DECRU®
A NetApp Company

ADMINISTRATION GUIDE

DataFort FC-Series
Version 2.2.0.2

security

DataFort Administration Guide for FC-Series DataFort Appliance

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

Part number: 210-03831 A0 (071307_FC2.2.0.2)

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'ACCÉS.

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

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

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

WARNUNG: Dieses Produkt ist darauf angewiesen, daß im Gebäude ein Kurzschluß- bzw. Überstromschutz installiert ist. Stellen Sie sicher, daß eine Sicherung oder ein Unterbrecher von nicht mehr als 240 V Wechselstrom, 10 A (bzw. in den USA 120 V Wechselstrom, 15 A) an den Phasenleitern (allen stromführenden Leitern) verwendet wird.

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

OPPMERKSAMHET: 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 LKM appliance, and attach the rail mounts to the rack. Then slide the appliance into the rack on the rails and secure the appliance in place using the provided screws.

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

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

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

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

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

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

Contents

Chapter 1 Introduction **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 17
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
Enabling TLS 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 DataFort Appliance 42
Unpacking the DataFort Appliance 42
Selecting a Location 42
Rack Mounting 42
Connecting the Decru DataFort Appliance 44
Inserting the System Card 44
Connecting the Rear Panel Ports 44
Connecting Power 47
Assigning the DataFort 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 DataFort Appliances 51
About the Setup Wizard 52
Setup Wizard Functions 52
Incomplete Setup Wizard 52
About Smart Cards and Readers 52
Initializing a Standalone DataFort or DataFort Cluster 53
Connect to Head of Cluster 54
Sign License Agreement 54
Recover From Database 55
Create Administrator 55
Configure Cluster and Recovery Schema 55
Network Settings 57
Add Licenses 60
Network and Certificates 61
Insert Recovery Card 62
Apply Settings 63
Adding a Member to a Cluster 65
Log in to Head of Cluster 65
Cluster and Recovery Schema 66

Network Settings 66
Add Licenses 67
Network and Certificates 67
Insert Recovery Card 67
Apply Settings 67

Chapter 6 DataFort Management Interfaces 69
Management Interfaces Overview 70
SecureView 70
Security Policies 71
Online Help 71
Connecting to the DataFort WebUI 72
Using the DataFort WebUI 72
Connecting via WebUI 72
Quick Links and Status 73
Connecting via WebUI using Dual Authorization 74
Connecting to the DataFort Command Line Interface 75
Using the CLI 75
Connecting via Standard CLI 75
Connecting via Secure CLI 75
Connecting via CLI using Dual Authorization 76
Connecting to CLI via WebUI 77
Accessing the Decru Management Console 78
Serial Console 79
Logging in to the Serial Console Port 79
Configuring IP Settings 79
Clearing IP Settings 79
Zeroizing DataFort 79
DataFort Front Panel LCD 80
Touch Panel Onscreen Buttons 80
SNMP Settings 81

Chapter 7 DataFort Admin Roles and Account Administration 82
Administrator Roles 83
Account Administration 85
Adding an Administrator 85
Requiring Authorization for Login 88
Changing the Administrator Password 89
Removing an Administrator 90
Changing a Card Association 90

Chapter 8 Before Storage Administration 91
Verifying DataFort Configuration 92
Verifying System Version 92
Checking Cluster State 92
Creating Additional Administrators 92
Configuring Remote Logging 92

Determining the Defense Setting 92
Configuring Disk or Tape Mode 93
Starting LKM 94
LKM Server 94
LKM Appliance 94

Chapter 9 Storage Administration 95
Creating Cryptainers 96
Cryptainer Creation Using Collections 96
Cryptainer Creation Without Collections 104
SAN Topology Page 105
DataFort WebUI Icons 106
Managing Hosts 107
Host Collection Menu 107
Host Menu 108
Edit Host Page 109
Managing Cryptainers 110
Cryptainer Collection Menu 110
Cryptainer Menu 111
Edit Cryptainer Page 112
Managing Storage 113
Storage Collection Menu 113
Storage Device Menu 114
LUN Menu 114
Managing Tapes 116
Tape Pool Collection Menu 116
Tape Pool Menu 117
Tape Device Menu 117
Edit Pool Page 118
ACL Learning 119
Managing Tape Settings 120
Pool Settings and Defaults 120
Global Default Pool 121
Tape Settings 122
Mixed-Tape Mode Rules 123
Managing SAN Storage Settings 124
Virtualization Settings 124
Setting Single or Multi ID Mode 125
Restoring a Cryptainer 126

Chapter 10 Key Administration 127
Managing Trustees 128
Trustee Scenarios 128
Setting Up Trustees 128
Importing and Exporting Keys 134
Managing DataFort Defense Responses 135
Defense Triggers and Responses 135
DataFort Defense Setting 135

Changing the Defense Setting 136
Clearing a Defense Alert 137
CryptoShred Button States 137
System Card CryptoShred 138
Configuring Management Security Settings 139
Managing Recovery Officers and Recovery Cards 140
Lost Recovery Card Best Practice 140
Replacing a Recovery Card 140
Changing a Recovery Card Password 142
Smart Card Reset 143

Chapter 11 Backup Administration 144
Saving Configurations to Lifetime Key Management Software 145
Best Practices for Secure Backups 145
Configuring Backups to LKM Software 145
Backing Up the Configuration to LKM Software 147
Key Purging 147
Downloading Configurations to a Remote Location 149

Chapter 12 Physical Security Administration 150
Setting Date and Time 151
Configuring and Viewing Logs 152
DataFort Log Storage Guidelines 152
Decru Signed Syslogd (DSS) 152
Configuring Log Storage 153
Windows Event Logging 154
Setting Up Syslog 155
Viewing the Log 156
Verifying Signed Log Messages 157
Zeroizing the Decru DataFort 158
Before Zeroizing 158
Zeroization Using the DataFort WebUI **159**
Zeroization Using the CLI 160
Zeroization Using the Serial Console 160
Emergency Serial Console Port Access 160

Chapter 13 Cluster Administration 162
Cluster Management 163
Maintaining the Cluster Quorum 163
Cluster-Wide Management via WebUI 164
Checking the Status of the Cluster 164
Resolving a Cluster Conflict 165
Adding and Removing Cluster Members 166
Adding a Cluster Member 166
Removing a Cluster Member 166
Replacing a DataFort in a Cluster 166
Recovering a Cluster 168

Changing Network Properties of a Cluster Member 169
Changing the IPsec Secret of a Cluster 169
Changing the IP Address of a Clustered DataFort 169
Changing the Hostname of a Clustered DataFort 170
Changing the Hostname on an FC1020 170

Chapter 14 Machine Administration 172
Network Settings 173
Upgrading DataFort 174
Setting Security Certificates 175
Setting a Local Security Certificate 175
Setting a Certificate Authority Signed Certificate 177
Managing Licenses 180
SNMP Settings 181
Supported SNMP and MIB Versions 181
Enabling SNMP 181
SNMP Configuration 181

Chapter 15 DataFort Appliance Settings and Status 183
Viewing Settings in the WebUI 184

Chapter 16 Decru Management Console Functions 186
Appliance Management 187
Adding an Appliance 188
Logging into Appliances 188
Removing an Appliance 188
Running the Setup Wizard 189
Verifying an Upgrade Package 189
Upgrading an Appliance 189
Backing Up an Appliance 189
Creating Trustees 189
Linking Appliances 189
Viewing Details 190
Accessing DataFort WebUI 190
Accessing Command Line Interface 190
Collecting Tech Support Info 190
Rebooting Appliances 190
Zeroizing Appliances 191
Exiting the Console 191
License and Administration Management 192
Managing Licenses 192
Adding a License 192
Managing Administrators 192
Adding an Administrator 192
Logging Configuration 194
Decru Management Console Menus 195
Appliance Menu 195

Edit Menu 196
View Menu 196
Trustee Menu 196
Configuration Menu 197
Help Menu 198

Chapter 17 CLI Administration 199
Using the CLI 200
Connecting to the CLI 200
CLI Help 200
Administration Commands 201
Administrator Roles 201
Creating a New Administrator Using the CLI 201
Cluster Management 202
System Properties and Log Management 203
Verifying System Logs 204
Stack Trace Settings 205
Network Management 205
Backup Management 205
Storage Management Commands 206
Disk Commands 206
Host Commands 208
Cryptainer Commands 209
Fibre Channel Kernel Commands 211
Manual Key Generation 212
Creating Cryptainer Keys 212
Viewing Cryptainer Keys 212
Changing DataFort Appliance Network Port Settings 213

Chapter 18 Troubleshooting 214
Restoring a DataFort Appliance 215
Front Panel LEDs 216
Power Supply LEDs 217
Network Connections and Management Interfaces 218
Clusters 220
Smart Cards 221
Hardware 222
Storage 223
Clusters 225
Decru DataFort Operation with EMC 226
Symmetrix 226
CLARiiON 226
Decru DataFort Operation with Linux 227
Multiple LUNs 227
Failover 227
Resync Speed 227

Decru DataFort Operation with Solaris 228
Migrating MetaTool Volumes to a DataFort 228
Veritas Volume Manager 230
Decru DataFort Operation with Legacy Encrypted Tapes 232
Decru DataFort Operation with Tivoli and STK Drives 233
Decru DataFort Operation with LTO2 Serialized Commands 234
Decru DataFort AIX Atape Failover Support 235
Atape Operation Limitations 235
Decru DataFort SCSI Reservation Handling Fixes 236

Appendix I Command Line Interface Quick Reference 237
Using the CLI 238
CLI Syntax 238
CLI Help 238
CLI Command Overview 239
Top Level Commands 239
Device Commands 239
Disk Commands 240
FC Site Commands 240
FCC Cryptainer Commands 240
Host Commands 241
KFC Commands 241
Pool Commands 241
Tape Commands 242
CLI Formatting Commands 242
Help Command 242
Quit Command 242
Active-Role Commands 242
Authorize Command 242
Password Command 242
Role Commands 243
User Commands 243
Whoami Command 243
Trustee Commands 243
Network Commands 243
Key Management Commands 243
LKM Management Commands 244
Cluster Commands 244
Database Commands 244
System Commands 244

Appendix II Logging Functions 246
DataFort Log Event and Priority Types 247
Log message parameters 247
Log Storage Locations 249
Log Presentation 250

Temporary Logs 250
Database Logs 250
Remote Logs 251
Log Purging 253
Audit Configuration 254

Appendix III Port IDs 256

Appendix IV Specifications 257
Supported Systems 258
DataFort Appliance Specifications 259

Appendix V Partial List of ISO Country Codes 262

Appendix VI Regulatory and Certifications 263
FCC B Declaration of Conformity 264
European Union 265
Canadian ICES-003 266
VCCI Class A Statement 267
CE Statement 268

Appendix VII Glossary 269

Index 273

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, DataFort 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. 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 guide describes the features and functions of the FC-Series DataFort appliances. This introduction includes the following sections:

- 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 as determined by 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 be 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 the 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 itself is compromised (stolen or tampered with).

The System Card's presence in the DataFort 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 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 be present with their associated cards in order to complete sensitive operations such as data recovery.

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), DataFort WebUI and DataFort CLI. SecureView™ licenses enable administration of multiple appliances at once 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 Appliance
- DataFort Documentation and Software CD-ROM. The documentation and software CD contains software necessary for DataFort operation, such as the smart card reader driver and Decru Management Console installer.
- Custom RJ45 to DB9 adapter and Category 5 cable for a serial connection
- AC power cord or cords appropriate for DataFort model
- DataFort smart cards, including System, Admin and Recovery Cards
- USB smart card reader
- Decru product licenses
- Slide rail mounting kit including hardware and instructions (included in the 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 you will be using to connect DataFort to the fabric. Each FC-Series DataFort HBA board has two fibre channel connections, so two switch ports per board are needed unless you are cabling directly in-line to a device.
- Network cables. Have the requisite number of network cables, of appropriate lengths. Each DataFort will require one standard RJ-45 Ethernet cable.
- Network switch ports. Determine which Ethernet switch ports you will be using to connect the DataFort appliances to your network. Each DataFort has one Ethernet connection, so one switch port per DataFort will be required.
- IP address, Subnet mask and Default Gateway. Each DataFort will require 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. Associating the specific IP addresses with their associated system names in your DNS configuration prior to installation will 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. Have the appropriate NTP time server information for each dedicated IP address to be used during installation. If you are not using an NTP server for time synchronization then this information is not required.
- Recovery schema. Determine what the recovery schema will be 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 DataFort WebUI menus is described from the top level down, using bold type, for example: Choose **System Config > System Users > 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
- Recommended Network Configurations
- Planning Data Backup and Restoration

Decru 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. You may have 7 virtual devices and 7 virtual hosts per 2-port DataFort and 35 virtual devices and 35 virtual hosts per 10-port DataFort.
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. You may have 7 virtual devices and 7 virtual hosts per 2-port DataFort and 35 virtual devices and 35 virtual hosts per 10-port DataFort.
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 IOs on single DataFort	512	DataFort should be installed so that no more than 512 IOs 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 will see 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 will 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. The solution is to update the drivers on these devices using the properties window.

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 will not interrupt data access through the cluster. The other members of the DataFort cluster will 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 your 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.

Your 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 your 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 will need to 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 135 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 a DataFort 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 a DataFort 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 will be 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 WebUI. Host HBAs are granted access to the Cryptainers via DataFort.

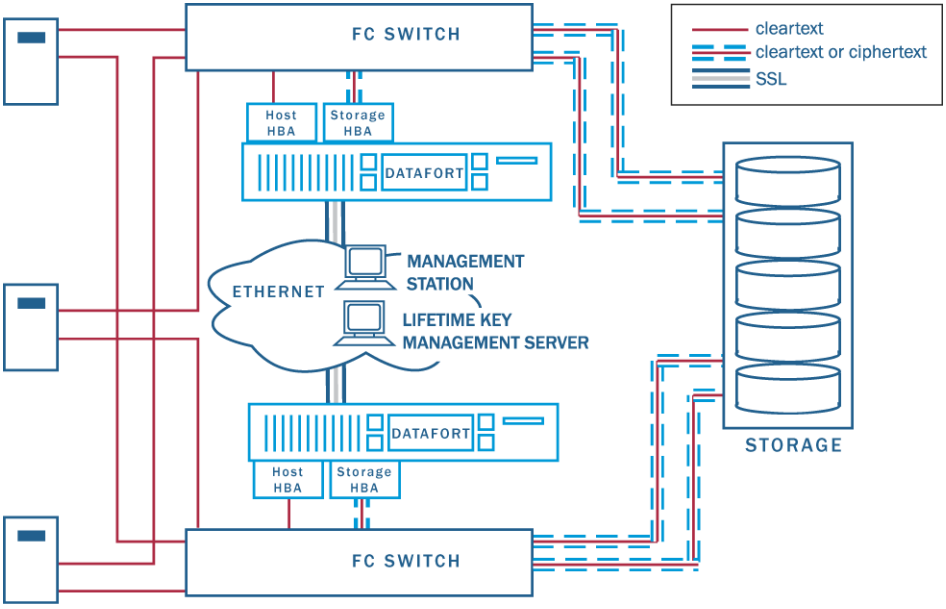


Figure 2-1: A DataFort cluster with two FC switches showing redundant paths

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.

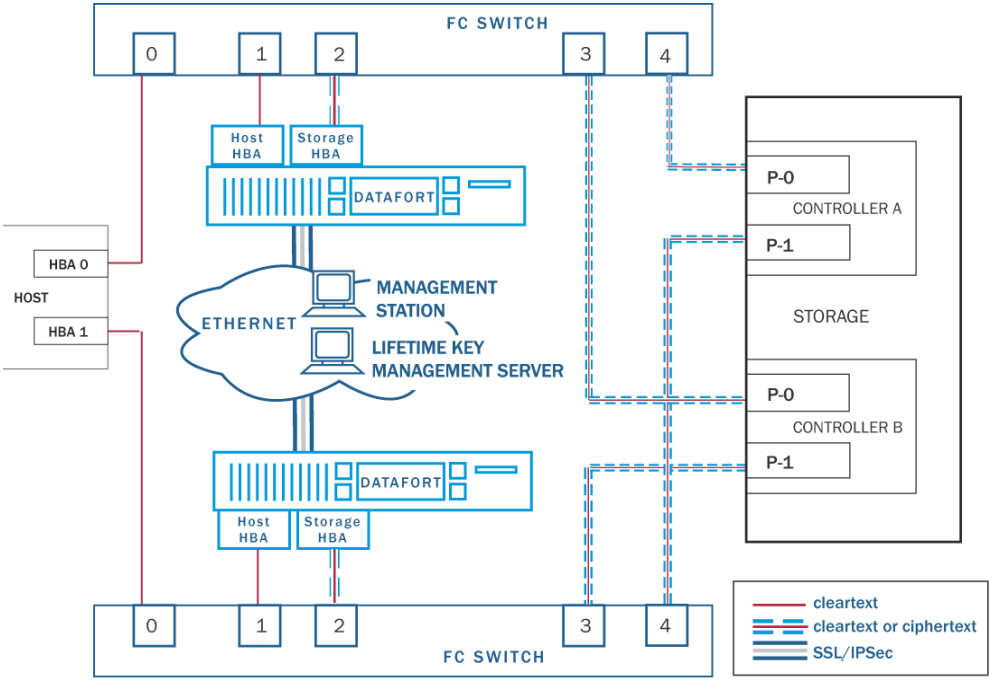


Figure 2-2: Fabric attached configuration

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.

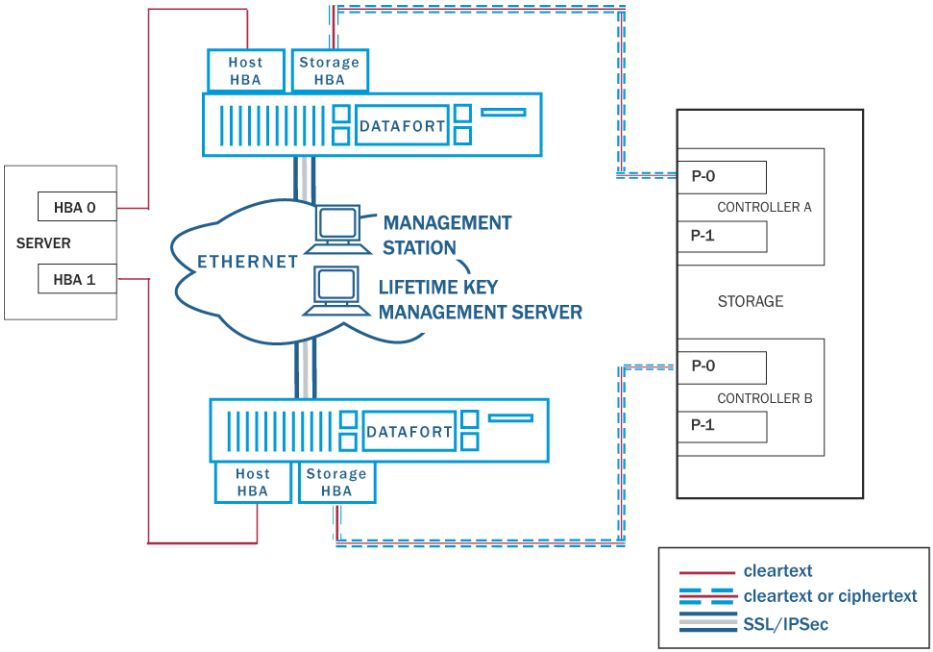


Figure 2-3: In-line configuration

Tape Backup

DataFort fully supports data backup to tape in cleartext or encrypted form. Tape read through DataFort will be determined to be encrypted or cleartext based on presence or absence of DataFort metadata. If no metadata is present, the read is passed through without encryption, but if metadata is present the data will be 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-Mode Tape Rules on page 123 for more information about DataFort behavior in a mixed-tape mode environment.

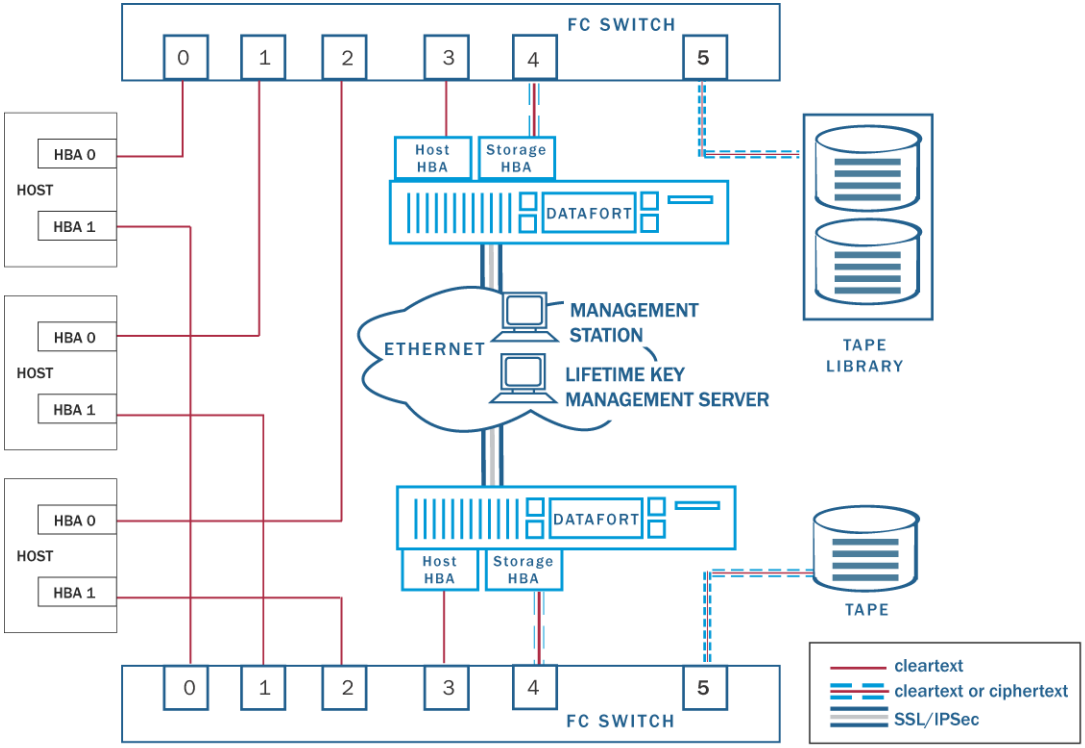


Figure 2-4: A DataFort cluster with two FC switches sending encrypted and cleartext data to tape

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 will channel the data path of every backup and restore through the DataFort. DataFort will pass 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 though 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 will be 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 *behind* 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 your 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 70 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	2	Connect LKM appliance OR LKM server to network	3	Connect DataFort appliances to network
	Install smart card reader and Decru Management Console (DMC)		LKM server—Install LKM software		Determine security settings and administrative roles
			LKM appliance—Assemble Recovery Cards and Recovery Officers and run Setup Wizard from Decru Management Console		Assemble Recovery Cards and Recovery Officers Run Setup Wizard from Decru Management Console
	Access management interfaces from the management station		Complete set up of LKM appliances from Decru Management Console		Complete set up of DataFort appliances from DataFort WebUI

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

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

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

Choose 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
Browser for DataFort WebUI	Internet Explorer version 6.0 (Service Pack 1) or greater. TLS must be enabled.
	Microsoft JVM or Sun JRE 1.4.2.08 or greater. (DMC installs Sun JRE 1.5_06.)
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, with no remote management enabled.

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

Enabling TLS

DataFort only allows Transport Layer Security (TLS) 1.0 based HTTPS connections to the WebUI because it is a more secure protocol than Secure Sockets Layer (SSL) 2.0 and SSL 3.0. TLS 1.0 must be explicitly enabled in Internet Explorer through the Internet Options dialog as follows:

1. Select **Tools > Internet Options...**
2. Select the Advanced tab.
3. Check the Use TLS 1.0 box under Security.
4. Click Apply and OK to save the setting.

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 will run automatically if autorun is on.
2. Click the installer link.
3. When prompted by the File Download screen to open or save the file, click the Open button.
4. Follow the prompts to start the installer.
5. Read and accept the terms of the license agreement.
6. Select the model number of your 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, choosing either the LKM software or the LKM appliance.

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.

If you are 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.

If you are using LKM software, install the software on a designated server. Make sure 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 DataFort Appliance
- Connecting the Decru DataFort Appliance
- Assigning the DataFort 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 DataFort Appliance

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

- Unpacking the DataFort Appliance
- Selecting a Location
- Rack Mounting

Unpacking the DataFort Appliance

When unpacking DataFort, 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 will damage the cardboard packaging. If the appliance is equipped with a Medeco lock, a tamper evident label will also be 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

DataFort 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 Decru DataFort Appliance

Insert the System Card into the slot on the front panel, then connect DataFort to the network.

- Inserting the System Card
- Connecting the Rear Panel Ports
- Connecting Power

Inserting the System Card

The System Card is used to handle key data. Insert the System Card BEFORE powering on DataFort.

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

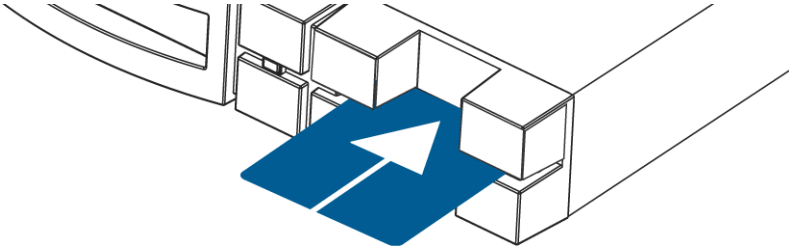


Figure 4-5: The front panel slot housing the System Card on a 1U DataFort

2. Slide the card into the slot firmly, with the gold contacts facing up and towards the back of the DataFort. 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 DataFort 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 DataFort rear panel ports as described in the following sections:

- Ethernet Connection
- Fibre Channel Connection
- Serial Console Port

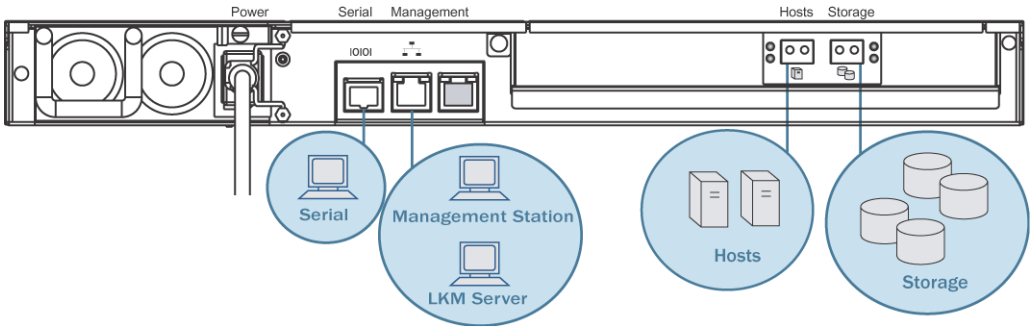


Figure 4-6: Rear panel connections 1U DataFort

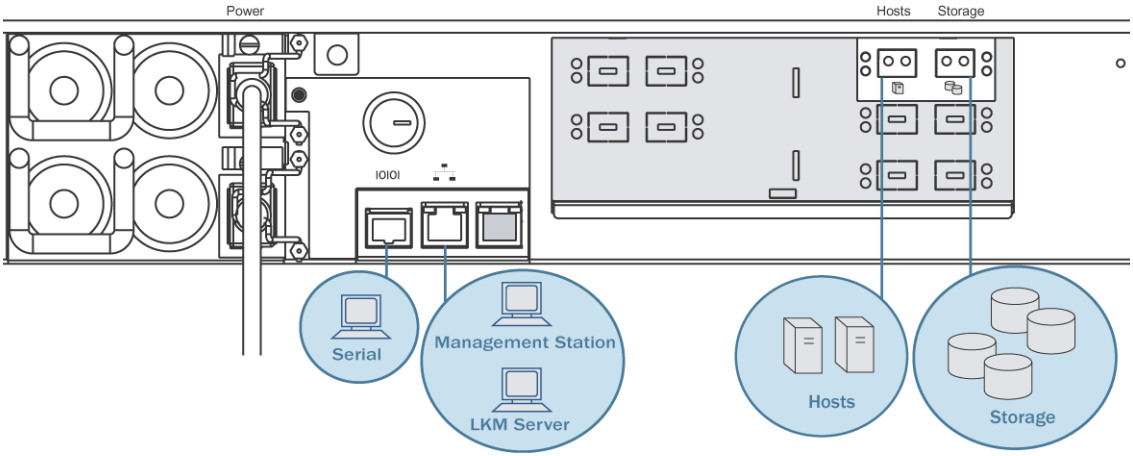


Figure 4-7: Rear panel connections 2U DataFort

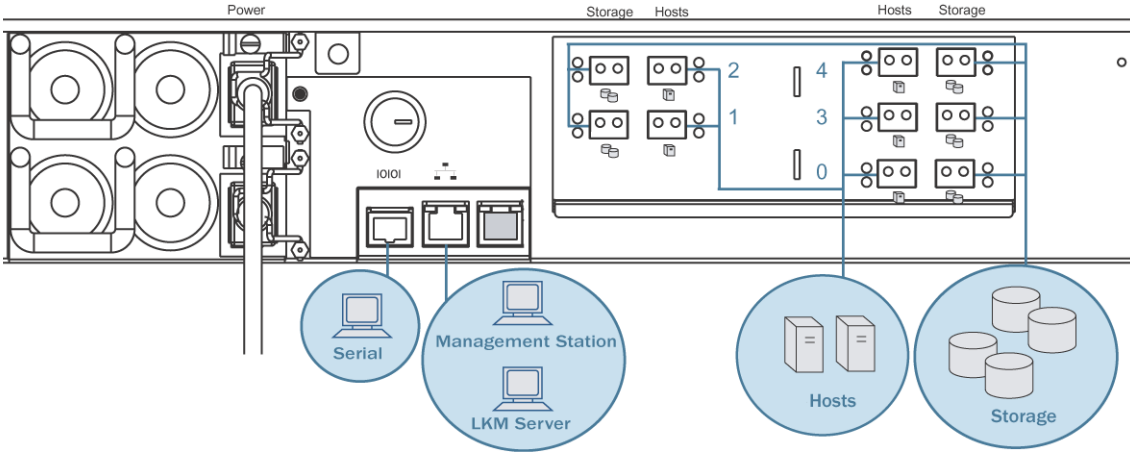


Figure 4-8: Rear panel connections 2U ten-port DataFort

Ethernet Connection

Use a Category 5 Ethernet cable to connect the DataFort 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 DataFort 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 DataFort.

