC
- After CLI login
- In the DataFort logs

After investigating the cause of the alert, and releasing the CryptoShred button if it has been pressed, the administrator can reset the appliance from the CLI or DMC.

If keys were cleared 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.

Resetting a Defense Alert via DMC

1. Select **Security > Clear Intrusion**.
2. Select the appliance(s) to clear alerts on.
3. Click Apply.
The appliance reboots, clearing the alert.
4. Close the connection to the appliance.

Resetting a Defense Alert via CLI

The CLI displays an alert after login.

1. Execute the `system tamper reset` command.
2. Execute the `system reboot` command.
Reboot the appliance as instructed to clear the alert.
3. Close the connection to the appliance.

CRYPTOSHRED BUTTON STATES

Some DataFort appliances come equipped with a CryptoShred button, which allows the DataFort appliance defense response to be automatically activated with one touch. There are two states for the button: normal and activated.

Normal State

In this state, the CryptoShred button is not depressed and DataFort operates normally. If the button is pressed once, the DataFort appliance defense response is triggered in accordance with the [DataFort Defense Settings](#). Recovery procedures can be completed by an administrator.

Activated State

Once the CryptoShred button has been pressed, DataFort remains in the defense response state until the button is pressed again to release it. As long as the button is depressed, recovery procedures are prevented.

SYSTEM CARD CRYPTOShRED

Data processing (encryption and decryption) can be halted manually on DataFort appliances that do not have the CryptoShred button by removing the System Card and turning off the appliance. If DataFort is rebooted without the System Card, attackers are prevented from accessing the cryptographic keys, rendering all data on protected storage devices unreadable. When the System Card is re-inserted and DataFort is rebooted, all data can be accessed normally.

1. Remove the System Card and store it in a safe place. To make it more difficult to access encrypted data after emergency shutdown, destroy or shred the card instead of storing it.
2. Power off DataFort by pressing the switch on the rear panel.

Emergency shutdown halts all encryption and decryption. Data remains encrypted and secure in storage, and cannot be decrypted unless the DataFort appliance is reactivated or replaced.

Restore Operation with System Card: To return DataFort to normal operations, re-insert the System Card into the front panel and re-power DataFort.

Restore Operation if System Card was Destroyed: To return DataFort to normal operations, DataFort has to be zeroized and reconfigured with the wizard and Recovery Officers. See [Zeroizing Appliances](#) on page 148. A new System Card has to be initialized. DataFort can be restored to the last configuration that was downloaded or backed up.

CONFIGURING MANAGEMENT SECURITY SETTINGS

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

Secure DMC

When enabled, a valid Admin Card is required to access the appliance via DMC. To allow access to the DMC without an Admin Card, disable this setting.

Secure CLI

When enabled, the administrator must log in to the appliance via DMC with an Admin Card in order to obtain a secure password that allows access to the CLI for appliance management. By default this option is disabled, and an administrator can log in to the CLI using only a valid name and password.

This setting does not apply to the DMC CLI.

1. In the DMC, select **Security > Management Security** to set the security policy according to the needs of the network.
2. Select the desired setting.
3. Click Apply.

MANAGING RECOVERY OFFICERS AND RECOVERY CARDS

Recovery Cards are not used in daily DataFort operation but they are essential for key and data recovery operations. Recovery Cards are initialized in sets, and each Recovery Card is associated with one Recovery Officer. If a Recovery Officer leaves the company or loses a Recovery Card, a quorum of Recovery Officers with their cards must assemble to initialize a replacement card and re-form the set. Changes made to a Recovery Card are replicated across the cluster.

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 cards in the 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 141.

REPLACING A RECOVERY OFFICER

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

1. In the Decru Management Console, from the appliance tree, select an appliance.
2. From the Security menu, select Replace Recovery Officer.
3. On the Replace Recovery Officer screen, click to select the card that will be replaced.
4. Insert the replacement card into the card reader and click Select, then click Authorize.

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

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

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

Repeat until all cards are processed.

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

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

6. On the Finish Replacement screen, insert the replacement card and enter the Card Label, security domain and password, then click Add Card.
 - If the card is already initialized, enter the security domain and/or password only and click Add Card.
7. When a message appears stating that the card has been replaced successfully, click OK.

CHANGING A RECOVERY CARD PASSWORD

Recovery Card password changes made on one cluster member are recognized by other cluster members automatically. Once changed, the new password is in effect for all clusters.

1. In the DMC, select **Security > Change Recovery Card Password**.
2. Insert the card for which the password will be changed into the Management Station smart card reader. 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.
5. Click Apply.

RESETTING SMART CARDS

The Decru Management Console includes smart card utilities that allow completely resetting a smart card and checking smart card versions and status.

WARNING: THIS PROCESS INVALIDATES THE CARD'S OLD SETTINGS AND RESETS IT FOR USE WITH A NEW INSTALLATION.

Resetting changes passwords to their defaults, and zeroizes all key material for secret sharing that resides on the card.

Do not reset a Recovery Card unless a quorum of Recovery Cards remains. Without a quorum, data recovery operations are not possible. Do not reset the only Admin Card for a Full Admin with authorizer privileges. Resetting is appropriate for redundant cards when there is a change of personnel. Additional blank smart cards are available from Decru.

1. In the DMC, select **Security > Smart Card Utilities**.
2. At the Smart Card Utilities screen, insert the card to be reset.
 - Click the Manufacturing Info button to show 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.

SETTING DATE AND TIME

Setting the appliance date and time is a security function, in part because time controls key expiration. To set the date and time:

1. Log in to an appliance via the DMC.
2. With an appliance selected from the appliance tree, select **Configuration > Date/Time**.
 - To change the current settings, enter the new date and time settings.
 - To use a time server, enter up to three full NTP server names (such as pool.ntp.org).
3. Click Apply.

CONFIGURING AND VIEWING LOGS

The appliance logs events in these categories:

- Security
- Operations
- Performance

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

- Temporary (RAM inside the appliance)
- Database (Appliance configuration database)
- Remote Logging Host (remote syslog server)
- Windows Event Log. See [Windows Event Logging](#) on page 145.

Note: It is recommended that logs be stored in more than one location. For an example of a secure logging configuration see [Recommended Configuration](#) on page 145.

For more information about logging, see [Logging Functions](#) on page 229.

APPLIANCE LOG STORAGE GUIDELINES

Keep in mind the following when configuring appliance logging:

- Decru recommends redirecting 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 syslog server configured to accept log data from the appliance.
- Decru recommends that critical operations 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 remain on the syslog host subject to its log rotation and storage policies.

DECRU SIGNED SYSLOG (DSS)

Log signatures can be turned on 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 syslog servers.

When Decru Signed Syslog (DSS) is enabled, the appliance adds metadata and a signature to each log message sent to a remote syslog server. The metadata and the signature can be used 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 syslog the source and timestamp are generated by the remote daemon and therefore cannot be trusted.

CONFIGURING LOG STORAGE

To configure the storage location for log information:

1. Select **Configuration > Log Configuration**.

Default settings are in effect until they are changed. To store log information remotely, indicate the storage location according to the instructions below.

2. Select the desired settings and then click Apply. Alternatively:
 - 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 and Enabling a Remote Storage Address

1. in the Remote Log Host box, enter an IP address or hostname for the machine that will be storing appliance log information.
2. Enter up to four separate servers, separated by commas, to configure the appliance to send logs to multiple locations.
3. If desired, activate Decru Signed Syslog (DSS) by specifying a remote syslog server and checking the Signed box.
4. Select the desired settings and then click Apply. Alternatively:
 - 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.

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
```

Recommended Configuration

Decru recommends configuring the appliance to send secure 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.

WINDOWS EVENT LOGGING

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

1. Select **Configuration > Log Configuration**.
2. Enter the following information about the user who will log 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 the box for each item to be logged.
Note: It is a 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.

Once configured, events from the appliance can be viewed on the Windows host by selecting **Administrative Tools > Computer Management > System Tools > 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 syslog 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

3. Signal the syslog daemon to start receiving messages from the appliance.

Syslog Mapping

[Table 15](#) shows the Descriptive Name, System Property Name, Syslog Facility and Level mapping for appliance logs.

TABLE 15: 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
performance low	sys.proc.syslogd.conf.perf_minor	local2.warning
performance high	sys.proc.syslogd.conf.perf_major	local2.info

Temporary Files Mapping

[Table 16](#) describes the mapping for temporary logs.

TABLE 16: TEMPORARY LOG MAPPING

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

VIEWING THE LOG

To view the appliance log:

- Select **Diagnostics > View System Log**.

To add and remove columns:

1. Right-click on a column title.
The Column Editor screen appears.
2. Select to add and remove columns.
3. Click OK.
 - Sort log entries by a particular column by clicking on its column title. Click the column title again to toggle sorting in ascending or descending order.
 - Select a log entry to view its full message details, displayed at the bottom of the pane.
 - Click Refresh to view new logs after making a change to the settings.

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, as indicated in [Recommended Configuration](#) on page 145) to verify that 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 187.

ZEROIZING APPLIANCES

Zeroizing DataFort appliances erases and invalidates all encryption keys in the system and erases all configuration information. Zeroization should always be followed either by running the Setup Wizard to assign a new configuration or by restoring a previous configuration. If a previous configuration is not restored, all existing key data from that configuration will be lost: Cryptainers will not be accessible and encrypted data will not be retrievable. The following procedures zeroize a DataFort appliance:

- [Zeroizing Using the DMC](#)
- [Zeroizing Using the CLI](#)
- [Zeroizing Using the Serial Console](#)
- [Emergency Serial Console Port Access](#)

When an appliance is zeroized, all key material is deleted from the appliance. Some key material may be recovered by selecting the recovery option of the Setup Wizard. Some keys are not recovered by running the wizard. The following table outlines the types of keys recovered during a restore:

TABLE 17: KEY RECOVERY AND ZEROIZATION

Key Type	Example	Recovered by Setup Wizard
Keys that protect user data	• Cryptainer keys • Parent keys which encrypt Cryptainer keys	Recovered using the wizard, in order to ensure data can be decrypted by the recovered DataFort.
Keys that authenticate one DataFort to another, or a DataFort to an end user	• SSL keys • SSH keys • IPsec keys	Not recovered, in order to prevent one DataFort appliance from falsely appearing to be a different DataFort appliance.
Secrets belonging to DataFort users	• User passwords	Recovered using the wizard, in order to allow the same users to access a recovered DataFort 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 HAVE BEEN PURCHASED, THEY WILL HAVE TO BE REPLACED.

BEFORE ZEROIZING

In order to protect against data loss, either decrypt encrypted data before zeroization and re-encrypt it with another DataFort, or back up the configuration database before zeroizing and restore the configuration from the backup after zeroizing. If the DataFort configuration was regularly backed up to LKM, LKM can provide a recent copy of the configuration database for recovery after zeroization.

Depending on the DataFort defense setting, 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.

If a standalone DataFort is zeroized, it can only be recovered using a backup copy of the configuration database. If the DataFort was in a cluster, the other cluster members will have retained all of the configuration information about the network.

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

ZEROIZING USING THE DMC

It may be necessary to back up the configuration database before zeroization is permitted. From the DMC, select **Utilities > Back up** and save the configuration to a secure location.

Note: If login to the DMC is impossible, zeroization can be performed using the CLI or serial console.

1. Be sure the System Card is inserted in the appliance.
2. In the Decru Management Console, from the appliance tree, select one or more appliance(s). Shift- or Ctrl-click to select multiple appliances.
3. From the Appliance menu, select 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.
6. If IP settings were not preserved by checking Keep IP address, assign the appliance IP settings as described in [Assigning the Appliance IP Address](#) on page 48.
7. Complete the configuration by running the Setup Wizard.

ZEROIZING USING THE CLI

In some situations it may be necessary to use the CLI to zeroize the appliance. Note that 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 as described in [Assigning the Appliance IP Address](#) on page 48.
7. Complete the configuration by running the Setup Wizard.

ZEROIZING USING THE SERIAL CONSOLE

If 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 47).
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 the Appliance IP Address](#) on page 48.
7. After the appliance has been assigned IP settings, complete the configuration by running the Setup Wizard.

EMERGENCY SERIAL CONSOLE PORT ACCESS

If all Admin Cards and passwords for an appliance are lost, it is not possible to log in to the DMC or CLI. It is still possible to connect to the appliance serial console using a valid Recovery Card from the set used when that appliance was initialized. This allows zeroizing and resetting the appliance.

1. Connect a Management Station or other PC to the appliance serial console port (see [Serial Console Port](#) on page 47).
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.
4. Make a note of the Recovery Card label (e.g. RecoveryCard1).
5. Remove the Recovery Card from the card reader.
6. Remove the System Card from the appliance front panel slot.
7. Insert the Recovery Card into the appliance front panel slot.
8. On the PC, launch a terminal client to connect to the appliance.
9. 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.

10. Enter option **z** to zeroize the appliance.

Once zeroized, initialize the appliance using the Decru Setup Wizard. See [Initializing a Standalone Appliance or Cluster](#) on page 54. If a current backup of the appliance configuration database is available, the configuration can be restored using the Recover from Database function of the wizard.

SETTING SECURITY CERTIFICATES

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

After the certificate is set and installed, no further security warnings appear when logging in to the appliance unless a change has been made to the IP address or hostname of the appliance, or cryptographic operations have been disabled. It may be desirable to install a certificate signed by a certificate authority as described in [Setting a Certificate Authority Signed Certificate](#) on page 151. 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 have been purchased, they will have to be replaced for zeroized appliances. See [Zeroizing Appliances](#) on page 148 for more about zeroization.

SETTING A SELF-SIGNED SECURITY CERTIFICATE

1. Using the DMC, log in to the appliance.
2. Select **Security > Certificates**.

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.

3. Enter the information for the self-signed certificate. This information appears when certificate details are viewed.

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

For a partial list of country codes, see [Partial List of ISO Country Codes](#) on page 242.

4. 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.

5. Review the certificate and accept it.

SETTING A CERTIFICATE AUTHORITY SIGNED CERTIFICATE

Generating the Certificate Request

1. From the DMC, log in to the appliance.
2. Select **Security > Certificates**.
3. 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). For a partial list of country codes, see [Partial List of ISO Country Codes](#) on page 242.

Setting the CA-signed Certificate

1. From the DMC, log in to the appliance.
2. Select **Security > Certificates**.
3. 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.
6. 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.

7. Review the certificate and accept it.

■ ■ ■ ■ 13 CLUSTER ADMINISTRATION

A cluster is created using the Setup Wizard. See [Chapter 5](#) for instructions on completing the wizard.

Note: Standalone DataFort appliances cannot be joined together to form a cluster.

An FC-Series DataFort cluster can include up to 8 DataFort appliances, no more than 4 of which are 10 Port DataFort appliances. All cluster members maintain configuration information for the entire cluster.

A Full Administrator can complete all cluster management procedures. A Machine Administrator can also add a member to a cluster.

Cluster administration tasks include:

- [Cluster Management](#)
- [Cluster-Wide Management via DMC](#)
- [Adding and Removing Cluster Members](#)
- [Recovering a Cluster](#)
- [Changing Network Properties of a Cluster Member](#)

CLUSTER MANAGEMENT

If members of the cluster go offline, some operations may be disabled to ensure data integrity. The offline cluster members should be recovered, disabled or removed to restore full cluster operation.

A minimum number of cluster members must be functioning in order for the cluster to remain formed. This minimum is the cluster quorum. The formula for determining the quorum is half of the number of total cluster members, plus one. In a cluster of two, both members must be online for the database to remain writable. [Table 18](#) offers some examples of cluster quorum requirements in smaller clusters. To maintain all data operations, be sure that the number of functioning cluster members does not drop below the minimum quorum.

Note: See [Cluster Management](#) on page 185 for information on using the CLI to manage clusters, including the ability to disable cluster members if necessary.

MAINTAINING THE CLUSTER QUORUM

If one DataFort in the cluster goes offline, the remaining appliances automatically take over operations. All cluster members keep the same configuration database. If strictly more than half of the cluster members are online, then the configuration database remains writable.

TABLE 18: CLUSTER QUORUM EXAMPLES

Number of DataFort Appliances in Cluster	Required Number of Online DataFort Appliances
2	2
3	2
4	3
5	3
6	4
7	4
8	5

CLUSTER-WIDE MANAGEMENT VIA DMC

Most DMC operations are cluster-wide and when completed on any member apply to the entire cluster.

CHECKING THE STATUS OF THE CLUSTER

To check the status of a cluster, log in to one of the cluster members via the DMC and select **Appliance > View Cluster Members**. Cluster status is defined by the Group State and Replication State of the configuration database shared by the cluster members. All cluster members are listed in the table in the View Cluster Members tab.

If the cluster is not in a committed/online state, some action may be required in order to resolve the cluster condition. Check [Table 19](#) for a description of cluster states.

TABLE 19: CLUSTER STATES

Replication State	Group State	
	committed	aborted
online	committed/online The cluster is stable. This is the only state in which changes to the configuration are permitted. A standalone DataFort will also show this as its cluster state.	n/a
recover	committed/recover Cluster members are synchronizing configuration information. When the process is complete the state will change to committed/online.	aborted/recover Cluster members are not communicating. Check network connections and cluster configuration. If one member of the cluster has failed, replace it with a new DataFort.
conflict	committed/conflict There is a conflict between configuration databases that cannot be automatically resolved.	n/a

RESOLVING A CLUSTER CONFLICT

A cluster that has not formed properly at the outset remains in an aborted/recover state. In rare cases, a cluster member may not join the cluster properly, resulting in a committed/conflict cluster condition. This problem can occur if a DataFort appliance reboots, causing its database to go out of sync with the rest of the cluster. In order to resolve a committed/conflict cluster condition, complete the following:

1. Determine which cluster member has an incorrect database. This may require logging in to the conflicted DataFort appliances and examining the configuration properties to determine which database is correct.
2. Log in to the cluster member with the incorrect database.
3. Select **Appliance > View Cluster Members**.
4. Right-click the DataFort appliance with the correct database and select Pull Information.

The database pull starts automatically. The process of updating the incorrect database and reforming the cluster can take up to five minutes. When complete, the cluster state changes to “committed/online.”

ADDING AND REMOVING CLUSTER MEMBERS

New DataFort appliances can be added to an existing cluster at any time. To create a cluster from the outset, follow instructions in [Chapter 5](#) which describe how to initialize a standalone DataFort and then add a cluster member by running the Setup Wizard on another DataFort.

A DataFort can also be removed from the cluster at any time. See [Removing a Cluster Member](#). The cluster quorum changes when a DataFort is removed—be sure that the number of remaining cluster members does not fall below the functional limit for a cluster. Keep in mind that in most cases once a DataFort is removed from the cluster, it must be zeroized and reintroduced to the cluster using the Setup Wizard. It is possible to use the CLI to disable a cluster member temporarily so that it can be taken out of the cluster and rejoined to the cluster again without requiring a wizard. See [Cluster Management](#) on page 185.

ADDING A CLUSTER MEMBER

Keep the following in mind when adding new DataFort appliances to form a cluster:

- A DataFort must be uninitialized when added to a cluster. Initialized standalone DataFort appliances cannot be joined to form a cluster. To zeroize an initialized DataFort so it can be added as a new cluster member, see [Zeroizing Appliances](#) on page 148.
- Cluster members are added by running the Setup Wizard for the existing DataFort appliance, not the appliance to be added. For detailed instructions on adding a member to a cluster, see [Adding a Member to a Cluster](#) on page 62.
- New cluster members can be added as long as a majority of members are online. In the simplest case, a new member can be added to a standalone DataFort appliance that is online. When adding to a cluster of two, both existing members need to be online.
- Existing cluster members can be deleted at any time. Non-existent or non-working members should be deleted before a new member is added.
- Only a Full or Machine Administrator can run the wizard and add a cluster member.

REMOVING A CLUSTER MEMBER

A DataFort appliance can be removed from a cluster. Note that in a cluster of two, the remaining DataFort continues to function as a standalone device.

Note: Do not put a cluster member into standalone mode during a rekey operation.

1. Log in to a DataFort in the cluster (not the one that will be removed).
2. Select **Appliance > View Cluster Members**.
3. Right-click the cluster member to be removed and select Delete.

Cluster status remains aborted/recover until the change to the cluster has been completed.

REPLACING A DATAFORT IN A CLUSTER

To replace an offline clustered DataFort, remove it and replace it with a new, uninitialized DataFort appliance. Add the new DataFort appliance using the Setup Wizard. DataFort replacement in a cluster requires:

- A new or zeroized DataFort.
 - A DataFort appliance remaining from the original cluster.
 - The minimum set of Recovery Officers and Recovery Cards as determined by the recovery schema of the cluster.
1. Power down the offline DataFort appliance and remove it from the network, disconnecting the cables.
 2. Log in to an online member of the cluster.
 3. Select **Appliance > View Cluster Members**.
 4. Right-click the offline DataFort appliance and select Delete.
 5. Log out of the online DataFort appliance.
 6. Replace the removed DataFort appliance with the new, uninitialized DataFort appliance.
 7. Assign an IP address to that DataFort appliance and connect it to the network.
 8. Run the Setup Wizard from an online member of the cluster, adding the new DataFort appliance. Note the option to assign the WWNs previously used by the offline DataFort appliance to the new DataFort appliance using the Customize FC Site settings feature. If this step is missed, log in to the CLI and run the following command to manually assign WWNs to the new DataFort appliance:

```
kfc wwn set [-n, --name <name>] <fcsite-idx> <client-port-wwn> <client-node-wwn> <storage-port-wwn> <storage-node-wwn>
```

RECOVERING A CLUSTER

Follow the cluster recovery procedures to return an entire cluster to a previous configuration or to replace all members of a cluster. This procedure is used to replace missing or damaged clustered DataFort appliances. The replacement DataFort appliances must be zeroized. See [Zeroizing Appliances](#) on page 148.

- If one cluster member is lost, it should not be restored using the wizard. It should be deleted from the cluster and replaced as described in [Adding a Cluster Member](#) on page 157. Use the wizard to restore the first member of a cluster only if all members have been lost.
- If no cluster members are online, run the wizard on one DataFort appliance, using a saved configuration database from a lost cluster member, then add the second cluster member.

This procedure requires:

- A saved configuration database from the previous configuration.
 - The minimum set of Recovery Officers and Recovery Cards required by the recovery schema selected when the original standalone DataFort was set up.
1. Connect the first (new or zeroized) DataFort appliance to the network and assign it the IP settings of one of the cluster members to be replaced.
 2. Connect the other (new or zeroized) DataFort appliance to the network, and assign it IP settings.
 3. Complete the setup wizard on the first DataFort appliance, using the saved configuration database from the old cluster. Add the second DataFort appliance during the wizard.

CHANGING NETWORK PROPERTIES OF A CLUSTER MEMBER

The network settings can be changed for a cluster member.

- [Changing the IPsec Secret of a Cluster](#)
- [Changing the IP Address of a Clustered DataFort Appliance](#)
- [Changing the Hostname of a Clustered DataFort Appliance](#)
- [Changing the Hostname on an FC1020](#)

Note: When changing the IP address for an appliance, remember to update its DNS entry accordingly in order for the DMC to be able to resolve its hostname to the new IP address. If the appliance is added to the DMC appliance tree by its IP address instead of hostname, remove the appliance from the DMC and then add it again by its new IP address.

CHANGING THE IPSEC SECRET OF A CLUSTER

A Full Administrator can change the IPsec secret of a cluster using the DMC or CLI. The change must be made manually for each member of a cluster.

Changing the IPsec Secret Using the DMC

1. In the DMC, from the appliance tree, Shift- or Ctrl-click to select all appliances that are members of the cluster.
 - If not all members are added to the DMC yet, add at least one by selecting **Appliance > Add**.
 - Once added, select the cluster member, then select **Appliance > Add Cluster Members** to automatically add all other appliances of the cluster to the DMC.
2. With all cluster members selected from the appliance tree, select **Appliance > Log in**.

Note: If the appliances do not have a SecureView license installed, or the administrator logins for each cluster member are different, repeat these steps for each cluster member individually. In this case, due to the temporary shared secret discrepancy, cluster status remains aborted/recover until the change to the cluster has been completed.

3. Select **Configuration > Set Cluster IPsec Shared Secret**.
4. Enter the new IPsec shared secret twice and click Apply.
5. Once the process is complete and all cluster members are updated, select **Appliance > View Cluster Members** to verify that cluster status has returned to committed/online.

Changing the IPsec Secret Using the CLI

- Log in to the CLI of each DataFort appliance in the cluster and set the new secret:

```
cluster config ipsec secret -s newsecret
```

CHANGING THE IP ADDRESS OF A CLUSTERED DATAFORT APPLIANCE

The IP address of a DataFort appliance can be changed while maintaining its membership in a cluster. Note that a configured DataFort appliance cannot be moved from one cluster to another. To move an initialized DataFort appliance to another cluster, it must be zeroized and added as described in [Adding a Cluster Member](#) on page 157.

1. Log in to the DataFort appliance with the IP address to be changed.
2. Select **Configuration > Network**.
3. Enter the new IP information and click Apply.
The connection from the DMC to the DataFort is lost.
4. Log in to another member of the cluster.
5. Select **Appliance > View Cluster Members**.
6. Right-click the DataFort appliance with the changed IP information and select Edit.
7. Enter the new IP information and click Apply.
8. Log back in to the cluster member with the newly changed IP.
9. Select **Appliance > View Cluster Members**.
10. Verify that the cluster status changes back to committed/online.

CHANGING THE HOSTNAME OF A CLUSTERED DATAFORT APPLIANCE

The hostname of a DataFort appliance can be changed while maintaining its membership in a cluster.

Note: A configured DataFort appliance cannot be moved from one cluster to another. To move an initialized DataFort appliance to another cluster, it must be zeroized and added. See [Adding a Cluster Member](#) on page 157.

- Log in to the CLI of the DataFort appliance with the hostname to be changed. Run the following commands to change the hostname and reboot the appliance for the change to take effect:

```
system property set net.hostname newhostname
clu config set-local --name newhostname
system property set sys.datafort.label newhostname
kfc wwn set -n newhostname.0 0 <client-port-wwn> <client-node-wwn>
<storage-port-wwn> <storage-node-wwn>
system reboot
```

CHANGING THE HOSTNAME ON AN FC1020

Numbered additions to the hostname are required for FC-Series DataFort appliance models which have more than 1 SEP board in a single chassis. For FC1020s, each DataFort SEP has a numerical designation:

board1 = hostname.0

board2 = hostname.1

board3 = hostname.2

board4 = hostname.3

board5 = hostname.4

When making changes to a hostname on an FC1020, make sure all five entries are changed when executing the **kfc wwn set** command.

- Log in to the CLI of the DataFort appliance which will have its address changed. Run the following commands to change the hostname and reboot the appliance for the change to take effect:

```
system property set net.hostname newhostname
clu config set-local --name newhostname
system property set sys.datafort.label newhostname
kfc wwn set -n newhostname.0 0 <client-port-wwn> <client-node-wwn>
<storage-port-wwn> <storage-node-wwn>
kfc wwn set -n newhostname.1 1 <client-port-wwn> <client-node-wwn>
<storage-port-wwn> <storage-node-wwn>
kfc wwn set -n newhostname.2 2 <client-port-wwn> <client-node-wwn>
<storage-port-wwn> <storage-node-wwn>
kfc wwn set -n newhostname.3 3 <client-port-wwn> <client-node-wwn>
<storage-port-wwn> <storage-node-wwn>
kfc wwn set -n newhostname.4 4 <client-port-wwn> <client-node-wwn>
<storage-port-wwn> <storage-node-wwn>
system reboot
```

■ ■ ■ ■ 14 MACHINE ADMINISTRATION

Machine administration includes various appliance management tasks.

A Full Administrator can complete all of the procedures described in this chapter. A specified Machine Administrator can only perform a subset of the operations described.

Note: A specified Machine Administrator can also add a new member to a cluster, as described in [Cluster Administration](#) on page 153.

A Full or Machine Administrator can complete the following machine administration tasks:

- [Changing Network Settings](#)
- [Upgrading Appliances](#)
- [Managing Licenses](#)

Only a Full Administrator can manage SNMP:

- [SNMP Settings](#)

Note: Appliance Date and Time can only be set by a Full or Security Administrator. See [Setting Date and Time](#) on page 142.

Additional appliance management tasks:

- [Adding an Appliance](#)
- [Logging into Appliances](#)
- [Creating Custom Appliance Groups](#)
- [Removing an Appliance from a Custom Group](#)
- [Removing a Custom Group](#)

CHANGING NETWORK SETTINGS

It is possible to change the network settings after setup, using the DMC.

1. To change IP settings for a standalone appliance, select **Configuration > Network**.
2. Change the IP settings and click Apply

Note: Changing the IP address causes the DMC to lose connection to the appliance. Update its DNS entry accordingly, in order for the DMC to be able to resolve its hostname to the new IP address. If the appliance is added to the DMC appliance tree by its IP address instead of hostname, remove the appliance from the DMC and then add it again by its new IP address.

UPGRADING APPLIANCES

Decru offers upgrades to the appliance operating system. Each upgrade package comes with its own set of instructions from Decru. Download the provided software package to the Management Station (or another local machine) and complete the steps outlined in the upgrade instruction packet. Upgrades can be completed by selecting **Utilities > Upgrade/Downgrade** in the DMC and browsing to the software package.

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

All upgrades require the administrator to power cycle the appliance by selecting **Appliance > Reboot** in the DMC. Note that the System Card must be inserted in the appliance before power is cycled.

VERIFYING AN UPGRADE PACKAGE

1. Select **Utilities > Verify**.
2. Browse to the Upgrade file and click Apply.
After the package is verified, a hash is displayed in a screen.
3. Verify the displayed hash with the known valid hash.

MANAGING LICENSES

Appliance features require a software license issued by Decru before they can be enabled. A Security Administrator or Full Administrator is required when adding or removing a license.

VIEWING LICENSES

1. Using the DMC, log in to the appliance.
2. Select **Configuration > View Licenses**.
3. Review currently installed licenses and verify they are valid.

A license becomes invalid when it expires. The license may be linked to the appliance serial number, in which case the license must be updated if an appliance is configured using a database from an appliance with a different serial number.

To remove an expired license, select it and click Delete.

ADDING LICENSES

If necessary, obtain a new license from Decru and add it by following these steps:

1. Using the DMC, log in to the appliance.
2. Select **Configuration > Add License**.
3. Enter the license into the License ID field.
4. Click Apply.

SNMP SETTINGS

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. Only a Full Administrator can configure SNMP settings. A separate [Appliance SNMP Alarms Guide](#) is available from Decru for reference.

Decru appliances support SNMP v1, v2c, v3 queries but send only v1 traps. The various types of traps, which are sent via the RMON mechanism, are described in the [Appliance SNMP Alarms Guide](#).

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. Using the DMC, log in to the appliance.
2. Select **Configuration > SNMP Agent**.
3. On the SNMP Agent screen, enable or disable SNMP for the appliance.
4. Enter the following:

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

Check to send queries using SNMPv3 (optional).

Username and Password—A single user and password can be configured for SNMPv3.

5. Click Apply.

ADDITIONAL APPLIANCE MANAGEMENT TASKS

ADDING AN APPLIANCE

Use the Appliance menu to add an appliance to the DMC so it can be managed by the console. Several appliances may be added at once if SecureView is enabled.

1. Select **Start > Programs > Decru > Decru Management Console**.
2. Select **Appliance > Add**.

The Add... pop-up screen appears.

3. Enter the IP address or hostname of the appliance.

More than one appliance can be added on this screen: enter the IP address or hostname for each appliance in the large text box provided. Separate multiple IP addresses or host names with a comma, a space, or by pressing Enter after each.

To add an IP address range for multiple appliances with consecutive IP addresses: enter the first IP address of the range in the IP range start field. Press Tab to move the cursor to the IP range end field and enter the end of the IP range.

4. Click OK.
5. A security certificate warning appears. Make the appropriate selection about trusting the certificate.

Note: If the appliance is not found, no certificate warning appears. The appliance is added to the console, but does not appear online.

Once added, the appliance appears in the console listed under Resources. Appliances appear offline until the administrator logs in via the DMC.

LOGGING INTO APPLIANCES

Several appliances may be logged in to at once if SecureView is enabled and the appliances share an administrator. Log into each appliance after adding it to DMC.

1. Select an appliance from the appliance tree and select the **Appliance > Log in** menu item.
2. Enter the administrator name and associated password at the Login page 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 172 for information about status icons.

CREATING CUSTOM APPLIANCE GROUPS

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

1. Select **View > 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. From the appliance tree, select an appliance.
 - Shift- or Ctrl-click to select multiple appliances.
4. Drag the appliance icon(s) into the group.

Note: When adding a DataFort appliance to the DMC on another Management Station, the appliance retains its existing custom group membership. If these custom groups do not yet exist on the other DMC, they are automatically created.

REMOVING AN APPLIANCE FROM A CUSTOM GROUP

1. In the Decru Management Console, from the appliance tree, select one or more appliance(s).
 - Shift- or Ctrl-click to select multiple appliances.
2. Select **View > Remove from Custom Group**.
3. When prompted, click Yes to remove the appliance from the custom group.

REMOVING A CUSTOM GROUP

1. In the Decru Management Console, from the appliance tree, select an appliance group or nested group.
2. Select **View > Remove Custom Group(s)**.
3. When prompted, click Yes to remove the custom group.

■ ■ ■ ■ 15 DECRU MANAGEMENT CONSOLE FUNCTIONS

The Decru Management Console (DMC) is a Java application that is installed on the Management Station and serves as the graphical management interface for Decru appliances.

The Decru Management Console offers the following drop-down menus for use with Decru appliances:

- [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 appliance tree of the DMC screen. [Table 20](#) shows possible state displays for appliances in the Management Console.

TABLE 20: APPLIANCE STATUS INDICATORS

Icon	Icon Appearance	Appliance State
	Blue	The two online states are reflected in the appearance of the appliance font: Online (black) and Linked (black bold).
	Blue with yellow alert	Online with error. See About the Appliances Tab on page 173. for status details.
	Gray with exclamation	Logged off. Administrator name and/or password is incorrect, or log in is timed out (this occurs after 30 minutes if inactive).
	Yellow with open icon	Not initialized. IP address is set, but setup wizard not completed.
	Red	Offline.
	Gray	Not logged in.

ABOUT THE APPLIANCES TAB

The Appliance tab contains the following default columns:

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

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

USING TAB TABLE COLUMNS

When information in a tab is displayed in 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 and remove columns and click OK.

APPLIANCE MENU

Log in	Log in to an appliance as an administrator. See Logging into Appliances on page 169.
Log out	Log out of an appliance.
Add	Add an appliance. See Adding an Appliance on page 169.
Add Cluster Members	Add a cluster member to DMC. See Adding a Member to a Cluster on page 62.
Add Linked Appliances	Add appliances linked to an LKM appliance to DMC. See the Lifetime Key Management Administration Guide .
Remove	Remove an appliance from the DMC appliance tree. Several appliances may be removed at once if SecureView is enabled. Shift- or Ctrl-click to select multiple appliances.
Link	Select a link policy to archive or share keys between two appliances, one of which must be an LKM. See the Lifetime Key Management Administration Guide .
Link LKM Software	Back up DataFort configuration and key database for emergency data recovery. See Saving Configurations to Lifetime Key Management on page 129.
View Link Report	View details about appliance links, including key sharing group, in the Linked Appliances table. See the Lifetime Key Management Administration Guide .
View Cluster Members	View a list of members in the cluster and their current state. See Checking the Status of the Cluster on page 155.
Set up	Set up an appliance by using the Setup Wizard. See Initializing a Standalone Appliance or Cluster on page 54.
Reboot	Reboot one or more selected appliances.
Zeroize	Zeroize one or more selected appliances. See Zeroizing Appliances on page 148.
Exit	Exit the Management Console.

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 DMC. The search is not case sensitive.
Find Again	Find next result in the same search.
Preferences	Select to stay logged in to prevent the DMC session with the selected appliance(s) from expiring. Select to refresh the selected appliance(s) at a regular customizable interval.

VIEW MENU

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

All	List all appliances in the Resource pane.
Type (default)	Display appliances sorted by type, including KM-Series, FC-Series, E-Series, and S-Series appliances.
Subnet	Display appliances sorted by subnet.
Custom Groups	Display custom UI groups.
Add Custom Groups	Add a custom appliance group to monitor appliances based on organizational hierarchies. See Creating Custom Appliance Groups on page 169.
Remove Custom Group(s)	Remove a custom appliance group. See Removing a Custom Group on page 170.
Remove from Custom Group	Remove an appliance from a custom appliance group. See Removing an Appliance from a Custom Group on page 170.
Refresh	Refresh the view of appliances.

CONFIGURATION MENU

View Administrators	View and manage administrators. See DataFort Admin Roles and Account Administration on page 78.
Add Admin	Add an administrator. See Adding an Administrator on page 81.
View Licenses	View licenses. See Viewing Licenses on page 166.
Add License	Add licenses. See Adding Licenses on page 166.
View OpenKey Clients	View OpenKey clients linked to an LKM. See the <i>Lifetime Key Management Administration Guide</i> .
View OpenKey License Usage	View OpenKey license usage. See the <i>Lifetime Key Management Administration Guide</i> .
Network	Update the hostname of the appliance, the IP address, and the netmask and gateway settings of an appliance. See Changing Network Settings on page 164.
SNMP Agent	Configure SNMP agent options. See SNMP Settings on page 167.
Date/Time	Update the date, time and time zone settings of an appliance. See Setting Date and Time on page 142.
Log Configuration	Configure appliance event logging and log storage. See Configuring and Viewing Logs on page 143.
Set Cluster IPsec Shared Secret	Change the IPsec shared secret of a cluster. See Changing the IPsec Secret of a Cluster on page 160.

KEYS MENU

View Parent Keys	View all parent keys stored on an appliance. See Key Management on page 17.
View Parent Keys from LKM	View all parent keys stored on an LKM appliance. See the <i>Lifetime Key Management Administration Guide</i> .
View Data Encryption Keys	Locate specific Data Encryption keys stored in LKM. See the <i>Lifetime Key Management Administration Guide</i> .
Translate Keys	Translate Cryptainer keys that have been decrypted from one DataFort appliance's parent key and encrypted with another DataFort's parent key, so that both appliances can access the Cryptainer. See the <i>Lifetime Key Management Administration Guide</i> .
Change Key Sharing Group for Appliance	Change a policy based key sharing group for DataFort appliances that are Trustees of an LKM appliance. See the <i>Lifetime Key Management Administration Guide</i> .
Change Key Sharing Group for Keys	Change a key sharing group for any individual key. See the <i>Lifetime Key Management Administration Guide</i> .
Move Unshared Keys into Key Sharing Group	Move unshared keys into a key sharing group. See the <i>Lifetime Key Management Administration Guide</i> .
Make Key Archive	Create a archive of parent keys for an LKM client. See the <i>Lifetime Key Management Administration Guide</i> .
Make Cryptainer Key Archive	Create an archive of parent keys for a Cryptainer. See the <i>Lifetime Key Management Administration Guide</i> .
Export Keys	Export key files to a local hard drive. The files can then be deleted from the LKM appliance, or imported back into an LKM appliance (the original or another one). Only key information is shared. See the <i>Lifetime Key Management Administration Guide</i> .
Import Keys	Import key files that have been exported from another LKM appliance. See the <i>Lifetime Key Management Administration Guide</i> .
Key Recovery	Recovers key files in the rare event the LKM appliance and its peers are down. See the <i>Lifetime Key Management Administration Guide</i> .
Purge Unused Keys	Remove unused keys from the DataFort database. See Key Purging on page 130.

TOPOLOGY MENU

Hosts and Devices	Manage SAN storage and Cryptainers. See Creating Cryptainers on page 89.
Hosts and Backup Pools	Manage Tape Pools. See Managing Tape Pools on page 106.
SAN Settings	Manage SAN storage settings. See Managing SAN Storage Settings on page 113.
Tape Settings	Manage Tape settings. See Managing Tape Settings on page 110.

UTILITIES MENU

Command Line	Opens the DMC Command Line Interface (CLI) for all selected appliances. Click Execute to run the command. The command is run on all selected appliances and the output returned on the screen. Click File to open a command file to run on the selected appliances. The commands are run when the file is opened. Note that the file must be an XML-formatted file. To save the output of a command that has been run, click Save, and save the file in a designated location.
Back up	Back up the configuration database of an appliance. See Saving Configurations to Lifetime Key Management on page 129.
Back up appliances to LKM	Back up configuration databases of all appliances linked to an LKM appliance to that LKM appliance. See the Lifetime Key Management Administration Guide.
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 the Lifetime Key Management Administration Guide.
Verify	Verify the validity of an upgrade package before upgrading. After the package is verified, the hash is displayed in an alert box.
Upgrade/Downgrade	Upgrade or downgrade an appliance. Perform upgrades and downgrades only after consulting Decru support. See Upgrading Appliances on page 165.

SECURITY MENU

View Recovery Cards

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

View Recovery Cards from LKM

View all Recovery Cards associated with appliances connected to an LKM appliance. Use to locate a card if an appliance is down.

Replace Recovery Officer

Replace Recovery Officers.

See [Replacing a Recovery Officer](#) on page 139.

Change Recovery Card Password

Recovery Card passwords can be changed for additional security.

See [Changing a Recovery Card Password](#) on page 140.

Smart Card Utilities

Reset a smart card and display card information.

See [Resetting Smart Cards](#) on page 141.

Management Security

Configure security levels for appliance management interfaces.

See [Configuring Management Security Settings](#) on page 138.

Defense

Specify the automatic appliance response to evidence of threat or intrusion.

See [Managing Appliance Defense Responses](#) on page 134.

Certificates

Configure appliance security certificates.

See [Setting Security Certificates](#) on page 151.

Clear Intrusion

Reset the tamper alert and reboot the system if an intrusion alert appears.

See [Clearing a Defense Alert](#) on page 135.

TRUSTEE MENU

Create Trustee Link	Create a Trustee relationship between two appliances. This allows the appliances to share key information. Both appliances must be selected. See Managing Trustees on page 118.
Start Trustee Creation	Create trustee relationship. See Setting Up Trustees on page 118.
Receive TEP	Allow selected appliance(s) to receive a Trustee Establishment Package. See Authorizing TAP Approval Locally on page 125.
Receive TAP	Allow selected appliance(s) to receive a Trustee Acceptance Package. See Authorizing TAP Approval Locally on page 125.
View Unapproved Trustees	Display list of trustees not yet approved (waiting to accept a TAP). See Delete Unapproved TAP Trustee on page 126.
View Trustees	Display list of trustees.
Export Trustee Keys, Import Trustee Keys	Once a trustee relationship is established it is possible to transfer keys between the two clusters using the import and export key options. See Importing and Exporting Keys on page 127.

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 143.
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	View information about SAN or SCSI storage devices.
Check Appliance Sensor	View the status of the hardware including Temperature Sensors, Fan Sensors, Voltage Sensors and Power Supply Sensors. This information can be 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 for troubleshooting appliances.

HELP MENU

Help Contents	Open a PDF file of the Administration Guide for the selected appliance type.
About	Show information about this version of the Decru Management Console.



■ ■ ■ ■ 16 CLI ADMINISTRATION

Some administrators may prefer to perform management tasks using the appliance command line interface (CLI). A few advanced appliance management procedures are only available via the CLI. Consider the following when using the CLI:

- The CLI cannot be used to replace smart cards, manage keys, or recover data.
- A Full Administrator logged in to the CLI can execute all CLI commands; specialty administrators are restricted to executing commands associated with their role.
- A list of top-level commands can be found in the [Command Line Interface Quick Reference](#) on page 220 of this guide. Refer to the separate [DataFort CLI Reference Guide](#) for a complete list of commands and parameters.
- If access to the appliance CLI via SSH is disabled, for example if the appliance is running in Common Criteria Mode, use the DMC CLI to issue commands by selecting **Utilities > Command Line**.

Procedures described in this chapter include:

- [Using the CLI](#)
- [Administration Commands](#)
- [Storage Management Commands](#)
- [Manual Key Generation](#)
- [Changing Appliance Network Port Settings](#)

USING THE CLI

Some CLI commands must be executed in a specific order for desired results. The command line provides usage guidelines when [CLI Help](#) is used. For some commands, it is good practice to execute a verification command (such as `list`) after an action that adds an item to the database. Always perform a backup of the database after any changes.

CONNECTING TO THE CLI

Connect to CLI from an SSH client (see [Connecting to the Command Line Interface](#) on page 72). By default, Secure CLI is disabled. See [Configuring Management Security Settings](#) on page 138. It is recommended that only one DMC or CLI session be open per cluster at one time.

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.
- Typing a partial command phrase followed by `?` gives the same results as above.
- 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.
- Pressing tab after a command autofills 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`.

ADMINISTRATION COMMANDS

The next sections provide examples of CLI administration in the following areas:

- [Administrator Roles](#)
- [Creating a New Administrator](#)
- [Cluster Management](#)
- [System Properties and Log Management](#)
- [Stack Trace Settings](#)
- [Network Management](#)

ADMINISTRATOR ROLES

Use the CLI to find out which administrators can execute particular CLI commands. Some commands are limited to a specialty administrator or a Full Administrator. The roles are:

<code>san-readonly-admin</code>	Read Only Administrator
<code>san-machine-admin</code>	Machine Administrator
<code>san-backup-admin</code>	Backup Administrator
<code>san-storage-admin</code>	Storage Administrator
<code>san-key-admin</code>	Key Administrator
<code>san-physical-security-admin</code>	Security Administrator
<code>san-datafort-account-admin</code>	Admin Account Administrator
<code>san-admin</code>	Full Administrator

1. Log in as the desired specialty administrator and enter:

```
cli doc -n
```

The list of commands executable by the type of administrator who is currently logged in appears.

2. Enter the name of the current administrator into the `system property get` command to see the current values of system properties, preceded by permissions for the named administrator role. RW indicates that the administrator logged in has read and write permission, R- indicates read-only permission. A lower-case w indicates a property that can only be changed via DMC.

```
system property get --role <role>
```

CREATING A NEW ADMINISTRATOR

New administrators can be created by a Full Administrator using CLI commands. When an administrator is created using the DMC, the new administrator is granted the authorizer role and replicated across the cluster by default. By default, any administrator created using the CLI requires prior authentication of another administrator before logging into the DMC or CLI.

To create an administrator using the DataFort CLI:

1. Log in to the CLI as a Full Administrator.
2. To create an administrator for a single DataFort, add a user, indicating the type from the list of [Administrator Roles](#) in the `<group>` field:

```
user add <group> <username>
```

3. To create an administrator that is replicated to cluster partners add a user with the `--replicate` flag, indicating the type from list of [Administrator Roles](#) in the `<group>` field:


```
user add --replicate <group> <username>
```
4. To add the authorizer role to the newly created administrator so that dual authentication is not required when logging in:

```
user role grant authorizer@DATAFORT_ADMIN username@DATAFORT_ADMIN
```

CLUSTER MANAGEMENT

The following commands are useful when managing clusters.

<code>cluster status</code>	Shows the status of a DataFort cluster, as well as a list of member DataFort appliances, their IPs and member IDs. Shows current status of the cluster as well as the IP addressees of each cluster member.
<code>cluster config</code>	Configures the cluster.
<code>cluster enable</code>	Enables clustering. This command breaks any pre-existing cluster connectivity and forces a re-negotiation of the cluster.
<code>cluster rexec</code>	Allows commands to be issued remotely to all other DataFort appliances in the cluster as identified by IP address or name. For example, <code>cluster rexec kfc list</code> would output <code>kfc list</code> from all the members of a cluster. Also allows commands to be issued to a remote DataFort: <code>cluster rexec --name datafort1 kfc list</code> would output <code>kfc list</code> for datafort1.
<code>cluster rsh</code>	Connects directly to another member of the cluster as identified by IP address or name. Pressing <code>Ctrl-d</code> on the keyboard breaks out of this into the previous shell.
<code>cluster disable</code>	Allows the temporary removal of a cluster member without having to run a wizard in order to reintroduce the cluster member. This is useful if a DataFort appliance needs to be moved or isolated for servicing. There is no indication in the DMC that the member has been disabled. This command can also be used if a cluster member goes down, thereby dropping the remaining cluster below quorum. If the failed member is disabled using this command, the maximum number of members in the quorum is redefined, and the cluster reforms without the offline DataFort appliance. To disable a member, log into another member of the cluster and execute the <code>cluster disable <member-ip or name></code> command, identifying the DataFort appliance to be removed by name or IP address. To allow the member back into the cluster, execute the <code>cluster enable <member-ip or name></code> command from another cluster member.

SYSTEM PROPERTIES AND LOG MANAGEMENT

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

system property get 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 that are permitted to change (set) those properties, use:

```
system property get -d
```

Output is of the form: **security-admin RW global
sys.security.web.usesmartcard: 0**

This output means that Security Administrators and up are able to modify the property, in this case Secure DMC. Only a Full Administrator is above a Security Administrator. RW indicates that the administrator logged in has read and write permission, R- indicates read-only permission. A lower-case w indicates that the property can be changed from the web only. The output (after the colon) shows the current value of the property. In this case 0 indicates that Secure DMC is off.

system selftest Performs a series of tests on the appliance and configured servers.

**system utility
lcdmessages** Displays text of any warnings currently on the appliance LCD.

system version 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.

system reboot Reboots the appliance. Adding the **-p** flag to **system reboot** power-cycles the box. This is necessary after upgrades.

system log list Lists system logs in the database. Various filtering options are available, for example:

Search for messages of priority 1 and type SEC:

```
system log list -p 1 -t SEC
```

Search for messages starting from 2002/1/17 1pm to 2pm (the interval **i** is in seconds):

```
system log list -b '2002-01-17 13:00:00' -i 3600
```

To search for messages of the last 24 hours:

```
system log list -b now -i -86400
```

To search for the last 10 messages:

```
system log list -o -10
```

VERIFYING SYSTEM LOGS

1. To verify a signed log message, use:

```
system log verify <msg>
```

The **<msg>** parameter is a log message to be verified in the form **"mesg-text [meta-data signature]"**

2. Single quotes, double quotes, and backslashes in the message must be preceded with a backslash and the entire message must be surrounded by double quotes. For example, to verify the following log message, execute the **system log verify** command that follows the log message:

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

Another example of this command is:

```
system log verify "boxmanager: Security property  
sys.security.groupreview was set to 1 [AAAAAAEAAAAHAAAAAnCruPg==  
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 "boxmanager: Security property  
sys.security.localacl was set to 1 [AAAAAAIAAAATAAAAnCruPg== /  
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.

Note: The Signed Log Authentication script is provided on the appliance user CD.