Connecting Power

The DataFort 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 DataFort will operate with only one power cord, but the second cord provides failover protection if connected to a different circuit.

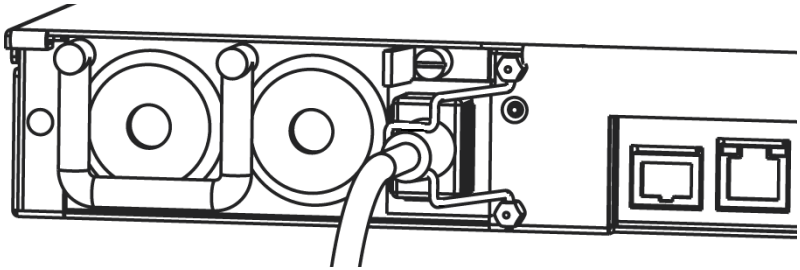


Figure 4-9: Power cord secured by the wire retaining clamp

2. When connected, DataFort will power on automatically. Wait two to three minutes while DataFort powers up.

   When power up is complete, the LCD will show “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 DataFort IP Address.

   Note: Leave DataFort powered on for normal operation. See Powering Up and Shutting Down on page 50 for instructions on powering off the appliance.

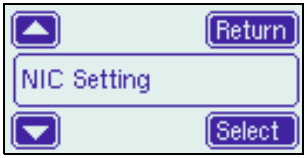
Assigning the DataFort IP Address

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

2U DataFort	Assign the DataFort 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 DataFort.
1U DataFort	Assign the DataFort 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.



3. Touch the Select button.
4. Touch the Edit button. The screen displays a kepad of numbers, and selectable fields for the Management Port IP address.
5. Touch the entry field to highlight it, and then touch the keypad buttons to enter each number. Use the decimal point to tab to the next field automatically.

6. When 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 will appear.
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: DataFort serial sessions time out after 90 seconds of inactivity. If this happens before you finish and save your configuration, log in again. Settings are not saved until the Save and Exit command has been completed.

Powering Up and Shutting Down

The 1U DataFort appliance has one power cord and the 2U DataFort appliance has two power cords. On the 2U DataFort, the second power cord should be plugged into a separate AC circuit to provide AC power redundancy. This will enable DataFort 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 DataFort powered on, with the System Card in the card slot.

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

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

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

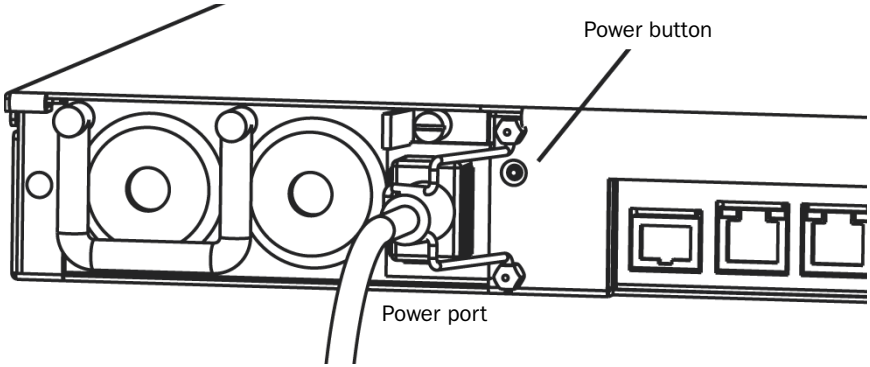


Figure 4-10: Rear panel power port and button on 1U appliance

5 Initializing DataFort 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, the DataFort WebUI and the DataFort CLI. See Chapter 6 for more about DataFort management interfaces.

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

- About the Setup Wizard
- Initializing a Standalone DataFort or DataFort Cluster
- Adding a Member to a Cluster

About the Setup Wizard

Consider the following when running the wizard:

- Initialization of a new DataFort appliance or cluster creates the first Full Administrator for that DataFort or DataFort 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	Initializing a Standalone DataFort or DataFort Cluster on page 53. The new appliance must be initialized and connected to the network.
Set up a new cluster	Initializing a Standalone DataFort or DataFort Cluster on page 53. All cluster members must be initialized and connected to the network.
Add a new member to an existing cluster	Adding a Member to a Cluster on page 65. A configured standalone appliance must already be set up. The new appliance to be added must be initialized and connected to the network.
Set up a new appliance with an existing saved configuration (restore a configuration)	Restoring a DataFort Appliance on page 215. A saved prior configuration must be accessible to the new appliance. The new appliance must be initialized and connected to the network.

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 completed steps. This is by design, and eliminates the need to reenter data when re-running the wizard. The retained wizard entries can be cleared if necessary. See troubleshooting Network Connections and Management Interfaces on page 218.

About Smart Cards and Readers

The setup process requires Recovery Cards and the Recovery Officers responsible for those cards. Cards are inserted into the smart card reader connected to the Management Station during setup.

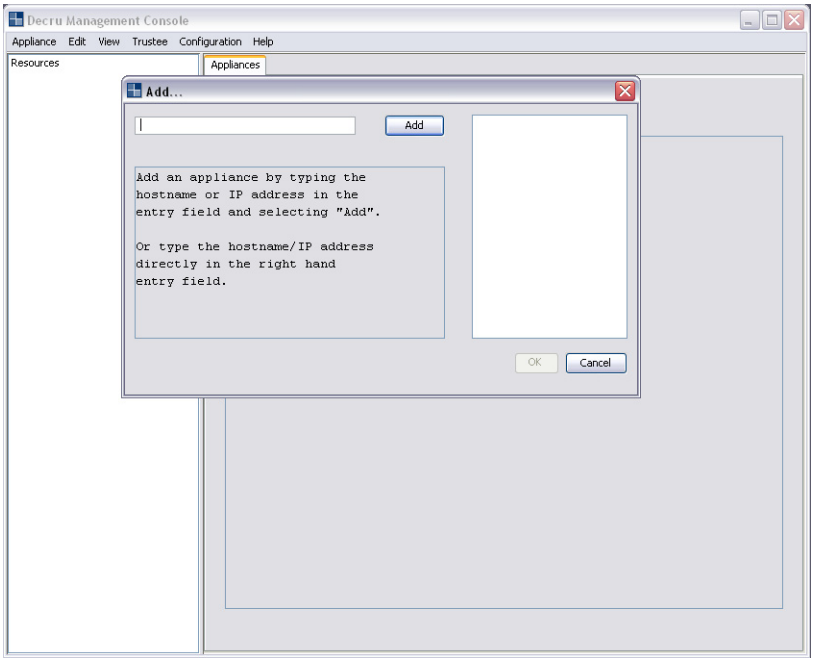
You can choose to connect multiple smart card readers to the Management Station, thereby making it possible to complete the wizard without having to switch cards. For example, if 2 out of 5 cards are required to initialize a cluster and two card readers are connected, both required Recovery Cards can be inserted at once and cards will not need to be switched.

Initializing a Standalone DataFort or DataFort Cluster

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

   DMC will start.

   - If no appliances have been added, the Add... pop-up screen appears automatically.
   - If appliances have been added, choose **Appliance > Add** to open the Add... pop-up screen.



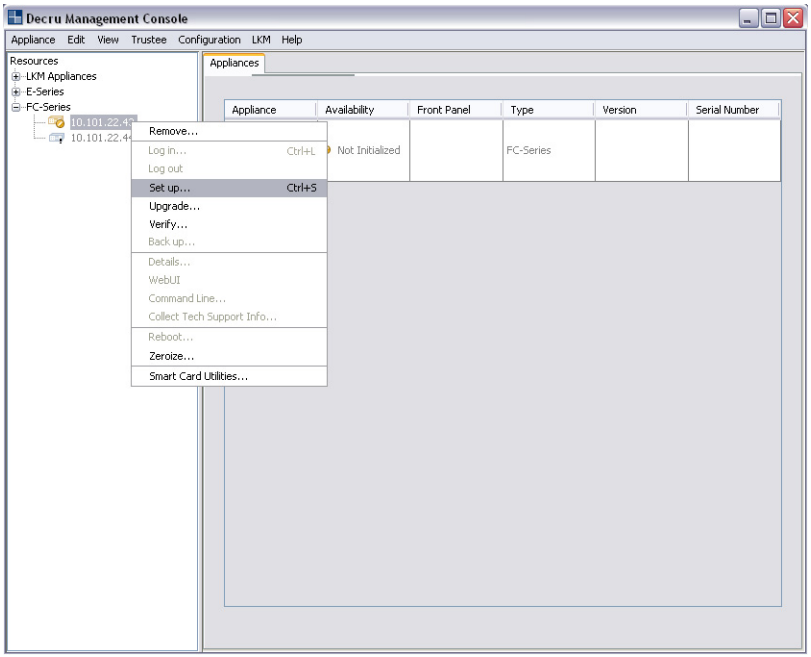
2. Enter the IP address or hostname of all appliances that will be set up.

   More than one appliance can be added on this screen: enter the IP address or hostname for each appliance in the single field provided and click Add after each, or add all IP addresses or hostnames directly into the pane on the right side of the screen.

3. Click OK when all addresses or hostnames are entered.
4. A certificate validating the connection between each appliance and the Management Console appears, choose to trust the certificate once or always.

   The added appliances will appear in the DMC.

5. From the Resources pane, right-click the first appliance you will configure, and choose Set up.



The Welcome page of the Wizard appears.

6. Click Start.

Connect to Head of Cluster

Initialize a standalone DataFort 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 DataFort, enter the IP address or resolvable hostname of the appliance (as configured during installation).

   Note: 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 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 DataFort will replace a previously existing DataFort and a configuration database from that previous DataFort will be used to configure this new DataFort. For information about this feature, see Restoring a DataFort Appliance on page 215.

- Click Next to skip the Recover from Database screen.

Create Administrator

Create an administrator for this appliance. This administrator will be a Full Administrator, and will have management privileges for all members of a cluster.

This administrative name and password will be 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 you to multi-select appliances and log 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 is also where you will indicate if this wizard is configuring a standalone DataFort 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

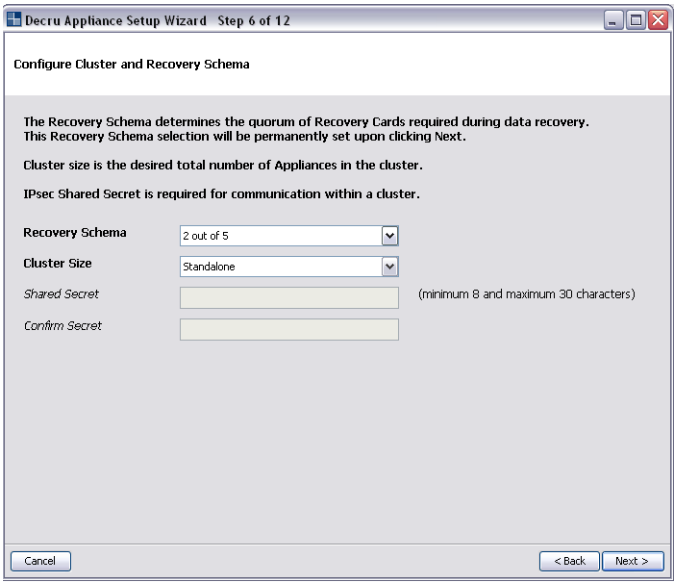
Setting the Recovery Schema

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 your organization.

2 out of 5 is the recommended data recovery setting, in which any 2 of the 5 Recovery Cards that are initialized during DataFort 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.

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



WARNING: DATA RECOVERY SETTINGS CANNOT BE CHANGED AFTER YOU CONTINUE TO THE NEXT STEP OF THE WIZARD. ONCE THE NEXT BUTTON IS CLICKED ON THIS SCREEN, THIS SETTING WILL BECOME PERMANENT.

Setting the Cluster Size

1. Select standalone or cluster size.

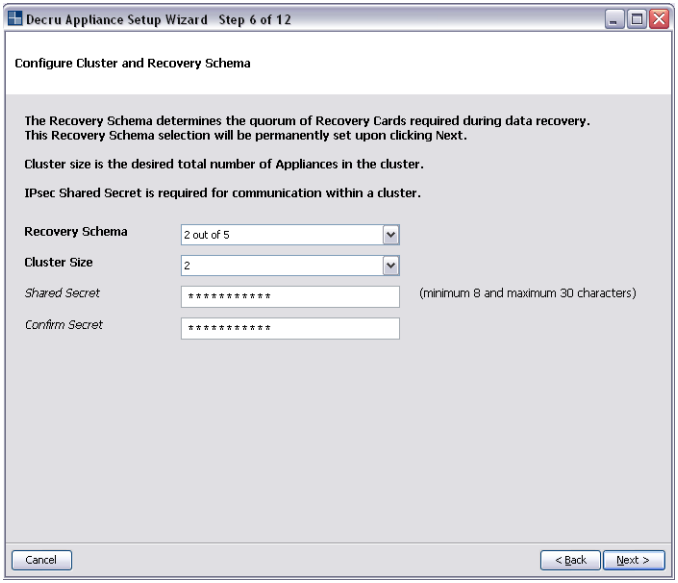
Standalone

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

Cluster

Cluster Size—Select a Cluster Size from the Cluster Size menu if this is the first DataFort in a cluster, or if this is a DataFort joining a standalone appliance in order to form a cluster.

IPSec Secret—Enter and confirm an IPsec secret for 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.



2. Click Next to proceed.

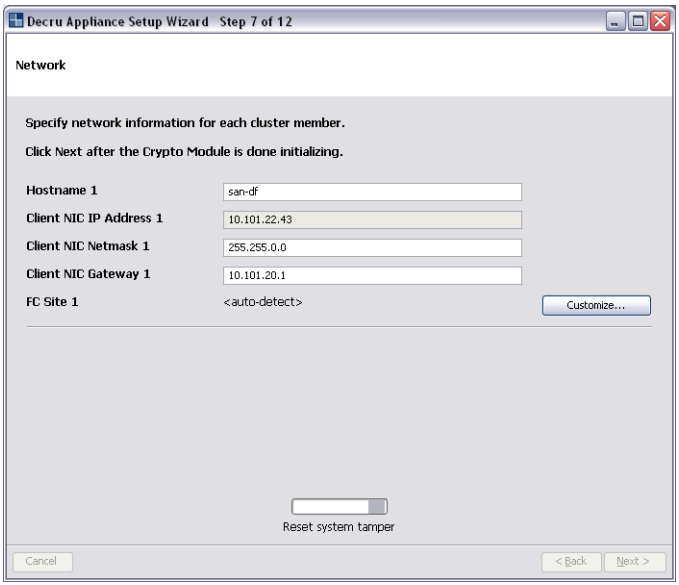
Network Settings

Enter the appropriate network settings.

- If Standalone was selected in the previous step, only one set of fields will appear. See Standalone Network Settings.
- If a Cluster Size was set in the previous step, a set of fields will appear for each cluster member. See Cluster Network Settings.

Standalone Network Settings

For a standalone DataFort, one set of fields will appear.



1. Enter a hostname for this DataFort.

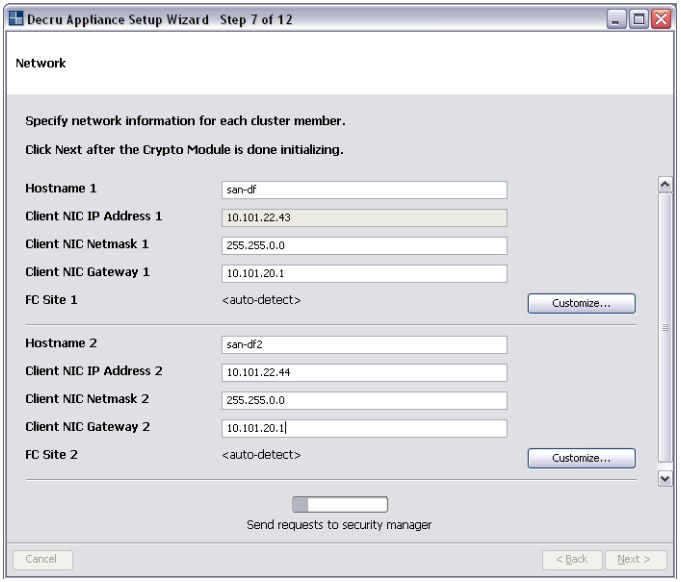
   The IP address, Netmask and Gateway set for the Clients NIC will appear. (These were set when Assigning the DataFort IP Address on page 48.)

2. The FC Site settings can be left at their default, or modified using the customize option. Clicking Customize will open 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.

3. Click Next.

Cluster Network Settings

For a DataFort cluster, one set of fields will appear for each DataFort.



1. Enter a hostname for the first DataFort.

   The IP Address, Netmask and Gateway set for the first DataFort will appear. (These were set when Assigning the DataFort IP Address on page 48.)

2. The FC Site settings can be left at their default, or modified using the customize option. Clicking Customize will open 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.
3. Enter a hostname for additional cluster members.
4. Enter IP Address, Netmask and Gateway information for additional cluster members.

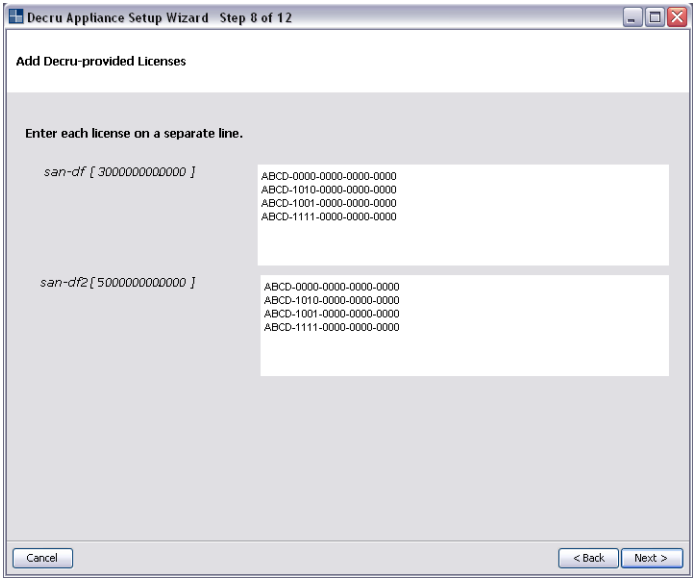
   Note: When setting up a cluster there may be a delay while the first member is being set up. This can mean that the Next button will not be available for 30 seconds or more.

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

Add Licenses

Make sure that each DataFort in the cluster has a license that supports the same features. Site-wide licensing is also available, which allows the same licenses to be used for all appliances in the cluster.

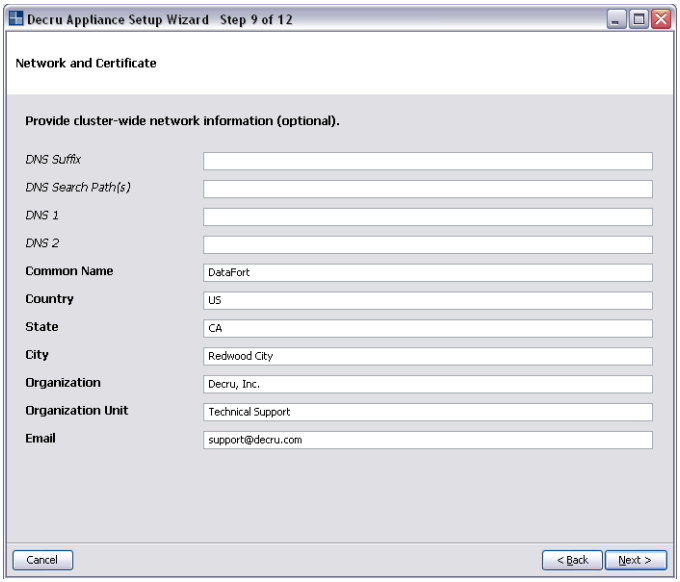
The FC-Series DataFort is licensed for use in environments with disk or tape storage. Disk features will not be available to customers with DataFort appliances licensed only for tape and vice versa.



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.
   - If site-wide licenses are in use, the same licenses should be entered for each DataFort.
2. Click Next.

Network and Certificates

Enter optional DNS information and set the security certificate for DataFort. While not required, DNS makes it easier to add servers and virtual servers to a DataFort 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

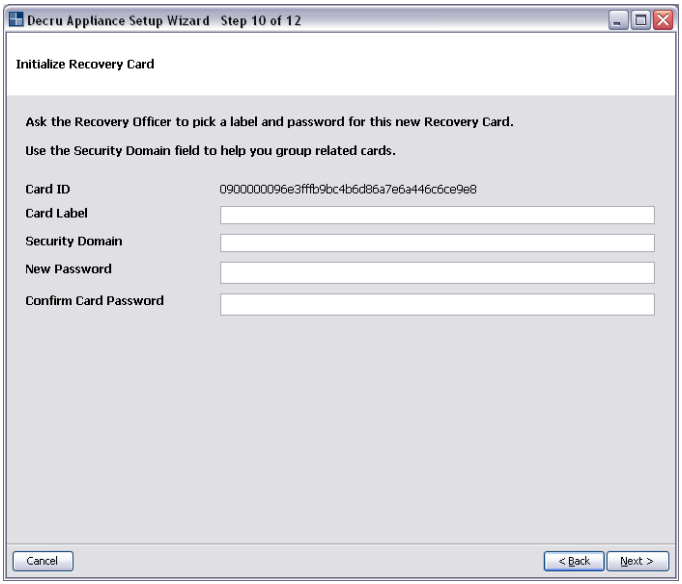
Configure DataFort to accept a self-signed security certificate to improve security for the SSL communication between the Management Station and DataFort.

1. Enter a name for the appliance.
2. Enter the country code for your 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 262.
3. Enter the rest of the required information about your location.
4. Click Next.

Insert Recovery Card

Recovery Officers responsible for Recovery Cards should be prepared to enter card label and password information into the provided fields.

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. The Recovery Officer responsible for this card should enter the required information into the provided fields.

Password and Label Limitations

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

Note: The Security Domain entered for the first card in the set will be applied to the entire set of Recovery Cards.

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 will be 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 will appear and the wizard will prompt for the password. The Recovery Officer responsible for this card provides this information.

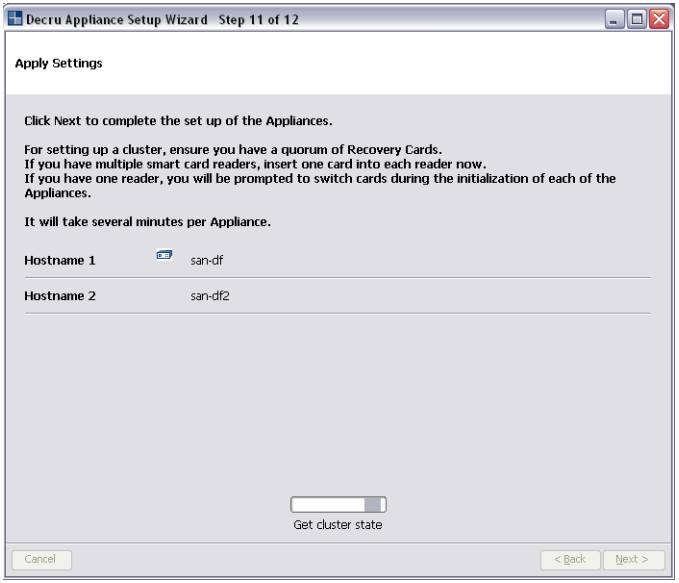
3. Click Next.
4. When prompted, remove the initialized card and insert a new one.

   Security Domain information from the first card will be entered automatically. You may change it if you want the card grouped 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 DataFort appliances that are being configured using the wizard.

   If this is a cluster, you will be asked to insert the quorum of Recovery Cards. If one smart card reader is in use, the cards will 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 will 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 DataFort WebUI. See Chapter 6 for a list of DataFort management interfaces.

- The DataFort WebUI provides complete management tools for a DataFort appliance or cluster. After the wizard is complete, you can close DMC and log into the WebUI to manage DataFort.
- The Decru Management Console offers a sub-set of the appliance management options available in the DataFort WebUI.

Adding a Member to a Cluster

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

- You will need the cluster quorum of Recovery Officers with their cards, and the shared secret of the cluster, as well as licenses for all cluster members.

1. Choose **Start > Programs > Decru > Decru Management Console**.

   DMC will start.

2. From the Resources pane, choose **Appliance > Add** to open the Add... pop-up screen.
3. Enter the IP address or hostname of the appliance that will be added to the cluster.

   More than one appliance can be added on this screen: enter the IP address or hostname for each appliance in the single field provided and click Add after each, or add all IP addresses or hostnames directly into the pane on the right side of the screen.

4. Click OK when all addresses or hostnames are entered.
5. A certificate validating the connection between each appliance and the Management Console appears, choose to trust the certificate once or always.

   The added appliance will appear in the DMC.

6. From the Resources pane, right-click an **existing** member of the cluster or a standalone appliance and choose Set up.

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

   The Welcome page of the Wizard appears.

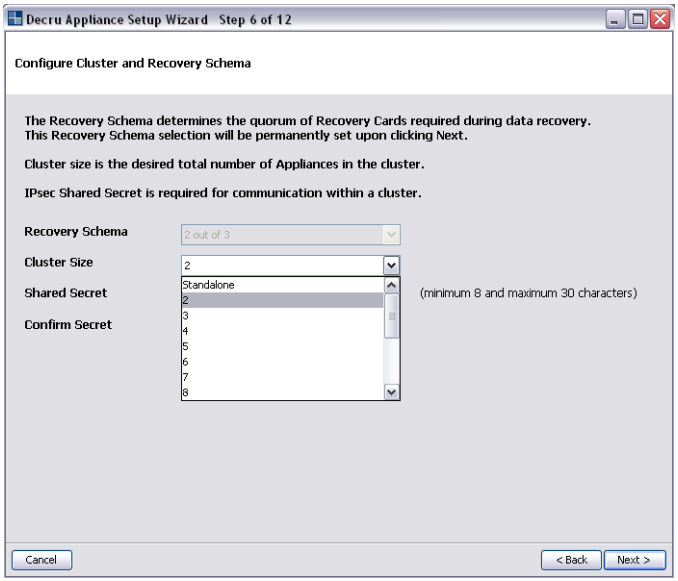
7. Click Start.

Log in 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

You will not be able to modify the Recovery Schema, 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 will appear. Enter the network settings for the appliance that will 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 will open 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 DataFort.

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 DataFort to accept a self-signed security certificate to improve security for the SSL communication between the Management Station and DataFort.

1. Enter a name for the appliance.
2. Enter the country code for your 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 262.
3. Enter the rest of the required information about your location and click Next.

Insert Recovery Card

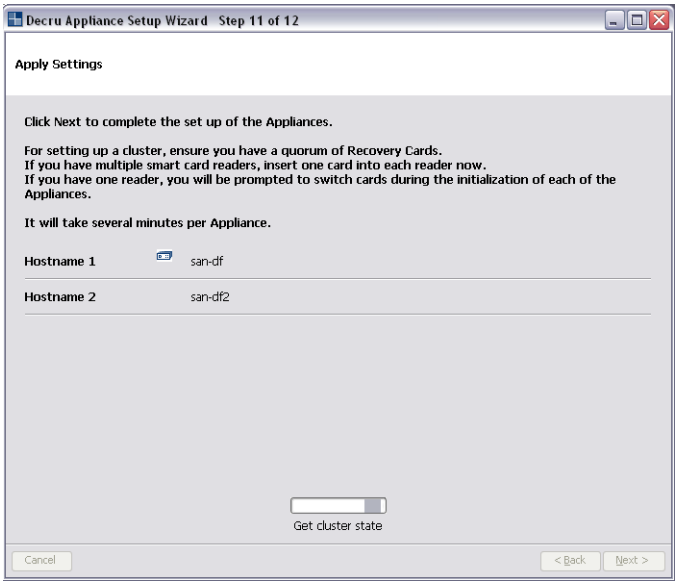
Recovery Officers should be prepared to enter the card label and password information for their Recovery Cards.

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. The Recovery Officer responsible for this card should enter the required information into the provided fields and click Next.
3. 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.
2. Insert the quorum of Recovery Cards. If one smart card reader is in use, the cards will 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 will not need to be switched.



3. 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 DataFort WebUI. See Chapter 6 for a list of available management interfaces.

- The DataFort WebUI provides complete management tools for a DataFort appliance or cluster. After the wizard is complete, you can close DMC and log into the WebUI to manage DataFort.
- The Decru Management Console offers a sub-set of the appliance management options available in the DataFort WebUI.

6 DataFort 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
- Connecting to the DataFort WebUI
- Connecting to the DataFort Command Line Interface
- Accessing the Decru Management Console
- Serial Console
- DataFort Front Panel LCD
- SNMP Settings

Management Interfaces Overview

After initial setup is complete use the management interfaces to configure and manage the DataFort appliance. The available management interfaces are summarized in Table 7.

Table 7: Management Interfaces

Interface	Description	Usage
Secure Sockets Layer (SSL) Transport Layer Security (TLS)	A secure HTTP (HTTPS) connection to the DataFort WebUI via a web browser from the Management Station. Can require smart card authentication in addition to password. See Connecting to the DataFort WebUI.	Primary method for creating and managing Cryptainers, DataFort settings, etc.
Decru Management Console (DMC)	A Java tool used for setup and management of LKM and DataFort 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. Provides additional management functions for DataFort appliances and all management for LKM appliances. SecureView enables many-at-once control of LKM and DataFort appliances. SecureView license required on all appliances that will be managed simultaneously.
	A limited DMC is shipped with each DataFort appliance. The full DMC product supports SecureView.	
Secure Shell (SSH)	A secure shell connection to DataFort CLI (command line interface) via secure shell client. Can require smart card authentication in addition to password. See Connecting to the DataFort Command Line Interface.	Alternative method for creating and managing Cryptainers, DataFort settings, users, etc. Also used for some advanced configuration.
Serial	A serial connection to DataFort can be used to enter network settings for an uninitialized DataFort. See Serial Console.	Set, clear, or reset DataFort IP settings. Zeroize DataFort when other interfaces are not available.
LCD	The DataFort front panel displays messages. The 2U DataFort appliance front panel also functions as a touch screen. See DataFort Front Panel LCD.	View status and throughput information. Use 2U DataFort touch panel buttons to enter IP settings for 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 DataFort. The standard MIB-II MIBs are exposed, as well as Decru's proprietary MIB. See SNMP Settings.	View DataFort 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 facilitate management of multiple appliances using SecureView, add the same administrator (with the same name and password) to all appliances. This will make 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 WebUI or CLI of an appliance. By default, DataFort is set not to require an Admin Card for WebUI or CLI access. To turn on Secure Web or Secure CLI (which require the presence of an Admin Card to log into DataFort), customize the security policy as described in Configuring Management Security Settings on page 139.