STACK TRACE SETTINGS

The appliance has 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 appliance 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. To change the stack trace setting, log into the CLI and run the appropriate `system property` command:

Stack trace is on by default. 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
```

NETWORK MANAGEMENT

The following network commands are useful in managing the network:

<code>net util arp</code>	Display or clears the ARP (Address Resolution Protocol) table: display using <code>net util arp -n</code> , clear using <code>net util arp -d</code> .
<code>net util host</code>	Resolve a given hostname to its IP address: <code>net util host <hostname></code> .
<code>net util ifconfig</code>	Display information about network interfaces. Display information about network interfaces which are up: <code>net util ifconfig -u</code> .
<code>net util ipsecstats</code>	Display IPsec statistics.
<code>net util netstat</code>	Display network status. Display the routing table: <code>net util netstat -r</code> . Display the state of all sockets: <code>net util netstat -a</code> . Display network memory buffer usage (mbufs): <code>net util netstat -m</code> .
<code>net util ping</code>	Ping a host by sending out the packet from the interface on which -i <local_addr> is configured and setting the source address on the packet to -S <local_addr>: <code>net util ping -i <local_addr> -S <local_addr></code> .

BACKUP MANAGEMENT

It is recommended that a database backup be performed after any changes.

<code>db export</code>	The CLI command <code>db export</code> can be used for manual configuration database backups, such as to LKM or another designated site. Enter <code>db export ?</code> to see the options, and see the LKM Appliance Administration Guide for more information. Using the interactive backup mode (<code>db export -u</code>) requires that a user name and password be entered.
------------------------	---

STORAGE MANAGEMENT COMMANDS

The CLI can be used to view Cryptainer information, create Cryptainers and manage Cryptainer encryption processes. The following commands allow storage to be managed from the CLI.

- [Disk Commands](#)
- [Host Commands](#)
- [Cryptainer Commands](#)
- [Fibre Channel Kernel Commands](#)

A list of top-level commands can be found in the [Command Line Interface Quick Reference](#).

DISK COMMANDS

To perform storage device management commands, first execute the `disk list` command to get necessary information such as the `<node-wwn>` `<port-wwn>` `<lun>` of the device.

<code>disk list</code>	Generates a list of all storage devices and their status on the cluster. Options include query offset and limit, hidden disk, host port WWN, node-wwn, disk node WWN, port-wwn, disk port WWN, disk LUN, disk name, Cryptainer id, disk with no associated Cryptainer, WWN of the DataFort HBA which discovered the disk and name of the DataFort appliance that has paths to the disk(s).
<code>disk rescan</code>	Rescans the fabric for disks. This command may be needed to update recent changes to disks. Note that disk rescans are potentially disruptive to disk I/O.
<code>disk remove</code>	Enter the device parameters into the command to remove it from the configuration database: <code>disk remove <port-wwn> <lun></code> . Options include specifying the host port WWN, the WWN of the DataFort HBA which discovered the disk and the name of the DataFort appliance that discovered the disk.
<code>disk rmall</code>	Enter the device parameters into the command: <code>disk rmall <port-wwn></code> . All devices associated with the indicated WWN are removed from the configuration database. There is also an option to indicate the host port WWN.
<code>disk blink</code>	Enter the disk parameters into the command: <code>disk blink <host-port-wwn> <lun> on off</code> . If the value is set on, the LED on the selected disk blinks, so that the disk can be visually identified in the JBOD. If the disk blinks, but does not appear in the configuration database, run the <code>disk rescan</code> command. Note that this only applies to JBOD devices.
<code>disk map</code>	To add a second path to an existing Cryptainer, first find the Cryptainer ID using the <code>fcery list</code> command. Enter device and Cryptainer parameters: <code>disk map <port-wwn> <lun> <cryptainer-id></code> . Use the option <code>--host-port-wwn <host-port-wwn></code> to indicate the host port WWN.

`disk rmmmap` Execute the `disk rmmmap` command to remove the path to the Cryptainer, using the same device and Cryptainer parameters: `disk rmmmap <port-wwn> <lun> <cryptainer-id>`. Use the option `--host-port-wwn <host-port-wwn>` to indicate the host port WWN.

Mapping a Device

If a device has two ports and multiple LUNs (and therefore many Cryptainers), it may be helpful to map the Cryptainer exposed by one port to the Cryptainer exposed by the other port. Use the DataFort device mapping feature to indicate that one device is equivalent to another. Once this device-level mapping is made, all future Cryptainers on that device are added with multiple paths.

1. To map a device use the `device map` command:

```
device map <primary-port-wwn> <alternative-port-wwn>
```

1. To remove a device mapping:

```
device rmmmap <primary-port-wwn> <alternative-port-wwn>
```

Replacing a Device Maintaining Cryptainer Mapping

This command maps a device's Cryptainer keys to a new device.

1. Use the `fccryptainer list` command to list the Cryptainers in the system. Identify the Cryptainer-ID of the Cryptainer to be replaced.
2. Use `disk list --cryptainer-id <cryptainer-id>` to retrieve the old node-WWN, port-WWN, LUN on which the Cryptainer was created originally.

Note: In a cluster, remove the secondary path (use the `disk rmmmap` command) before replacing the device. Remap the new secondary path information to the replaced device.

3. Use `disk list` to retrieve the `<new-node-wwn> <new-port-wwn> <new-lun>` parameters for the replacement (new) device.
4. Execute the `disk replace` command with the device information:

```
disk replace <old-port-wwn> <old-lun> <new-port-wwn> <new-lun>
```

HOST COMMANDS

To perform host management commands, first execute the `host list` command to get necessary information about the host.

<code>host list</code>	Generates a list of all hosts and their status on the cluster.
<code>host rescan</code>	Rescans the cluster, forcing a loop reset on the Host side of the fabric. This command may be needed to update recent changes to hosts.
<code>host add</code>	Enter information about the host that will be added: <code>host add <node-wwn> <port-wwn> <name></code> .
<code>host remove</code>	The indicated host is removed from the configuration database: <code>host remove <port-wwn></code> .

Virtualizing a Host

The DataFort appliance presents host HBAs to storage. Some devices reserve space for a specific host as identified by its WWN. These devices require the appliance to virtualize the host so that storage devices can see it. To support heterogeneous hosts and LUN masking, the appliance allows the host to be virtualized: the appliance presents the host information to the storage device.

Note: Since JBOD devices (or any devices that are not set up with LUN masking) show up on every port, they should NOT be used with virtualized hosts. Do not select a virtualized host when creating a Cryptainer on a JBOD.

1. Check that virtualization is enabled:

```
system property get -k dfc.isp.max
```

Both virtual port settings should be set at 7:

```
global dfc.isp.max_host_vp:7
```

```
global dfc.isp.max_storage_vp:7
```

If virtualization is off, settings will be set at 0. To turn virtualization on:

```
system property set dfc.isp.max_host_vp 7
```

```
system property set dfc.isp.max_storage_vp 7
```

2. Use the `host virtualize` command to virtualize a host:

```
host virtualize [--vpindex <vpindex>] [--forward-wwn] <port-wwn>
```

The Virtual Port Index option `--vpindex <vpindex>` is useful for reconfiguring a system. If the previously assigned vpindex is known, assign it again (this gives the same default WWN). The Forward Port WWN option `--forward-wwn` uses the host's original WWN. This is recommended only if the host is not connected to the same fabric as the appliance's Storage HBA. It can cause problems with WWN-based zoning.

CRYPTAINER COMMANDS

To perform Cryptainer management commands, first execute the `fccryptainer list` command to get necessary information about Cryptainers in the configuration database. Note that `fccryptainer` can be shortened to `fccry`. Note that some commands are only applicable to disk and not to tape drives.

<code>fccryptainer list</code>	View all Cryptainers hosted by the cluster. Options include offset and limit, host port WWN, disk node WWN, disk port WWN, disk LUN, WWN of the DataFort HBA with a path to the Cryptainer, name of the DataFort that discovered the disk where the Cryptainer is located, Cryptainer ID, or Cryptainers not accessible from host port or node WWN.
<code>fccryptainer path</code>	Lists all paths to Cryptainers. Options include offset and limit, host port WWN, disk node WWN, disk port WWN, disk LUN, WWN of the DataFort HBA with a path to the Cryptainer, name of the DataFort appliance that discovered the disk where the Cryptainer is located, Cryptainer ID, or Cryptainers not accessible from host port or node WWN.
<code>fccryptainer perm list</code>	Lists permissions on all Cryptainers. Options include offset and limit, host node WWN, host port WWN, disk node WWN, disk port WWN, disk LUN and Cryptainer ID.
<code>fccryptainer rekey list</code>	Lists all rekey jobs with status.
<code>fccryptainer rekey request</code>	Request a rekey job: <code>fccry rekey request <cryptainer-id></code> . Options include indicating that data will be decrypted, that the Cryptainer is empty, block access to the Cryptainer, the WWN of the DataFort HBA which should do the rekey and the name of the DataFort appliance to be used to do the rekey.
<code>fccryptainer rekey notify</code>	Reactivate a stalled or stopped rekey job. This activates all new or changed key requests.
<code>fccryptainer add</code>	Add a Cryptainer, specifying disk information and mapping options: <code>fccry add <map-type> <port-wwn> <lun></code>. Indicate <code>map-type</code> as <code><lunmap portmap></code>. Options include a description, the option to create a cleartext Cryptainer (assigning no key), create a Cryptainer that can be exported to trustees, enter the start and end LBA for unencrypted region to allow for partial encryption, indicate the host port WWN, forward port WWN. Specify that the Cryptainer be added as cleartext (unencrypted) with the <code>nokey</code> option (disk Cryptainers only): <code>fccry add --nokey <map-type> <port-wwn> <lun></code>.

<code>fccryptainer createall</code>	Automatically create one Cryptainer per LUN in a multi-disk target. Specify disk information and mapping type: <code>fccry createall <map-type> <port-wwn></code> . Options are the same as when using <code>fccry add</code> .
<code>fccryptainer clone</code>	Reuses one Cryptainer's key for another Cryptainer, creating a new Cryptainer for a copied LUN. Specify Cryptainer information: <code>fccry clone <cryptainer-id> <map-type> <port-wwn> <lun></code> . Options include description, host port WWN and forward port WWN.
<code>fccryptainer remove</code>	Removes the keys and access associated with a Cryptainer from the configuration database: <code>fccry remove <cryptainer-id></code> . Use the <code>[-f, --force]</code> option to attempt to remove the Cryptainer without prompting for confirmation. A removed Cryptainer can be restored as long as the storage device on which it was created remains. To aid in recovery, record the port WWN and LUN number of the Cryptainer before removal. Note that the appliance stores information about Cryptainers, even deleted Cryptainers, indefinitely unless they are purged when saved to LKM.
<code>fccryptainer rmall</code>	Remove all Cryptainers from the configuration database. Use the <code>[-f, --force]</code> option to attempt to remove all Cryptainers without prompting for confirmation.

The following sections give examples of using Cryptainer commands.

Rekeying a Cryptainer

This command is available for Cryptainers created on disk only.

Note: Do not make any changes to the configuration while a Cryptainer is being rekeyed.

1. Use `fccry list` to obtain a list of Cryptainers.
2. Use `fccry rekey request` to change the encryption key for an existing Cryptainer. To rekey multiple Cryptainers, repeat the command for each Cryptainer.

`fccry rekey request <cryptainer-id>`

3. To activate this command use `fccry rekey notify`.
4. Use `fccry rekey list` to retrieve and monitor the encryption process.

Note: To start rekey at a later time, use a cron script to initiate step 3.

Granting Host Access to a Cryptainer

1. Use `host list` to obtain host information.
2. Use `fccry list` to obtain Cryptainer information.
3. Use `fccry grant` to grant the host access to the specified Cryptainer.

`fccry grant <permissions> <cryptainer-id> <host-port-wwn>`

Revoking Host Access to a Cryptainer

1. Use `host list` to obtain host information.
2. Use `fccry list` to obtain Cryptainer information.

```
fccry revoke <permissions> <cryptainer-id> <host-port-wwn>
```

Note: To remove all host access to a Cryptainer use the `rvall` command:

```
fccry rvall access <cryptainer-id>
```

FIBRE CHANNEL KERNEL COMMANDS

Use Fibre Channel kernel commands to view fabric status.

`kfc list`

Generates a list of all devices attached to the Fibre Channel kernel as well as Cryptainers that are associated with disks on those devices. This command also shows whether storage devices are offline or online, and shows the Loop ID of the hosts (hosts that are offline will have a Loop ID of 9999). Note that Loop IDs in this context are internal values used by the appliance to identify hosts, assigned based on the state of the firmware of each appliance at the time that the host table entries were made.

There is no coordination of Loop ID assignments between DataFort appliances, therefore it is possible to have different Loop IDs assigned to the same host on different appliances. In addition, Loop ID assignments can change when a change in the fabric occurs.

At the bottom of the output is a matrix including Cryptainer IDs and the host port WWN, identified as the Loop ID. If the host has access to the Cryptainer the DataFort shows a **Y**.

`kfc sync`

Activates a resync of the Fibre Channel kernel to the fabric.

`kfc util stat list`

Shows a list of Fibre Channel statistics (such as bytes in and bytes out, interrupts and buffers).

`kfc util ckstat list`

Displays the changing key status. (disk licensed DataFort only)

`fcsite list`

Lists all of the devices with HBAs in the cluster configuration database. Options include offset, limit, storage-side-wwn, host-side-wwn, name and unused.

MANUAL KEY GENERATION

The DataFort appliance supports manual generation of encryption keys. Using this feature, an administrator can generate keys before a pool is created, and specify which keys are to be used for the pool. Manually generated keys are associated with a tape pool using the `pool key set` command. For more about this command, see [Pool Defaults](#) on page 110.

A Full or Key Administrator can manually create and assign keys. Manual Cryptainer key generation involves the following steps:

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

CREATING CRYPTAINER KEYS

Create keys in advance of manually assigning them to pools. To manually create keys, use the `keyman cryptainerkeys generate` command. This command takes three arguments: index, name and number of keys. The number of keys to be created is a required parameter. Giving keys descriptive names using the optional name and index arguments is highly recommended. When creating more than one key, the keys are numbered sequentially starting with 0 or the supplied index option.

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

```
keyman cryptainerkeys generate [-i, --index <index>] [-n, --name  
<name>] <no-of-keys>
```

Some examples of key generation using the command options follow.

Name defined—The following generates two keys with the names jim0 and jim1.

```
keyman cryptainerkeys generate -n jim 2
```

Name, index and number defined—The following generates 10 keys with names jim100, jim101 etc.

```
keyman cryptainerkeys generate -i 100 -n jim 10
```

VIEWING CRYPTAINER KEYS

To view keys that have been manually created, use the `keyman cryptainerkeys list` command.

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

```
keyman cryptainerkeys list
```

2. Review the output and identify the manually-created keys by Key Name.
3. Record the Key IDs so that the keys can be assigned to new or existing pools.

CHANGING APPLIANCE NETWORK PORT SETTINGS

By default, the media type is set to auto negotiate on all appliance Ethernet network interfaces. Valid settings are defined in [Table 21](#).

TABLE 21: VALID MEDIA TYPE VALUES

Interface	Valid Values
net.admin.media	1000baseTX
	100baseTX
	auto (default setting)
net.admin.mediaopt	half-duplex
	full-duplex

Note: 1000baseTX half-duplex is not a valid configuration. The appliance automatically changes it to full-duplex in this case.

For the DataFort FC-Series appliance, the management port is the only interface affected by these values.

Note: The following changes should only be performed during a scheduled maintenance window as they could temporarily affect cluster stability.

To change the media type of the appliance management port:

- Log in to the appliance CLI and run the following commands:

```
system property set net.admin.media [value]
system property set net.admin.mediaopt [value]
```
- Apply the settings by running the following command:

```
net apply
```

■ ■ ■ ■ 17 TROUBLESHOOTING

This chapter provides general troubleshooting information for Decru appliances. Appliance event logs provide additional information about security, operations, and performance issues.

- [Restoring an Appliance](#)
- [Front Panel LEDs](#)
- [Power Supply LEDs](#)
- [Network Connections and Management Interfaces](#)
- [Clusters](#)
- [Smart Cards](#)
- [Hardware](#)
- [Storage](#)

This chapter also includes troubleshooting tips for using DataFort in specific environments including:

- [Decru DataFort Operation with EMC](#)
- [Decru DataFort Operation with Solaris](#)
- [Decru DataFort Operation with Legacy Encrypted Tapes](#)
- [Decru DataFort Operation with Tivoli and STK Drives](#)
- [Decru DataFort Operation with LT02 Serialized Commands](#)
- [Decru DataFort AIX Atape Failover Support](#)
- [Decru DataFort SCSI Reservation Handling Fixes](#)

RESTORING AN APPLIANCE

If a standalone appliance is lost, a saved configuration database from that appliance can be used to configure a replacement appliance. The recovered appliance is then able to retrieve data that was encrypted using the previous appliance. The Setup Wizard assigns a new appliance the configuration from a pre-existing appliance. The replacement appliance retains all parameters stored in the configuration database of the original appliance, including network, Cryptainer, access control and encryption key information.

If a cluster member is lost, it should not be restored using the wizard. It should be deleted from the cluster and replaced as described in [Adding a Cluster Member](#) on page 157. Use the wizard to restore the head of a cluster only if all members have been lost.

The procedure is conducted by a Full Administrator. The recovery procedure requires:

- A new or reset System Card.
 - A new or zeroized appliance.
 - The minimum set of Recovery Officers and Recovery Cards as determined by the recovery schema of the cluster.
 - A saved database from the appliance that is to be restored.
1. Connect the new or zeroized appliance to the network and assign it the IP settings of the old appliance. See [Assigning the Appliance IP Address](#) on page 48.
 2. From the DMC appliance tree, right-click the appliance to restore and select Set up to start the wizard. See [Initializing Appliances](#) on page 51.
 3. Click Start, then click Next.
 4. Accept the certificate.
 5. If prompted, accept the license agreement.
 6. At the Recover from Database page, browse to the saved configuration database. This file, with the extension .XDF, was created previously when backing up the appliance configuration in the DMC by selecting **Utilities > Back up**. See [Backing Up Configurations to a Remote Location](#) on page 132.
 7. Create a new administrator account (optional), then click Next.
 8. Select the cluster size and recovery schema, then click Next.
 9. Edit the network settings (optional), then click Next.
 10. Edit the license information (optional), then click Next.
 11. Enter DNS and certificate information (optional), then click Next.
 12. DataFort needs the minimum number of Recovery Cards required for recovery procedures (as set in the original configuration). Insert Recovery Cards from the original appliance configuration as prompted, then click Next.
 13. Click Next to apply the settings.
 14. Click Finish when the wizard is finished.

For more detailed information about wizard steps, see [Initializing Appliances](#) on page 51.

FRONT PANEL LEDs

Depending on the type of chassis, the appliance front panel features one or two bicolored LEDs that signal the status of the appliance, as summarized in the tables below.

TABLE 22: FRONT PANEL DUAL LEDs - 2U

LED Name	Position	Color	Behavior	Indication
Status LED	Top	Green	Solid	DataFort on network, no errors
		Red	Solid	Error Alarm: appliance not functional. Check LCD for messages.
Network LED	Bottom	Green	Solid	Network link
		Red	Solid	Network error

TABLE 23: FRONT PANEL LEDs - 1U

Color	Behavior	Indication
Green	Solid	Appliance on network, no errors, no traffic
Green	Blinking	Appliance on network, no errors, with traffic
Red	Solid	Network error, no traffic
Red	Blinking	Error found, with traffic

POWER SUPPLY LEDs

The power supply module on the 2U model appliance provides a single external bicolor LED to indicate the status of the power supply. When AC is applied to the power supply unit and standby voltages are available, the LED blinks green. The LED is solid green to indicate that all the power outputs are available. It is solid amber to indicate that the power supply has failed, there is a shutdown due to over-current, over-temperature, or the unit is likely to fail.

TABLE 24: POWER SUPPLY LEDs

Power Supply Condition	Power Supply LED
No AC power to all power supply units	Off
No AC power to this power supply unit only	Amber
AC present / only standby outputs ON	Blink green
Power supply DC outputs ON and OK	Green
Power supply failure (includes voltage and/or temperature exceeded)	Amber
VRM (voltage regulator module) failure, cage related	Blink green
240VA limit (cage related)	Blink green
Current limit	Amber

NETWORK CONNECTIONS AND MANAGEMENT INTERFACES

[Table 25](#) contains troubleshooting tips for the network and management connections to the appliance.

TABLE 25: NETWORK CONNECTIONS AND MANAGEMENT INTERFACES

Problem	Possible Cause and Solution
No Fibre Channel configuration or Ethernet network connection	- Both HBA ports must be connected. Check the link lights on the FC switch connected to DataFort. - Check link lights on the rear of the DataFort appliance. Check the LCD on the front panel for messages. - The appliance must have an IP address assigned. See Assigning the Appliance IP Address.
Power not on	- On 2U appliance: 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 both power cables, and if necessary, plug the power cables into another power source. - On 1U appliance :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 the appliance 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 on the appliance.
Cannot log in via serial connection	- Verify that the login username and password are correct. - 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 the Appliance IP Address. - Be sure the Management Station can reach the appliance IP address on the network.
Cannot connect to domain name of appliance	The appliance's 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.
Cannot clear alert after using CryptoShred button	The CryptoShred button must be in a normal state to allow operations to be restored. See CryptoShred Button States.
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 a Defense Alert.

TABLE 25: NETWORK CONNECTIONS AND MANAGEMENT INTERFACES (CONTINUED)

Problem	Possible Cause and Solution
LCD asks for System Card, or Status LED is red on 2U appliance	• A System Card must be inserted before the appliance is powered on. Once it 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 DataFort may have a security setting in place that halts operations if the DataFort appliance is rebooted without a System Card. See Managing Appliance Defense Responses.
Cannot log in to DataFort appliance	• To access the appliance via DMC the Management Station must have access to the appliance IP address. Ensure the appliance and the Management Station are on the same network. • The network switch port connected to the appliance should be set to auto-negotiate. • Verify any firewall for the Management Station is disabled, and that web traffic is not going through a proxy. • In Add/Remove Programs verify the following programs are installed: Decru Management Console, Gemplus Smart Card Reader Tools. • If Secure DMC is enabled, a valid administrator and Admin Card are required to log in. • If Secure DMC is on, Terminal Services and Remote Desktop cannot access the DMC. • Some administrators may require 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 Requiring Authorization for Login.
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 DataFort CLI	• Verify that the login username and password are correct. • Try logging in again using the defaults: User: user, Password: MTKNMTKN. • Check that Secure CLI is disabled.
Login information for sole administrator lost	• Log in using a Recovery Card, and zeroize the appliance. See Emergency Serial Console Port Access.
Need to disable DMC smart card requirement (Secure DMC) via CLI	• If the administrator is unable to access the DMC in order to disable the smart card requirement, this can be done via CLI: • Log in to the CLI and run the command system property get sys.security.web.usesmartcard to check the setting. A setting of 1 requires the Admin Card in order to log in to the DMC; 0 disables the requirement. If necessary, run the command system property set sys.security.web.usesmartcard 0 to disable the smart card requirement. A Security or Full Administrator can set this property.
CLI sessions take a long time to establish	• This can occur if the DNS servers are unavailable. Log in through the DMC and change the DNS servers, or wait for the CLI session to establish and then change the DNS servers from the CLI.

CLUSTERS

Table 26 includes troubleshooting tips for cluster management issues.

TABLE 26: CLUSTERS

Problem	Possible Cause and Solution
Cluster does not form	• If the cluster will not form (it remains in an aborted/recover state), verify network settings of all DataFort devices. • Be sure each DataFort has a valid, unexpired license for clustering. • Run the command <code>cluster stat</code> on each of the members in the cluster. • If there are two members that are not communicating, disable both of them by running the command <code>cluster disable</code>, and then bring them back one at a time, making sure that the cluster forms with each addition. • Check for other problems with a cluster member that does not join the cluster, such as crypto errors.
Cluster member goes down and cluster does not reform	• Check that the loss of the cluster member has not dropped the number of devices in the cluster below quorum. • Use the <code>cluster disable</code> command to remove an offline member from the cluster and redefine the number of members required for the quorum.
Cluster goes into standalone mode during rekey	If a clustered DataFort is put into standalone mode during a rekey, and the Cryptainer being rekeyed had a path to the DataFort that left the cluster, additional steps are required in order to complete the Cryptainer rekey on the remaining standalone DataFort. Unmap any paths from the offline DataFort to Cryptainers that are still in the process of rekeying: • In the DMC, select the offline path or paths to the Cryptainer. • Right-click the offline path to the Cryptainer and select Unmap. • Right-click the Cryptainer and select Encryption/Decryption > Encrypt/Resume... to resume the rekey.

SMART CARDS

[Table 27](#) contains troubleshooting tips for working with smart cards.

TABLE 27: SMART CARDS

Problem	Possible Cause and Solution
Management Station doesn't detect Admin Card	- The DataFort 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
	Verify 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	The appliance needs a new or reset System Card in order to complete the setup wizard. If the System Card was not inserted into the appliance chassis during zeroization or if it was not properly reset during zeroization, manually reset it. See Resetting Smart Cards.
Lost System Card	Zeroize, insert a new System Card and run the Setup Wizard.
DMC 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.
Lost Admin Card with Secure DMC enabled	- Log in with a different Admin Card and associate a replacement Admin Card with an existing or new administrator. - If all Admin Cards are lost and Secure CLI is not on, log in to the CLI and turn off Secure DMC by running the CLI command <code>system property set sys.security.web.usesmartcard 0</code> to disable the smart card requirement for the DMC. Then log in to the DMC and associate a replacement Admin Card with an existing or new administrator. A Security Administrator or Full Administrator can change the system property. A Full Administrator is required to create or change associations with an Admin Card. - If both CLI and DMC login are smart card enabled and all Admin Cards are lost, zeroize DataFort using the serial console.
Problem with multiple smart card readers	Multiple card readers are not supported for Cluster Recovery operations. Multiple card readers are only supported at the time of cluster formation.
Lost Recovery Card	Assemble a quorum of Recovery Officers and replace the Recovery Card.
Wrong System Card found error appears on LCD or in logs.	- Appliance 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 using the following steps: - CLI: Run the command: <code>system version</code> - DMC: Insert the System Card into the smart card reader, then select Security > Smart Card Utilities. Check the Smart Card Version field.
Smart card errors appear	Use an eraser to clean the metal contact on the smart card.

HARDWARE

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.

STORAGE

[Table 28](#) includes troubleshooting tips for the storage network.

TABLE 28: STORAGE

Problem	Possible Cause and Solution
Cannot see storage or hosts	• Check switch configuration. Hosts and storage should be on separate zones of a zoned switch, or connected to two different FC switches. • Verify all storage devices are in one zone along with the storage side HBA of the DataFort. Each host HBA should be paired off with the host side HBA of the DataFort and zoned separately. Any virtual WWNs created by port mapping should also be added to each appropriate host zone. • Verify all necessary licenses are installed.
Devices do not appear in DMC	• DataFort must be zoned so that the Host HBA is zoned with network hosts, and the Storage HBA is zoned with storage devices. • Cluster status must be online for new devices to appear in the DMC. • Check FC switch zoning: DataFort HBAs should appear. • Check LUN masking to verify that the DataFort appliance has access to volumes. • The Storage and Host HBA WWNs can be found by selecting Diagnostics > View Storage Details in the DMC. 2U appliances also display this information on the front panel LCD. • Execute a Disk Rescan operation from DataFort to force a rescan by the HBA. Note that a disk rescan is potentially disruptive to disk I/O.
Storage appears with incorrect WWNs	• The DataFort appliance syncs its FC information with the network. Use the kfc sync command to resync the FC information.
Devices are inaccessible	• The WWN name and possibly the SCSI path changed, causing the host to appear to the operating system as a new device. Reinstall device drivers. • Check host settings. Some hosts are configured to see only certain WWNs. The DataFort WWN (or any virtual ports that have been created) may need to be added to a list of approved WWNs. • Check persistent binding settings. If persistent binding is used by the host, then settings must be changed after installing DataFort.
Host can't detect the storage presented by DataFort	• Verify that the DataFort appliance detects the host device: check the DMC. • If possible, perform a rescan by the host. • If necessary, reboot the host.
DataFort performance degrades/connectivity to storage devices is lost	• DataFort performance degrades when the number of simultaneous I/O commands exceeds 512. Issuing more than 512 simultaneous I/O commands causes I/O failures and may result in a loss of connectivity to storage devices. • Use the kfc util stat list command to view the maximum simultaneous I/Os seen by the DataFort appliance. If the displayed maximum exceeds 512, load through DataFort should be reduced.

TABLE 28: STORAGE

Problem	Possible Cause and Solution
"Data channel allocation failed" error appears in DataFort log	If too many backup jobs are run concurrently through a DataFort appliance, it can run out of encryption contexts. If this message appears, it means more drives are connected than are supported. As long as 7 drives or fewer are in use at one time, this message should not appear. If there is a reason that 8 or more drives must be used concurrently, write buffering should be reduced by running the following CLI command: <code>system property set dfc.num_buffered_tape_write_requests 2</code>
Delay when changing permissions	- When permissions are changed for a port-mapped Cryptainer, the default DataFort behavior is to disable the virtual port, wait 10 seconds, then re-enable the virtual port. This behavior was added to cause NetApp filers to rescan the fabric and register the new tape devices. This 10 second outage interrupts I/O for other hosts and can be problematic in disk configurations. - Disable this behavior by setting <code>dfc.isp.reenable_host_side_vp</code> to false. This should be done in all disk environments.
Cannot write to a used tape	- The application instructs DataFort where to write on the tape. DataFort reads blk0 to determine if it is a cleartext tape or an encrypted tape. If it is a cleartext tape, then it waits for a command to write blk0. If it can successfully write blk0, then it can write to the tape. If the application tries to skip writing blk0 but instead tries to append to the tape, DataFort denies the access through an encrypted pool. - In NBU, fix this by expiring the tapes by using the <code>bpexpdate -m <media_id> -d 0 -force</code> command. This creates a blank tape and permits DataFort to write blk0 when instructed to do so. When expiring the tape in NBU using this command and initiate a write through DataFort, all data on the tape/media_id in question is gone. - In Legato, the "label media" command does the same thing. There are equivalents in other backup applications.
DataFort appliance cannot see host or storage; error "Proxy is not initialized or an invalid board number is specified: Invalid argument"	- Possible cause #1: DataFort was restored from an XDF backup file but not rebooted. Solution: Log in to the DataFort CLI and run the command <code>system reboot -p</code>. - Possible cause #2: DataFort is in a cluster and was rebooted while the cluster was in a disabled state. Solution: When a cluster is in aborted state, the functional DataFort appliances should not be rebooted unless the offline member(s) are disabled. If the DataFort has been rebooted, or to disable the offline members, log in to the DataFort CLI and run the command <code>cluster disable <MEMBER_IP name></code>. This allows the cluster state to become committed and online. Until the cluster communication is fixed, however, cluster replication does not occur. Once the cluster replication issue has been fixed, re-enable clustering on the disabled members by running the command <code>cluster enable <MEMBER_IP name></code>.

DECRU DATAFORT OPERATION WITH NETAPP FILER

CISCO MDS 92XX SERIES FC SWITCH - NETAPP FILER APPEARS OFFLINE

A NetApp® filer may appear as offline with Port ID 99999 on the DataFort appliance, or fail to detect devices through the DataFort appliance when using a Cisco MDS 92XX series FC switch.

Use the following steps to configure the filer to work with DataFort and Cisco MDS 92XX switches. When presenting new devices to a NetApp filer, old aliases must be deleted and the filer HBA must be disabled and then re-enabled.

1. On the Filer, run the command `storage unalias -a` to purge all existing tape and media changer aliases.
2. On the FC switch, zone the filer HBA in the same zone as the Host HBA of the DataFort appliance.
3. On the DataFort appliance, create Cryptainers and grant access to the Filer.
4. On the Filer, disable the Filer HBA by running the command `fcadmin offline <HBA #>`.
5. On the Filer, re-enable the Filer HBA by running the command `fcadmin online <HBA #>`.
6. On the Filer, run the commands `storage show tape` and `storage show mc` commands to see the tape drives and media changers.
7. On the Filer, run the command `sysconfig -t` to see the tape name that will be used by the backup program.
8. On the DataFort appliance, verify that the Filer is online.

If the NetApp Filer appears offline on the DataFort appliance following a permission change on Cryptainers, run the command `show storage tape` on the NetApp Filer to bring it back online.

DECUR DATAFORT OPERATION WITH FUJITSU SIEMENS CENTRICSTOR

Fujitsu Siemens Computers CentricStor is a virtual tape library for open systems and mainframe environments. FSC and Decru have certified the devices for interoperability where the Decru DataFort appliance sits between the backend CentricStor IDP(s) and the physical Fibre Channel tape drives.

Consider the following to ensure interoperability and optimal performance of the system.

- A SCSI driver running on top of the CentricStor's tape-side FC miniport is only capable of utilizing target IDs from 0-15. By default, the first virtual storage device at the DataFort appliance appears at target ID 130. Therefore, CentricStor cannot address the default device mappings from the DataFort appliance.
- CentricStor only communicates with LUNs 0 and 1 on a given target. Tape drives can only be used at LUN 0; robots may exist at LUNs 0 and/or 1. Therefore, tape drives secured via LUN Mapped Cryptainers cannot be addressed by CentricStor.
- Virtual tape targets (ICPs) on the host-side of CentricStor compress data before writing it to the disk cache in the VTL. Compressed data is then read from the disk cache and written to tape drives by the storage-side data movers (IDPs). This is a consideration when deciding whether to enable compression with the DataFort appliance when using ICP compression.

To allow CentricStor to address DataFort appliance targets, the loop ID of the DataFort appliance host side must be set to a number that will map to an addressable target ID at CentricStor. When the system property `dfc.isp.host_vp_base_loopid` is set to a non-zero value, the base DataFort WWN is discovered at the specified target ID. The 1st virtual storage device appears at target ID+1, the 2nd virtual target at ID+2, and so on. For CentricStor interoperability, ensure that all virtual targets are set to target IDs of 15 or lower.

To set the system property, log in to the DataFort CLI and run the following command:

```
system property set dfc.isp.host_vp_base_loopid <non_zero_integer>
```

LUN Mapped Cryptainers are not supported with CentricStor. To allow CentricStor to address virtual targets and LUNs at the DataFort appliance, use Port Mapped Cryptainers.

Note: Not all Fibre Channel switches support the FL-login required for creating multiple virtual storage targets at the DataFort appliance.

Leave compression enabled at the DataFort appliance, even if ICP compression is enabled at CentricStor. The ICP compression is not as efficient as tape drive compression; Fujitsu Siemens reports that tape drives will typically be able to compress the ICP-compressed data by an additional 10 percent or more. The DataFort appliance realizes compression ratios comparable to those of LTO-family drives, and customers realize better performance and tape utilization characteristics when compression is enabled.

DECRU DATAFORT OPERATION WITH EMC

Consider the following when operating DataFort with EMC (disk licensed DataFort only).

SYMMETRIX

1. Create zones between the Symmetrix and DataFort Storage HBA, and between the server and DataFort Host HBA.
2. Using Port Mapping, create a Cryptainer on LUN 0 of the Symmetrix (the VC MDB) and DO NOT encrypt it (the Symmetrix will not allow it).

ESN running on the host will be able to find it and communicate through the DataFort appliance to allocate more volumes to the DataFort storage HBA.
3. Run `symcf discover` to find the Symmetrix devices connected to the host. Run `vcmf find` to verify that the host can communicate with the Symmetrix.

At this point ESN Manager will work as usual. ESN Manager will show the DataFort appliance's Storage HBA as belonging to the host.

If multiple hosts are connected to a Symmetrix through a shared DataFort, ESN Manager will show that all the volumes secured by the DataFort appliance are assigned to the host on which ESN Manager is running. This is expected because all access to the Symmetrix is through the DataFort's storage HBA, so the Symmetrix is accessed through a single WWN.

4. Using the DMC, assign the Cryptainers to individual hosts.

CLARiiON

After proper zoning, the DataFort WWN should log in to the CLARiiON (this may require a reboot of the DataFort). After that, complete the following:

1. In Navisphere's host tab, right-click on the CLARiiON and go to the Connectivity Status link. This launches a window detailing all the connected systems.
2. The DataFort appliance's WWN shows up here but, due to no agent, it is unregistered.
3. After selecting the DataFort appliance's WWN, click on the Register button.
4. Register the DataFort appliance either as a standalone (add it as new) or a cluster (add the first as new and for the second use the existing option).
5. After this the Decru storage group appears in Navisphere. Click the LUN tab in this group to bring up the available LUNs.

DECRU DATAFORT OPERATION WITH SOLARIS

If a Solaris host is attached directly to the DataFort, verify that the Qlogic HBAs are configured to be in "loop only" mode.

It is recommended to use persistent name binding on Solaris:

- For Emulex HBA: use lputil64
- For QLogic HBA: edit the /kernel/drv/qla2200.conf file.

The comments in the file explain the syntax.

Bind the HBA to a specific name so that it always comes up as hba0:

```
hba0-adapter-node-name="200000e08b000716"  
hba0-adapter-port-name="515000e08b000716"
```

Replacing a DataFort appliance requires modification of the name binding for the Primary Port (used for LUN Mapping) of the DataFort appliance. The Virtual Ports (used for Port Mapping) retain the originally assigned WWNs.

The device names of storage presented by the DataFort appliance may be different than device names when connected directly. Therefore when attaching to a stripe or RAID-5 volume on Solaris, the system must be updated with the new name assigned.

It is not recommended to put all copies of the volume database on the disks that are secured by the DataFort appliance.

MIGRATING METATOOL VOLUMES TO A DATAFORT

Change persistent binding settings on the host so that the device numbers do not change after DataFort installation.

On Solaris this is done by editing the <hba driver>.conf file. The procedure should be outlined in the host's HBA documentation.

After changing persistent binding settings, see:

- [Stripe](#)
- [RAID](#)

Stripe

Create a stripe on Solaris by doing the following:

1. Run the following command:

```
# metainit d0 1 3 c1t32d0s6 c1t33d0s6 c1t34d0s6
```

This describes a 3 disk stripe volume using the user partition of disks at target id 32, 33, and 34. This is the directly connected case.

2. The disks must first be labeled. Create a file system on the 3 disk stripe volume.