Note: All administrator types can log in to the WebUI 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 DataFort appliance. Selecting an appliance in DMC and choosing the Help menu will open an online version of the administrative guide for the selected appliance. See Decru Management Console Menus on page 195 for details about the DMC Help menu.

Connecting to the DataFort WebUI

By default, the Secure Web setting is not in effect, allowing any valid administrator to log in with a password. This requirement can be changed to require the presence of an Admin Card as well.

- Using the DataFort WebUI
- Connecting via WebUI
- Quick Links and Status
- Connecting via WebUI using Dual Authorization

Using the DataFort WebUI

A DataFort administrator accesses the DataFort WebUI by logging in from the Management Station.

- To return to the Home page from any other page of the WebUI, click the Decru logo.
- Hover the cursor over key on-screen elements for more information.
- Pages identified as Cluster-wide in the top right-hand corner display a configuration that applies to the entire cluster.
- Do not open other browser windows while running the DataFort WebUI.
- If Secure Web access is turned on, DataFort cannot be managed by accessing the WebUI through Windows Terminal Services or Remote Desktop.
- Due to card reader restrictions, it is only possible to have one DataFort WebUI instance open at a time on any given Management Station. In general, it is recommended that only one management interface be open for a given cluster at any one time. The Management Station should be connected to only one DataFort WebUI at a time.
- Windows display properties on the Management Station should set the screen area for at least 1024 x 768 pixels.
- The DataFort WebUI times out after 30 minutes of inactivity.

Connecting via WebUI

This is the standard method of logging an administrator in to the DataFort WebUI.

1. From Internet Explorer on the Management Station, enter **`https://`** followed by the IP address or resolvable hostname assigned to DataFort. (Be sure to enter https.)

   Note: TLS 1.0 must be enabled as described in Preparing the Management Station on page 37.

2. Click Yes to acknowledge the security certificate message.
3. Click Yes to agree to load the Decru management applet.

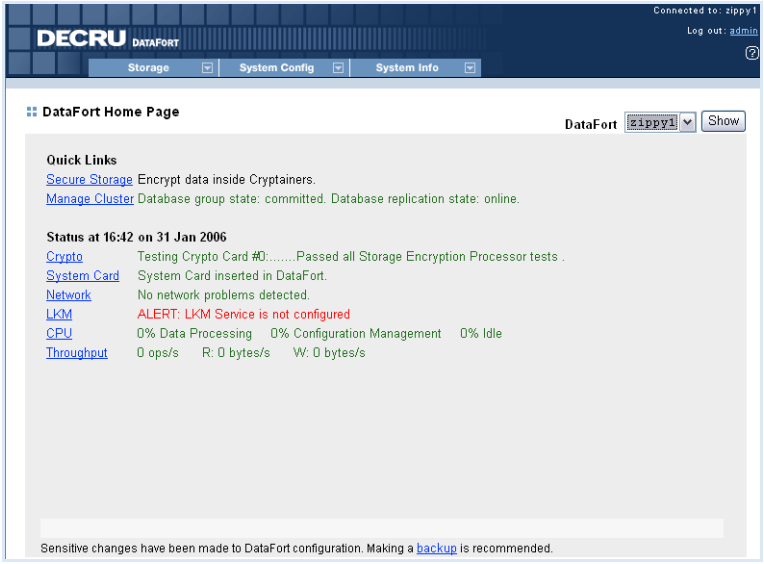
   The DataFort Login page appears.

   If Secure Web is in effect, insert an Admin Card that is associated with a valid administrator for this DataFort.

4. Enter the username and password that was set for the administrator and click Log In.

   Note: Click No if Windows offers to store password information.

   The DataFort Home page is displayed when an administrator logs in to the DataFort WebUI.



All management functions are available from the pull-down menus at the top of the screen; some are also available from quick links. The most common commands can be entered as keyboard shortcuts. While holding down the **D** key, press one of the following letters to display WebUI pages:

D+T	SAN Topology
D+B	Back Up Configuration
D+L	Log
D+C	LCD
D+W	WebCLI

To return to the Home page from any other WebUI page, click the Decru logo. Use the browser's Back button to go to a previous page. To log out of the WebUI, click the admin name beside the Log out link at the upper right of any WebUI page.

Quick Links and Status

The DataFort WebUI Home page for a standalone DataFort includes quick links including those for:

- Managing secure storage
- Managing the cluster
- Adding a license
- Configuring Lifetime Key Management functionality
- Viewing status and performance of system components

Some status categories are dynamic. Alerts are displayed in red if action is required.

Note: If the DataFort defense response has been triggered, a warning will appear on the Home page. DataFort will not accept any management commands in this state. To address this warning, see Clearing a Defense Alert on page 137.

Cluster Member Access

The pull-down menu at the top right of the screen enables you to view that same page on the WebUI of another cluster member. Select a member and click Show to view its WebUI.

Connecting via WebUI using Dual Authorization

By default, all administrators created using the DataFort WebUI can log in to the WebUI without additional authorization. By default, administrators created using the CLI will require prior authentication before they can log in to the WebUI or CLI. In addition, if the login privilege is revoked for a given administrator, that administrator will require the presence of an authorizing administrator in order to log in to the WebUI or CLI. See Requiring Authorization for Login on page 88 for details. The authorizing administrator can be any administrator who does not require authorization.

To log in when dual authentication is required:

1. First the administrator with authorization privileges must log in. From Internet Explorer on the Management Station, enter **`https://`** followed by the IP address, or the hostname assigned to DataFort if it has been registered with the domain name server. (Be sure to enter https.)
2. Click Yes to acknowledge the security certificate message.
3. Click Yes to agree to load the Decru management applet.

   The DataFort Login page appears.
4. The authorizing administrator logs in (inserting the associated Admin Card if Secure Web is on), by entering their username and password and clicking Log In.
5. Choose **System Config > System Users > Administrators**.
6. In the Known Administrators panel, select the administrator requiring authentication and click Authorize Login.
7. The administrator with authorization privileges should log out of the WebUI by clicking the name by the Log out link at the top of the page.
8. The authorized administrator now has one minute to log in at a Management Station from Internet Explorer, as follows:
   - From Internet Explorer, enter **`https://`** followed by the IP address or the hostname assigned to DataFort.
   - Click Yes to acknowledge the certificate message. Agree to load the Decru applet.
   - Insert the authorized administrator's Admin Card (if Secure Web is on), enter the authorized admin username and password, and click Log In.

   When authentication is complete, the DataFort Home page is displayed.

Connecting to the DataFort Command Line Interface

By default, the standard CLI setting is in effect, allowing the administrator to log in to the DataFort 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 WebUI

Using the CLI

- See Using the CLI on page 238 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, DataFort is set for standard CLI, which allows login without first obtaining a temporary password from the DataFort WebUI.

1. Open an SSH client on a workstation connected to the same network as the DataFort.
2. Enter the IP address or hostname assigned to DataFort.
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 WebUI 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 WebUI and accessing the Security Policy settings page, as described in Configuring Management Security Settings on page 139. Secure CLI requires that a session-specific password be furnished via the WebUI before the administrator can log in.

1. Insert the Admin Card of a valid administrator into the Management Station smart card reader and access the WebUI Login page from the Management Station as described in Connecting to the DataFort WebUI on page 72.
2. Click the button: Obtain a One Time Password for the CLI.

   Note: This button is present only if Secure CLI is in effect.

3. Enter the username and password for an administrator associated with the Admin Card that is inserted in the Management Station smart card reader.
4. Click Log In.

   A one-time login password (in hexadecimal format) will appear on the screen.
5. Copy the password that is provided.
6. Close the connection to the WebUI.

   Note: Log in to the CLI immediately after retrieving the password from the WebUI. Do not log in to the WebUI after generating the Secure CLI password, as it will invalidate CLI access.
7. Open an SSH client on a workstation connected to the same IP network as the DataFort.
8. Enter the IP address or hostname assigned to DataFort.
9. At the prompt, enter the same administrator login name.
10. When prompted for the administrator password, paste or type the Secure CLI password from step 5 into the command line. The CLI prompt is ready for commands.

Connecting via CLI using Dual Authorization

By default, all administrators created using the DataFort WebUI can log in to the WebUI without additional authorization. By default, administrators created using the CLI will require prior authentication before they can log in to the WebUI or CLI. In addition, if the login privilege is revoked for a given administrator, that administrator will require the presence of an authorizing administrator in order to log in to the WebUI or CLI. See Requiring Authorization for Login on page 88 for details. 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 DataFort.

2. Enter the IP address or hostname assigned to DataFort.
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 DataFort from an SSH client, entering the IP address or hostname assigned to DataFort, and entering his or her 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 WebUI

The DataFort WebUI offers a direct link to a simplified version of the CLI. Note that WebCLI does not support all features of the true DataFort CLI.

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

- From the WebUI choose **System Config > General > WebCLI.**

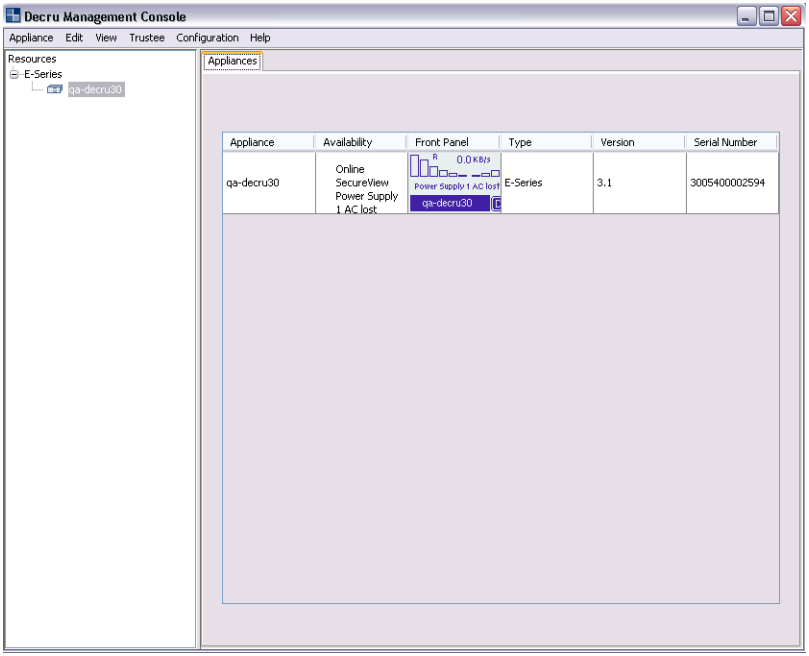
Accessing the Decru Management Console

Use the console to manage LKM and DataFort appliances from a central location.

- Choose **Start > Programs > Decru > Decru Management Console** from the Management Station. Any appliances which have been added to DMC will appear.
- See Decru Management Console Menus on page 195 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*.



Serial Console

The DataFort serial console port can be used to assign IP settings, and to temporarily or permanently clear the settings of an initialized DataFort.

Use only the supplied crossover RJ45 to DB9 adapter and standard straight through Ethernet cable to connect to the serial console port on the DataFort's rear panel. See Serial Console Port on page 46 for details.

Logging in to the Serial Console Port

Log in to an uninitialized DataFort with DataFort's default login name and password. Log in to an initialized DataFort with an administrator username and password that is valid for that DataFort.

DataFort serial sessions time out after 90 seconds of inactivity. If a session times out before you finish and save your configuration, log in again. Settings will not be 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 will appear.
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 DataFort 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 DataFort is being moved to a different network but zeroization is not required. When a DataFort is moved to a different network that does not recognize the DataFort IP address, the administrator can temporarily clear the settings so that access via WebUI and CLI are possible. To change the IP settings permanently, see Network Settings on page 173.

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 will appear.
2. Select option `C`.

   The IP settings will be cleared.
3. Select option `3` to save the settings, and exit the terminal window.

Zeroizing DataFort

Enter the zeroize command from the serial console to return the DataFort appliance to an uninitialized state. See Zeroization Using the Serial Console on page 160 for details.

DataFort Front Panel LCD

After setup, the DataFort front panel LCD displays messages and a bar graph showing data read and write rates. If the DataFort appliance is equipped with a touch-sensitive panel, onscreen buttons will provide more options. The left side of the graph indicates the rate (in bytes per second) at which DataFort reads data, or decrypts encrypted data. The right side of the graph depicts the rate at which DataFort writes, or encrypts data. The read/write display differs according to the type of DataFort 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	1K - 10K
2 bars	10K - 100K
3 bars	100K - 1M
4 bars	1M - 10M
5 bars	10M - 100M
6 bars	100M and up

Table 9: Read/Write Rate Display on 1U DataFort Appliances

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

Touch Panel Onscreen Buttons

If your DataFort 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 DataFort information (including software version and serial number). Use the up and down arrows to navigate the menu options, touching the Select button to access more information about the selected topic, and the Return button to return to the previous screen.

Network Touching the Network Settings and Select buttons on an uninitialized DataFort will allow you to access the Edit button, which you can use to set the IP address, subnet mask and gateway for the DataFort.

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

DataFort supports both MIB II and the read-only private Decru MIB. The Decru MIB is included on the DataFort 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 181 for details. A separate Dat*aFort 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 speciality 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 DataFort Appliances. The Full Administrator can complete all administrative tasks including: • Initializing DataFort Appliances • Account Administration • Storage Administration • Key Administration • Backup Administration • Physical Security Administration • 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 exportable keys • Purging keys upon backup to LKM as described in Key Purging • Managing DataFort Defense Responses • 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 Physical Security Administration. Security Administrator tasks include: • Setting Date and Time • Configuring and Viewing Logs • Zeroizing the Decru DataFort
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 Software • Downloading 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: • Network Settings • Upgrading DataFort • Setting Security Certificates • 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

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

- At least two Full Administrators should be associated with each DataFort or DataFort cluster. Associating more than one Admin Card is recommended.
- DataFort administrators should be highly trusted individuals in your organization.
- Administrators should remove the Admin Card from the smart card reader when they are logged out of the DataFort WebUI.

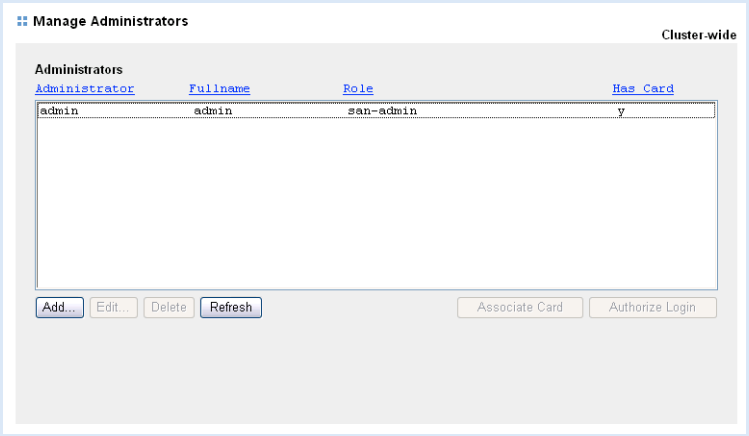
DataFort offers considerable flexibility in assigning roles and smart cards to administrators. One or more administrators can be associated with a single Admin Card; administrators can also be added without an association to an Admin Card. A Full or Accounts Administrator can add administrators and delegate 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
- Changing a Card Association

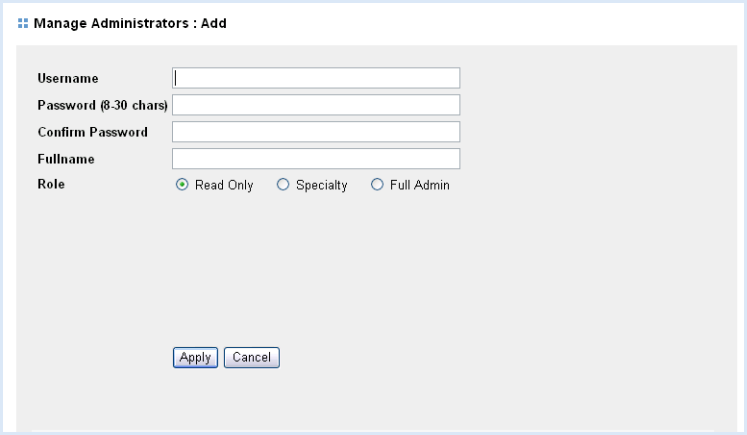
Adding an Administrator

1. Log in to the DataFort WebUI as a Full Administrator or an Accounts Administrator.
2. Select **System Config > System Users > Administrators**.

   Administrators known to this DataFort appliance are listed.



3. Click Add.



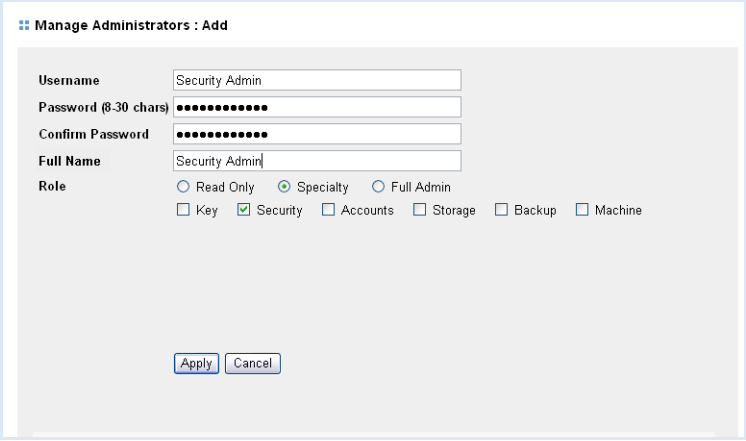
4. Enter the name of the new administrator, and a password for that administrator. Strong passwords are an important part of the overall security of the system. Select a password consisting of at least 8 valid, randomly chosen characters.

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

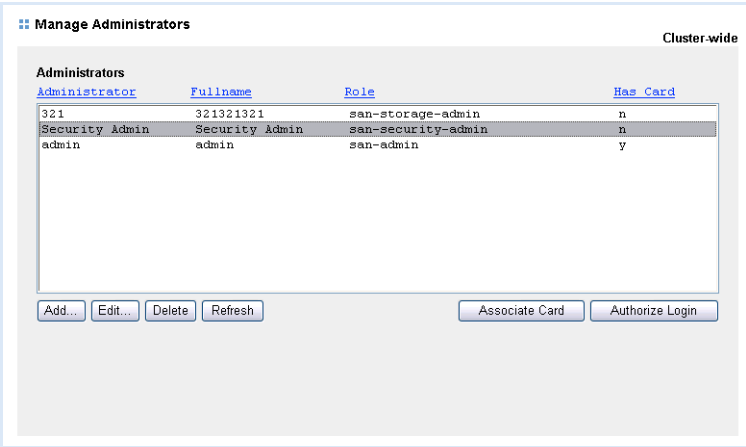
5. Confirm the password.
6. Enter a full name for the administrator.
7. Select the type of administrator you want to create. The default selection is Read Only. See Administrator Roles on page 83 for details. You can also require that an administrator be authenticated before being able to log in to DataFort. See Requiring Authorization for Login on page 88 for more information.

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

   - Select **Read-only** to create an administrator who can view DataFort settings, but cannot modify them.
   - Select **Specialty** to create specialized administrators. With Specialty selected, you can check multiple special types to combine permissions for one administrator.
   - Select **Full Admin** to create a Full Administrator role.



8. Click Apply.



9. Select the newly created administrator from the list.
10. If you wish to associate this administrator with an Admin Card for additional security, insert the Admin Card you wish to associate with this administrator in the Management Station smart card reader and click Associate Card.

    The Admin Card in the reader will now be associated with the administrator name and password.

Requiring Authorization for Login

By default, administrators created using the DataFort WebUI can log in to the WebUI or CLI without additional authorization. However, some administrators will require prior authentication before they can log into the Webui or CLI. By default, administrators created using the CLI will always require prior authentication before they can log in to the WebUI or CLI. In addition, if the login privilege is specifically revoked for a given administrator, that administrator will require the presence of an authorizing administrator in order to log in to the WebUI or CLI. The authorizing administrator can be any administrator who does not require authorization.

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

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:

- Creating an Administrator Requiring Authorization Using the WebUI
- Creating a New Administrator Using the CLI

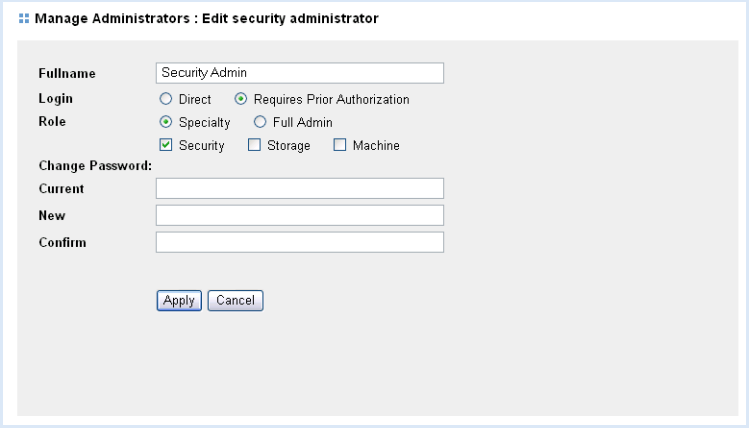
Protecting Against Insider Attacks

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 set up 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 WebUI.
- The administrator must be sure that DataFort is configured to require an Admin Card for authentication of WebUI and CLI access.
- In subsequent logins, both the authorizing administrator and the limited administrator must log in in order to access the WebUI 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 WebUI or CLI.

Creating an Administrator Requiring Authorization Using the WebUI

1. Log in to the WebUI and choose **System Config > System Users > Administrators**.
2. Create a new administrator or select an existing administrator and click Edit.



3. Select the Requires Prior Authorization button and click Apply.

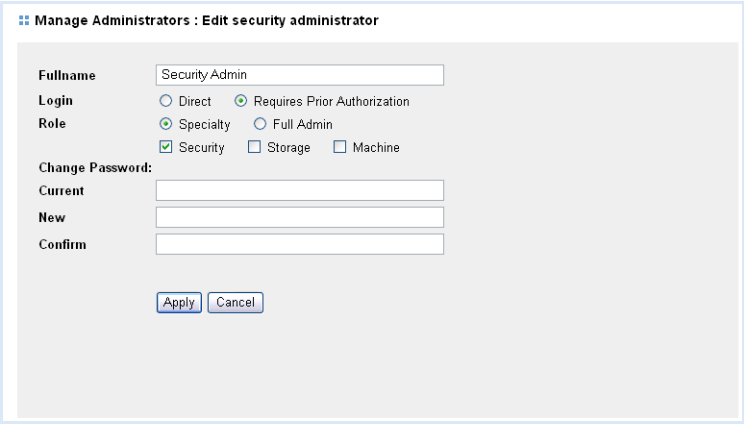
   Now this administrator will need authorization to log in to the DataFort. See Connecting via WebUI using Dual Authorization on page 74 for authorizing WebUI login, and Connecting via CLI using Dual Authorization on page 76 for authorizing CLI login.

   Note: To remove the requirement for login authorization, access the same page, deselect Requires Prior Authorization, 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 or her own password.

1. Log in to the WebUI and choose **System Config > System Users > Administrators**.
2. Select the administrator whose password will be changed and click Edit.



3. Enter the current password for the administrator.
4. 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.
5. 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 a DataFort appliance's list of known administrators, the DataFort or DataFort cluster will no longer authenticate that administrator. A Full Administrator or an Accounts Administrator can delete an administrator.

1. Log in to the WebUI and choose **System Config > System Users > Administrators**.
2. Select the name of the administrator to remove and click Delete.

Changing a Card Association

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

1. From the WebUI, select **System Config > System Users > Administrators**.

   Administrators known to this DataFort are listed, with their role and card status.
2. To add a listed administrator to those who are authorized to use the inserted Admin Card, select the administrator and click Associate Card.
3. To remove an administrator's association with the inserted Admin Card, select the administrator and click Dissociate Card.
4. To change an administrator's association with a different Admin Card for the DataFort or cluster, select the administrator, insert the other card, and click Associate Card or Dissociate Card.

8 Before Storage Administration

DataFort is ready to create Cryptainers after the Setup Wizard is complete, but you may wish to take additional steps to prepare for Cryptainer creation and DataFort operation.

These operations are performed using the WebUI. For login instructions see Connecting to the DataFort WebUI on page 72. Note that the Decru Management Console (DMC) can also be used to perform some of these operations. See Chapter 16 for DMC menu options.

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

- Verifying DataFort Configuration
- Starting LKM

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

Verifying DataFort Configuration

Verifying System Version

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

- From the DataFort WebUI, choose **System Info > About**.
- Check the Local System Version entry for the Platform FW Build ID. The Platform FW Build ID should end with an underscore and the word `secure`. If it does not, take the DataFort offline and notify Decru support.

Checking Cluster State

A cluster must be in a committed/online state for proper operation. The DataFort WebUI Home page of any cluster member will display the status of the cluster at the Manage Cluster quick link. See Checking the Status of the Cluster on page 164 for information about cluster states.

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 .

- From the DataFort WebUI, choose **System Config > System Users > Administrators**.
- Create an additional administrator. If desired, associate one or both administrators with an Admin Card. See Adding an Administrator on page 85 for instructions.

Configuring Remote Logging

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

- From the WebUI, choose **System Config > General > Configure Log**.
- Determine which log messages should be sent to a remote syslog server on your network. See DataFort Log Storage Guidelines on page 152 for details.

Determining the Defense Setting

Determine the level of defense necessary when an intrusion to the DataFort 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 an appropriate defense setting for your site involves deciding:

- The relative importance of the defense triggers.
- The need for an automatic response vs. a manual response at the DataFort 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:

- From the WebUI, choose **System Config > Security > Defense Settings**.
- Choose the appropriate defense setting. See Defense Triggers and Responses on page 135.

Configuring Disk or Tape Mode

While the FC-Series DataFort appliance supports encryption of data both on disk and tape, the appliance may not perform properly if used for both disk and tape concurrently.

Proper configuration settings and features may differ across disk and tape deployments and could destabilize DataFort if it is operated in mixed environments. 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 or WebCLI. See Connecting to the DataFort Command Line Interface on page 75 for detailed instructions.
2. Enter the IP address or hostname assigned to DataFort.
3. In the terminal window, enter the administrator login name and password.
4. Set the system properties to disable tape support:

```
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 will interact with tape devices. Note that these features are only available if a DataFort license controlling tape features is present.

- From the DataFort WebUI, choose **Storage > Tape Settings.**
- Select whether DataFort will encrypt, compress or encrypt and compress data as it is sent to tape devices for backup.

Starting LKM

Decru provides two solutions for key management: Lifetime Key Management software (LKM Server) and the Lifetime Key Management appliance (LKM Appliance). When set up to use either LKM solution, LKM data automatically updates when there is a change to encryption keys.

- Before configuring DataFort, set up the LKM management solution. See Setting Up Lifetime Key Management on page 39.

LKM Server

If using the LKM server, its IP address must be specified using the DataFort WebUI to allow DataFort to send backups of key material to the LKM server automatically

- From the WebUI, click the LKM link or choose **System Config > Recovery > LKM Settings**.
- Set the LKM server information for automatic backup. See Saving Configurations to Lifetime Key Management Software on page 145. All LKM settings are propagated across cluster members, therefore it is sufficient to enter LKM settings once for each cluster.

LKM Appliance

If you are using an LKM appliance, set up the appliance using the Decru Management Console as described in the *LKM Appliance Administration Guide*. Use the Decru Management Console to create a link between all DataFort appliances and the LKM appliance.

9 Storage Administration

This chapter includes instructions for using the DataFort WebUI 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 can perform all of the functions outlined in this chapter.

- Creating Cryptainers
- Managing Hosts
- Managing Cryptainers
- Managing Storage
- Managing Tapes
- 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 SAN Topology page of the DataFort WebUI for Cryptainer creation and management. The SAN Topology page shows all known hosts and storage devices, along with any Cryptainers that have been created. See SAN Topology Page on page 105 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 WebUI 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 DataFort WebUI, see:

- Cryptainer Creation Using Collections (recommended)
- Cryptainer Creation Without Collections

Cryptainer Creation Using Collections

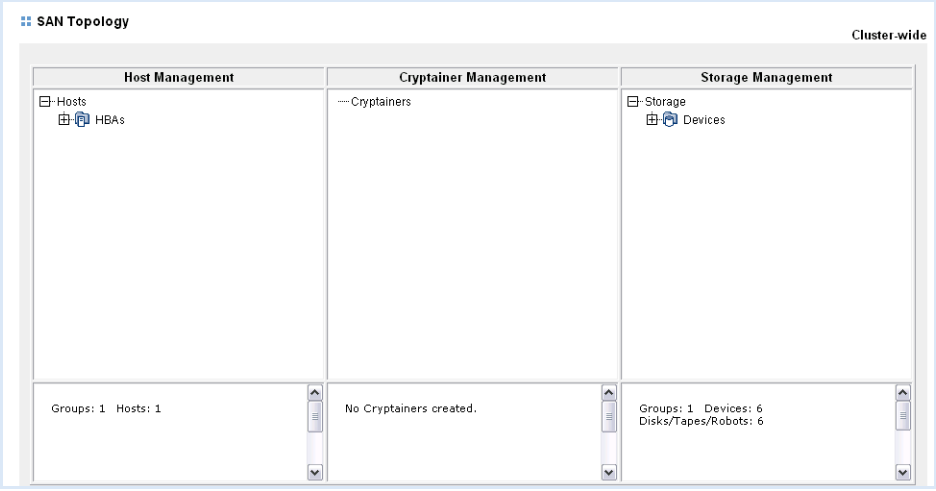
To create Cryptainers using the collection features of DataFort, complete these steps:

- Create a Collected Host
- Create a Collected Storage Device
- Create a Cryptainer
- Assign Permissions to a Cryptainer
- Encrypt Cryptainer Data

1. A Full Administrator or Storage Administrator must be logged in to the WebUI to create Cryptainers. See Connecting to the DataFort WebUI on page 72 for login instructions.
2. Access the SAN Topology page by selecting **Storage > SAN Topology** from the WebUI menu, by clicking the Secure Storage link on the Home page of the WebUI, or holding down **D** and pressing **T** on the Management Station keyboard once connected to the WebUI.

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

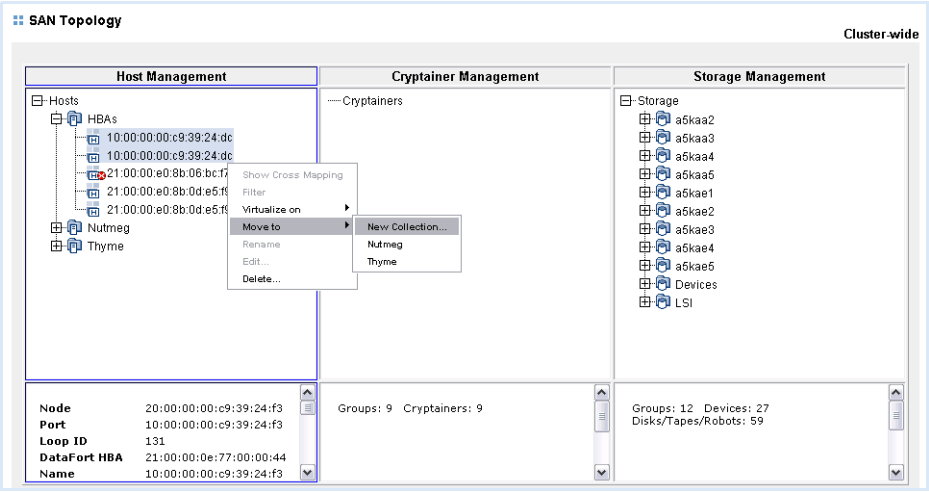
   All discovered hosts and targets will appear on the SAN Topology page. Click the tree to expand the view and see individual hosts and targets.



Create a Collected Host

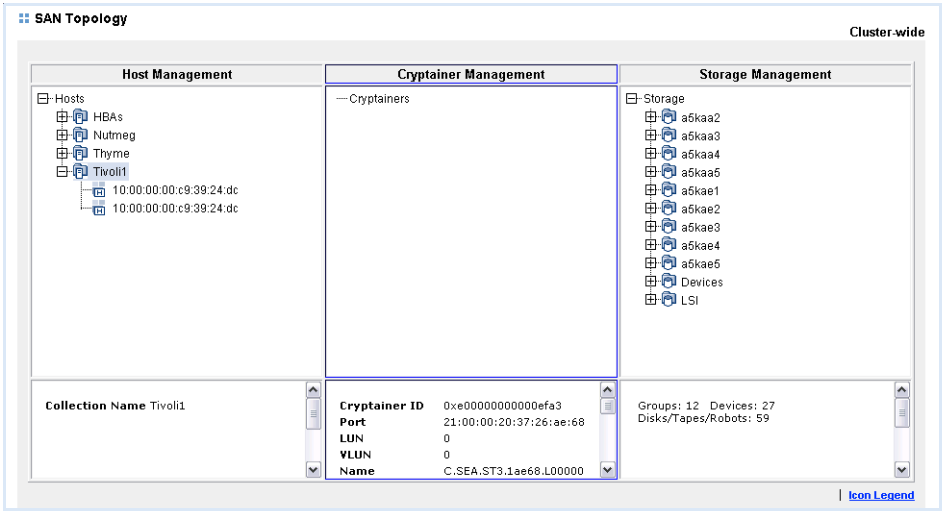
In a standard highly available clustered configuration the same host will appear more than once as each path from that host to storage is represented in the WebUI. The number of appearances of the host is based on the number of connections it has to the fabric. For ease of management, group the instances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

1. Multiple-select host instances by control or shift-clicking them in the Host Management pane.
2. Right-click to view the Host Collection Menu and select **Move to > New collection...**



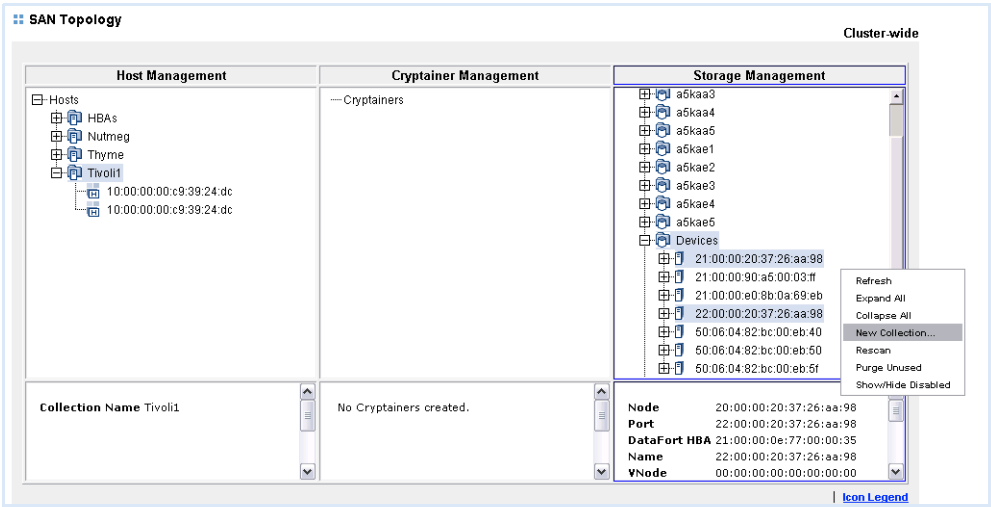
3. Enter a name for the collection and click OK.

   The new collection appears in the WebUI.



Create a Collected Storage Device

1. Multiple-select storage device instances (use WWN information to identify paths to the same device) by control or shift-clicking them in the Storage Management pane.
2. Right-click to view the Storage Collection Menu and select **Move to > New collection...**



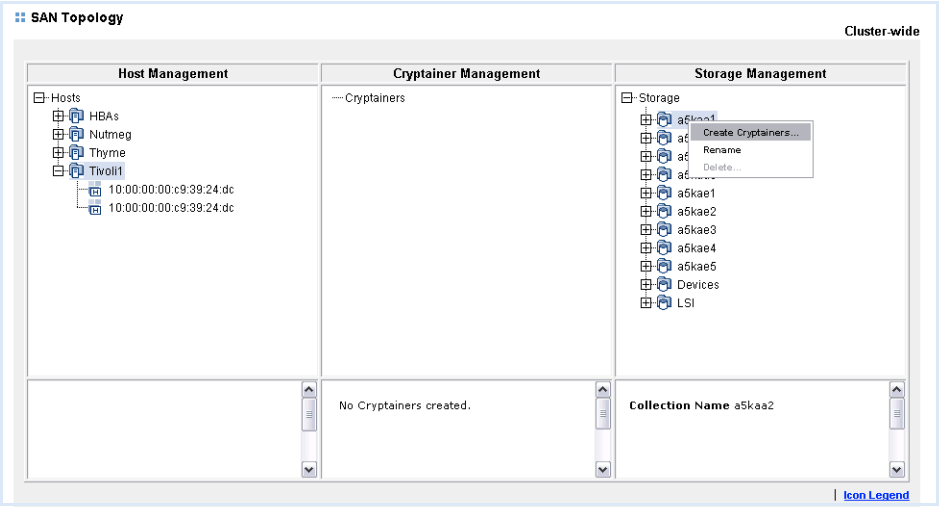
3. Enter a name for the collection and click OK.

   The new collection appears in the WebUI.

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 will be created for each LUN in the collection.



   The Create Cryptainer page appears.

2. Select the settings for the Cryptainer on this device. See Options When Creating a Cryptainer on page 100 for a list of options and their defaults.

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.

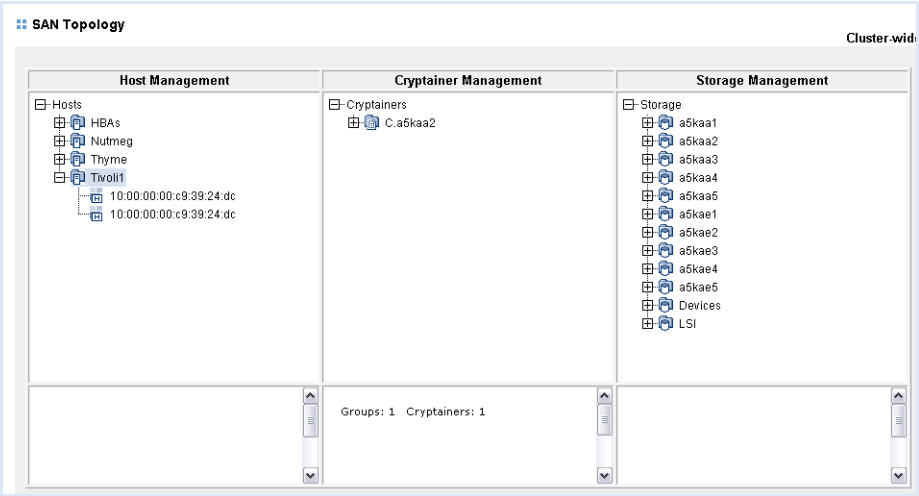
Options When Creating a Cryptainer

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.

Port Mapped (on by default)	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 will preserve 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 will match the real LUN of the disk for which the Cryptainer was created.
LUN Mapped (off by default)	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 will appear 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.
Host of Masked LUNs (empty by default)	If a host has been virtualized, a Cryptainer can be created for that particular host by specifying that host's WWN in this option. Commands sent to this Cryptainer's disk will be sent via the storage-side virtual port that was created when the user virtualized the host. See Managing Hosts for more about virtualizing hosts.
Assign Key (off by default)	If set to ON, DataFort will not preserve the data on the target disk, and will automatically encrypt the contents of the Cryptainer. If set to OFF, DataFort will preserve the data on the Cryptainer's disk and will not encrypt/decrypt data being written or read from the disk automatically. The Cryptainer will have to be manually rekeyed to enable encryption. See Managing Cryptainers for more about data encryption.
Exportable (off by default)	This option allows the Cryptainer being created to be shared with trustees. If this option is set to OFF, then the corresponding Cryptainer can never be exported to a trustee. Once set during Cryptainer creation, this option is set for the lifetime of the data inside the Cryptainer. See Managing Trustees on page 128 for more about trustees.

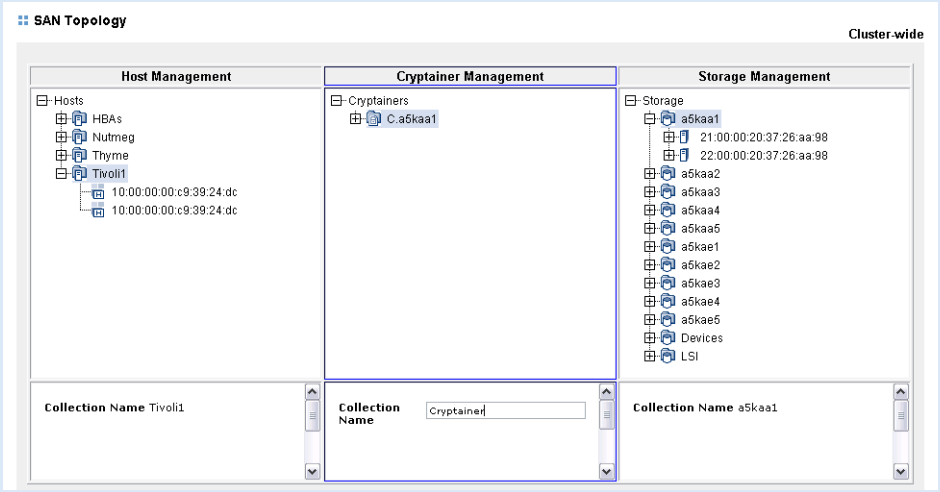
Port Forwarding (off by default)	If set to ON, the virtual port created for a port mapped Cryptainer will have the same exact WWN as the disk's Cryptainer. If this feature is used, it is recommended that the host side and storage side HBAs of the DataFort be on separate fabrics, or that port zoning be used on the FC switch. When virtualizing a host device and using Port Forwarding, the device's WWN will appear on both storage and host sides of DataFort. If a shared fabric is used on the host and storage sides and soft zoning is used, interoperability issues can occur. To avoid this, use hard zoning (zoning by port), virtual SANs or separate the fabrics.

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 Rename.

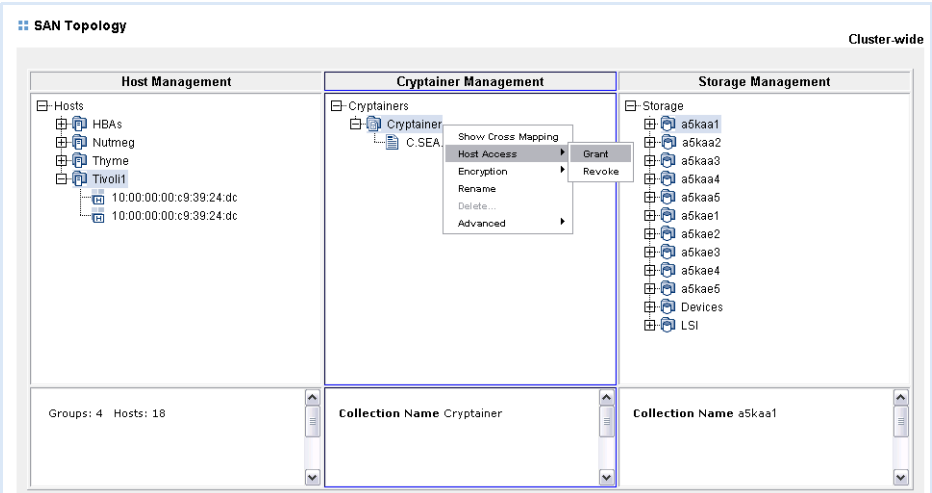
   The name field will open in the lower pane.



5. Enter the new name. To save the change, leave the cursor in the name field and hit Return on the Management Station keyboard.

Assign Permissions to a Cryptainer

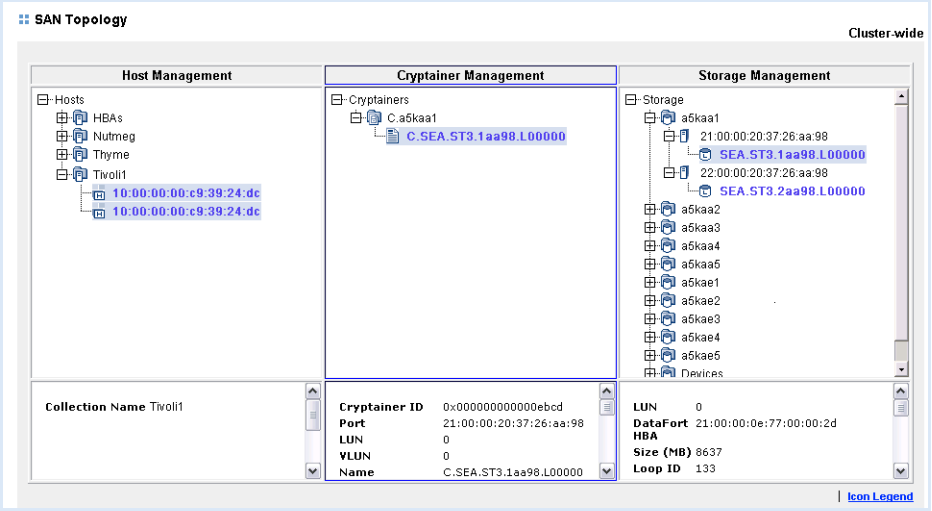
1. Select a collected host and then right-click a Cryptainer. Select **Host access > Grant**.



The associated host collection will have access to the Cryptainer.

2. To view the results, right-click the Cryptainer and select Show Cross Mapping.

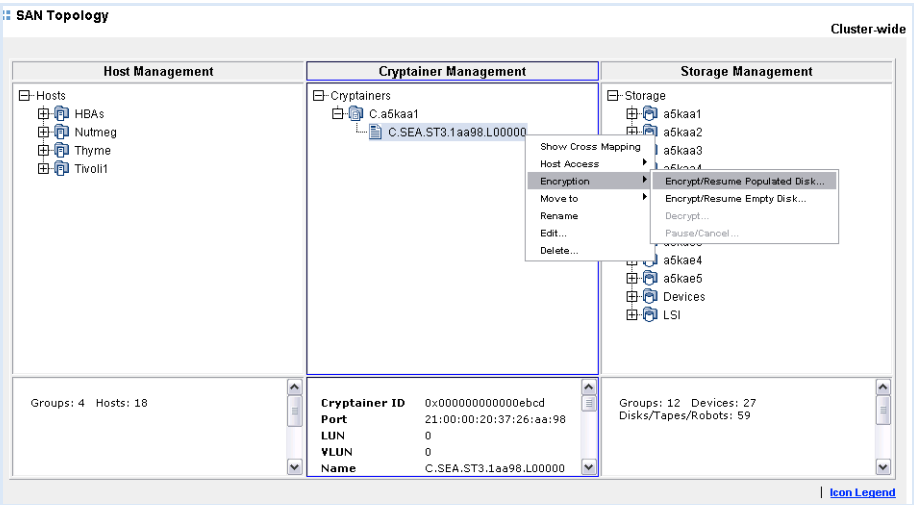
   Bold text indicates the storage location of the Cryptainer and which host has access.



Encrypt Cryptainer Data

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

1. 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 device or LUN in the Storage Management pane. You can select the entire storage device, or a specific LUN.
   - Select the entire storage device: This will create a Cryptainer per LUN for the entire device.
   - Select an individual LUN: This will create a Cryptainer only on the selected LUN.
   - Shift-click and select multiple LUNs to create Cryptainers on them.
2. Select Create Cryptainer.
3. Select Port or LUN Mapping depending on the needs of your environment. Note that the same mapping method must be used for all LUNs within a given device. See Options When Creating a Cryptainer.

   The Cryptainer is added to the Cryptainers Management pane. The default name automatically reflects the storage device where the Cryptainer was created.
4. Rename the Cryptainer if desired by right-clicking it and selecting Rename.

   The rename field in the lower pane will be activated.
5. Enter a name and hit the Return key on the Management Station keyboard to accept the new name.
6. Select the host you wish to grant access to the Cryptainer, then right-click the Cryptainer and select **Host Access > Grant**.
7. Right-click the Cryptainer and select Show Cross Mapping.

   Bold text indicates the location of the Cryptainer on the storage device and the host with access to the Cryptainer.
8. 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, right-click the Cryptainer and select **Encryption > Encrypt/Resume Populated Disk**.
   - To encrypt a Cryptainer without data for the first time, or to rekey an existing Cryptainer without data, right-click the Cryptainer and select **Encryption > Encrypt/Resume Empty Disk**. Any data on the disk will be lost.

SAN Topology Page

The SAN Topology page of the WebUI shows all known hosts and targets, along with any Cryptainers that have been created.

Access the SAN Topology page by selecting **Storage > SAN Topology** from the WebUI menu, by clicking the Secure Storage link on the Home page of the WebUI, or by holding down **D** and then pressing **T** on the Management Station keyboard once connected to the WebUI. 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. Double-click an item onscreen to update its information in the details pane.
Collections	Option to collect onscreen objects for ease of management.
Multiple device select	Select multiple devices by control or shift-clicking them onscreen.
Filter	Change the view so that only items relevant to the selected filter object will expand onscreen. Multiple filters can be set. They can be removed by clicking the onscreen buttons that appear after they have been set.
Icons	Icons show the state of the device. Click the Icon Legend link on the SAN Topology page for an overview of icons.

The following sections describe menu options on the Storage Network Topology page:

- Managing Hosts
- Managing Cryptainers
- Managing Storage

DataFort WebUI Icons

Icons display status information about network devices including hosts, targets and Cryptainers. Images will be combined to describe multiple conditions (for example, an encrypted Cryptainer that is offline will show 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 on the SAN Topology page 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 WebUI 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, refresh or rescan the pane view and add a new host or collection of hosts. Note that a rescan is potentially disruptive to disk IO.
Host Collection Menu	Right-click a collected host to use the menu to manage all host instances together. See Host Collection Menu on page 107.
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 on the SAN Topology page or see DataFort WebUI Icons on page 106.

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.

Show Cross Mapping	Right-click the collection and select Show Cross Mapping to view which Cryptainers the collection can access, and the location of those Cryptainers.
Filter	This option restricts the WebUI view to show only the Cryptainers and storage devices the selected host collection can access.
Virtualization	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 **Virtualization > On**. The host will be virtualized on available virtual ports.
Rename	To rename the collection, right-click it and select Rename. The name field will open in the lower pane. Enter the new name. To save the change, leave the cursor in the name field and hit Return on the Management Station keyboard.

Advanced	**Advanced > 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 Tapes features.
	Advanced > Port Lock On/Off: Right-click the collection and select **Advanced > 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 will show if port locking is on. The setting also appears in the lower pane. Note that port locking is only available on Brocade and McData switches.

Host Menu

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

Show Cross Mapping	Right-click a host and select Show Cross Mapping to view which Cryptainers and targets the host can access.
Filter	Restricts the WebUI view to only the Cryptainers and storage devices the selected host can access.
Virtualize On	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. At the host level, it is possible to assign a specific virtual port for an HBA. Right-click the host and select Virtualize On, then select a specific virtual port, or select Available Port to allow any available port to be assigned.
Move To	Move the selected host instance to a specified collection.
Rename	Select Rename. The name field will open in the lower pane. Enter the new name. To save the change, leave the cursor in the name field and hit Return on the Management Station keyboard.
Edit	Opens the Edit Host page where the Name, Label of Default Pool, Port Lock Mode and RAID admin mode can be set for the selected host. See Edit Host Page.
Delete	Right-click the host and select Delete to remove it from the WebUI. This option removes the host from the WebUI. The host is not deleted from the fabric. If the host is still online and zoned with the DataFort, it will reappear at the next rescan.

Edit Host Page

The Edit Host page allows the Name, Label of Default Pool, Port Lock Mode and RAID Admin mode to be set for the selected host.

Name	Change the name of the host.
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.
Port Lock Mode (off by default)	Turn Port Lock on 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 turned off if the host is moved, and reset at the new port. Individual Host Icons will show if port locking is on. The setting also appears in the lower pane. Note that port locking is only available on Brocade and McData switches.
RAID Admin (off by default)	Turn RAID Admin on to support device management software running a server (host) that needs direct access to the device through the Fibre Channel. When RAID Admin is enabled on a host, DataFort will pass 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. Turning RAID Admin on allows such vendor-unique commands to pass through DataFort.

Managing Cryptainers

The Cryptainer Management pane of the WebUI 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, add a new collection or filter the view to show only the Cryptainers and disks relevant to a specified DataFort.
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 will show whether the Cryptainer has been encrypted or is in clear text form, is in the process of being encrypted or is waiting for encryption, and whether the Cryptainer is healthy or not. An unhealthy Cryptainer will be indicated if at least one device that maps to the Cryptainer is offline. For more information click the Icon Legend link on the SAN Topology page or see DataFort WebUI Icons on page 106.

Cryptainer Collection Menu

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

Show Cross Mapping	Right-click a Cryptainer collection and select Show Cross Mapping to view which hosts have access to the collection of Cryptainers and to see on which storage device the Cryptainers are located.
Host Access	Select a host in the host pane, then right-click a Cryptainer collection and choose **Host Access > Grant** to grant that host access to the selected collection. To revoke host access, select the host then right-click the collection and select **Host Access > Revoke**. Do not change permissions when I/O is occurring. When permissions are changed for a port-mapped Cryptainer, DataFort disables the virtual port, waits 10 seconds, then re-enables the virtual port so that new tape devices can be registered. (Note that in a disk environment this should be disabled, see Troubleshooting for more information).

Encryption	Data within a Cryptainer created on disk will not be encrypted until the encryption process is begun using this option. Cryptainer icons will indicate whether a Cryptainer is already encrypted or if it is in cleartext, in the process of being encrypted or waiting to be encrypted. If the disk contains data, select **Encrypt/Resume Populated Disk**. If the disk does not contain data, select **Encrypt/Resume Empty Disk**. Any data on the disk will be lost. Select **Decrypt** to return the data to cleartext form. Use **Cancel** to halt the encryption process.
Rename	Select Rename. The name field will open in the lower pane. Enter the new name. To save the change, leave the cursor in the name field and hit Return on the Management Station keyboard.

Cryptainer Menu

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

Show Cross Mapping	Right-click a Cryptainer and select Show Cross Mapping to view which hosts have access to the Cryptainer and to see on which storage device the Cryptainer is located.
Host Access	Select a host in the host pane, then right-click a Cryptainer and choose **Host Access > Grant** to grant that host access to the selected Cryptainer. To revoke host access, select the host then right-click the Cryptainer and select **Host Access > Revoke**. Do not change permissions when I/O is occurring. When permissions are changed for a port-mapped Cryptainer, DataFort disables the virtual port, waits 10 seconds, then re-enables the virtual port so that new tape devices can be registered. (Note that in a disk environment this should be disabled, see Troubleshooting for more information).
Encryption	Data within a Cryptainer created on disk will not be encrypted until the encryption process is begun using this option. Cryptainer icons will indicate whether a Cryptainer is already encrypted or if it is in cleartext, in the process of being encrypted or waiting to be encrypted. If the disk contains data, select **Encrypt/Resume Populated Disk**. If the disk does not contain data, select **Encrypt/Resume Empty Disk**. Any data on the disk will be lost. Select **Decrypt** to return the data to cleartext form. Use **Cancel** to halt the encryption process. Note that this menu can also be used to rekey an existing Cryptainer.
Move To	Move the selected Cryptainer to a specified collection.

Rename	Select Rename. The name field will open in the lower pane. Enter the new name. To save the change, leave the cursor in the name field and hit Return on the Management Station keyboard.
Edit	Opens the Edit Cryptainer page where settings can be changed for the selected Cryptainer. See Edit Cryptainer Page.
Delete	Right-click the Cryptainer and select Delete to remove it from the WebUI. The Cryptainer can be restored from its original location using the Advanced Storage option described in Restoring a Cryptainer. A removed Cryptainer can be restored as long as the storage device on which it was created remains (disk only). To aid in recovery, record the port WWN and LUN number of the Cryptainer location and Cryptainer ID before deletion. This information appears in the lower pane.

Edit Cryptainer Page

The Edit Cryptainer sets the Name on the selected Cryptainer.

Name	Change the name of the Cryptainer. Enter the new name and click Apply.

Managing Storage

The Storage Management pane features the following elements:

Storage Pane Menu	Right-click in the Storage pane to use the top level storage menu. The menu offers options to modify, refresh or rescan the pane view and add a new collection of storage devices. Note that a rescan is potentially disruptive to disk IO.
Storage Collection Menu	Right-click a collection of Storage devices to use the collection menu. See Storage Collection Menu.
Individual Storage Device Menu	Right-click a storage device to view the storage device level menu. See Storage Device Menu.
Individual LUN Menu	Right-click a LUN to view the LUN level menu. See LUN Menu.
Individual Storage Icons	The icons in the WebUI 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 on the SAN Topology page or see DataFort WebUI Icons on page 106.

Storage Collection Menu

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

Create Cryptainers	Create a Cryptainer on the device (a Cryptainer per LUN for the entire device). See Options When Creating a Cryptainer on page 100. 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.
Rename	Select Rename. The name field will open in the lower pane. Enter the new name. To save the change, leave the cursor in the name field and hit Return on the Management Station keyboard.

Storage Device Menu

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

Create Cryptainers	Create a Cryptainer on the device (a Cryptainer per LUN for the entire device). See Options When Creating a Cryptainer on page 100. 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.
Paths	Map/Unmap devices to add or remove a path from a Cryptainer to a storage device. This feature is used when a Cryptainer has been 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.
Rename	Select Rename. The name field will open in the lower pane. Enter the new name. To save the change, leave the cursor in the name field and hit Return on the Management Station keyboard.
Disable	Disable will cause the selected device to disappear from the storage panel. Disabled devices will be grayed out and will not be manageable from the WebUI. To restore disabled images, right-click in the white space and select Show/Hide Disabled.

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.

Show Cross Mapping	Select the device and click Show Cross Mapping to display which hosts have access to which storage devices, and which storage devices Cryptainers are mapped to.
Create Cryptainer	Create a Cryptainer on the LUN. See Options When Creating a Cryptainer on page 100.
Paths	Select the storage device and choose **Paths > Show Alternate Paths** to view all paths to the device.
	Paths > Map to Cryptainer/Un-map from Cryptainer allows you to add a path to a Cryptainer, or remove it. Map to Cryptainer will add a path to a selected Cryptainer on the LUN. Select the Cryptainer, then shift-click the LUN and select Map to Cryptainer.

Beacon On	Blink the LED on the physical disk to help identify it in the rack. This is intended for disk use (JBOD) only.
Rename	Select Rename. The name field will open in the lower pane. Enter the new name. To save the change, leave the cursor in the name field and hit Return on the Management Station keyboard.
Delete	This option removes the storage device from the WebUI. Select the device and choose Delete. The device is not deleted from the fabric. If the device is still online and zoned with the DataFort, it will reappear at the next rescan.
Crypto Copy to Cryptainer	Crypto Copy to Cryptainer will copy the contents of the disk to a Cryptainer so it can be copied in encrypted form from one disk to another. This provides the benefit of copying a volume within a storage device, and across distance. The encrypted data is safe in transit. This can be useful in environments which include a primary data center and a disaster recovery data centers with a disk mirroring facility (such as SRDF for EMC storage devices) between them. This feature is intended for disk use only. Select a disk and Cryptainer and choose Crypto Copy to Cryptainer to copy the contents of that disk to the Cryptainer. Once the copy is complete, the contents of the Cryptainer can be copied in turn to another disk.
Crypto Copy from Cryptainer	Crypto Copy from Cryptainer will copy the contents of a Cryptainer in encrypted form from one disk to another. This feature is intended for disk use only. Select the Cryptainer and choose Crypto Copy from Cryptainer to copy the contents of that Cryptainer to the selected disk.
Export key	Export key allows the Cryptainer key for this LUN to be exported to a trustee. See Managing Trustees on page 128.
Import key	Import key allows a Cryptainer key for this LUN to be imported from a trustee. See Managing Trustees on page 128.
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 you wish to restore the Cryptainer and choose Restore Cryptainer. The Restore Cryptainer page will appear. 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.

Managing Tapes

Choose **Storage > Manage Tapes** to view the Manage Tapes page. This page is only visible if the license controlling tape support is installed. The Tape Management Pane features the following elements:

Tape Pane Menu	Right-click in the Tape Management pane to use the top level menu. The menu offers options to modify or refresh the pane view and add a new collection of tapes or a new pool. It also offers a Settings menu option, which opens the Tape Settings page. See Managing Tape Settings on page 120.
Tape Pool Collection Menu	Right-click a collection of tapes to use the collection menu. See Tape Pool Collection Menu on page 116. A pool will 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 117.
Individual Tape Device Menu	Right-click a tape device to view the device level menu. See Tape Device Menu on page 117.
Individual Tape Device Icons	The icons in the WebUI indicate the condition and type of tape device. A red X indicates offline status, a yellow alert indicates a problem. For more information click the Icon Legend link on the SAN Topology page or see DataFort WebUI Icons on page 106.

Tape 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 will be displayed in the WebUI once encrypted data is written to the tape.

Host Access	Grant/Revoke host access to the tape pool collection. Do not change permissions when I/O is occurring. When permissions are changed for a port-mapped Cryptainer, DataFort disables the virtual port, waits 10 seconds, then re-enables the virtual port so that new tape devices can be registered.
Rename	Select Rename. The name field will open in the lower pane. Enter the new name. To save the change, leave the cursor in the name field and hit Return on the Management Station keyboard.
Delete	This option removes the collected pool from the WebUI.

Tape Pool Menu

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

Show Cross Mapping	Right-click a tape pool and select Show Cross Mapping to view which hosts have access to the tape pool.
Host Access	Select a host in the host pane, then right-click a tape pool and choose **Host Access > Grant** to grant that host access to the selected pool. To revoke host access, select the host then right-click the pool and select **Host Access > Revoke**. Do not change permissions when I/O is occurring. When permissions are changed for a port-mapped Cryptainer, DataFort disables the virtual port, waits 10 seconds, then re-enables the virtual port so that new tape devices can be registered.
Assign 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.
Manage Key	Import or export key assigned to tape pool.
Move To	Move the selected pool to a specified collection.
Edit	Opens the Edit Pool page where the Name, Key Policy and Key Export settings can be changed. See Edit Pool Page.
Delete Tapes	Right-click the pool and select Delete Tapes to remove the tapes associated with the pool from the WebUI, but leave the pool.
Delete	Right-click the pool and select Delete to remove it from the WebUI. All tapes must be deleted before the pool will be removed.

Tape Device Menu

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

Keys	Import or export key assigned to tape device.
Delete	Right-click the device and select Delete to remove it from the WebUI.

Edit Pool Page

Right-click a pool and select Edit to view the Edit Pool page. The Edit Pool allows the Name, Key Policy and Key Export policy to be changed for the selected pool. Change settings if desired, then click Apply to save settings.

Name	Change the alias for the pool as it is displayed in the WebUI. 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 WebUI. See Managing Tape Settings on page 120.
Key Read/Write Span	Sets the read/write life span of the key used to encrypt tape contents. Read/write represents the span in days that the key may be used for writing.
Key Lifespan	Sets the lifespan of the key assigned to tapes in the pool. Lifespan represents the span in days that the key may be used for reading.
Key Exportable	Select whether the Cryptainer key for this LUN can be exported to a trustee. See Managing Trustees on page 128.

ACL Learning

Use the onscreen link to turn ACL Learning on or off. When on, DataFort will monitor backup activity on the network and record which devices have access to storage. When ACL Learning is turned off, DataFort will enforce the access controls recorded when ACL Learning was on. This restricts the use of DataFort and backup pools to only the hosts which were used when ACL Learning was ON.

Once ACL Learning is on, clicking the onscreen ACL Learning is on link will bring up the Tape Settings page. It is recommended that ACL Learning be turned on initially while backups are run as usual for a period of time, after which ACLs should be reviewed and adjusted if necessary.

Managing Tape Settings

Access the Tape Settings page to configure settings for the DataFort, including those for pools and tapes. 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.

Note: Tape Settings appears only if a license controlling tape features is installed on DataFort.

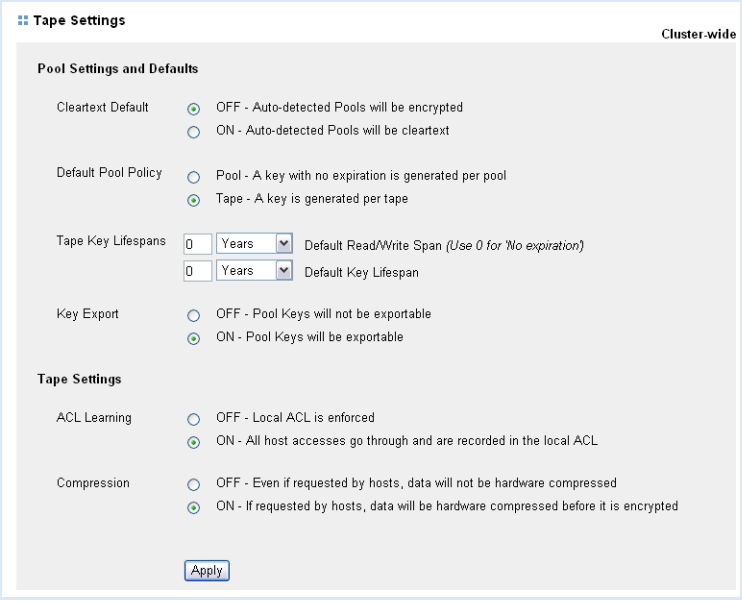
1. Access the Tape Settings page by selecting **Storage > Tape Settings**.

   The page can also be accessed from the Manage Tapes page of the WebUI:

   - Right-click in the Tape Management pane and select Settings.
   - Click the ACL Learning is On link.

2. Select the desired setting and click Apply to set the changes. Tape settings include:

   - Pool Settings and Defaults
   - Tape Settings



Pool Settings and 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 Default	Determines whether pools that are automatically detected by DataFort will be encrypted or not by default.
Default Pool Policy	Determines whether keys are generated per tape or per pool by default. Select per-tape to manage key life spans.
Tape Key Lifespans	Sets the default read/write life span and read life span of the key used to encrypt tape contents. Read/write represents the span in days that the key may be used for writing. Lifespan is the span in days 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 Export	Determines whether keys can be exported to trustees by default. See Managing Trustees on page 128.

Global Default Pool

The global default pool allows a single pool to be set across all hosts for applications which do not support pools or for ease of use. Using this feature requires logging into the DataFort CLI and changing the default settings of the DataFort appliance.

Enabling Global Default Pool

To override the application pools which are auto-detected by the DataFort appliance, set the default pool override to true:

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