```
# newfs /dev/md/rdisk/d0
```

3. Mount the file system at the point /mnt/volume.

```
# mount /dev/md/dsk/d0 /mnt/volume
```

The volume is now available for use.

Unmount the volume to attach through the DataFort appliance:

1. Create cleartext Cryptainers for each disk in the stripe (in this case the disks at targets 32, 33, and 34).
2. Use the 'devfsadm -C -v' command in Solaris once the cleartext Cryptainers are created and shared with the Solaris host.
3. Verify that the disks are shared in the Solaris 'format' utility.
4. If zoning is used, the original names of the disks should no longer be listed.

Create a stripe with the new disk names through the DataFort appliance (there is a 1 to 1 relationship for each disk). It is critical to create a cleartext Cryptainer for each disk in order of the stripe.

1. Locate the device names of the disks presented by the DataFort appliance (for this example, c1t109d1s6, c1t109d2s6 and c1t109d3s6 are used). The information can be found in the output of devfsadm or in /var/adm/messages.

```
# metainit d1 1 3 c1t109d1s6 c1t109d2s6 c1t109d3s6
```

In the previous line, the disk previously named c1t32d0 is shared as a cleartext container in the DataFort appliance as VLUN 1, and has the new name c1t109d1, etc.

There is no need to create a file system since that is already done.

2. A mount should work right away:

```
# mount /dev/md/dsk/d1 /mnt/volume
```

The existing data should appear at this point.

3. Next delete the old stripe and rename the new to the old.

```
# metaclear d0
```

```
# metarename d1 d0
```

RAID

Create a RAID-5 volume on Solaris.

1. Run the following command:

```
# metainit d0 -r c1t48d0s6 c1t49d0s6 c1t50d0s6
```

This describes a 3 disk RAID-5 volume on the usr partition of disks at target ids 48, 49, and 50. This is the directly connected case.

2. The disks must first be labeled in format. Create a file system on the 3 disk RAID-5 volume. Run the following command:

```
# newfs /dev/md/rdisk/d0
```

This creates a file system on the 3 disk RAID-5 volume.

3. Mount the file system at the point /mnt/volume.

```
# mount /dev/md/dsk/d0 /mnt/volume
```

Now use the volume as storage as needed to attach through the DataFort appliance.

4. Unmount the volume.
5. Create cleartext Cryptainers for each disk in the RAID-5 volume (in this case the disks at targets 48, 49, and 50).
6. Use the '# devfsadm -C -v' command in Solaris once the cleartext Cryptainers are created and shared with the Solaris host.
7. Verify that the disks are shared in the Solaris 'format' utility. If zoning is used, the original names of the disks should no longer be listed.

It is critical to create a cleartext Cryptainer for each disk in order of the RAID-5 volume.

Create a RAID-5 volume with the new disk names through the DataFort appliance as follows. There is a 1 to 1 relationship for each disk.

1. Run the following command:

```
# metainit d1 -r c1t109d1s6 c1t109d2s6 c1t109d3s6 -k
```

In the previous line, the disk named c1t48d0 is shared as a cleartext container in the DataFort appliance as VLUN 1 and has the new name c1t109d1, etc.

There is no need to create a file system since that is already done.

The '-k' option at the end of the metainit command is critical, since the existing data should not be affected at all and by default the RAID is re-initialized.

2. A mount should work right away:

```
# mount /dev/md/dsk/d1 /mnt/volume
```

The existing data should appear at this point.

3. Next, delete the old stripe and rename the new to the old:

```
# metaclear d0
# metarename d1 d0
```

VERITAS VOLUME MANAGER

Replacing DataFort in a Cluster Connected to a Solaris Host with Veritas

1. If the path through the DataFort appliance is currently active, first disable the controller in Veritas DMP (assuming c2 is the controller connected to the DataFort appliance):

```
# vxdmpadm disable ctrlr=c2
```

The other path is now responsible for transferring all data.

2. Replace the DataFort appliance and reestablish the cluster. For details see [Replacing a DataFort in a Cluster](#) on page 158.
3. Re-enable the controller:

```
# vxdmpadm enable ctrlr=c2
```

The second path should be back and available to transfer data.

If the second path was not active at the start, the operating system has likely disabled the failed secondary path.

4. Rescan using Veritas on the host:

```
# vxdiskconfig
```

In this case the path provided by the secondary DataFort appliance is shown as a third path. One is unavailable and there are again two available paths.

```
c2t1d1s2      Disabled
c2t0d1s2      Enabled
c3t1d1s2      Enabled
```

The operating system has held onto the earlier failed path. The failed path can be removed, but this breaks the data transfer. It is not necessary and should be done when convenient:

```
# reboot -- -r
```

On a Microsoft Windows host, right-click the Not Healthy path and select Purge Disks.

DECRU DATAFORT OPERATION WITH LEGACY ENCRYPTED TAPES

In order for tapes encrypted by previous DataFort versions (including 1.6 and 1.8 releases) to be read:

1. Log in to the CLI of one member of the cluster and run the following command:
`system property set crypto.legacy.loadr1r2 true`
2. Power cycle all DataFort appliances in the cluster.
3. Follow the instructions in the guide Upgrading the DataFort FC-Series from Version 1.6 or 1.8 to Version 2.1 available from Decru.

DECRU DATAFORT OPERATION WITH TIVOLI AND STK DRIVES

On certain operating systems (mainly AIX), Tivoli cannot be easily configured to use a block size of more than 256K, the maximum supported block size for STK 9840 and 9940 tape drives. In this case, DataFort must be put into preserve-block-size mode.

1. Log in to the CLI of one cluster member and run the following commands (in this order):

```
sys prop set dfc.tape_compression_forced true
sys prop set dfc.tape_preserve_blocksize true
```

No reboot is necessary.

Note: If these tapes are restored by another DataFort cluster, it is important to set these properties on the destination cluster too.

DECRU DATAFORT OPERATION WITH LT02 SERIALIZED COMMANDS

If a backup or restore to an LT02 tape drive fails and the drive returns CheckCondition, Aborted Command and Overlapped Command Attempted (0x4e/0x00), run the following CLI command while there is no data I/O:

```
system property set dfc.serialize_storage_cmds true
```

DECRU DATAFORT AIX ATAPE FAILOVER SUPPORT

Atape (Tape Driver) on AIX provides device driver level support for tape failover. If an AIX host with Atape multipathing enabled has two or more paths to a tape drive, the Atape driver keeps track of these different paths, and in the event of errors on one path, it switches traffic to one of the alternate paths. This switch is transparent to the application in control of the tape drive.

With DataFort in the system, AIX Atape should be able to provide same support for different paths to one tape drive. The typical scenario would have AIX host connected to two clustered DataFort appliances through different HBAs. The two DataFort appliances would see the same tape drive connected using different ports.

If the primary (PRI) path fails during a backup, the Atape driver tries to switch over to the alternative (ALT) path, and then due to the other DataFort appliance not having proper key information, the switchover fails. The solution is to broadcast key information to all members of a cluster with paths to a Cryptainer. To support this configuration, run the following CLI command:

```
system property set dfc.tape_multipathing_enable true
```

ATAPE LOAD BALANCING SUPPORT

Atape provides dynamic load balancing support to optimize resources for devices that have physical connections to multiple HBAs in the same machine. Dynamic load balancing uses all HBAs whenever possible, and balance the load between them to optimize the resources in the machine. With DataFort in the system, Atape should be able to provide same support for different paths to one tape drive. To support this configuration, run the following CLI command:

```
system property set dfc.tape_multipathing_enable true
```

ATAPE OPERATION LIMITATIONS

Atape failover support is only available for the host-side connection of the DataFort appliance. If a link failure occurs on the host-side connection during a backup job, it properly fails over to the other DataFort appliance and continues the job.

If the link failure occurs on the storage-side connection during a backup job, that particular job aborts, and failover does not occur. However, in this case switchover still occurs, meaning that even though the job failed, the host receives an error and switches over to run the next backup job over the other HBA.

For Atape driver versions 9.5.8.0 and above, the DataFort appliance must be set to IEEE Registered Name mode, meaning the host-side HBA of the DataFort appliance must be set to the same WWN as the IBM tape device. This is required as Atape drivers (9.5.8.0 and above) use hard-coded checks for IBM WWNs to enable multipathing on drives.

The Atape multipathing feature is supported on clustered DataFort appliances or between different boards of the FC1020 DataFort appliance. Standalone DataFort appliances cannot be used for Atape multipathing.

DECRU DATAFORT SCSI RESERVATION HANDLING FIXES

Reservation state is handled by DataFort when hosts are not virtualized. This is necessary because all hosts are presented to storage by a single (DataFort storage-side) WWN.

SCSI-2 and SCSI-3 reservation handling is supported by DataFort for both LUN and Port-mapped Cryptainers. A Host can reserve a disk through the DataFort appliance.

Note: This feature is disabled when hosts are virtualized.

To set DataFort to handle SCSI-3, run the following CLI command:

```
system property set dfc.handle_persistent_reserve true
```

To list the SCSI reservations:

```
kfc reservation list
```

To clear the SCSI reservations:

```
kfc reservation clear <disk port wwn> <disk lun>
```



■ ■ ■ ■ **APPENDIX I COMMAND LINE INTERFACE QUICK REFERENCE**

The CLI gives the administrator access to many DataFort management functions, but cannot be used for functions that require the presence of smart cards. The DMC is the only interface that allows management of smart card enabled operations. This chapter includes the following topics:

- [Using the CLI](#)
- [CLI Command Overview](#)

Refer to the separate [DataFort CLI Reference Guide](#) for a complete list of commands and parameters.

USING THE CLI

Some CLI commands must be executed in a specific order for desired results. For some commands, it is good practice to execute a verification command (such as `list`) after an action that adds an item to the database. Always perform a backup of the database after any changes.

- For login instructions, see [Connecting to the Command Line Interface](#) on page 72. There are two levels of security that can be set for DataFort CLI login, one of which requires first accessing the DMC before logging into the CLI.
- As a security measure, the CLI times out after 10 minutes of inactivity.

CLI SYNTAX

- In the following pages, an ellipsis (...) after an entry indicates that the entry is a hierarchy, rather than a command. The top level commands include `system...` because there is no end command `system` although there is a system hierarchy of commands (`system reboot`, etc.).
- The plus (+) symbol indicates that an entry is a command which can take arguments. The command `quit` is not followed by + because it does not take arguments.
- Note that + and ... are not intended to be typed in as commands, but serve as indications that more can be typed after a given entry.

CLI HELP

Note: The DMC CLI does not have the same help features as the full CLI. Type `help` to use help in the DMC CLI.

- 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.
- Typing a partial command phrase followed by `?` gives the same results as above.
- 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.
- Pressing tab after a command autofills 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`.

CLI COMMAND OVERVIEW

TOP LEVEL COMMANDS

Type **help** to view top level commands.

device...	SAN storage device commands...	Device Commands
disk...	SAN disk commands...	Disk Commands
fcsite...	DataFort Fibre Channel site configuration commands...	FC Site Commands
fccryptainer...	SAN Cryptainer commands...	FCC Cryptainer Commands
host...	SAN host commands...	Host Commands
kfc...	SAN kernel commands.	KFC Commands
pool	SAN pool (tape) commands...	Pool Commands
tape...	SAN tape commands...	Tape Commands
cli...	Command line commands...	CLI Formatting Commands
help +	Command line usage help	Help Command
quit	Quit the current client session	Quit Command
active-role...	Active role commands...	Active-Role Commands
authorize +	Authorize admin login	Authorize Command
password +	Change user password	
role...	Role commands...	Role Commands
user...	User commands...	User Commands
whoami	Display effective user ID	Whoami Command
trustee	Trustees management commands...	Trustee Commands
net...	Network commands...	System Commands
keyman...	Key management commands...	Key Management Commands
lkm...	LKM management commands...	LKM Management Commands
cluster...	Cluster commands...	Cluster Commands
db...	Database administration commands...	Database Commands
system...	System commands...	System Commands

DEVICE COMMANDS

Type **device ?** to view device commands

group...	Device group commands...
list +	List all storage devices
map +	Setup Paths from Primary storage device to an Alternative storage device
rmmap +	Remove Paths from Primary storage device to an Alternative storage device
set +	Set storage device settings

DISK COMMANDS

Type **disk ?** to view disk commands

blink +	Blink LED on a disk (JBOD device)
cryptocopy...	Crypto Copy commands...
list +	List all disks in the configuration database
map +	Map a disk to a Cryptainer
metadata...	Disk metadata commands...
path +	List all paths to the disk
purge	Purge disks that are offline and have no Cryptainers
remove +	Remove a disk/LUN by its port WWN
replace +	Replace a disk
rescan	Force DataFort to rescan the fabric for disks
rmail +	Remove all LUNs of a disk
rmmmap +	Remove mapping of a disk to a Cryptainer
set +	Set disk settings
unhideall	Show all hidden disks

FC SITE COMMANDS

Type **fcsite ?** to view fcsite management commands.

list +	List all the FC sites in the configuration database
remove +	Delete the FC site settings for the specified DataFort
replace +	Make the local DataFort a replacement for the specified FC site

FCC CRYPTAINER COMMANDS

Type **fccryptainer ?** to view Cryptainer management commands.

add +	Add a Cryptainer
clone +	Create a new Cryptainer for a copied LUN
createall +	Create Cryptainers
grant +	Grant permission on Cryptainer to a host
group...	Cryptainer group commands...
keys...	SAN Cryptainer keys commands...
list +	List Cryptainers
path +	List Cryptainer paths to disks
perm...	SAN Cryptainer permission commands...
rekey...	SAN Cryptainer rekey commands...
remove +	Remove one Cryptainer and its contents
restore +	Restore a Cryptainer using the specified key
revoke +	Revoke permission on Cryptainer from a host
rvall +	Revoke all permissions from a Cryptainer
rmail +	Remove all Cryptainers from database
set +	Change Cryptainer settings

HOST COMMANDS

Type **host ?** to view host management commands.

add +	Add a host
auth...	Host WWN authentication commands...
group...	Host group commands...
list +	List hosts
purge	Purge hosts that are offline and have no permissions to Cryptainers
remove +	Remove a host
rescan	Force DataFort to rescan the fabric for hosts
set +	Set host settings
unvirtualize+	Unvirtualize a host
virtualize+	Virtualize a host

KFC COMMANDS

Type **kfc ?** to view fibre channel kernel commands.

config	Configure FC kernel
fw...	SAN kernel firmware commands...
list +	Display SAN kernel statistics
link...	SAN kernel link commands...
request...	SAN kernel Request commands...
reservation...	SAN kernel Reservation commands...
sync	Query the fabric to update the status of all devices
util...	SAN kernel utility commands...
vp...	SAN kernel virtual port commands...
wwn...	Fibre Channel primary port node/port WWN utils...

POOL COMMANDS

Type **pool ?** to view pool commands.

add +	Add a pool
grant +	Grant pool access to a host
group...	Pool group commands...
key...	Pool key commands...
list +	List pools
perm...	List pool permissions...
remove +	Remove a pool
revoke +	Revoke pool access from a host
set +	Set pool settings

TAPE COMMANDS

Type **tape ?** to view tape commands.

history +	List tape keys history
list +	List tapes
remove +	Remove a tape

CLI FORMATTING COMMANDS

Type **cli ?** to view CLI formatting commands.

complete +	Command line completion
cshep...	CLI context-sensitive help commands...
documentation +	Print CLI documentation (cli documentation according to the role of user that is logged in)
format +	Change CLI display format
pager +	Turn on/off screenful CLI output display pager

HELP COMMAND

Type **help** to view the top level command list.

help +	Command line usage help
---------------	-------------------------

QUIT COMMAND

Type **quit** to quit the CLI session.

quit	Quit the current client session
-------------	---------------------------------

ACTIVE-ROLE COMMANDS

Type **active- ? role to** view active role commands.

add +	Activate an authorized role
list	List active roles
remove +	Remove an active role

AUTHORIZE COMMAND

Type **authorize** to authorize an admin login

authorize	Authorize an admin login
------------------	--------------------------

PASSWORD COMMAND

Type **password** to change an admin password.

password +	Change password
-------------------	-----------------

ROLE COMMANDS

Type **role ?** to view role commands.

list +	List roles
path...	Role path commands...

USER COMMANDS

Type **user ?** to view user commands.

add +	Add a user account
list +	List all users in database
remove +	Remove a user from the database
role...	User role commands...
set +	Set user settings

WHOAMI COMMAND

Type **whoami** to see the current user ID.

whoami	Display effective user ID
---------------	---------------------------

TRUSTEE COMMANDS

Type **trustee ?** to view trustee commands.

delete +	Remove trustee from the system
keys..	Trustee key export and import commands...
list +	List all the approved trustees in the system
unapproved..	Trust establishment commands for unapproved trustees...

NETWORK COMMANDS

Type **net ?** to view network management commands.

apply +	Apply network changes
connection...	Network connection administration commands...
interface...	Network interface commands...
status +	Display network status
util...	Network utilities...

KEY MANAGEMENT COMMANDS

Type **keyman ?** to view key management commands.

cryptainerkeys +	Query Cryptainer Keys
lkmkeys +	LKM key management commands...
masterkeys +	Query Master Keys
purgekeys	Purge unused Cryptainer and Master Keys

LKM MANAGEMENT COMMANDS

Type `lkm ?` to view Lifetime Key Management commands.

<code>status</code>	Check the status of the connection to the configured LKM System
<code>server...</code>	Server commands...

CLUSTER COMMANDS

Type `cluster ?` to view the cluster commands.

<code>config...</code>	Cluster configuration commands...
<code>disable +</code>	Disable clustering
<code>enable +</code>	Enable clustering
<code>rexec +</code>	Execute a command on member DataFort(s)
<code>rsh +</code>	Execute a remote shell on one member DataFort
<code>status</code>	Check configuration database status

DATABASE COMMANDS

Type `db ?` to view database management commands.

<code>begin</code>	Begin a transaction
<code>commit</code>	Commit the current transaction
<code>connect +</code>	Connect to configuration database
<code>export</code>	Export the configuration database as xml to stdout
<code>index...</code>	Indexing administration commands...
<code>record +</code>	Get a configuration database record
<code>rollback</code>	Rollback the current transaction
<code>save</code>	Checkpoint database and save changes to disk
<code>size +</code>	Display database available space
<code>status</code>	Display configuration database status
<code>trx...</code>	Transaction administration commands...
<code>xlog...</code>	Transaction log administration commands...

SYSTEM COMMANDS

Type `system ?` to view system commands.

<code>agreement...</code>	Agreement commands...
<code>crypto...</code>	Crypto commands...
<code>check +</code>	Perform basic system checks
<code>date...</code>	Date commands...
<code>httpd...</code>	HTTPD commands...
<code>license...</code>	License commands...
<code>log...</code>	System log commands...
<code>ntpd...</code>	NTPD commands...
<code>property...</code>	Property commands...
<code>reboot +</code>	Reboot the system

selftest +	Perform system selftest
sensors	Display system sensors
serial	Display DataFort serial number
snmp...	SNMP commands...
sshd...	SSHD private key commands...
tamper...	Tamper commands...
timers...	System timer commands...
timezone...	Timezone commands...
upgrade +	Upgrade the system
util...	System utilities...
version +	Display the version of all system components
zeroize +	Zeroize all key material and delete configuration database

■ ■ ■ ■ APPENDIX II LOGGING FUNCTIONS

The appliance audit function logs security-relevant operations, errors, and warnings as well as many operations, errors and warnings that are not relevant to security.

Log messages are stored in one of multiple appliance logs, depending on the origin 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 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). See the following sections for information about logging:

- [Appliance Log Event and Priority Types](#)
- [Log Storage Locations](#)
- [Log Presentation](#)
- [Log Purging](#)

Log messages are detailed in a separate [Logging Addendum](#).

See [Configuring and Viewing Logs](#) on page 143 for information about configuring and viewing logs.

APPLIANCE LOG EVENT AND PRIORITY TYPES

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

TABLE 29: 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 30: 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.
<client>	IFC: The 8 byte WWN of the host requesting the information flow, formatted as 8 hex character bytes: XX:XX:XX:XX:XX:XX:XX:XX
	Audit: IP address from which the user is authenticating
<cryptainer>	The 16 byte ID of the Cryptainer from which the information flow is requested: 0xxxxxxxxxxxxxxxxxxxxxxxxxxxx
<cryptainer_group>	This parameter indicates a group of Cryptainers, as defined by the appliance administrator. The parameter is a text string, up to 31 characters.
<domain>	Domain name of the user that changed the configuration parameter
<host>	This parameter refers to a host, by WWN.

TABLE 30: PARAMETERS IN LOG MESSAGES (CONTINUED)

<host_group>	This parameter indicates a group of hosts, as defined by the appliance administrator. The parameter is a text string, up to 31 characters.
<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.
<pool>	Tape pool.
<pool_group>	Group of tape pools, as defined by the appliance administrator. The parameter is a text string, up to 31 characters.
<prop_name>	Name of a logging facility configuration property.
<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.
<serial_number>	Serial number of the appliance that denied or allowed the information flow.
<user>	Name of user that changed a configuration parameter or attempted to authenticate.
<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.
<wwn>	The 8 byte WWN of the host that is authenticating (DHA), formatted as 8 hex character bytes: XX:XX:XX:XX:XX:XX:XX:XX

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 the configured storage location(s). 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 31: DEFAULT LOG STORAGE LOCATIONS

Log	Default Location
High priority security log	database storage
Low priority security log	database storage
Operations alert log	database storage
Operations warning log	database storage
Operations informational log	database storage
Operations debug log	RAM storage: /var/log/operation
High priority performance log	database storage
Low priority performance log	RAM storage: /var/log/performance

LOG PRESENTATION

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

TEMPORARY LOGS

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