```
system property set dfc.override_with_default_pool true
```

Note: To return to normal pool mode log in to the DataFort CLI and run the command `system property set dfc.override_with_default_pool false.`

Creating the Global Default Pool

To create a pool and assign it as the default pool:

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

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

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

Assigning Key to Global Default Pool

To assign the encryption key from an existing default pool to a new default pool (optional):

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

```
pool key set [-n, --nokey] [-k, --pk-id ] [-e, --exportable] [--
days] [--rw-days ] <new global default pool label>
```

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

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 ] [-e, --exportable] [-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

Tape settings section of the determine whether ACL learning and Compression are on or off by default. If you enable tape compression on a host, DataFort may compress data sent to tape, depending on the host settings to the tape drive.

- If the host sets the drive to compress, DataFort will compress data.
- If the host disables compression on a tape drive, DataFort will not compress data.

Some tape systems automatically compress all data written to tape. Since encrypted data is not compressible, DataFort offers its own compression option. If compression is on, DataFort compresses the data.

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 will be allowed to access storage.

Compression

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

Compressed data will take up less tape space and be 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.

Continue to use the compression functions of your backup software and tape library. Both DataFort and application or tape library compression must be set ON if compression is desired.

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, access the SAN Storage Settings page by choosing **Storage > SAN Settings**. SAN Storage Settings include:

- Virtualization Settings
- Setting Single or Multi ID Mode

Virtualization Settings

Virtualization can be turned on or off for any DataFort port using the SAN Storage Settings page of the WebUI. 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 will function.

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 will operate in Single ID mode, while a DataFort HBA with virtualization ON will operate in Multi ID mode. The suggested settings for different environments are:

Tape configurations

It is recommended that virtualization be ON for the Host HBA, and OFF 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 OFF, the DataFort HBA will log in to a switch in fabric mode.

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

Keeping virtualization ON for the Host HBA allows features such as Port Mapping to be used to create Cryptainers (see Options When Creating a Cryptainer).

Disk configurations

It is recommended that virtualization be ON for both the Host HBA and Storage HBA of a DataFort in most disk configurations. Having virtualization on allows the full range of DataFort features to function.

When virtualization is ON, DataFort will log 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 ON can Port Mapping be used to create Cryptainers (see Options When Creating a Cryptainer).

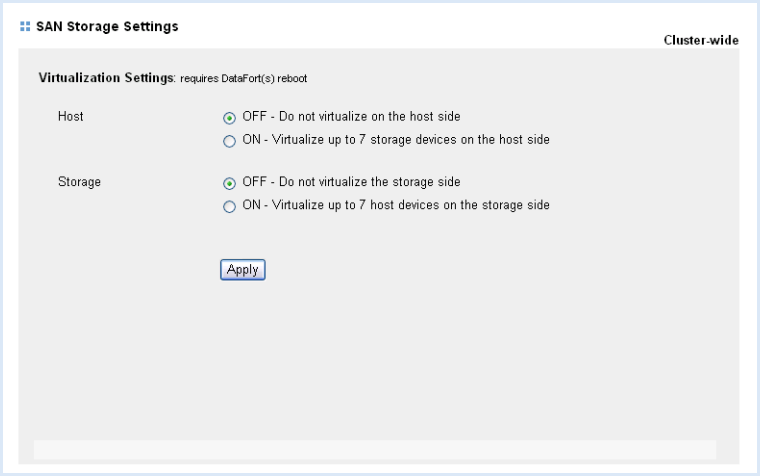
Note: It may be necessary to turn virtualization OFF on both HBAs if connecting to a switch that does not support loop logins, or in a situation where a specific hardware configuration problem needs to be addressed.

Setting Single or Multi ID Mode

Each port on the DataFort appliance can be configured independently to function in either Single ID or 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. To set the virtualization mode, access the **Storage > SAN Settings** page. Keep in mind the following:

- Any paths set through DataFort virtual ports before changing the virtualization mode will become inaccessible.
- After changing virtualization settings DataFort will prompt for a reboot.
- When in Single ID mode, some unsupported settings in the WebUI will be greyed out.

1. From the DataFort WebUI, access the **Storage > SAN Settings** page.
2. Select the ON or OFF radio button for each HBA to set Multi ID or Single ID mode.



3. Click Apply.

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 that no more than one instance of a particular Cryptainer can exist simultaneously (you cannot 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 will recover the Cryptainer information for you). Any DataFort using the configuration database that contains information about the original Cryptainer will work.

1. In the WebUI, right-click the device onto which you wish to restore the Cryptainer. Choose **Advanced > Restore Cryptainer.**

   The Restore Cryptainer page will appear. It displays information about the device you have selected, and a list of Cryptainer Keys that can be assigned to the Cryptainer when it is restored.
2. Select the correct key (using the Cryptainer ID information you have for the original Cryptainer).
3. Select the correct mapping method for this device, and click Restore.

10 Key Administration

This chapter describes administrative functions that involve key management or key creation after initial DataFort setup.

A specified Key Administrator or a Full Administrator can perform the following functions:

- Managing Trustees
- Managing DataFort Defense Responses
- Managing Recovery Officers and Recovery Cards

Any administrator can reset smart cards:

- Smart Card Reset

Managing Trustees

A trustee is a remote DataFort with which a trust relationship has been formed, allowing exportable 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	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	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	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:

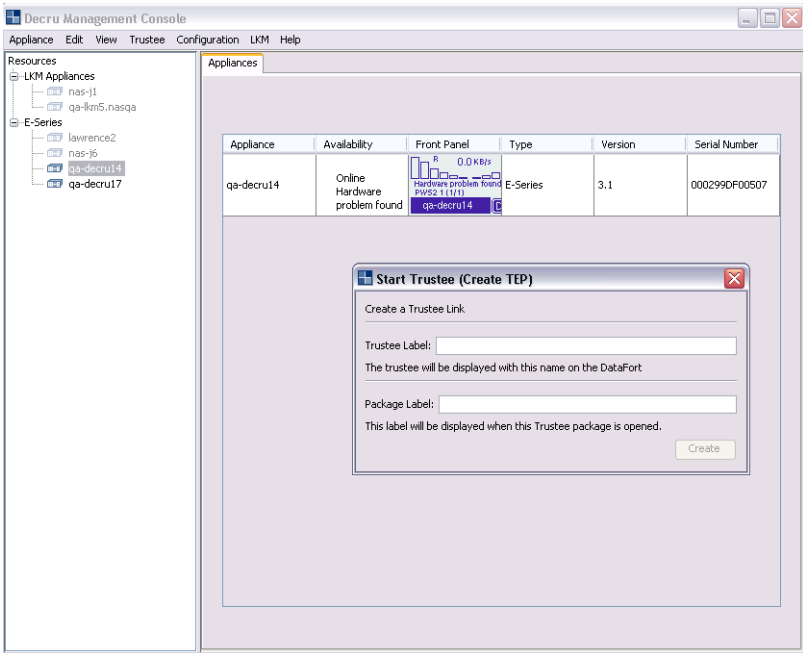
- A Key or Full Administrator (with permissions to create trustees) at each site.
- The quorum of Recovery Officers and their Recovery Cards at each site/for each appliance. If the Security Setup requires 2 out of 5 cards, for example, two people will have to be present to insert their cards and enter 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.

Create the Trustee Link

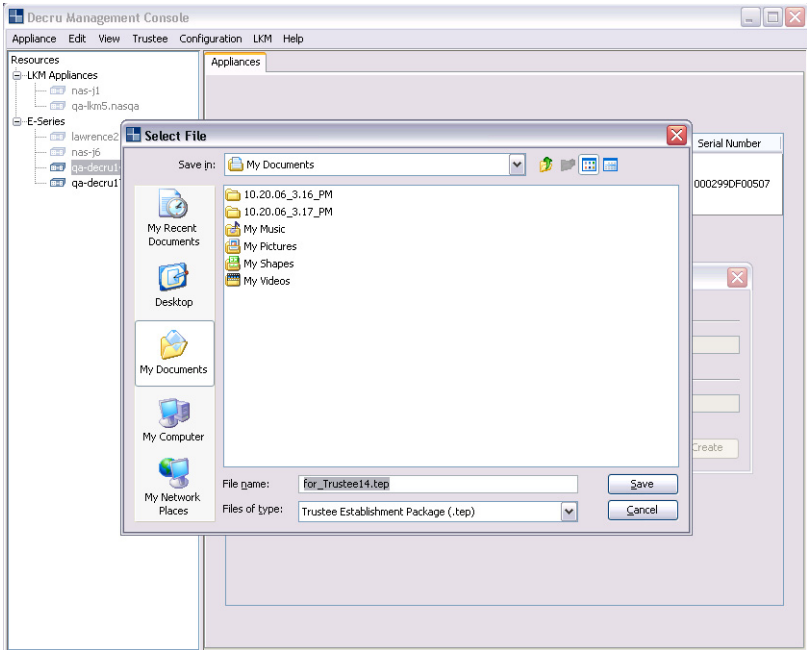
Trustee management requires the use of the Decru Management Console (DMC). See Decru Management Console Functions on page 186 for information about this interface.

1. Choose **Start > Programs > Decru > Decru Management Console**.
2. From the Resources pane, select the first DataFort that will become a trustee.

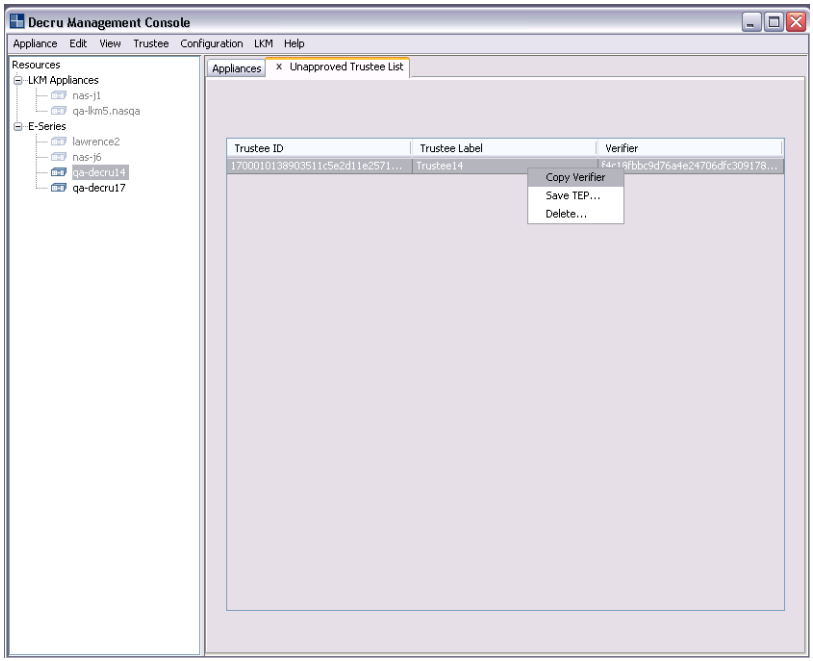
3. From the Trustee menu, select Start Trustee Creation.



4. In the Start Trustee (Create TEP) window, enter the Trustee Label (usually the name of the other appliance) and the Package Label (the identifier for this file), and click Create.



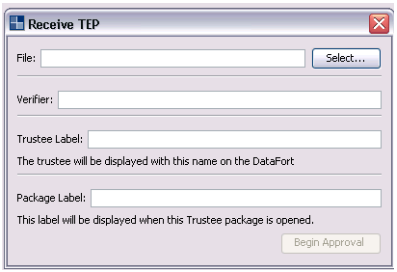
5. In the Select File window, keep the default name and choose a directory in which to save the TEP file.
6. From the Trustee menu, select Unapproved Trustee list.
7. Right-click the newly-created trustee and select Copy Verifier.



8. Paste the verifier into a text file.
9. Communicate the file and the verifier to the administrator of the other appliance, if there is a different administrator.

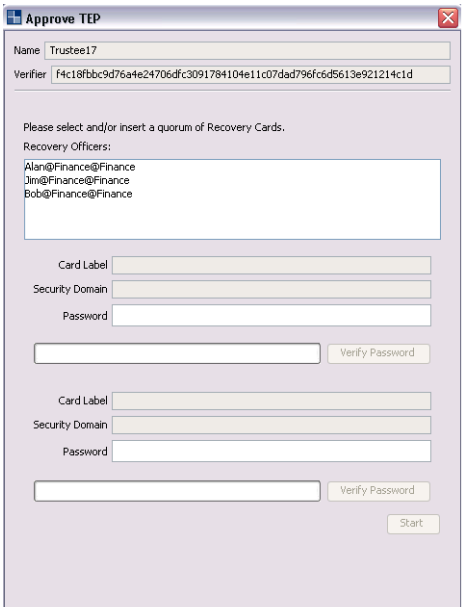
   The verifier must be communicated in a secure manner – Decru recommends communicating the information by phone or direct contact rather than email. This is the only form of authentication for key sharing and is considered sensitive material.

   The other administrator will need to browse to the TEP and use the verifier when they complete trustee setup.
10. From the Decru Management Console, in the Resource pane, select the other appliance.
11. From the Trustee menu, select Receive TEP.



12. Browse to the TEP file saved in step 5 and copy the verifier from step 8 into the provided field.
13. Enter the Trustee Label (usually the name of the other appliance) and the Package Label (the same one entered in step 4) and click Begin Approval.

    The approve TEP panel appears.

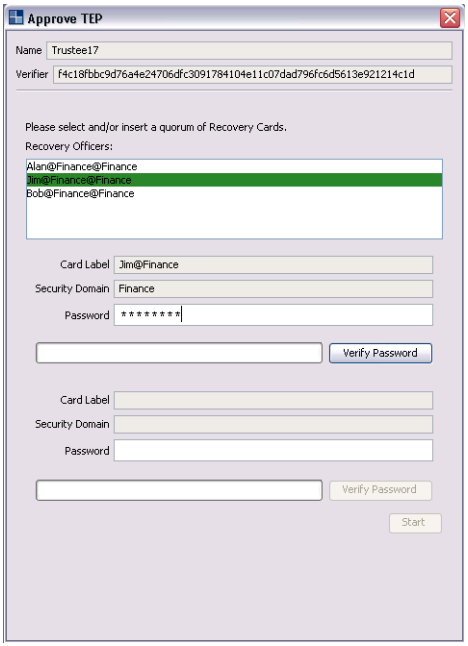


The next step requires that the smart cards be presented to DMC. The number of cards required is established by the recovery schema set for each appliance at the time it was initialized.

Note: Multiple readers will allow you to move through this process quickly since you can insert multiple cards at once. Otherwise, insert one card at a time into the single reader.

14. Insert a card and enter the password information. Then insert the next card in insert password information for that card. If multiple readers are in use, enter password information for the inserted cards.

    Note: Use the Verify password button to check that a password is correct before starting the procedure.



15. Click Start.

    Wait for the progress bar to appear. Approval is being obtained from the card. Do not remove it from the reader.

16. If using a single card reader, when prompted insert the other card and click Start.

    Wait for the progress bar to appear.

17. In the Select File box, keep the default file name and choose a directory in which to save the TAP file.
18. From the Trustee menu, select Unapproved Trustee list.
19. Right-click the newly-created trustee and select Copy Verifier.
20. Paste the verifier into a text file.
21. Communicate the file and the verifier to the administrator of the other appliance, if there is a different administrator.
22. Select the first DataFort again.
23. From the Trustee menu, select Receive TAP.
24. In the Receive TAP window, for the File field, select the TAP file saved in step 17. For the Verifier field, paste the verifier ID copied in step 20.
25. In the Approve TAP window, insert or select Recovery Cards and enter the passwords.

26. Click Start.

    When finished, a Trustee created message will appear.

27. From the Trustee menu, select Trustee List to see the created trustee link.

Importing and Exporting Keys

Once a trustee relationship is established it is possible to freely transfer keys between the two clusters using the import and export key options of the WebUI.

Exporting a Key

1. At the exporting DataFort, right click on the LUN, tape or pool which will have its key exported. For a LUN select Export key. For a tape device select **Keys > Export.** For a pool select **Manage keys > Export**. This will open a screen showing the available trustee relationships.
2. Select the trustee that the key will be transferred to and select Export.
3. There will be a prompt to download a .kdf file.
4. 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, right-click any storage device or pool and select Import. For a LUN select Import key. For a tape device select **Keys > Import.** For a pool select **Manage keys > Import**.
2. A prompt for the .kdf file location will appear. Once this file is uploaded the key will be known to the cluster.

Managing DataFort Defense Responses

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

Defense Triggers and Responses

A defense response can be triggered by the following:

Chassis Intrusion	If DataFort is opened, this causes an automatic defense response. If chassis intrusion has been detected, there should be physical evidence (such as scratches, a broken lock or a stolen chassis key).
Loss of Power	If DataFort is left without power for a long time (more than 3 weeks) a defense response can be triggered. The DataFort battery powers the intrusion-detection circuit even when DataFort is switched off. When this battery becomes low (because DataFort has been powered off for an extended period), it becomes possible for an intrusion to occur without DataFort detection or notification. For this reason, a low battery triggers an intrusion alert.
CryptoShred Button	If DataFort 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 unusable for cryptographic operations. It will still be possible to access management interfaces and view logs, but encrypted data will be inaccessible. To resume normal operation and data access you can perform an administrative reset (see Clearing a Defense Alert on page 137).
- 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:** CHOOSE THE LOWEST LEVEL IF UNCERTAIN. THE DEFENSE LEVEL CAN BE INCREASED IN STRENGTH LATER IF IT SEEMS ADVISABLE, BUT NOT DECREASED.

DataFort Defense Setting

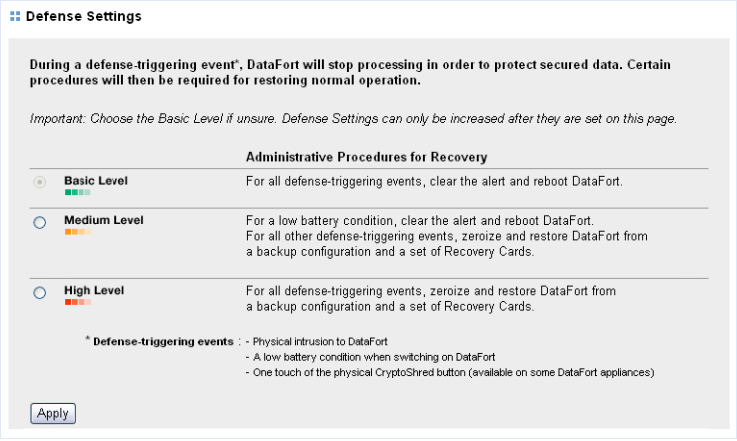
Defense levels are summarized in Table 13. If in doubt, choose the Basic level.

TABLE 13: 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.	Encryption and decryption disabled.	After administrator determines the cause of the intrusion and resets DataFort.
		CryptoShred button pressed.		
		Battery too low when system is powered on.		
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.	Encryption and decryption disabled and encryption keys cleared.	After DataFort zeroization and restoration using Setup Wizard and Recovery Cards.
		CryptoShred button pressed.		
		Battery too low when system is powered on.		

CHANGING THE DEFENSE SETTING

1. Log into the WebUI as a Full Administrator and choose **System Config > Security > Defense Settings**.
2. Select the level of desired defense 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 DataFort to resume encryption and decryption operations. For a DataFort with a Basic level defense setting, alerts will appear in the following places:

- On the front panel LCD
- On every page of the WebUI
- 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 DataFort from the CLI or WebUI.

If keys were cleared under a Medium or High level defense setting, a simple reset is not possible. DataFort must be zeroized and recovered before normal operation can resume.

Resetting a Defense Alert via WebUI

1. Click the Reset link from the Home page, or from the bottom of any page.
2. Click OK to dismiss the message alerting you about the reset.

   The DataFort will reboot, clearing the alert.
3. Close the connection to the DataFort.

Resetting a Defense Alert via CLI

The CLI displays an alert after login.

1. Execute the `system tamper reset` command.

   You will be instructed to reboot the DataFort to clear the alert.
2. Execute the `system reboot` command.
3. Close the connection to the DataFort.

CryptoShred Button States

Some DataFort appliances come equipped with a CryptoShred button, which allows the DataFort 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 will operate normally. If the button is pressed once, the DataFort defense response will be 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 will remain 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 will remain encrypted and secure in storage, and cannot be decrypted unless the DataFort 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.

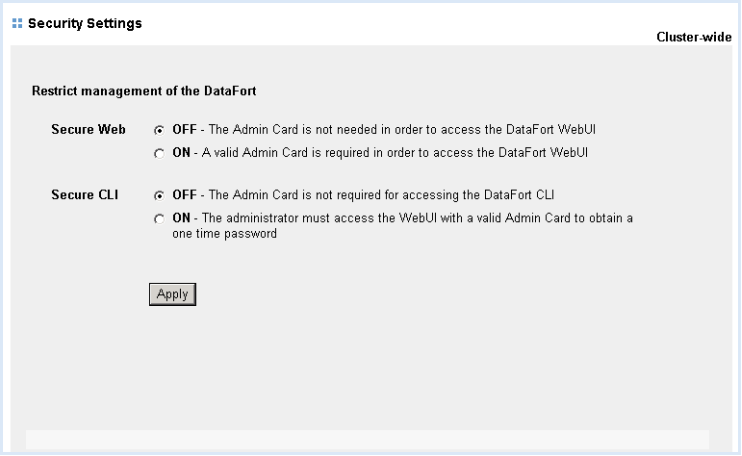
   Restore Operation if System Card was Destroyed: To return DataFort to normal operations, DataFort will have to be zeroized and reconfigured with the wizard and Recovery Officers. See Zeroizing the Decru DataFort on page 158. A new System Card will have to be initialized. DataFort can be restored to the last configuration that was downloaded or backed up.

Configuring Management Security Settings

DataFort offers configurable levels of security for DataFort management interfaces.

Secure Web	When on, a valid Admin Card is required to access the DataFort WebUI. To allow access to the WebUI without an Admin Card, turn this setting off.
Secure CLI	When on, the administrator must log in to DataFort with an Admin Card in order to obtain a secure password that will allow access to the CLI for DataFort management. By default this option is off, and an administrator can log in to the CLI using only a valid name and password.

1. Choose **System Config > Security > Settings** from the WebUI to set the security policy according to the needs of the network.
2. Leave defaults in place, or select the radio button beside the desired setting and click Apply to save the changes.



Managing Recovery Officers and Recovery Cards

Recovery Cards are not used in daily operation of the DataFort, 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 quorum. This will eliminate 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 instructions see:

- Replacing a Recovery Card
- Smart Card Reset

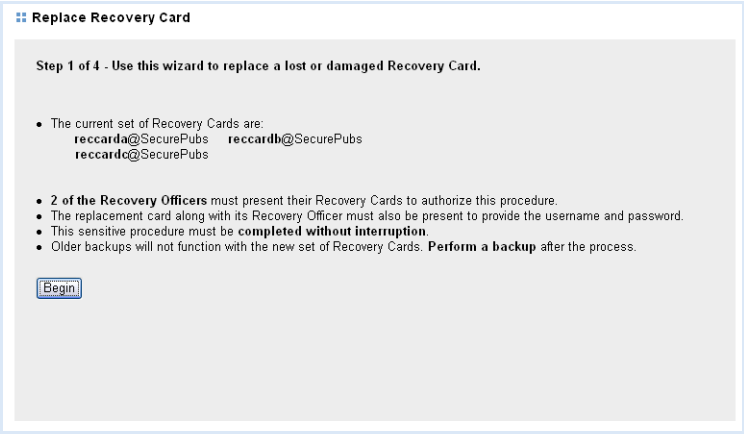
Replacing a Recovery Card

Note: Card replacement procedures are sensitive, and should not be interrupted by any other configuration or activity.

Card replacement procedures require:

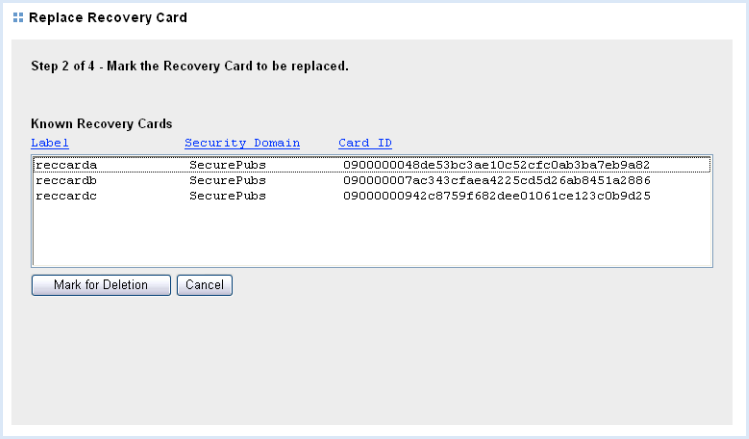
- A replacement card
- The required quorum of Recovery Officers and their Recovery Cards. If the quorum requires 2 out of 5 cards, for example, two people will have to be present to insert their cards and enter the label name and password for the card, in order to create a new Recovery Card.

1. Log in to the WebUI and choose **System Config > Recovery > Replace Recovery Card**.



The current set of cards is displayed.

2. Click Begin.



3. In the Known Recovery Cards window select the card that will be replaced and click Mark for Deletion.
4. Insert the card that will replace the deleted card into the Management Station smart card reader.
5. Click Introduce.

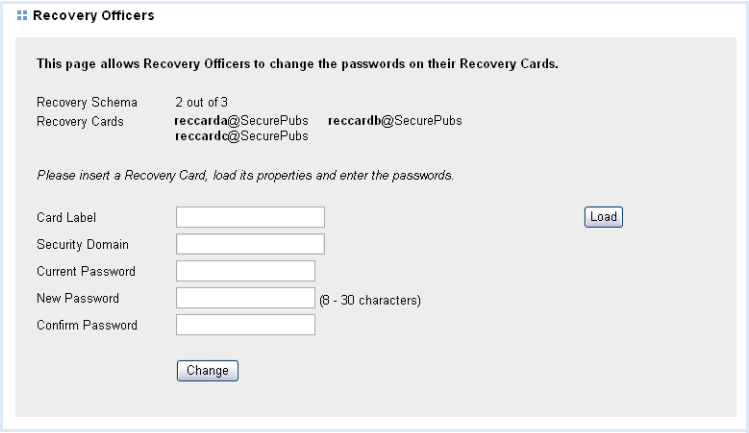
   The wizard will indicate how many cards are required to authenticate the replacement.
6. Insert a Recovery Card from the original set which included the card that is now being replaced and click Begin.

   The system will prompt for the old Recovery Cards. Recovery Officers should insert their cards as prompted, and enter the label and password information for each card. A quorum of Recovery Officers must present cards. Each card owner must supply the password for his or her card.
7. When prompted, insert the remaining cards from the set one by one, clicking OK when prompted.
8. Enter the password for each card and click Log In.
9. Repeat for as many cards as are needed.
10. When prompted that the replacement card is authorized, insert it into the reader and click OK.
11. Enter the label and password information for the card and click Log In.
    - If an uninitialized card is being used as a replacement, enter a card label and password, then click Log In.
    - If an initialized card is being used as a replacement card, existing values will appear. You cannot change the Security Domain of an initialized card. Enter the password information for the existing card, then click Log In.
12. Complete a configuration database backup.

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. Log into the WebUI and choose **System Config > System Users > Recovery Officers**.



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. Click Load.
4. Enter the existing password.
5. Enter the new password.
6. Click Change.

Smart Card Reset

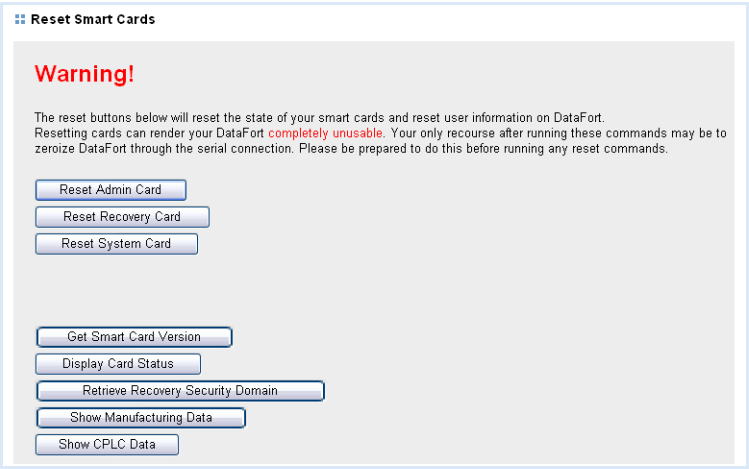
It is possible to completely reset a smart card using a special DataFort Reset Smart Cards page. This page also allows the administrator to check smart card versions and status.

> **WARNING:** THIS PROCESS WILL INVALIDATE THE CARD'S OLD SETTINGS, AND RESET IT FOR USE WITH A NEW INSTALLATION.

1. Enter the following path into the browser window:

   https://<nameofDataFort>/resetcards.htm

   The Reset Smart Card page will appear.



2. To check the status of a smart card, insert it into the smart card reader and click any of the buttons at the bottom of the page.
3. To reset a smart card, insert it into the smart card reader, and click the appropriate Reset button.

   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 will not be 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.
4. After clicking the Reset button, confirm the transaction.

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 WebUI. 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 Software
- Downloading 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 WebUI to configure backups to an LKM appliance. Refer to the *LKM Appliance Administration Guide* for instructions.

Saving Configurations to Lifetime Key Management Software

The LKM software will manage keys for an entire cluster, offering a centralized approach to 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 LKM documentation for more information.

In order to configure DataFort to back up the configuration database to LKM automatically, provide DataFort with the IP address of the server on which LKM software is running. As soon as DataFort has the IP address of a working LKM server, configuration changes will be backed up automatically every hour. The configuration can also be backed up to LKM manually.

> **Note:** All LKM settings are propagated across cluster members, therefore it is sufficient to enter LKM settings once for each cluster.

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 your 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.
- This backup must be stored per organizational retention guidelines.
- Old copies must be considered sensitive and must be shredded per 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.

Configuring Backups to LKM Software

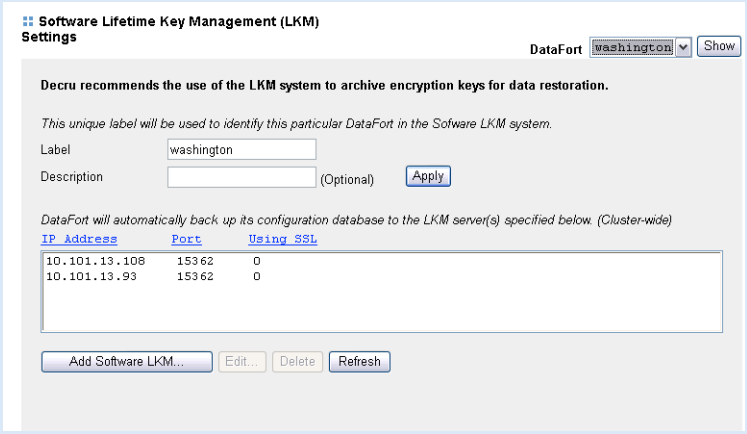
Use this procedure to set up regular automatic backups to LKM software.

> **Note:** These instructions only apply to LKM software. For LKM appliance operation, refer to the *LKM Appliance Administration Guide*.

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.

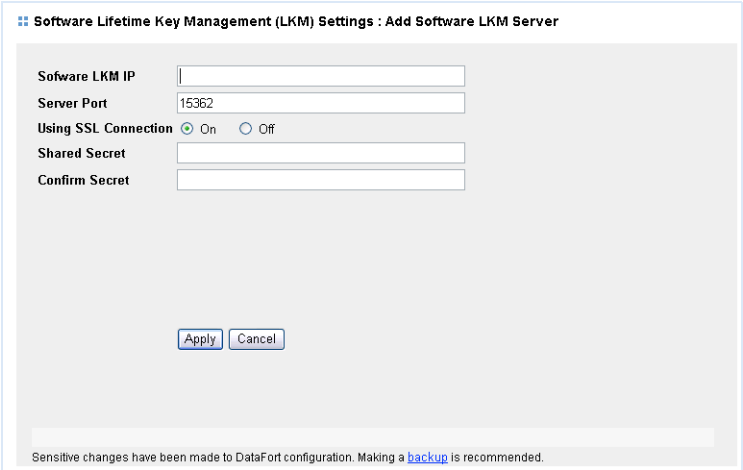
> **Note:** The following steps can be repeated four times to support a maximum of four LKM servers

1. Log in to the WebUI, and choose **System Config > Recovery > LKM Settings**.
2. Enter a label and description that will identify this DataFort in the LKM interface.



3. Click Add.

   Note: This can only be used to add LKM software, not an LKM appliance. Refer to the *LKM Appliance Administration Guide* for instructions on linking appliances.



4. Enter the IP address of the LKM software server.
5. Leave the Server Port at its default setting. If the default port is not available on the LKM server, see the LKM documentation for instructions for changing the setting.

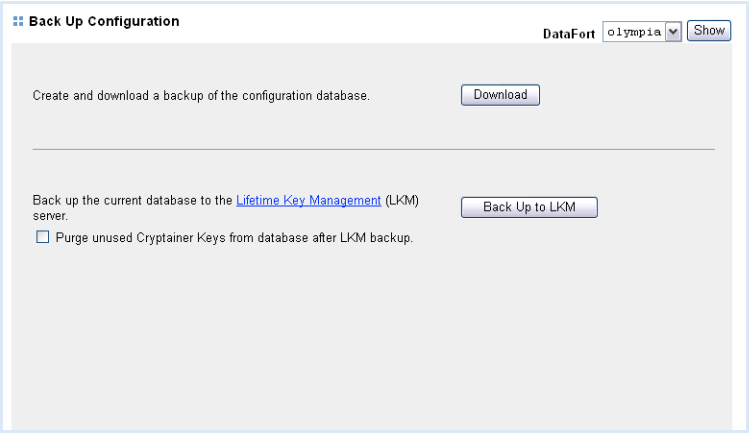
   To configure DataFort to communicate with the LKM server across a secure SSL connection, leave Using SSL Connection enabled.

6. Enter and confirm a shared secret for SSL. The shared secret can be any string of up to 32 characters, including spaces.
7. As soon as possible, plan to enable SSL and enter the same shared secret into the LKM software UI. Until this is done, secure (SSL) backups to the LKM software server will not proceed.
8. Click Apply.

Backing Up the Configuration to LKM Software

Use this procedure when you want to perform a manual backup to the LKM server. When backing up to LKM manually, you have the option to purge keys. See Saving Configurations to Lifetime Key Management Software for details.

1. Choose **System Config > Recovery > Backup**.



2. Choose whether or not to purge unused keys after backup to LKM.

   Keys for deleted or re-keyed data can be removed from the configuration database after a copy of the database has been backed up to an LKM server. Removing keys can help control the size of the DataFort configuration database. Since LKM is designed to retain all keys, it is not necessary to keep them in the DataFort configuration database as well.

3. Click Back Up to LKM.

   The configuration will be sent to the LKM server, connecting to the ports configured on the LKM Settings page, and using SSL if that option was selected.

Key Purging

Keys are automatically backed up to LKM when LKM is in use. When backing up to LKM manually, you have the option to purge keys by checking the Purge unused Cryptainer keys... box on the Back Up Configuration page of the WebUI. 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 will return a table of entries and a percent full number. Should the database be more than 75% full, consider purging keys. The **`keyman purgekeys`** command allows you to specify which keys are purged at backup. Using the **`keyman purgekeys start -a`** command allows you to define the age of the keys to be purged in days.

The tape settings policy in use will effect the frequency with which keys may need to be purged. Table 14 on page 148 outlines the relationship between tape settings and key generation. See Managing Tape Settings on page 120 for information about tape settings.

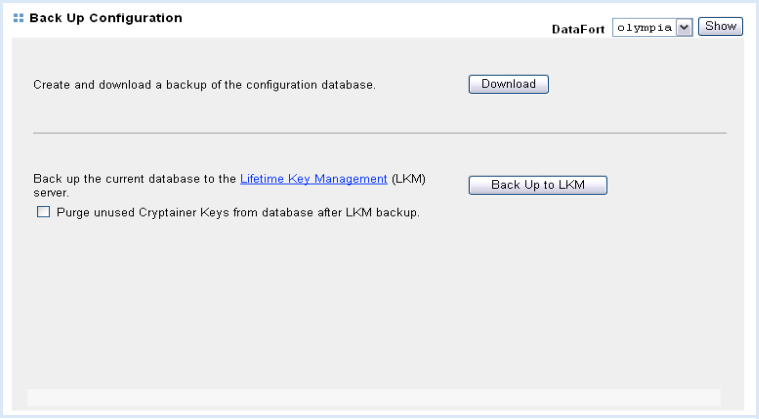
TABLE 14: TAPE POLICY AND KEY PURGING

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.
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.

Downloading 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 the WebUI and choose **System Config > Recovery > Backup**.



2. Click Download.
3. Determine a secure remote location for the backup copy of the configuration database.
4. Save the backup.
5. Accept or modify the recommended filename.

12 Physical Security Administration

This chapter describes key management functions after initial DataFort setup. A specified Security Administrator or a Full Administrator can perform the following functions:

- Setting Date and Time
- Configuring and Viewing Logs
- Zeroizing the Decru DataFort

Setting Date and Time

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

1. From the WebUI, choose **System Config > General > Date/Time**.
   - To change the current settings, click Adjust and enter the new information.
   - To use a time server, if these settings were not entered during setup, enter the requested information.
2. Click Apply Settings.

Configuring and Viewing Logs

DataFort logs events in these categories:

- Security
- Operations
- Performance

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

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

Note: It is recommended that logs be stored in more than one location. See Recommended Configuration on page 153 for an example of a secure logging configuration.

For more about logging, see Logging Functions on page 246.

DataFort Log Storage Guidelines

Keep in mind the following when configuring DataFort logging:

- Decru recommends that you redirect all logs to a remote syslog server, and that you turn the Decru Signed Syslog feature on for remote logs. Remote log storage is supported for a system running a standard syslogd configured to accept log data from the DataFort.
- 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 DataFort, while the remote syslog is not encrypted and is not secure.
- The DataFort 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 will remain on the syslog host subject to its log rotation and storage policies.

Decru Signed Syslogd (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 syslogd.

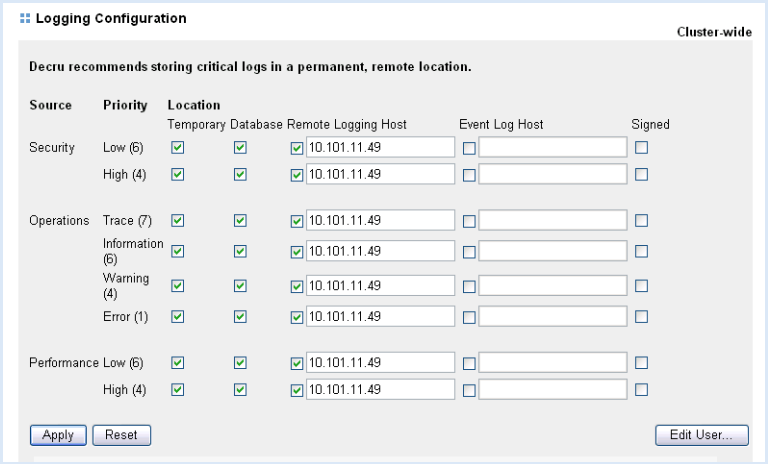
When Decru Signed Syslogd (DSS) is turned on, DataFort adds metadata and a signature to each log message sent to a remote syslog server. The metadata and the signature can be used to:

- 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 syslogd the source and timestamp are generated by the remote daemon and therefore cannot be trusted.

CONFIGURING LOG STORAGE

1. To configure the storage location for log information, choose **System Config > General > Configure Log**.



2. The default settings are in effect until they are changed. If you want log information to be stored remotely, indicate the storage location according to the instructions below.
3. Select the desired settings and then click Apply. Clicking Reset restores the default settings.

Setting and Enabling a Remote Storage Address

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

   Clicking Reset restores the default settings.

Recommended Configuration

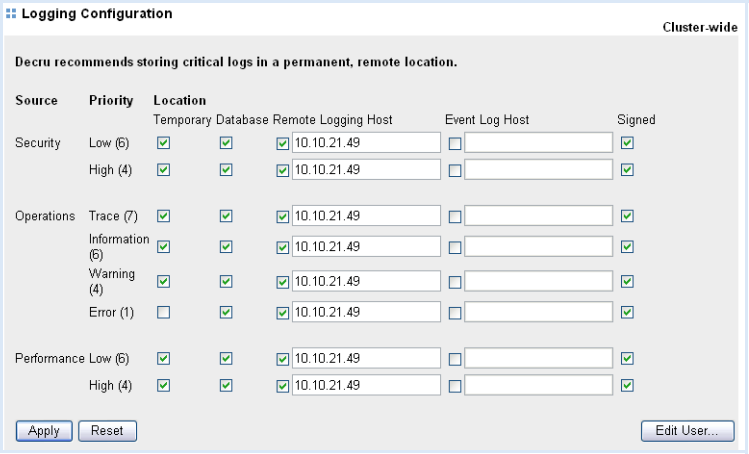
A recommended logging configuration will set DataFort to send secure DSS logs to multiple locations. For high security installations, configure DataFort logging as follows:

- 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.

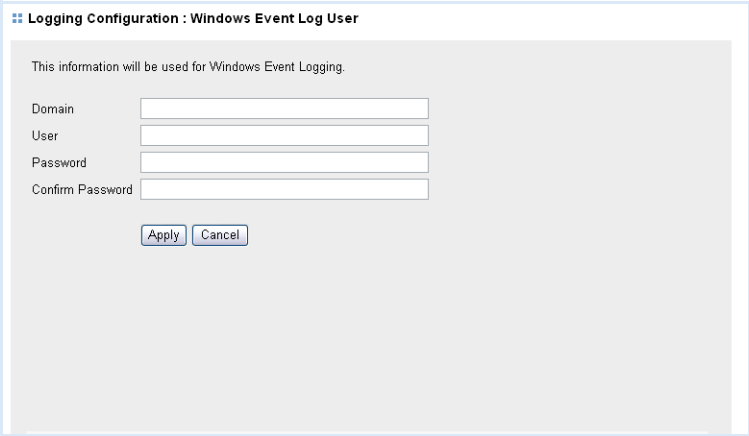
Windows Event Logging

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

1. From the DataFort WebUI, choose **System Config > General > Configure Log**.



2. Set up the Event User by clicking Edit User.



3. Enter information about the user who will log into the Windows host to generate the events including the domain to which that user belongs, and the name and password of the user. This user must have permission to log events to that host.
4. Click Apply.
5. Choose **System Config > General > Configure Log.**

6. In the Event Log Host column, check each box that should be logged to the Windows host and enter the IP address of the Windows host in these boxes.

   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.

7. Click Apply.

   Once configured, events from the DataFort source can be viewed on the host at **Computer Management > Event Viewer > Application**.

Setting Up Syslog

1. On a system running a syslog daemon configured to accept syslog messages from remote hosts (specifically DataFort), create an empty file to store the system log. You can use any name, but in this example it is DataFort1.

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

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

   ```
   local0.* /var/log/DataFort1
   ```

   # local0 is for Security messages

   ```
   local1.* /var/log/DataFort1
   ```

   # local1 is for Operations messages

   ```
   local2.* /var/log/DataFort1
   ```

   # local2 is for Performance messages

3. Signal syslogd to start receiving messages from DataFort.

Syslogd Mapping

Table 15 shows the Descriptive Name, System Property Name, Syslog Facility and Level mapping for DataFort 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.

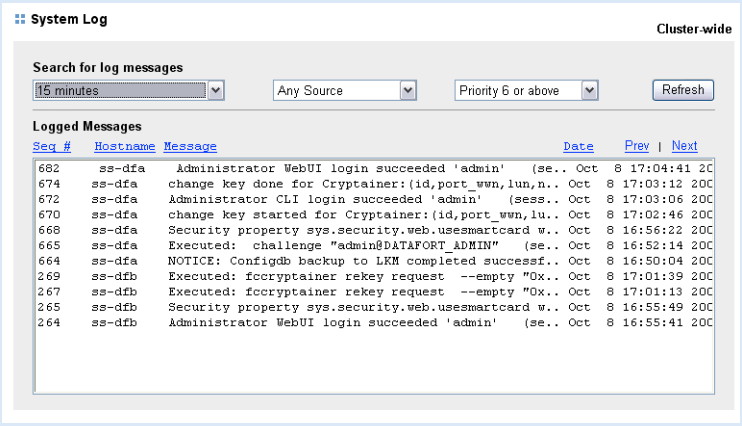
TABLE 16: TEMPORARY LOG MAPPING

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

VIEWING THE LOG

DataFort log information can be viewed from the WebUI. Select a view that includes all log information, or one that filters the logs according to date, type of event or priority.

1. Choose **System Info > Log**.



View all recent log events, or a filtered selection. Sort and scroll items in the Message window.

- To filter the view by time, select a display period from the drop-down menu at the left. You may display events from the last minute, 5 minutes, 15 minutes, 1 hour, 1 day, 1 week or Any Time Frame.
- To select a single type of event to view, select Security, Operations, Performance from the Source drop-down menu.
- To select only events of certain priorities, select the priority level from the Priority Limit menu on the right.
- Double-click an entry to view details.
- 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 DataFort and the remote server.
- syslogd died on the remote server.

If logs appear to be missing, compare the logs saved to separate remote locations (logs can be sent to up to four locations, as indicated in Recommended Configuration on page 153) to verify breaks in the log are replicated. Remote logs can also be compared to the internal DataFort 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 204.

Zeroizing the Decru DataFort

Zeroizing DataFort 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:

- Zeroization Using the DataFort WebUI
- Zeroization Using the CLI
- Zeroization 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.

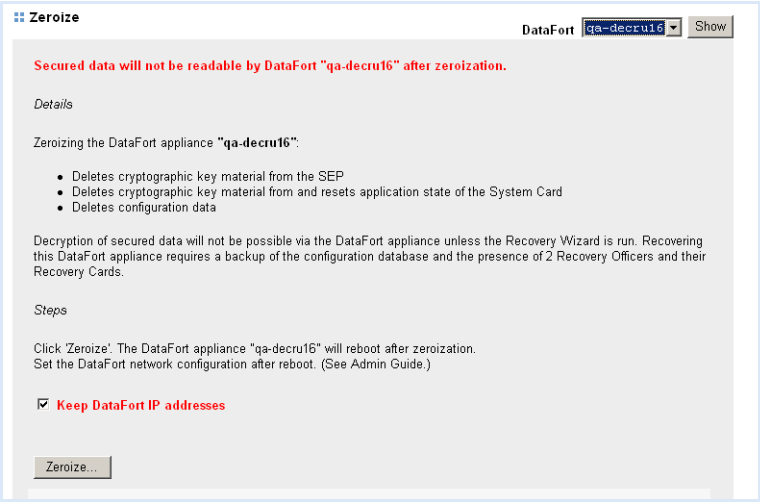
WARNING: BEFORE ZEROIZING DATAFORT, BACK UP THE CONFIGURATION DATABASE TO ENABLE DATA RECOVERY OPERATIONS.

Zeroization Using the DataFort WebUI

It may be necessary to back up the configuration database before zeroization is permitted. From the WebUI, choose **System Config > Recovery > Backup** and click the Download button.

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

1. Be sure the System Card is inserted in the DataFort appliance.
2. From the DataFort WebUI, choose **System Config > Security > Zeroize**.
3. If it is desirable to preserve the IP address assigned to DataFort, leave the Keep DataFort IP addresses box checked.



4. Click Zeroize.
5. Type the provided code into the popup box to verify that you want to zeroize this DataFort.

   After providing the code in the popup box, you will are automatically logged out of the WebUI and redirected to the login screen.

   DataFort will reboot.
6. If IP settings were not preserved by checking the Keep DataFort IP addresses box, assign the DataFort IP settings as described in Assigning the DataFort IP Address on page 48.
7. Complete the configuration by running the Setup Wizard.

Zeroization Using the CLI

In some situations it may be necessary to use the CLI to zeroize the DataFort. Note that if Secure CLI is enabled, a valid Admin Card will still be required to access the CLI in order to zeroize the DataFort. (Never reset all Admin Cards before zeroization unless Secure CLI is off.)

Note: It is not possible to zeroize from the CLI if a backup is necessary. It may be necessary to execute the `db export` command from the CLI before zeroization is allowed.

1. Be sure the System Card is inserted in the DataFort appliance.
2. Log in to the DataFort 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. You will be prompted 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 DataFort reboots.
6. If they were not preserved, reassign the DataFort IP settings as described in Assigning the DataFort IP Address on page 48.
7. Complete the configuration by running the Setup Wizard.

Zeroization Using the Serial Console

If it is not possible to complete the Setup Wizard for some reason, you can reset the DataFort using the serial connection.

1. Be sure the System Card is inserted in the DataFort appliance.
2. Connect the DataFort serial console port (see Serial Console Port on page 46).
3. Log in to the serial console with a valid administrator username and password.
4. To zeroize DataFort, enter option `z`.
5. Enter a confirmation code when prompted.

   The DataFort will reboot.
6. Assign the DataFort IP settings. See Assigning the DataFort IP Address on page 48.
7. After the DataFort 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 a DataFort are lost, it is not possible to log in to its WebUI or CLI. However it is still possible to connect to the DataFort serial console using a valid Recovery Card from the set used when that DataFort was initialized. This allows the appliance to be zeroized and reset.

1. Connect a Management Station or other PC to the DataFort serial console port (see Serial Console Port on page 46).
2. Connect a smart card reader to the PC connected to the serial port.
3. Insert one of the Recovery Cards for the DataFort appliance into the smart card reader.

4. Enter the following path into a browser window:

   https://<nameofDataFort>/resetcards.htm

   The Reset Smart Card page will appear.
5. Click Retrieve Recovery Security Domain.
6. Make a note of the Recovery Card label (e.g. RecoveryCard1).
7. Remove the Recovery Card from the card reader.
8. Remove the System Card from the DataFort front panel slot.
9. Insert the Recovery Card into the DataFort front panel slot.
10. On the PC, launch a terminal client to connect to the DataFort appliance.
11. At the login prompt, enter the Recovery Card label as the username and enter the Recovery Card password.

    If authentication succeeds, the console menu will be displayed.
12. Enter option **z** to zeroize the DataFort appliance.

    Once zeroized, initialize the DataFort appliance using the Decru DataFort Wizard. See Initializing a Standalone DataFort or DataFort Cluster on page 53. If a current backup of the DataFort configuration database is available, the configuration can be restored using the Recover from Database function of the wizard.

13 Cluster Administration

A cluster is created using the Setup Wizard. See Chapter 5 for instructions on completing the wizard. Note that 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 WebUI
- 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 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.

Use the Manage Cluster page of the WebUI to add, edit or delete cluster members. See Cluster-Wide Management via WebUI, Adding and Removing Cluster Members and Changing Network Properties of a Cluster Member for details.

Note: See Cluster Management on page 202 for information on using the CLI to manage clusters, including the ability to disable cluster members if necessary.

Maintaining the Cluster Quorum

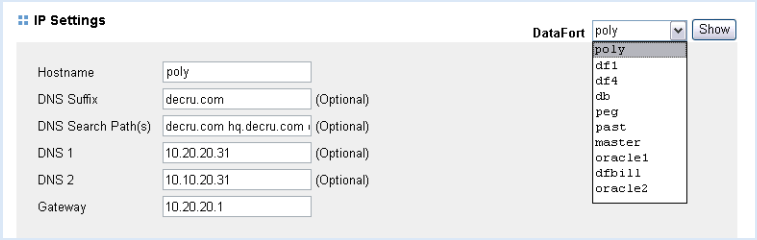
If one DataFort in the cluster goes offline, the remaining appliances will automatically take over operations. All cluster members keep the same configuration database. If strictly more than half of the cluster members are online, then the configuration database will remain writable.

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

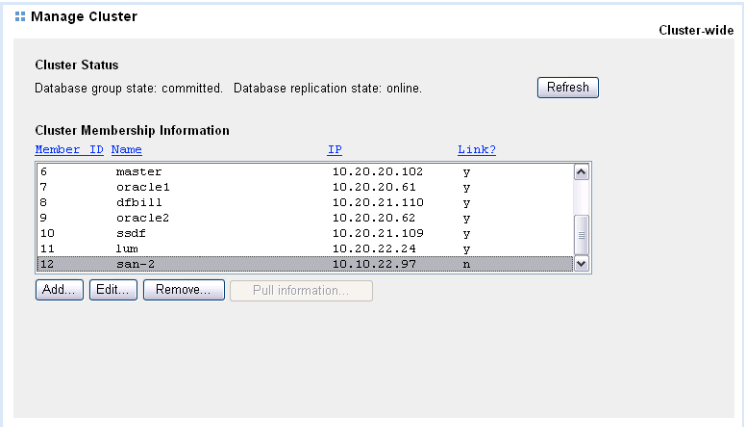
Cluster-Wide Management via WebUI

Most WebUI operations are cluster-wide and when completed on any member will apply to the entire cluster. The text **Cluster-wide** appears in the upper right corner of relevant WebUI pages to indicate this. Other settings are specific to individual DataFort appliances, but can still be set from any member of the cluster by using the onscreen pull-down menu to switch from one DataFort to the other.



Checking the Status of the Cluster

To check the status of a cluster, log in to the WebUI of a cluster member and click the Manage Cluster link. You can also view the Manage Cluster page of either cluster member by choosing **System Config > Cluster > Manage Cluster**.



Cluster status is defined by the Group State and Replication State of the configuration database shared by the cluster members. All cluster members will be listed in the Membership Information box.

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.	
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.	

RESOLVING A CLUSTER CONFLICT

A cluster that has not formed properly at the outset will remain 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 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 into the conflicted DataFort appliances and examining the configuration properties to determine which database is correct.
2. Log into the WebUI of the cluster member with the incorrect database. An alert will appear on the Home page near the Manage Cluster link.
3. Click the Manage Cluster link on the Home page or choose **System Config > Cluster > Manage Cluster**.
4. Highlight a DataFort with the correct database, and click Pull Information.
5. 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 will change 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 will change 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 202.

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 the Decru DataFort on page 158.
- 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 will continue to function as a standalone device.

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

1. Log into the WebUI of a DataFort in the cluster (not the one that will be removed).
2. Click the Manage Cluster link on the Home page or choose **System Config > Cluster > Manage Cluster**.
3. Select the cluster member to be removed in the Cluster Membership Information panel and click Remove.
4. Type YES to confirm the removal of the member, and click OK.

   Cluster status will be 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. Add the new DataFort using the Setup Wizard. DataFort replacement in a cluster requires:

- A new or zeroized DataFort.
- A DataFort remaining from the original cluster.

- The minimum set of Recovery Officers and Recovery Cards as determined by the recovery schema of the cluster.
- A valid cluster license from Decru for each DataFort that will be in the new cluster.

1. Power down the offline DataFort and remove it from the network, disconnecting the cables.
2. Log in to the WebUI of an online member of the cluster and click the Manage Cluster link on the Home page (or choose **System Config > Cluster > Manage Cluster**).
3. Select the offline DataFort in the Cluster Membership Information window and click Remove.
4. Log out of the WebUI of the online DataFort.
5. Replace the removed DataFort with the new, uninitialized DataFort.
6. Assign an IP address to that DataFort and connect it to the network.
7. Run the Setup Wizard for the new DataFort. Note the option to assign the WWNs previously used by the offline DataFort to the new DataFort using the Customize FC Site settings feature.

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 uninitialized or zeroized (see Zeroizing the Decru DataFort on page 158).

- 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 166. 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, 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.
- A valid cluster license from Decru for each DataFort unit.
- 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 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, using the saved configuration database from the old cluster. Add the second DataFort 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
- Changing the Hostname of a Clustered DataFort
- Changing the Hostname on an FC1020

Changing the IPsec Secret of a Cluster

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

Changing the IPSec Secret Using the WebUI

1. Log in to the WebUI of one DataFort appliance in the cluster.
2. Navigate to **System Config > Cluster > Manage Cluster** and click Add.

   The Set Up Cluster Step 1 of 3 screen appears.
3. Enter the new IPSec shared secret into both text fields and click Next.
4. Click OK at the warning to Continue.

   The Set Up Cluster Step 2 of 3 screen appears.
5. Without selecting anything, click Next.

   The Set Up Cluster Step 3 of 3 screen appears.
6. Click OK. The main Manage Cluster screen appears

   Note: Due to the temporary shared secret discrepancy, cluster status will be aborted/recover until the change to the cluster has been completed.
7. Repeat all steps on each cluster member.

   Once the process is complete and all cluster members are updated, cluster status automatically returns 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

The IP address of a DataFort can be changed while maintaining its membership in a cluster. Note that a configured DataFort cannot be moved from one cluster to another. To move an initialized DataFort to another cluster, it must be zeroized and added as described in Adding a Cluster Member on page 166.

1. Log in to the WebUI of the DataFort appliance which will have its address changed and choose **System Config > Network > IP Settings**.
2. Change the IP address and network mask to the new values. Click Apply.

The connection to the DataFort will be lost.

3. Log in to another member of the cluster and click the Manage Cluster link on the Home page or choose **System Config > Cluster > Manage Cluster**.
4. Select the entry for the changed DataFort in the cluster window and click Edit.
5. Enter the new IP information for the changed DataFort and click OK.
6. Check that the cluster status on the Home page indicates the cluster is committed/online.

Changing the Hostname of a Clustered DataFort

The hostname of a DataFort can be changed while maintaining its membership in a cluster. Note that a configured DataFort cannot be moved from one cluster to another. To move an initialized DataFort to another cluster, it must be zeroized and added as described in Adding a Cluster Member on page 166.

- Log in to the CLI of the DataFort appliance which will have its address changed. Execute the following commands:

```
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 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. Execute the following commands:

```
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 tasks that allow network properties to be set and DataFort upgrades to be executed.

A Full Administrator can complete the 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 162.

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

- Network Settings
- Upgrading DataFort
- Setting Security Certificates
- Managing Licenses

Only a Full Administrator can manage SNMP:

- SNMP Settings

Note: DataFort appliance Date and Time can only be set by a Full or Security Administrator. See Setting Date and Time on page 151.

Network Settings

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

1. To change IP settings for a standalone DataFort, choose **System Config > Network > IP Settings**.
2. Change the IP settings and click Apply

   Note: If you change the IP address, you will lose connection to the WebUI and will need to log back in to the new IP address.

UPGRADING DATAFORT

From time to time, Decru offers upgrades for DataFort. 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 accessing the **System Config > General > Upgrade** page of the WebUI and browsing to the Upgrade file from Decru. There is also an option to upgrade from the WebUI of a zeroized DataFort by using the link provided in the setup wizard.

> **Note:** While the DataFort 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 DataFort.

Some upgrades require that DataFort power to be cycled by the administrator. If it is required, recycle power on DataFort by clicking the Cycle Power button on the System Software Upgrade page of the WebUI. Note that the System Card must be inserted in the DataFort before power is cycled.

Setting Security Certificates

Internet Explorer will notify you any time a secure connection is made certified by an unrecognized authority. To eliminate this warning, and to protect against security attacks that could occur between DataFort and the Management Station, a locally signed certificate is generated during the Setup Wizard. After the certificate is set and installed, the security warning will not appear when logging in to the DataFort unless there has been a change made to the IP address or hostname of the DataFort, 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 177. Keep the following in mind:

- A certificate must be generated independently for each DataFort 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 the Decru DataFort on page 158 for more about zeroization.

Setting a Local Security Certificate

1. From the WebUI, choose **System Config > Security > DataFort Certificate**.

2. Click Use Self-Signed.

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

3. Enter the information for the locally signed certificate. This information will appear 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 262.

4. Click Sign and Set as Certificate.
5. To set the certificate, click OK.
6. Log out of the WebUI.
7. Open an HTTPS connection to the DataFort.

   The certificate warning appears.

8. Click View Certificate.

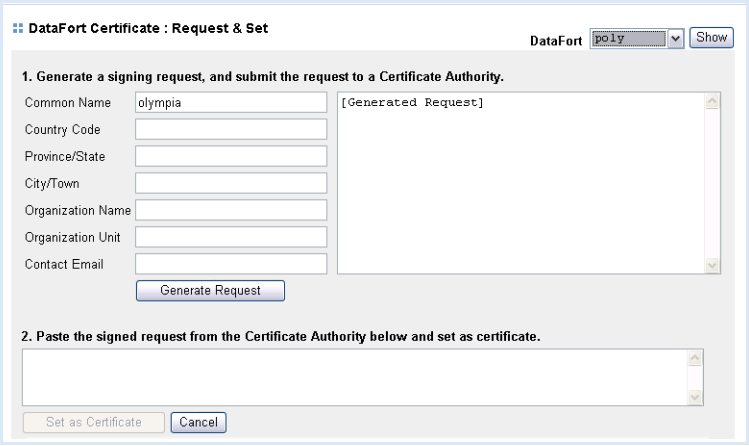
9. Click Install Certificate.
10. Complete the Install Certificate Wizard.

    The certificate has been installed. When you connect to the WebUI, no security certificate warning should appear; instead you will see a valid certificate message.

Setting a Certificate Authority Signed Certificate

1. Choose **Security > DataFort Certificate**.

2. Click Use CA-Signed.



3. Enter the required information into the fields provided and click Generate Request. 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 262.

4. When you receive the signed request from the CA, paste it into the box provided. Cut and paste the entire contents of the certificate file, including the BEGIN and END lines.
5. Click Set as Certificate.
6. Log out of the WebUI.
7. Open an HTTPS connection to the DataFort.

   The certificate warning appears.

8. Click View Certificate.

9. Click Install Certificate.
10. Complete the Install Certificate Wizard.

    The certificate has been installed. When you connect to the WebUI, no security certificate warning should appear.

Managing Licenses

DataFort 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.

1. To view the license for a DataFort, choose **System Config > General > Licensing**.
2. Check that the license is valid.

   A license becomes invalid when it expires. The license may be linked to the DataFort serial number, in which case the license will need to be updated if a DataFort is configured using a database from a DataFort with a different serial number.
3. If necessary, obtain a new license from Decru and use the Add button to add the license.
   - To remove an expired license, select it and click Delete.
   - To add a new license, click Add and enter the required information.

SNMP Settings

DataFort supports both MIB II and the read-only private Decru MIB. All Decru MIBs are read-only for security reasons. The Decru MIB provides standard MIB-II as well as Decru MIB messages.

A separate *DataFort Appliance SNMP Alarms Guide* is available from Decru. See the following for configuration information:

- Supported SNMP and MIB Versions
- Enabling SNMP
- SNMP Configuration

Supported SNMP and MIB Versions

DataFort supports the following:

SNMP version	SNMPv1, SNMPv2c., SNMPv3
SNMP tools	Generally available SNMP tools can be used to query SNMP MIBs.
MIBs	Standard MIB-II (Internet MIB) as described in RFC 1157.
	Private Decru MIB. See the DataFort SNMP Reference Guide for details.

For a complete list of DataFort 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 DataFort appliance (fan speeds, temperatures, battery voltages, etc.).
System Alerts	Useful for monitoring the software running on the DataFort (number of processes, file system usage, etc.).

Enabling SNMP

Only a Full Administrator can configure SNMP settings. Use the Disabled and Enabled radio buttons to turn SNMP on and off.

1. Choose **System Config > Network > SNMP Agent.**
2. Enable or disable SNMP using the radio button. See SNMP Configuration if enabling SNMP.

SNMP Configuration

The following can be configured using the SNMP page of the WebUI.

System location	sysLocation.0 under MIB-II. A description of the physical location where the device is installed or operating.
System contact	sysContact.0 under MIB-II. The contact information for the person or organization responsible for managing the device.

SNMP parameters	Read Community: community string used to read SNMP MIB. Trap Host: hostname (or IP address) which SNMP traps are sent to. Trap Community: community string used to send SNMP traps.

To set the SNMP connection to DataFort for use with SNMP tools such as HP OpenView:

1. Choose **System Config > Network > SNMP Agent**.
2. Enable SNMP using the radio button.

System

3. Enter the System Location. The System Location field is a string that describes the location of the system (the DataFort appliance).
4. In the System Contact field, enter the contact information for the person responsible for managing SNMP.

Trap

5. Enter the IP address or name of the Trap Community if a trap location is specified on the network. The Trap Community should be set to the community string used when sending messages to the Trap Host.
6. Enter the IP address or name of the Trap Host if a trap location is specified on the network.
7. Enter the Read Community name. For highest security, Decru recommends that the default community name (public) not be used.

Version

8. Check SNMPv1/v2c or SNMPv3. If you need both SNMPv1/v2c and SNMPv3, check both boxes.
   - For SNMPv1/v2c, enter the Read Community.
   - For SNMPv3, enter the username and password.
9. Click Apply.

15 DataFort Appliance Settings and Status

DataFort provides information on status and settings in the WebUI, LCD, SNMP and CLI interfaces:

- See Viewing Settings in the WebUI for an overview of status and settings visible in the WebUI.
- The DataFort Front Panel LCD provides throughput and IP information.
- Configure SNMP Settings to allow network and hardware status information to be sent to the SNMP interface.
- The CLI provides security configuration settings and a way to view Stack Trace Settings.

Viewing Settings in the WebUI

The DataFort WebUI can be used to view current settings, including:

- View DataFort Logs
- View DataFort Throughput and CPU Usage
- View Storage Diagnostics
- View DataFort Date and Time Setting
- View DataFort System Users
- View DataFort Network Settings
- View Crypto Status of DataFort
- View Information About DataFort
- View DataFort Sensors
- View DataFort LCD in WebUI

View DataFort Logs

Choose **System Info > Log**. To filter the view by time, select a display period from the drop-down menu at the left. Events can be displayed from the last minute, 5 minutes, 15 minutes, 1 hour, 1 day, or 1 week. To select a single type of event to view, select Security, Operations or Performance from the Source drop-down menu. To select only events of certain priorities, select the priority level from the Priority Limit drop-down menu. To configure logs see Configuring Log Storage on page 153.

View DataFort Throughput and CPU Usage

From the Home page of the WebUI, click the CPU or Throughput link, or choose **System Info > Status > Activity**. The Local Activity page graph indicates the activity level of the DataFort appliance over time. A set of bars represents activity when the activity page is loaded. The page auto-refreshes every few seconds, adding a new set of bars to show updated values. Mouse over any bar to see the value represented by the image.

View Storage Diagnostics

To view storage network information, choose **System Info > Diagnostics** from the WebUI. This display will show DataFort WWN settings as well as information about all known devices on the fabric.

View DataFort Date and Time Setting

From the DataFort WebUI, choose **System Config > General > Date/Time**. The date and time setting on the DataFort are displayed.

View DataFort System Users

From the DataFort WebUI, choose **System Config > System Users**. DataFort system users include administrators and Recovery Officers.

View DataFort Network Settings

From the DataFort WebUI, choose **System Config > Network > IP Settings**. The settings assigned to this DataFort are displayed.

View Crypto Status of DataFort

DataFort continually monitors the state of its cryptographic system, halting file serving operations if a failure occurs. DataFort runs a self-test of its Storage Encryption Processor (SEP) every time the WebUI Home page is loaded. The results of this test are displayed on the Home page. From the DataFort WebUI, choose **System Info > Status > Crypto**. When the page loads, the test will run automatically.

View Information About DataFort

From the DataFort WebUI, choose **System Info > About**. The defense setting, recovery settings (schema and card labels) and system version for this DataFort, including the serial number, are displayed.

View DataFort Sensors

From the DataFort WebUI, choose **System Info > Status > Sensors**. This will show the status of the hardware including Temperature Sensors, Fan Sensors, Voltage Sensors and Power Supply Sensors. This information can be used by Decru support personnel to diagnose problems with the DataFort hardware.

View DataFort LCD in WebUI

From the DataFort WebUI, choose **System Info > Status > LCD**. The DataFort LCD graph and messages are displayed in the WebUI.

16 Decru Management Console Functions

The Decru Management Console (DMC) is the only interface for running the Setup Wizard for a DataFort appliance. The DMC is also the sole management interface for the Lifetime Key Management (LKM) Appliance. For full documentation of the DMC, see the *LKM Appliance Administration Guide*.

The DMC provides an alternate interface for some DataFort management functions generally performed from the DataFort WebUI. If Lifetime Key Management appliances are in use, the DMC can be used to manage both LKM and DataFort appliances from a central location.If equipped with SecureView licenses, multiple appliances can be managed at one time.

The DMC console menus provide tools for the following:

- Appliance Management
- License and Administration Management
- Logging Configuration

See Decru Management Console Menus for an overview of DMC menus.

Appliance Management

The Decru Management Console is installed on the Management Station so the DataFort setup wizard can be run, as described in .

1. Choose **Start > Programs > Decru > Decru Management Console**.

   Once an appliance is added to the Decru Management Console, icons show appliance status. Table 20 shows possible state displays.

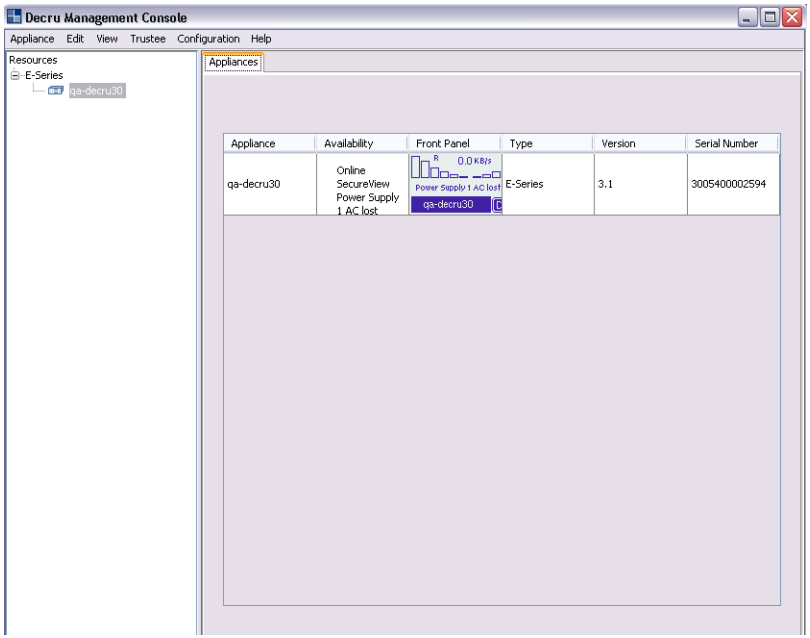


Table 20: Appliance Status Indicators

Icon	Icon Appearance	Appliance State
	Yellow with open icon	Uninitialized: IP address set, but setup wizard not completed
	Gray with !	Incorrect login: administrator name and/or password incorrect
	Blue	Online with no errors
	Blue with yellow alert	Online with error: double-click icon to check appliance details

TABLE 20: APPLIANCE STATUS INDICATORS (CONTINUED)

Icon	Icon Appearance	Appliance State
	Red	Offline
	Gray	Unknown: no login has taken place

ADDING AN APPLIANCE

Use the Appliance menu to add an LKM or DataFort appliance so it can be managed by the console. Several appliances may be added at once if SecureView is enabled.

1. Choose **Start > Programs > Decru > Decru Management Console**.
2. Choose **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 single field provided and click Add after each, or add all IP addresses or hostnames directly into the pane on the right side of the screen.
4. Click OK when all addresses or hostnames are entered.

   The certificate warning appears.
5. Agree to trust the certificate once or always.

   Note: If the appliance is not found, no certificate warning will appear. The appliance will be added to the console, but will not appear online.

   Once added, the appliance will appear in the console listed under Resources. Appliances will appear offline until you log in using the console. See Logging into Appliances.

LOGGING INTO APPLIANCES

Several appliances may be logged in to at once if SecureView is enabled and the appliances share an administrator in common.Log into each appliance after adding it to DMC.

1. Select an appliance in the Resources pane and choose 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 will change to online. See Appliance Status Indicators on page 187 for information about status icons.

REMOVING AN APPLIANCE

Remove an appliance from the Management Console. Several appliances may be removed at once if SecureView is enabled.

- Select an appliance in the Resources list and choose **Appliance > Remove**.

Running the Setup Wizard

Use the wizard to configure LKM and DataFort appliances. Several appliances may be configured at once if SecureView is enabled.

1. Select an appliance in the Resources list and choose **Appliance > Setup**.
2. Run the wizard for the appliance. See Initializing DataFort Appliances on page 51 for detailed instructions.

Verifying an Upgrade Package

Verify an upgrade package before running it on the appliance.

1. Select an appliance in the Resources pane and choose **Appliance > Verify**.
2. Browse to the upgrade file and click Apply.

   After the package is verified, the hash will display in an alert box.

Upgrading an Appliance

Upgrade the appliance version with an upgrade package from Decru. Several appliances may be upgraded at once if SecureView is enabled.

Note: Follow the instructions that are provided with the upgrade package from Decru.

1. Select an appliance in the Resources pane and choose **Appliance > Upgrade**.
2. Browse to the upgrade file and click Apply.

Backing Up an Appliance

Back up the configuration database of the selected appliance. Several appliances may be backed up at once if SecureView is enabled.

1. Select an appliance in the Resources pane and choose **Appliance > Back Up**.
2. Choose a location for the file to be saved and click Save.

Creating Trustees

Select two appliances to form a trustee relationship between them. Creating trustees allows data encryption keys to be shared between DataFort appliances that have no Recovery Cards in common, and may not even be on the same network. Once a trustee relationship is established it is possible to freely transfer keys between the two clusters using the import and export key options of the WebUI.

Use the DMC to set up trustees. See Managing Trustees on page 128 for instructions.

Linking Appliances

Create a link between an LKM and DataFort appliance so that the LKM appliance can manage keys for that DataFort appliance.

1. Select both appliances in the Resources pane of the console.
2. Select **LKM > Link Appliances**.
3. An alert will appear when the connection is made.

Or:

1. Select the icon for a DataFort appliance in the Resources pane of the console.
2. Drag the icon for the DataFort appliance to the icon for the LKM appliance.

   An alert will appear when the connection is made.

   Note: A zeroized appliance will lose its secure links to other appliances. After zeroization, that appliance's links must be removed in DMC and reformed using the Link function of DMC.

Viewing Details

Shows the system version information for the appliance.

1. Select an appliance in the Resources pane and choose **Appliance > Details**.
2. The system version command will be run on the CLI and the output displayed.

Accessing DataFort WebUI

Opens the WebUI for the DataFort appliance.

Note: This option is only valid for DataFort appliances.

- Select a DataFort appliance in the Resources pane and choose **Appliance > WebUI**.

  Note: DMC and WebUI will both attempt to use the smart card reader resource. Performance may improve if both management interfaces are not open at the same time.

Accessing Command Line Interface

Opens the Command Line Interface (CLI) for all selected appliances.

1. Select an appliance in the Resources pane and choose **Appliance > Command Line**.

   The CLI will open. See CLI Administration on page 199 for commonly-used commands.
2. Enter the command into the field provided.
   - Click Execute to execute the command. The command will be 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 will be 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.

Collecting Tech Support Info

Runs a script on the selected appliance to collect information useful to technical support when evaluating a problem.

- Select an appliance in the Resources pane and choose **Appliance > Collect Tech Support Info** and save the file to a designated location.

Rebooting Appliances

Reboots selected appliances.

- Select an appliance in the Resources pane and choose **Appliance > Reboot**.

Zeroizing Appliances

Zeroizes selected appliance. This erases and invalidates all encryption keys in the system and erases all configuration information. Zeroization should be followed either by running Setup from the Management Console to assign a new configuration or restore a previous configuration.

Note: Read the cautions outlined in Zeroizing the Decru DataFort on page 158 before zeroizing an appliance.

1. Select an appliance in the Resources pane and choose **Appliance > Back up**.
2. Save the backup file of the configuration.
3. With the appliance still selected, choose **Appliance > Zeroize**.
4. Choose whether or not to preserve the appliance's IP Address.
5. Enter the confirmation code: `ZeroizeYes` and click Apply.

Exiting the Console

Choosing **Appliance > Exit** exits the Decru Management Console. Alternatively, use the close box at the upper right-hand corner of the console screen.

License and Administration Management

The Configuration Menu offers the following options for managing licenses and administrators:

- Managing Licenses
- Adding a License
- Managing Administrators
- Adding an Administrator

Managing Licenses

To view the licenses on selected appliances:

- Select an appliance in the Resources pane and choose **Configuration > License**.

  All known licenses for the selected appliances appear.

  Licenses can be removed by right-clicking the license on screen and selecting Delete.

Adding a License

To add licenses to selected appliances:

1. Select an appliance in the Resources pane and choose **Configuration > Add License**.
2. Enter the license into the provided field and click Apply.

   All known licenses for the selected appliances appear.

Managing Administrators

To view the administrators with permission to manage selected appliances:

1. Select an appliance in the Resources pane and choose **Configuration > Administrators**.

   All known administrators for the selected appliance appear.

   Administrators can be managed from this view. See Adding an Admin Card to an Administrator, Removing an Admin Card from an Administrator and Deleting an Administrator.

Adding an Admin Card to an Administrator

- On the Administrators page, right-click an administrator and select Add Admin Card.

Removing an Admin Card from an Administrator

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

Deleting an Administrator

- On the Administrators page, right-click an administrator and select Delete.

Adding an Administrator

Administrators can be added to any appliances visible in the Management Console. All administrative tasks can be carried out by a Full Administrator. The appliance also supports the creation of specialized administrators. To add an administrator to selected appliances:

1. Select an appliance in the Resources pane choose **Configuration > Add Admin**.

The Add Administrator page appears.

2. Enter the name of the administrator to be added to the selected appliance.
3. Enter and confirm the password for the administrator.
4. Select the type of administrator to add.

Read-only	Select this to create an administrator who can view DataFort settings, but cannot modify them.
Specialty	Select this to create specialized administrators. With Specialty selected, you can check multiple special types to combine permissions for one administrator.
Full Admin	Select this to create a Full Administrator role.

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

Specialty administrators can be used to separate tasks for increased security. The roles have separately defined permissions, ensuring that administrators only have permission to execute certain designated commands. If desired, compound administrators possessing the characteristics of more than one speciality administrator can also be created. See Administrator Roles on page 83 for more information about administrator roles.

Logging Configuration

The Configuration Menu offers the Log Configuration menu. Appliances log events in these categories:

- Security
- Operations
- Performance

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

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

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

For more about logging, see Logging Functions on page 246.

1. Select an appliance in the Resources pane and choose **Configuration > Log Configuration**.

   The Logging Configuration page will appear.

2. Select the desired settings and then click Apply.

Decru Management Console Menus

The Decru Management Console offers the following drop-down menus for use with DataFort appliances:

- Appliance Menu
- Edit Menu
- View Menu
- Trustee Menu
- Configuration Menu
- Help Menu

Note: The LKM Menu functions are described in the *LKM Appliance Administration Guide*.

Some menu options initiate operations which are described in more detail in the Decru Management Console Functions chapter of this guide.

Appliance Menu

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

Add	Add an appliance to the Management Console. See Adding an Appliance on page 188.
Remove	Remove an appliance from the Management Console.
Log in	Log in to an appliance as an administrator. See Logging into Appliances on page 188.
Log out	Log out of an appliance as an administrator.
Set up	Set up an LKM or DataFort appliance by running the Setup Wizard. See Initializing a Standalone DataFort or DataFort Cluster on page 53.
Verify	Verify the validity of an upgrade package before upgrading. See Verifying an Upgrade Package on page 189.
Upgrade	Upgrade an appliance. Upgrades should be done only after consulting Decru support. See Upgrading an Appliance on page 189.
Back up	Back the configuration database up as a file to a specified location. See Backing Up an Appliance on page 189.
Link Appliances	Create a link between appliances. This is used for two purposes: link a DataFort and LKM appliance so that LKM can manage keys for that DataFort appliance, or link LKM appliances so that they share key information. Both appliances must be selected to create a link. See Linking Appliances on page 189. The same is achieved by dragging the DataFort appliance icon to the LKM appliance icon as described in Linking Appliances on page 189.

Details	Shows the system version for the selected appliance. See Viewing Details on page 190.
WebUI	Opens the WebUI of the selected appliance (DataFort only). See Accessing DataFort WebUI on page 190.
Command Line	Opens the CLI. Whatever command is run will be executed on all selected appliances. See Accessing Command Line Interface on page 190.
Collect Tech Support Info	Creates a file containing information useful to technical support when troubleshooting for the selected appliance. The file is by default placed in the tech support folder of the Decru Management Console directory. See Collecting Tech Support Info on page 190.
Reboot	Reboot the selected appliance. See Rebooting Appliances on page 190.
Zeroize	Zeroize the selected appliance. See Zeroizing Appliances on page 191.
Smart Card Utilities	Resets a smart card and displays card information.
Exit	Exit the Management Console. See Exiting the Console on page 191.

Edit Menu

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

Find	Searches for text in the active pane of the Management Console. The search is not case sensitive.
Find Again	Finds next instance of same search.

View Menu

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

All	Lists all appliances.
Type (default)	Displays appliances sorted by type, including LKM Appliance, FC-Series Appliance, E-Series Appliance and S-Series Appliance.
Subnet	Displays appliances sorted by subnet.
Refresh	Refresh view of listed appliances.

Trustee Menu

A trustee relationship between two appliances allows encryption keys to be shared between those appliances even if they have no Recovery Cards in common, and are not on the same network.

Trustees send messages to establish a relationship before key sharing. The first message is the Trustee Establishment Package (TEP). The second message is the Trustee Acceptance Package (TAP).

Create Trustees Link	Create a Trustee relationship between two DataFort appliances. This allows the appliances to share key information. Both appliances must be selected. See Creating Trustees on page 189.
Start Trustee Creation	Starts the process of creating a trustee for selected appliance. See Creating Trustees on page 189.
Receive TEP	Allows selected appliance to receive a Trustee Establishment Package. See Creating Trustees on page 189.
Receive TAP	Allows selected appliance to receive a Trustee Acceptance Package. See Creating Trustees on page 189.
Unapproved Trustee List	Displays list of trustees not yet approved (waiting to accept a TAP). See Creating Trustees on page 189.
Trustee List	Displays list of trustees. See Creating Trustees on page 189.

Configuration Menu

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

License	View licenses. See Managing Licenses on page 192.
Add License	Add licenses. See Adding a License on page 192.
Administrators	View and manage administrators. See Managing Administrators on page 192.
Add Admin	Add an administrator. See Adding an Administrator on page 192.
Log Configuration	See Logging Configuration on page 194
Replace Recovery Officer	The Configuration Menu offers the Replace Recovery Officer menu. This allows you to replace a Recovery Card in the set, thereby replacing the associated Recovery Officer as well. See Removing an Administrator on page 90 for instructions on using the DataFort WebUI to manage administrators. To replace a recovery card using DMC, refer to the *LKM Appliance Administration Guide.*

Help Menu

Help	Opens online help for selected appliance type. Select the appliance in the Resources pane and choose Help. The administrative guide for the selected appliance will open.
About	Shows information about this version of the Management Console.

17 CLI ADMINISTRATION

Some administrators may prefer to perform management tasks using the DataFort command line interface (CLI). A few advanced DataFort management procedures are only available via the CLI. COnsider the following when using the CLI:

Note: 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 will be 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 237 of this guide. Refer to the separate *DataFort CLI Reference Guide* for a complete list of commands and parameters.

Note: If access to the DataFort CLI via SSH is disabled (for example if DataFort is running in Common Criteria Mode) use the WebCLI to issue commands by accessing **System Config > General > WebCLI**.

Procedures described in this chapter include:

- Using the CLI
- Administration Commands
- Storage Management Commands
- Manual Key Generation
- Changing DataFort Appliance Network Port Settings

Using the CLI

Some CLI commands must be executed in a specific order for desired results. The command line will provide 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 DataFort Command Line Interface on page 75). By default, DataFort is set for standard CLI. It is recommended that only one WebUI or CLI session be open per cluster at one time.

CLI Help

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

Administration Commands

The next sections provide examples of CLI administration in the following areas:

- Administrator Roles
- Creating a New Administrator Using the CLI
- 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:

`san-readonly-admin`	Read Only Administrator
`san-machine-admin`	Machine Administrator
`san-backup-admin`	Backup Administrator
`san-storage-admin`	Storage Administrator
`san-key-admin`	Key Administrator
`san-physical-security-admin`	Security Administrator
`san-datafort-account-admin`	Admin Account Administrator
`san-admin`	Full Administrator

1. Log in as the specialty administrator whose permitted commands you want to see 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 WebUI.

   ```
   system property get --role <role>
   ```

Creating a New Administrator Using the CLI

New administrators can be created by a Full Administrator using CLI commands. When an administrator is created using the WebUI, the new administrator is granted the authorizer role and replication across the cluster by default. By default, any administrator created using the CLI will require prior authentication of another administrator before logging into the WebUI 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.

`cluster status`	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.
`cluster config`	Cluster configuration commands.
`cluster enable`	Enables clustering. This command breaks any pre-existing cluster connectivity and forces a re-negotiation of the cluster.
`cluster rexec`	Allows commands to be issued remotely to all other DataFort appliances in the cluster as identified by IP address or name. For example, `cluster rexec kfc list` would output `kfc list` from all the members of a cluster. Also allows commands to be issued to a remote DataFort: `cluster rexec --name datafort1 kfc list` would output `kfc list` for datafort1.
`cluster rsh`	Connects directly to another member of the cluster as identified by IP address or name. The `ctl-d` command breaks out of this into the previous shell.
`cluster disable`	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 WebUI 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 will reform without the offline DataFort. To disable a member, log into another member of the cluster and execute the `cluster disable <member-ip or name>` command, identifying the DataFort to be removed by name or IP address. To allow the member back into the cluster, execute the `cluster enable <member-ip or name>` 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 permitted to change (set) those properties use: **system property get -d** Output will be of the form: **security-admin RW global sys.security.web.usesmartcard: 0** This output means that Security Administrators and up will be able to modify the property, in this case Secure Web. 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 Web is off.
system selftest	Performs a series of tests on the DataFort and configured servers.
system utility lcdmessages	Displays text of any warnings currently on the DataFort 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 DataFort. Adding the **-p** flag to **system reboot** will power cycle 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, where the **<mesg>** parameter is a log message to be verified **"mesg-text [meta-data signature]"**:

```
system log verify <msg>
```

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)  [AAAAAEMAAAAFAAAAgnUpQA== 3NKQl8/
5r3x6n+Rw]
```

```
system log verify "boxmanager: Executed: share virtual add  --ip
\"his\" \\\\\\\\his\\\\chi \"nas-hiro1\"  (sess id: 228933632)
[AAAAAEMAAAAFAAAAgnUpQA== 3NKQl8/5r3x6n+Rw]"
```

The **<mesg>** parameter is a log message to be verified **"mesg-text [meta-data signature]"** as in this example:

```
system log verify "boxmanager: Security property
sys.security.groupreview was set to 1 [AAAAAAEAAAAHAAAAnCruPg==
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 [AAAAAAIAAAAIAAAAnCruPg== /
x1uPgNyIsypvlnx]"
```

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: See the DataFort CD for the DataFort Signed Log Authentication script.