```
/var/log/security  
/var/log/operations  
/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 the DMC or CLI.

- [Viewing database logs via DMC](#)
- [Viewing database logs via CLI](#)

Viewing database logs via DMC

The administrator may view log messages stored in the database by selecting **Diagnostics > View System Log** in the DMC. See [Configuring and Viewing Logs](#) on page 143 for more information.

All log messages include:

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

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 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 the log containing 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 Alert Log
- <17.4>: Operations Warning Log
- <17.6>: Operations Informational Log
- <17.7>: Operations Debug 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.
- <20.6> Audit Log

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

<MSG> is the log message.

REMOTE LOGS

The formatting for exported log messages corresponds to the syslog protocol as specified in the syslog RFC. Exported log messages are listed in the following format:

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

<PRI> contains a syslog facility and severity indication as specified in the syslog RFC. The appliance logs map to syslog facilities and severities.

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

<MSG> is the log message.

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

```
<134>Mar  4 13 :49:36 boxmanager: Administrator login
from 10.10.10.10 succeeded 'admin' (sess id: 298053632)
```

TABLE 32: 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 Alert Log	LOG_LOCAL1 (17)	1,0
Operations Warning Log	LOG_LOCAL1 (17)	4
Operations Informational Log	LOG_LOCAL1 (17)	6
Operations Debug 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

Signed Logs

The appliance can be configured to sign log messages. See [Configuring and Viewing Logs](#) on page 143 for more information. The configuration option is available separately for each appliance log. If configured, metadata and signature fields are appended to the exported log message:

```
<PRI> <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 33: 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 Alert Log Operations Warning Log Operations Informational Log Operations Debug Log	Combined size of all operations logs	1000kB
High priority Performance Log Low priority Performance Log	Combined size of both performance logs	500kB

If numerous 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

A 10 second timer triggers 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.

■ ■ ■ ■ APPENDIX III PORT IDS

The DataFort FC-Series 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 1: 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	Mgmt/Client	no	no
500	UDP	ISAKMP	DataFort cluster isakmp interface	Mgmt/Client	yes	no
514	UDP	Syslog	DataFort remote logging interface	Mgmt/Client	no	no
15360	TCP	IPsec	Cluster heartbeat	Mgmt/Client	no	no
15361	TCP	IPsec	Cluster heartbeat	Mgmt/Client	no	no
16000	TCP	DCS	DCS	Mgmt/Client	no	no
N/A	ICMP	Ping	DataFort Ping Response	Mgmt/Client, Storage	yes	N/A
N/A	ARP	ARP	ARP network broadcast	Mgmt/Client	yes	N/A

A Communication Interface of “Mgmt/Client, Storage” means the appliance listens on the Mgmt/Client interface, and talks on the Storage interface (but does not listen on it).



■ ■ ■ ■ **APPENDIX IV SPECIFICATIONS**

- [Supported Systems](#) lists support for components of the DataFort system.
- [DataFort Appliance Specifications](#) lists DataFort hardware specifications.

SUPPORTED SYSTEMS

Please visit the Decru website for the most up-to-date information about DataFort interoperability.

TABLE 2: SUPPORTED PLATFORMS

Item	Component	Requirement
Management Station	System Requirements	2Ghz 1GB RAM 4GB free hard drive space An available USB port for the smart card reader from Decru (If no USB port is available, a serial smart card reader is available from Decru.) A CD drive for installing software Windows XP SP2 or Windows 2000 SP4 or Windows 2003 SP1
Hosts	System Requirements	Major Windows or Unix hosts, including Solaris, Linux, AIX, Irix, FreeBSD, Windows
Storage	Device Type	All leading storage devices, including JBOD, RAID and Enterprise Storage Systems.

DATAFORT APPLIANCE SPECIFICATIONS

TABLE 3: DATAFORT APPLIANCE SPECIFICATIONS

Item	Detail	Specification	
Hardware	Rack mountable	E515/FC525	Standard 19" EIA rack - 1U
		E510/FC520/ FC1020/S110	Standard 19" EIA rack - 2U
	Weight	E510	14.2 kg (31.3 lbs)
		E515	10.4 kg (22.9 lbs)
		FC520	12.8 kg (28.3 lbs)
		FC525	10.4 kg (22.9 lbs)
		FC1020	16.0 kg/35.3 lbs
		S110	13.7 kg/30.2 lbs
	Size	E515/FC525	43.2 cm W x 48.3 cm D x 4.4 cm H (17.00" W x 19" D x 1.73" H)
		E510/FC520/ FC1020/S110	43.2 cm W x 48.3 cm D x 8.9 cm H (17.00" W x 19" D x 3.5" H)
	Security	SEP FIPS Level 3 Physical Security, Tamper Evident Label, Intrusion Detection Circuit, Optional Chassis Lock, Optional CryptoShred button	
	Network Ports	E510/E515	2 Gigabit Ethernet (IEEE 802.3ab compliant) ports 10/100/1000Base-T, autonegotiation required
		FC520/FC525	1 dual-port HBA for storage network connectivity
		FC1020	5 dual-port HBAs for storage network connectivity
		S110	2 LVD SCSI (one host, one storage supporting daisy chaining)
	Management Ports	2 10/100/1000Base-T Ethernet ports (one used)	
	Serial Port	RJ45 serial console port	
	Power Supply	E510/FC520/ FC1020/S110	2 Redundant/Hot-Swappable/Universal Input 100-240V ~47-63 Hz, 5A
		E515/FC525	1 Cold-Swappable/Universal Input 100-240V ~47-63 Hz, 5A
	Fans	E510/FC520/ FC1020/S110	2 Hot-Swappable
		E515/FC525	1 Cold-Swappable
	LED	Power Status/Network Activity/ Fault Status	
	LCD	E510/FC520/ FC1020/S110	Liquid Crystal Display with touch screen
		E515/FC525	Liquid Crystal Display
	Smart Card	1 smart card reader	
Environment	Temperature	Operating Temperature: 5°C to 40°C (41°F-104°F) Storage Temperature: -10°C to 60°C (14°F-140°F)	
	Humidity	Operating Humidity: 85% RH at 40°C	

TABLE 3: DATAFORT APPLIANCE SPECIFICATIONS

Item	Detail	Specification
Regulatory Compliance	EMC	Canada ICES-003 Class B United States FCC Class B Japan VCCI Class A Korea RRL Class B European 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 6095 0-1
	Safety	United States UL 60950 - 1 Canada CSA 60950 - 1 Japan IEC 60950 -1 European Community EN60950, TUV R 2845 China CCC International CB IEC 60950 -1

■ ■ ■ ■ **APPENDIX V 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 4: 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 VI REGULATORY AND CERTIFICATIONS**

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

FCC B DECLARATION OF CONFORMITY

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

EUROPEAN UNION

Marking by the symbol CE indicates compliance of this Decru, A NetApp Company device to the EMC directives and the Low Voltage Directives of the European Union.

This is a class A product. In a domestic environment, this product may cause radio interference, in which case, the user may be required to take adequate remedial measures.

CANADIAN ICES-003

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

VCCI CLASS A STATEMENT

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用する
と電波妨害を引き起こすことがあります。この場合には使用者が適切な対策
を講ずるよう要求されることがあります。

VCCI- A

This is a Class A 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.



CE STATEMENT

The standards compliance label on the appliance contains the CE mark which 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:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

The following harmonized standards have been applied:

- EN55022: 1998 +A1: 2000 and A2: 2003, CISPR22:1997
- EN61000-3-2 (2000) / IEC 61000-3-2 (2000) Harmonics
- EN61000-3-3 +A1 (2001) / IEC 61000-3-3 (1994) Flicker
- EN55024: 1998 Plus A1: 2000 & A2: 2003, CISPR24:1997
- EN60950-1: 2001+A11: 2004
- EN 60825-1/IEC 60825-1, Class 1 Laser

KOREA MIC

사용자 안내문 : A 급기기

이기는 업무용으로 전자파 적합등록을 받은 기기 이오니, 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.

Note that this device has been approved for business purposes with regard to electromagnetic interference. If you find that this device is not suitable for your use, you may exchange it for a non-business device.

TAIWAN BSMI

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

This is a Class A Information Product. When used in residential environment, it may cause radio frequency interference. Under such circumstances, the user may be requested to take appropriate countermeasures.

■ ■ ■ ■ ■

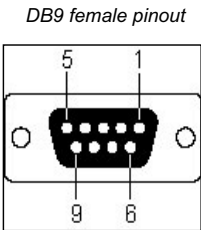
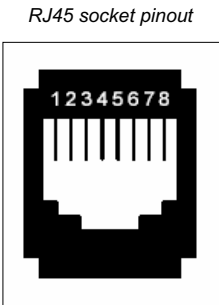
APPENDIX VII DATAFORT SERIAL ADAPTER

The Decru serial adapter is configured with the following pinouts.

Decru Serial Adapter Pinout

RJ45 (socket) - DB9 (female)

Sort by RJ45				Sort by DB9			
RJ45 (socket)	Color	Signal Name	DB9 (female)	RJ45 (socket)	Color	Signal Name	DB9 (female)
1	Blue	CTS	8	3	Black	RD	2
2	Orange	DCD/DSR	6	6	Yellow	TD	3
3	Black	RD	2	7	Brown	DTR	4
4	Red	RI	9	5	Green	SGND	5
5	Green	SGND	5	2	Orange	DCD/DSR	6
6	Yellow	TD	3	8	White	RTS	7
7	Brown	DTR	4	1	Blue	CTS	8
8	White	RTS	7	4	Red	RI	9



■ ■ ■ ■ APPENDIX VIII GLOSSARY

administrator	A type of user with specific privileges. The DataFort Full Administrator has the right to manage, create and delete user accounts, to create and delete Cryptainers, to control user access to certain Cryptainers, and to configure and maintain the DataFort.
Admin Card	A smart card used to authenticate a DataFort administrator. An individual possessing the Admin Card and the username and password for that card has privileges of a DataFort administrator. DataFort detects the presence of this card in the smart card reader attached to the Management Station.
AES	Advanced Encryption Standard. The official U.S. replacement for DES (and 3DES). AES allows for significantly stronger encryption than 3DES or DES, which was the official U.S. encryption algorithm until it was replaced by AES.
authentication	The process by which identity is established on a network. Typically, identity is established with username/password combinations (logging in to a computer) or using physical tokens (keys, smart cards). By default, DataFort requires both a username/password combination and a token to authenticate the DataFort administrator and Recovery Officers. DataFort can be configured to require only a username and password for management.
block cipher	An encryption algorithm in which data is segmented into fixed size blocks before processing. An algorithm is applied to each block.
chassis	The physical encasement of a device. DataFort is designed to resist and detect any attempt to open the chassis.
ciphertext	Encrypted data. A cryptographic cipher transforms cleartext data into ciphertext. Ciphertext appears to be random, obscuring the meaning of the original data. After encryption, only those with access to the encryption key can read the data.
cleartext	Data before encryption. Unencrypted data is clear in the sense that anyone with access to the data can read it.
cluster	A cluster is a set of interconnected devices. If one fails, the other can continue providing the service. By clustering DataFort appliances, total system redundancy is increased, reducing the likelihood of any downtime.
Common Criteria Mode	The Common Criteria is an international standard for evaluating information technology security. The ability to run in a mode qualified to meet Common Criteria standards is an enhanced security option for DataFort.

configuration database	The database stored inside DataFort hardware which contains network and security information, ACLs and encrypted key material.
Cryptainer	A Cryptainer is a specially designated directory or LUN. Data within a Cryptainer can be 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.
DataFort CLI	The command line interface used to manage the DataFort device. The CLI allows remote users to log in to DataFort and administer it by entering text commands over SSH.
Decru Management Console (DMC)	A graphical user interface used to manage the DataFort device via a Java application run on the Management Station over a secure connection.
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 SAN appliances (such as the 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.
JBOD	Just a Bunch of Disks. A collection of disks in a single chassis. Disks in a JBOD are exposed directly to the network. They may be virtualized by a network appliance or by software running on the servers.
key	In cryptography, a key is a value applied to cleartext (using an algorithm) in order to generate ciphertext, or applied to ciphertext to generate cleartext. Each cipher requires a key in order to encrypt or decrypt data.
Lifetime Key Management (LKM)	Decru's proprietary solution for encryption key management. LKM software and the LKM appliance both store key information.
Management Station	A Windows PC equipped with a smart card reader, from which a DataFort administrator can manage the DataFort appliance via the Decru Management Console (DMC).
Master Key	The Master Key is generated by DataFort at initialization time, and is unique to each DataFort. It is ultimately required in order to decrypt other keys in the configuration database.

MIB	Management Information Base. A set of network objects that can be managed using the Simple Network Management Protocol (SNMP).
Mirroring	When a disk is mirrored, its content is written to a second disk at real-time or near real-time with every write to the disk. The disk can be mirrored block-for-block or file-for-file. The mirroring process can be initiated and managed by a server, by a SAN appliance, or by the storage system itself. Applications include backup and disaster recovery.
Node WWN	A 64-bit identifier used to associate several Fibre Channel ports connected to the same device.
NTP	Network Time Protocol, used to synchronize computer clocks on the Internet.
Port Mapping	Associating a storage device with a virtual device presented by the DataFort. Port Mapping creates a virtual port which DataFort maps to the actual storage port on the target.
Port WWN	A 64-bit identifier that uniquely identifies a Fibre Channel port. A device will typically have a single, unique, node WWN and one port WWN for each port on each HBA.
quorum	The minimum number of Recovery Officers required to complete sensitive DataFort management procedures.
Recovery Cards	Recovery Cards are special smart cards used in sets to store and recover DataFort encryption keys by sharing a secret. Recovery Cards are given to the Recovery Officers, who will have to present them in order to perform security-sensitive procedures.
Recovery Officers	Recovery Officers are entrusted with keeping Recovery Cards and their associated passwords safely. Recovery Officers must present their cards and passwords to initialize a new DataFort. A quorum of Recovery Officers is required for other sensitive options such as data recovery, cluster authentication, and Recovery Card replacement.
SAN	A Storage Area Network (SAN) is a high-performance network dedicated to the transmission of storage data. It is often (but not necessarily) implemented with Fibre Channel.
secret sharing	A split knowledge procedure, whereby several parties are each given a portion of some secret data. In order to recover the data, a predetermined number of parties must combine their portions. In the DataFort system, this process is used when DataFort assigns a portion of a high-level cryptographic key to each Recovery Card. A quorum of Recovery Cards is required to reconstitute the key.
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 DataFort appliances.

smart cards	Credit card-sized devices with embedded microchips used by DataFort for authentication procedures.
SNMP	Simple Network Management Protocol. A protocol for network management and monitoring of network devices.
SSH	Secure Shell or Secure Socket Shell. A command interface and protocol used for remote access to a computer. SSH communication with the remote computer is encrypted.
SSL	Secure Sockets Layer. A protocol providing secure message transfer over the Internet. Used to secure transmission of data via web browsers.
Storage Encryption Processor (SEP)	DataFort's hardware encryption/decryption engine, which enables gigabit-speed, full duplex encryption.
System Card	A smart card provided by Decru which is inserted at the front panel of DataFort for boot-up to enable DataFort encryption services. The System Card may be removed during normal operation to prevent unauthorized use of DataFort upon reboot.
TLS	Transport Layer Security. A protocol providing secure message transfer over the Internet. Used to secure transmission of data via web browsers.
Trustee	A trustee is a remote DataFort with which a trust relationship has been formed, allowing Cryptainer Keys to be shared. A trustee may import from or export to a trustee.
Trustee Acceptance Package (TAP)	The second message between DataFort appliances when setting up a trustee relationship.
Trustee Establishment Package (TEP)	The first message sent between DataFort appliances when setting up a trustee relationship.

INDEX

A

- access control for tape 110, 112
- active I/O limit per appliance 23
- adapter, crossover RJ45 to DB9 75
- adding and removing cluster members 157
- Admin Card 18, 19, 252
- administrator 19, 252
 - add 81, 86
 - change password 84
 - change the card association 84
 - delete profile 84
 - log in to CLI 72
 - number recommended 81
 - require login authorization 82
 - roles outlined 79
 - specialty administrator, create 81
- administrator roles, CLI 184
- AES 16, 252
- alert, clearing 135
- appending ciphertext 108
- appending cleartext 108
- appliance
 - CLI, connecting to 72
 - defense setting 134, 135
 - licenses 166
 - menu 174
 - recovery 198
 - remove, custom group 170
 - restoring a previous configuration 198
 - upgrading 165
 - zeroizing 148
- ARP table 188
- Atape 218
- authentication 18, 252
- authorization for login 82
- authorizing administrator 82
- auto-detected pools 110, 112

B

- back up
 - appliance configuration 27, 128, 132
- backup topologies 33
- backup, data

- Client-free 33
- LAN-based 33
- LAN-free by Client 33
- planning 33
- SAN Mirroring 34
- Server-free 33
- battery v, 41
- block cipher 252

C

- Category 5 cable 20, 47
- certificates
 - setting security certificate 151
- certificates lost after zeroization 148
- change password
 - administrator 84
- change password, Recovery Card 140
- changing media type 196
- chassis 17, 252
 - intrusion 134
- ciphertext 16, 252
- ciphertext and cleartext 25, 92, 94, 252
- CLARiiON 210
- clear all appliance settings 148
- clear an intrusion (defense alert) 135
- clear smart cards 141
- cleartext 16, 92, 94, 101, 110, 252
- cleartext Cryptainer 92, 94
- cleartext pools 110
- cleartext tape 29
- CLI 72
 - command help 183, 221
 - commands and admin roles 184
 - connect from SSH client 72
 - disable Secure DMC 202
 - disk management 189
 - DMC access 74
 - documentation 183, 221
 - general information 183, 221
 - help 225
 - host management 191
 - log in 72
 - permissions 182

- quick reference 220
- quit 225
- system commands 186, 227
- time-out 221
- top level commands 222
- CLI login with dual authentication 73
- cluster 252
 - adding member 157
 - change to standalone 157
 - check cluster state 86
 - commands, CLI 227
 - configuration 26
 - conflict 156
 - disable command 185, 203
 - forming, after initial setup 157
 - IPsec tunnel 26
 - management 153
 - management using CLI 185
 - network diagram 29, 32
 - quorum 157, 185
 - recovery guidelines 159
 - remove member 157
 - replace an offline member 158
 - requirements 157
 - resolving conflict 156
 - restore previous configuration 159
 - size 153
 - state 155
 - switch connections, planning 26
 - troubleshooting 203
- cluster-wide operations 155
- Command Line Interface
 - log in 72
- Common Criteria 16
- configurable security levels 138
- configuration
 - menu 176
- configuration backup 132
- configuration database 18, 253
 - applied to new appliance 198
 - back up using DMC 132
 - backup to LKM 129
 - changes synchronized in cluster 26
 - commands, CLI 227
 - contents 128
 - event log capacity 143
 - size 130
 - used for recovery 198

- configuring table columns 173
- create
 - custom group 169
- create a Cryptainer 103
- Cryptainer 253
 - before creating 85
 - collections 89
 - creating, with DMC 89
 - creation and management 89
 - defined 17
 - encryption after creation 92, 94
 - encryption key 17
 - granting host access, CLI 193
 - management with DMC 100
 - management, with DMC 102
 - permissions 92
 - rekey with CLI 193
 - remove all host access, CLI 194
 - restore 116
- Cryptainer ID 116, 189, 194
- Cryptainer Key ID 104
- Cryptainer management
 - with CLI 192
 - with DMC 102
- Cryptainer management menu 100
- CryptoShred 17, 134, 137
- CryptoShred button 17, 134, 135, 136
 - states 136
- custom group
 - create 169
 - remove 170
 - remove appliance 170

D

- data
 - encryption 17
- data size when encrypted 16
- DataFort
 - assigning IP settings 48
 - capacity 23
 - cluster 26
 - emergency shutdown 137
 - in SAN 29
 - licenses 58
 - specifications 240
 - users 19
 - where installed 16, 29
- DataFort CLI 253

- DataFort CLI Reference Guide 182, 220
- DataFort HBAs 240
- DataFort hostname limitations 36
- date and time
 - setting from DMC 142
- Decru licenses 58
- Decru Management Console 19, 68, 70, 171
 - defined 253
 - dual authorization 71
 - logging in 70
 - menus 171
 - Secure 71
 - Standard 70
- Decru MIB 77
- Decru Signed Syslogd (DSS) 143
- defense
 - alert, clearing 135
 - response 134
 - triggers 134
- defense setting 28, 134
 - changing after setup 134
 - summary 135
- deleted Cryptainer
 - restoration 116
- diagnostic
 - menu 181
- disabling a cluster member 185
- disk
 - management with CLI 189
 - management with DMC 102
 - rescan 189
- display
 - state 172
- DMC 19, 68, 70, 171
 - access to cluster members 155
 - defined 253
 - device grouping 95
 - device information pane 95
 - dual authorization 71
 - logging in 70
 - menus 171
 - multiple device selection 95
 - Secure 71
 - Standard 70
- DMC CLI 74
- DNS 20
- dual authentication login, CLI 73
- dual authorization 71, 73, 82

E

- edit
 - menu 175
- EMC 210
- emergency shutdown 137
- emergency zeroization via serial console 150
- encryption 16
- escrow service 27
- Ethernet cable 20
- event logs 143

F

- failover 26, 252, 253
- fan modules, replacing 205
- fan specifications 240
- FC Site settings 57, 63
- FC switch
 - in network diagram 29, 32
- feature licenses 58
- Fibre Channel
 - cables 20
 - networks 15
 - restrictions 29
 - switch ports 20
- front panel
 - display 76
 - LCD used to assign IP address 48
 - LEDs 199
 - System Card slot 44
- Fujitsu Siemens CentricStor 209
- full database 130

G

- global default pool 110
- grant host access to Cryptainer
 - CLI 193

H

- hardware maintenance 205
- hardware specifications 240
- HBA (host bus adapter)
 - host HBA, connecting to FC network 46
 - hosts 25
 - storage 25, 46
- help
 - menu 181
- host collection 90
- host default pools 110, 112

- host HBA
 - interface for unencrypted data 46
- host icons 97
- host management menu 97
- host virtualization enabled 115
- host virtualization with CLI 191
- hostname limits for DataFort 36
- hosts
 - managing with CLI 191
 - managing with DMC 97
 - supported platforms 239
- Hosts and Devices tab 89, 95

I

- I/O limit 23
- icon legend 95, 96, 97, 100, 102, 106
- icons
 - host 97
- installation
 - in rack 42
 - planning 25
 - precautions v, 43
 - requirements 20
- International Organization for Standardization (ISO) 152, 242
- intrusion detection 134, 135
- IP address 20
 - DataFort, assigning 48
- IP settings
 - assigning from LCD 48
 - changing, with DMC 164
 - DataFort, assigning from serial console 49
- IPsec 26, 253
- ISO 242
- IT power systems iv, 41

J

- JBOD 189, 191, 253

K

- key, chassis 134
- keys 253
 - encryption keys 17
 - key escrow service 27
 - manual assignment 195
 - menu 177
 - purge 129

L

- LCD 68, 76
 - assigning DataFort IP settings 48
 - bar graph 76
 - buttons 76
 - touch panel interface 68
- LEDs 199
 - power supply 200
- legacy cleartext tape 29
- legacy encrypted tapes 215
- licenses 20
 - managing 166
- lifespan of tape keys 107, 109, 112
- Lifetime Key Management (LKM) 18, 253
- limited administrator 82
- limits
 - Cryptainers on the primary port 23
 - LUNs on a single device 23
 - non virtualized hosts 23
 - number of Cryptainer or tape keys 23
 - number of DataFort appliances in a cluster 23
 - number of tape drives 23
 - virtual devices per DataFort 23
 - virtual hosts per DataFort 23
- Lithium battery v, 41
- LKM 27
 - appliance setup 39
 - number of supported servers 129
 - software setup 39
- LKM servers
 - number supported 129
- log types 143
- login
 - CLI 72
 - CLI, dual authorization 73
- logs 143
 - configuring storage location 144
 - Decru Signed Syslogd (DSS) 143
 - syslog mapping table 146
 - temporary file mapping 146
 - viewing, with DMC 146
- Loop ID 194
- LT02 217
- LUN Mapping 23, 91, 103

M

- management console installation 38

- management interface access security 138
- management port
 - connecting to Ethernet network 46
- management security settings 138
- Management Station
 - requirements 239
- management station 18, 253
 - management console installer 38
 - requirements 37
 - security 37
- manual assignment of keys 195
- mapping a device with CLI 190
- Master Key 17, 253
- media type 196
- menu
 - appliance 174
 - configuration 176
 - diagnostic 181
 - edit 175
 - help 181
 - keys 177
 - security 179
 - topology 178
 - trustee 180
 - utilities 178
 - view 175
- MetaTool 211
- MIB 77, 254
- mixed-mode tape mode 112
- mounting DataFort in rack 42
- multi ID mode
 - non NL-ports 115
- multi-appliance management 171
- multiple DataFort appliances in cluster 26

N

- NAS 15
- NetApp Filer 208
- network
 - diagram, SAN 25, 29, 32
 - information needed for setup 36
 - manage, with CLI 188
 - planning backup and restore 33
 - settings, changing 164
- Network Attached Storage (NAS) 15
- network commands, CLI 188
- network switch ports 20
- network time servers 142

- network, IP Settings 164
- NL-Port 115
- NTP time server 20, 142

O

- online help 69

P

- Parent Key 17
- password
 - administrator, changing 84
 - one-time, CLI 72
 - Recovery Card, changing 140
- password and label limitations 59
- pool display 106, 107
- port
 - FC ports 46
 - management 46
- port lock mode 99
- port locking
 - switches supported 98, 99
- Port Mapping 23, 91, 103, 254
- power
 - precautions iv, 41
- power button 50
- power cord 20
- power supply
 - LEDs 200
 - notice iv, 41
 - replaceable 205
- power supply specifications 240
- protect against insider attacks 82
- purging encryption keys 130

Q

- quorum 19, 27, 139, 141, 203, 254

R

- rack installation 42
- rack mounting kit 20
- RAID Admin 99
- Recovery Cards 18, 139, 254
 - change password 140
 - lost 139
 - replace 139
- Recovery Officers 19, 254
 - required for forming cluster 159
 - required for replacing appliance 198

- required for replacing DataFort 158
- required for replacing Recovery Card 118
- required for Setup 52
- rekeying a Cryptainer
 - CLI 193
- remote authorization 53
- Remote Desktop 202
- remove
 - custom group 170
- remove all host access to a Cryptainer
 - CLI 194
- replacing an offline cluster member 158
- reset appliance 148
- reset smart cards 141
- reset System Card 204
- restore a Cryptainer 104, 116
- restore, planning 33
- RJ45 to DB9 adapter 20, 47

S

- SAN 15
 - network diagram 25, 29, 32
 - supported hosts and storage devices 239
- SAN Storage Settings 113
- SCSI reservation handling 219
- secret share 254
- Secure CLI 69, 138
 - login 72
- Secure DMC 69, 138
 - enable/disable via CLI 202
- SecureView 19, 68
- security
 - menu 179
- security certificate
 - certificate authority signed, generating request 151
 - certificate authority signed, installing 152
 - self-signed, installing 151
 - warning 54
- security certificate, setting 151
- security domain 19, 254
 - planning 25
- security policy
 - planning 27
- security settings 138
- security, implementing and maintaining 25
- security, zeroize 149
- SEP 17, 255
 - serial console 68, 75
 - assigning DataFort IP settings 49
 - clearing IP Settings 75
 - connecting serial port 47
 - emergency access 150
 - zeroizing appliance 75
 - serial console port
 - adapter 75
 - log in 75
 - servicing appliance 205
 - set
 - SNMP options 168
 - single ID mode 115
 - size of data when encrypted 16
 - size of the configuration database 130
 - smart card reader 18, 20
 - using multiple 52
 - smart cards 20, 255
 - checking versions and status 141
 - reset procedure 141
 - summary 18
 - troubleshooting 204
 - SNMP 68, 255
 - chassis alerts 167
 - configuration 167
 - crypto alerts 167
 - MIB 77
 - options 167
 - set options 168
 - system alerts 167
 - Solaris 211
 - specifications 238
 - SSH 68, 255
 - CLI access 72, 73, 183
 - SSL 255
 - stack trace 188
 - standard CLI 72
 - standard rack mount 42
 - state displays 172
 - Storage Area Network (SAN) 15
 - storage device collection 90
 - storage devices 239
 - Storage Encryption Processor (SEP) 17
 - storage HBA
 - connecting to FC network 46
 - interface for encrypted data 46
 - storage management menu 102
 - storage management with CLI 189

- storage troubleshooting 206
- supported platforms 239
- switch connections in a cluster 26
- Symmetrix 210
- syslog, syslogd (syslog daemon) 143, 145
- System Card 18, 255
 - inserting 44
 - removing, in emergency 137
 - resetting 204
- system logs, verifying 187
- system properties, CLI 186
- system requirements 239
- system users, administrators 86

T

- tab
 - appliance 173
- table columns
 - configuring 173
- TAP 118
- tape key 107, 109, 112
 - deletion 107, 109, 112
 - expiration 107, 109, 112
 - lifespan 107, 109, 112
- tape pool types 110, 112
- ten port DataFort rear panel 46
- TEP 118
- Terminal Services 202
- time and date
 - setting from DMC 142
- time servers 142
- time-out
 - CLI 72
 - DMC 70
 - serial session 75
- Tivoli 216
- topology
 - menu 178
- troubleshooting 197
 - cluster 203
 - management interfaces 201
 - network connections 201
 - smart cards 204
 - storage 206
- trustee
 - managing 118
 - menu 180
- Trustee Acceptance Package 118

- Trustee Acceptance Package (TAP) 120
- Trustee Establishment Package 118
- Trustee Establishment Package (TEP) 119, 120, 121, 123, 124
- trustee relationship
 - approve TAP, on local network 121
 - approve TAP, on remote network 125, 126
 - approve TEP, on local network 120
 - approve TEP, on remote network 123, 124
 - authorizing trustees locally to approve TEP/
TAP, on a local network 119
 - create TEP, on remote network 122
 - create trustee link, on local network 119
 - create, on local network 119
 - create, on remote network 122
 - delete unapproved TAP trustee 126
 - initiating remote authorization to approve
TAP, on local network 121
 - initiating remote authorization to approve
TAP, on remote network 125
 - initiating remote authorization to approve
TEP, on local network 120
 - initiating remote authorization to approve
TEP, on remote network 124
 - receive TAP, on remote network 125
 - receive TEP, on remote network 122
- types of keys recovered during a restore 148

U

- updating hosts in a Microsoft operating system
25
- upgrading appliances 165
- USB 20
- utilities
 - menu 178

V

- Veritas 214
- view
 - menu 175
- virtualization settings 115

W

- WAN 26
- Windows event logging 145
- Windows Event Viewer 145
- WWN configuration 57, 63
- WWNs

Index

assigning an override setting 57, 63

Z

zeroization without admin card 150

zeroizing appliance 148

 using DMC or CLI 149

 using serial console 150

zones 46