Stack Trace Settings

DataFort 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 DataFort 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 execute 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:

net util arp	Display or clears the ARP (Address Resolution Protocol) table: display using **net util arp -n,** clear using **net util arp -d**.
net util host	Resolve a given hostname to its IP address: **net util host <hostname>.**
net util ifconfig	Display information about network interfaces.
	Display information about network interfaces which are up: **net util ifconfig -u.**
net util ipsecstats	Display IPsec statistics.
net util netstat	Display network status. Display the routing table: **net util netstat -r**. Display the state of all sockets: **net util netstat -a**. Display network memory buffer usage (mbufs): **net util netstat -m**.
net util ping	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>: **net util ping -I <local_addr> -S <local_addr>**.

Backup Management

It is recommended that a database backup be performed after any changes.

db export	The CLI command **db export** can be used for manual configuration database backups, such as to the LKM server or another designated site. Enter **db export ?** to see the options, and see LKM documentation for more information. Using the interactive backup mode (**db export -u)** will require 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.

disk list	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 that has paths to the disk(s).
disk rescan	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 IO.
disk remove	Enter the device parameters into the command to remove it from the configuration database: **disk remove <port-wwn> <lun>**. Options include specifying the host port WWN, the WWN of the DataFort HBA which discovered the disk and the name of the DataFort that discovered the disk.
disk rmall	Enter the device parameters into the command: **disk rmall <port-wwn>**. All devices associated with the indicated WWN will be removed from the configuration database. There is also an option to indicate the host port WWN.
disk blink	Enter the disk parameters into the command: **disk blink <host-port-wwn> <lun> on|off**. If the value is set on, the LED on the selected disk will blink, so that the disk can be visually identified in the JBOD. If the disk blinks, but does not appear in the configuration database, execute the **disk rescan** command. Note that this only applies to JBOD devices.
disk map	To add a second path to an existing Cryptainer, first find the Cryptainer ID using the **fccry list** command. Enter device and Cryptainer parameters: **disk map <port-wwn> <lun> <cryptainer-id>**. There is also an option to indicate the host port WWN.
disk rmmap	Execute the **disk rmmap** command to remove the path to the Cryptainer, using the same device and Cryptainer parameters: **disk rmmap <port-wwn> <lun> <cryptainer-id>**. There is also an option 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 will be 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 rmmap <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 rmmap** 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>

Using Crypto Copy

Crypto Copy moves data in an encrypted form between volumes. Note that the volume that will be copied should be prepared for backup (database applications should be coalesced and file systems unmounted or synced). This command is available for Cryptainers created on disk only.

Note: The target device should be the same size or larger than the volume that will be copied.

1. Use the **disk cryptocopy request** command to queue Cryptainers for Crypto Copy:

   disk cryptocopy request <port-wwn> <lun> <direction>
   <cryptainer-id>

2. Launch the copy:

   disk cryptocopy notify

3. Monitor the progress of the copy:

   disk cryptocopy list

Host Commands

To perform host management commands, first execute the **host list** command to get necessary information about the host.

host list	Generates a list of all hosts and their status on the cluster.
host rescan	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.
host add	Enter information about the host that will be added: **host add <node-wwn> <port-wwn> <name>**.
host remove	The indicated host will be removed from the configuration database: **host remove <port-wwn>.**

Virtualizing a Host

DataFort presents host HBAs to storage. Some devices reserve space for a specific host as identified by its WWN. These devices require that DataFort virtualize the host so that storage devices can see it. To support heterogeneous hosts and LUN masking, DataFort allows the host to be virtualized: DataFort presents the host information to the storage device.

Note: Since JBOD devices (or any devices that are not set up with LUN masking) will 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

   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 you know the previously assigned vpindex, you can assign it again (this will give the same default WWN). The Forward Port WWN option **--forward-wwn** will use the host's original WWN. This is recommended only if the host is not connected to the same fabric as the DataFort'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.

fccryptainer list	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.
fccryptainer path	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 that discovered the disk where the Cryptainer is located, Cryptainer ID, or Cryptainers not accessible from host port or node WWN.
fccryptainer perm list	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.
fccryptainer rekey list	Lists all rekey jobs with status.
fccryptainer rekey request	Request a rekey job: **fccry rekey request <cryptainer-id>**. 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 to be used to do the rekey.
fccryptainer rekey notify	Reactivate a stalled or stopped rekey job. This will activate all new or changed key requests.
fccryptainer add	Add a Cryptainer, specifying disk information and mapping options: **fccry add <map-type> <port-wwn> <lun>**. Indicate **map-type** as **<lunmap|portmap>**. 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 **nokey** option (disk Cryptainers only): **fccry add --nokey <map-type> <port-wwn> <lun>**.
fccryptainer createall	Automatically create one Cryptainer per LUN in a multi-disk target. Specify disk information and mapping type: **fccry createall <map-type> <port-wwn>**. Options are the same as when using **fccry add.**

fccryptainer clone	Reuses one Cryptainer's key for another Cryptainer, creating a new Cryptainer for a copied LUN. Specify Cryptainer information: **fccry clone <cryptainer-id> <map-type> <port-wwn> <lun>.** Options include description, host port WWN and forward port WWN.
fccryptainer remove	Removes the keys and access associated with a Cryptainer from the configuration database: **fccry remove <cryptainer-id>**. Use the **[-f, --force]** 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 DataFort stores information about Cryptainers, even deleted Cryptainers, indefinitely unless they are purged when saved to LKM.
fccryptainer rmall	Remove all Cryptainers from the configuration database. Use the **[-f, --force]** option to attempt to remove all Cryptainers without prompting for confirmation.

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 will also show whether storage devices are offline or online, and show 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 DataFort to identify hosts, assigned based on the state of the firmware of each DataFort at the time that the host table entries are 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 DataFort 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 will show 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`	View 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

DataFort 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 Settings and Defaults on page 120.

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. If you are creating more than one key, the keys will be numbered sequentially starting with 0 or the supplied index option.

- Log in to the DataFort CLI and execute the command:

```
keyman cryptainerkeys generate [-x, --exportable <on|off>] [-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 execute:

```
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 DataFort Appliance Network Port Settings

By default, the media type is set to auto negotiate on all DataFort 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. DataFort automatically changes it to full-duplex in this case.

For the FC-Series DataFort, the management port is the only interface affected by these values. To change the media type of the DataFort management port:

1. Log in to the DataFort CLI and run the following commands:

```
system property set net.admin.media [value]
system property set net.admin.mediaopt [value]
```

2. Apply the settings by running the following command:

```
net apply
```

18 Troubleshooting

This chapter provides general troubleshooting information for DataFort. DataFort event logs provide additional information about security, operations, and performance issues.

- Restoring a DataFort 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 Linux
- Decru DataFort Operation with Solaris
- Decru DataFort Operation with Legacy Encrypted Tapes
- Decru DataFort Operation with Tivoli and STK Drives
- Decru DataFort Operation with LTO2 Serialized Commands
- Decru DataFort AIX Atape Failover Support
- Decru DataFort SCSI Reservation Handling Fixes

Restoring a DataFort Appliance

If a standalone DataFort is lost, a saved configuration database from that DataFort can be used to configure a replacement DataFort. The recovered DataFort will then be able to retrieve data that was encrypted using the previous DataFort. The Setup Wizard assigns a new DataFort the configuration from a pre-existing DataFort. The replacement DataFort will retain all parameters stored in the configuration database of the original DataFort, 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 166. 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 DataFort.
- The minimum set of Recovery Officers and Recovery Cards as determined by the recovery schema of the cluster.
- A saved database from the DataFort that is to be restored.

1. Connect the new or zeroized DataFort to the network and assign it the IP settings of the old DataFort. See Assigning the DataFort IP Address on page 48.
2. Start the wizard. See Initializing DataFort Appliances on page 51.
3. At the Recover from Database page, browse to the saved configuration database.

   DataFort will need the minimum number of Recovery Cards required for recovery procedures (as set in the original configuration). You will be prompted to insert Recovery Cards from the original DataFort configuration.
4. Complete the wizard.

Front Panel LEDs

Depending on the type of chassis, the DataFort front panel features one or two bicolored LEDs that signal the status of DataFort, 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; DataFort not functional. Check LCD for messages.
Network LED	Bottom	Green	Blinking	Network link, activity
			Solid	Network link, idle
		Red	Solid	Network error

Table 23: Front Panel LEDs - 1U

Color	Behavior	Indication
Green	Solid	DataFort on network, no errors, no traffic
Green	Blinking	DataFort 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 DataFort 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 will blink green. The LED will be solid green to indicate that all the power outputs are available. It will be solid amber to indicate that the power supply has failed, there is a shutdown due to over-current, over-temperature, or if the unit is indicating a predictive failure.

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 over voltage, over temperature)	Amber
VRM failure (voltage regulator module - 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 DataFort.

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. Check the LCD on the front panel for messages.
	• DataFort must have an IP address assigned. See Assigning the DataFort IP Address.
Power not on	• On 2U DataFort: 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. • 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 DataFort 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 DataFort.
Cannot log in via serial connection	• Check that you are logging in with a valid username and password. • Try logging in again using the defaults: User: `user`, Password: `MTKNMTKN`.
Cannot connect to IP address	• Check that IP settings were set and saved after initialization. See Assigning the DataFort IP Address. • Be sure the Management Station can reach the DataFort IP address on the network.
Cannot connect to domain name of DataFort	• The DataFort 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 DataFort is opened. Log in to the DataFort WebUI and reset the tamper detection alert. See Clearing a Defense Alert.
LCD asks for System Card or Status LED is red on 2U DataFort	• A System Card needs to be inserted before DataFort is powered on. Once DataFort is powered on, the System Card can be removed. Messages appear about this condition. • For a DataFort that has not been configured, power DataFort off, and re-insert the System Card before powering DataFort 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 will halt operations if the DataFort is rebooted without a System Card. See Collecting Network Information.

TABLE 25: NETWORK CONNECTIONS AND MANAGEMENT INTERFACES (CONTINUED)

Problem	Possible Cause and Solution
Cannot log in to DataFort WebUI	• To access the DataFort WebUI you must have access to the DataFort's IP address from the Management Station. Make sure DataFort and the Management Station are on the same network. • The network switch port connected to the DataFort should be set to auto-negotiate. • Check that the supported browser (Internet Explorer 6.0 and up) is in use. • Be sure no firewall is turned on for the Windows Management Station, and be sure web traffic is not going through a proxy. • Check that the correct version of Java is installed. In Add/Remove Programs make sure the following programs are installed: Decru DataFort Smart Card Reader, Gemplus Smart Card Reader Tools, Java 2 Runtime Environment, SE v1.4.2_08 or less. • If Secure Web is on, a valid administrator and Admin Card are required to log in. • TLS 1.0 must be enabled in Internet Explorer. See Preparing the Management Station. • If Secure Web is on, Terminal Services and Remote Desktop cannot access the WebUI. • Some administrators are created requiring login authorization by another administrator. If dual authentication is required for the administrator attempting to log in, an authenticating administrator must log in first. See Requiring Authorization for Login.
Establishing the initial connection to the WebUI is slow or times out	• In the Internet Explorer Tools > Internet Options > Advanced > Security menu, uncheck the "Check for publisher's certificate revocation option." When checked, Internet Explorer will connect to companies that provide certificate revocation checking and download a CRL (Certificate Revocation List) file. If the Management Station has no connection to the Internet, this may time out.
Need to clear the saved entries from an incomplete wizard	• Zeroize the DataFort 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	• Check that you are logging in with a valid username and password. • Try logging in again using the defaults: User: `user`, Password: `MTKNMTKN`. • Check that Secure CLI is not on.
Lost login information for only administrator	• Log in using a Recovery Card and zeroize the appliance. See Emergency Serial Console Port Access.
Need to turn off WebUI smart card requirement (Secure Web) via CLI	• If you are unable to access the WebUI in order to turn off the smart card requirement, you can do so via CLI: • Log in to the CLI and enter: `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 WebUI; `0` disables the requirement. If necessary, enter: `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 WebUI and change the DNS servers, or wait for the SSH to connect and then change the DNS servers from the CLI.
WebUI displays "Loading images..." but no fabric information	• Connect to the CLI and run the command `kfc sync`. Reopen the WebUI.

Clusters

Table 26 includes troubleshooting tips for cluster management issues.

Table 26: Clusters

Problem	Possible Cause and Solution
Cluster won't form to start with	• 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. • Execute `cluster stat` on each of the members in the cluster. • If there are two members that are not communicating, disable both of them and then bring them back one at a time, making sure that the cluster forms with each addition. Use the `cluster disable` command for this. • Check for other problem with a cluster member that will not join the cluster, including any crypto errors.
Cluster member goes down and cluster will not reform	• Check that the loss of the cluster member has not dropped the number of devices in the cluster below quorum. • Use the `cluster disable` 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, some 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 WebUI, select the offline path or paths to the Cryptainer. • Right-click the offline path to the Cryptainer and select Paths > Un-map from Cryptainer. • Right-click the Cryptainer and select Encryption > 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 and IE 6.0 or greater.
	• Be sure the Admin Card is properly inserted in the smart card reader. Re-insert the card if necessary. The reader LED should flash and then light continuously.
Need to reset System Card	• DataFort needs a new or reset System Card in order to complete the setup wizard. If the System Card was not inserted into the DataFort chassis during zeroization or if it was not properly reset during zeroization, you must manually reset it. See Smart Card Reset.
Lost System Card	• Zeroize, insert a new System Card and run the Setup Wizard.
DataFort WebUI does not recognize type of card inserted into Management Station smart card reader	• The reader may identify the type of smart card incorrectly. Pull out and re-insert the card. Wait a few seconds for the card reader to detect card insertion (indicated by the status light turning green) before clicking OK. • Disconnect and re-connect the smart card reader. • Close and open the web browser. • Do not open the WebUI for more than one DataFort at a time on a single Management Station.
Lost Admin Card when Secure WebUI is turned on	• 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 Web by entering: `system property set sys.security.web.usesmartcard 0` to disable the smart card requirement for the WebUI. Then log in to the WebUI 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 WebUI login are smart card enabled and all Admin Cards are lost, you will have to 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.	• DataFort 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: Enter the command: system version at the CLI. • WebUI: Insert the System Card into the smart card reader, open a browser window and navigate to https://DataFortNameorIP/resetcards.htm. Click the Get Smart Card Version button.
Smart card errors appear	• Use an eraser to clean the metal contact on the smart card.

HARDWARE

DataFort 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 DATAFORT. 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.
	• Make sure 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.
Devices do not appear in DataFort WebUI	• 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 WebUI.
	• Check FC switch zoning - DataFort HBAs should appear. • Check LUN masking to verify that the DataFort has access to volumes. • The Storage and Host HBA WWNs can be found by choosing System Info > Status > Fibre Channel in the WebUI. 2U DataFort 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 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 are 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 detects the host device - check the WebUI. • If possible, perform a rescan by the host. • Reboot the host if necessary.
DataFort performance degrades/loss of connectivity to storage devices	• DataFort performance will degrade when the number of simultaneous IO commands exceeds 512. Issuing more that 512 simultaneous IO commands will cause IO failures and may result in a loss of connectivity to storage devices. • Use the `kfc util stat list` command to view the maximum of simultaneous IO seen by the DataFort appliance. If the displayed maximum exceeds 512, load through DataFort should be reduced to a lower level.

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: `system property set dfc.num_buffered_tape_write_requests 2`
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 will interrupt I/O for other hosts and can be problematic in disk configurations. • Disable this behavior by setting `dfc.isp.reenable_host_side_vp` 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 you can successfully write blk0, then you can write to the tape. If the application tries to skip writing blk0 but instead tries to append to the tape, DataFort will deny the access through an encrypted pool. • In NBU, fix this by expiring the tapes by using the bpexpdate -m <media_id> -d 0 -force command. This essentially creates a blank tape and permits DataFort to write blk0 when instructed to do so. If you do expire the tape in NBU using this command and initiate a write through DataFort, all data on the tape/media_id in question will be gone. • In Legato, the "label media" command does the same thing. There are equivalents in other backup applications.

Clusters

Table 26 includes troubleshooting tips for cluster management issues.

Table 29: Clusters

Problem	Possible Cause and Solution
Cluster won't form to start with	• 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. • Execute `cluster stat` on each of the members in the cluster. • If there are two members that are not communicating, disable both of them and then bring them back one at a time, making sure that the cluster forms with each addition. Use the `cluster disable` command for this. • Check for other problem with a cluster member that will not join the cluster, including any crypto errors.
Cluster member goes down and cluster will not reform	• Check that the loss of the cluster member has not dropped the number of devices in the cluster below quorum. • Use the `cluster disable` 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, some 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 WebUI, select the offline path or paths to the Cryptainer. • Right-click the offline path to the Cryptainer and select Paths > Un-map from Cryptainer. • Right-click the Cryptainer and select Encryption > Encrypt/Resume… to resume the rekey.

Decru DataFort Operation with EMC

The following steps will assist you 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 VCMDB) 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 to allocate more volumes to the DataFort storage HBA.
3. Run `symcf discover` to find the Symmetrix devices connected to the host. Run `vcmfind` 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'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 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. Assign the Cryptainers to individual hosts using the DataFort WebUI.

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 will launch a window detailing all the systems connected.
2. The DataFort's WWN will show up here but, due to no agent, it will be unregistered.
3. After selecting the DataFort's WWN, click on the Register button.
4. In this window, DataFort can either be registered as a standalone (add it as new) or 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 and it will bring up the available LUNs.

Decru DataFort Operation with Linux

Linux limitations require that the following be kept in mind when operating the DataFort with Linux.

Multiple LUNs

The Linux kernel must be rebuilt before Linux can see multiple LUNs. This is a problem on the client not with DataFort.

1. Set the kernel option: CONFIG_SCSI_MULTI_LUN to YES and rebuild the kernel.
2. Once this is done, add this line to lilo.conf for the Linux boot:

```
append="max_scsi_luns=128"
```

All LUN numbers must be contiguous for a Linux client. For example if the DataFort exports LUNs 0-25 and then 28, only 0-25 will appear. It will stop the scan once a LUN ID is skipped. Note that the Linux max is 128 LUNs.

Failover

In a predefined array with X disks, where X - 1 are active disks and the additional disk is setup as a hot-standby disk, as long as permissions are given to the server by the DataFort for the hot-standby disk, the disk failover will occur automatically. When the failed disk is removed and replaced, server access permissions must be assigned in the DataFort before the server will be able to recognize the disk. After permissions are assigned, the new hot-standby disk can be added to the logical array.

Resync Speed

The default speed of resyncing of RAID volumes in Linux is slow - the minimum speed is 100KB/sec. This speed is used because resyncing does not want to take time from the system. At this speed, resyncing can take a long time.

The file /usr/src/linux/drivers/md/md.c controls this speed:

```
static int sysctl_speed_limit_min = 100;
static int sysctl_speed_limit_max = 100000
```

Modify the value of sysctl_speed_limit_min to get greater speed:

```
static int sysctl_speed_limit_min = 10000
```

This will increase the creation speed to 10MB/sec.

Decru DataFort Operation with Solaris

If a Solaris host is attached directly to the DataFort, make sure 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 your 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 will require modification of the name binding for the Primary Port (used for LUN Mapping) of the DataFort. The Virtual Ports (used for Port Mapping) will retain the originally assigned WWNs.

The device names of storage presented by the DataFort 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 will be secured by the DataFort.

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 your host's HBA documentation.

After changing persistent binding settings, see:

- Stripe
- RAID

Stripe

Create a stripe on Solaris by doing the following:

1. Execute 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.

   ```
   # newfs /dev/md/rdsk/d0
   ```

   This will create a filesystem on the 3 disk stripe volume.

   ```
   # mount /dev/md/dsk/d0 /mnt/volume
   ```

This mounts the filesystem at the point /mnt/volume.

Once this is done, the volume is available for use.

To attach through the DataFort, first unmount the volume:

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 Solaris' format utility.
4. If zoning is used, the original names of the disks should no longer be there.

   It is critical to create a clear text Cryptainer for each disk in order of the stripe.

   Create a stripe with the new disk names through the DataFort (there is a 1 to 1 relationship for each disk):
5. Locate the device names of the disks presented by the DataFort (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 as VLUN 1, and has the new name c1t109d1, etc.

   There is no need to create a filesystem since that is already done.

   A mount should work right away:

   ```
   # mount /dev/md/dsk/d1 /mnt/volume
   ```

   You should see the existing data at this point.
6. 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 by doing the following.

1. Execute 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. Execute the following command:

   ```
   # newfs /dev/md/rdsk/d0
   ```

   This will create a filesystem on the 3 disk RAID-5 volume.
3. Execute the following command:

   ```
   # mount /dev/md/dsk/d0 /mnt/volume
   ```

This mounts the filesystem at the point /mnt/volume.

Once this is done, use the volume as storage as needed to attach through the DataFort.

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 Solaris' 'format' utility. If zoning is used, the original names of the disks should no longer be there.

   It is critical to create a cleartext Cryptainer for each disk in order of the RAID-5 volume.
8. Create a RAID-5 volume with the new disk names through the DataFort like this. There is a 1 to 1 relationship for each disk.

   ```
   # metainit d1 -r c1t109d1s6 c1t109d2s6 c1t109d3s6 -k
   ```

   In the previous line, the disk named c1t48d0 is shared as a cleartext container in the DataFort as VLUN 1 and has the new name c1t109d1, etc.

   There is no need to create a filesystem since that is already done.

   The '-k' option at the end of the metainit command is critical, since you don't want to affect the existing data at all and by default the RAID is re-initialized. A mount should work right away:

   ```
   # mount /dev/md/dsk/d1 /mnt/volume
   ```

   You should see the existing data at this point.
9. Next, delete the old stripe and rename the new to the old:

   ```
   # metaclear d0
   # metarename d1 d0
   ```

Veritas Volume Manager

Changing a DataFort in a Cluster Connected to a Solaris Host with Veritas

1. If the path through the DataFort is currently active, first disable the controller in Veritas DMP (assuming c2 is the controller connected to the DataFort):

   ```
   # vxdmpadm disable ctlr=c2
   ```

   The other path will now be responsible for transferring all data.
2. Replace the DataFort and reestablish the cluster (check the manual).
3. Re-enable the controller:

   ```
   # vxdmpadm enable ctlr=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 will be shown as a third path. One will be 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 will break 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 into one member of the cluster and set the system property as follows:

```
sys prop set crypto.legacy.loadr1r2 true
```

2. Power cycle all DataFort appliances in the cluster.

Decru DataFort Operation with Tivoli and STK Drives

On certain operating systems (mainly AIX), Tivoli cannot be easily configured to use a blocksize of more than 256K, the maximum supported blocksize for STK 9840 and 9940 tape drives. In this case, DataFort must be put into preserve-block-size mode.

1. Log into the CLI of one cluster member and execute 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 will be restored by another DataFort cluster, it is important to set these properties on the destination cluster too.

Decru DataFort Operation with LTO2 Serialized Commands

If a backup or restore to an LTO2 tape drive fails and the drive returns CheckCondition, Aborted Command and Overlapped Command Attempted (0x4e/0x00), set the following system property (while there is no data I/O):

```
sys prop 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 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, add the required DataFort system property and enable it:

```
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 will use 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, add the required DataFort system property and enable it:

```
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 will properly fail over to the other DataFort and continue the job.

If the link failure occurs on the storage-side connection during a backup job, that particular job will abort, and failover will not occur. However, in this case switchover will still occur, meaning that even though the job failed, the host will receive an error and switch 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.

Note: This feature is disabled when hosts are virtualized.

To set DataFort to handle SCSI-3, set the following command to true:

```
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 DataFort WebUI 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 DataFort Command Line Interface on page 75. There are two levels of security that can be set for DataFort CLI login, one of which requires first accessing the DataFort WebUI before logging into the CLI.
- As a security measure, the CLI will time 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 WebCLI does not have the same help features as the full CLI. Type **`help`** to use help in the WebCLI.

- Typing a partial command phrase (not word) will result in a listing of the possible next words in a phrase to complete the command.
- Typing a partial command phrase followed by **`?`** will give the same results as above.
- Typing a command with too few arguments will display the full help listing for that command.
- Typing a command and a **`?`** with too few arguments will display a short description of the next argument required.
- Typing a command preceded by **`help`** will display a full description: purpose, usage, parameters and options
- Typing **`cli documentation`** will display the CLI documentation.

CLI Command Overview

Top Level Commands

Type `help` to view the 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
`fcccryptainer...`	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	Type `authorize` to authorize an admin login
`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 the 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 the 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
rmall +	Remove all LUNs of a disk
rmmap +	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
rmall +	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
`cshelp...`	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.

`status`	Check the status of the connection to the configured LKM System
`server...`	Server commands...

Cluster Commands

Type `cluster ?` to view the cluster commands.

`config...`	Cluster configuration commands...
`disable +`	Disable clustering
`enable +`	Enable clustering
`rexec +`	Execute a command on member DataFort(s)
`rsh +`	Execute a remote shell on one member DataFort
`status`	Check configuration database status

Database Commands

Type `db ?` to view database management commands.

`begin`	Begin a transaction
`commit`	Commit the current transaction
`connect +`	Connect to configuration database
`export`	Export the configuration database as xml to stdout
`index...`	Indexing administration commands...
`record +`	Get a configuration database record
`rollback`	Rollback the current transaction
`save`	Checkpoint database and save changes to disk
`size +`	Display database available space
`status`	Display configuration database status
`trx...`	Transaction administration commands...
`xlog...`	Transaction log administration commands...

System Commands

Type `system ?` to view system commands.

`agreement...`	Agreement commands...
`crypto...`	Crypto commands...
`check +`	Perform basic system checks
`date...`	Date commands...
`httpd...`	HTTPD commands...
`license...`	License commands...
`log...`	System log commands...
`ntpd...`	NTPD commands...
`property...`	Property commands...
`reboot +`	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 DataFort audit function logs security relevant operations, errors, and warnings and many non-security relevant operations, errors and warnings.

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

- DataFort Log Event and Priority Types
- Log Storage Locations
- Log Presentation
- Log Purging
- Audit Configuration

Log messages are detailed in a separate *Logging Addendum* for the DataFort appliance.

DataFort Log Event and Priority Types

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

Table 30: Log types

Type	Definition
Security Logs	Security Log messages give information about access control, logins and DataFort 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 DataFort appliance.
	Security Management logs record changes to authentication policies.
	Integrity Logs record events that might modify the integrity of the DataFort 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 DataFort appliance.
Audit Logs	Audit logs are generated by the DataFort 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 31: 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 a DataFort 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:0xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
<cryptainer_group>	This parameter indicates a group of Cryptainers, as defined by the DataFort administrator. The parameter is a text string, up to 31 characters.
<domain>	Domain name of the user that changed the configuration parameter

TABLE 31: PARAMETERS IN LOG MESSAGES (CONTINUED)

<host>	This parameter refers to a host, by WWN.
<host_group>	This parameter indicates a group of hosts, as defined by the DataFort 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. • WEBUI—The user is authenticating to the WebUI interface. Note that administrators may use the WebCLI interface after authenticating to the WebUI interface. • SERIAL—The user is authenticating to the DataFort MenuShell interface.
<pool>	Tape pool.
<pool_group>	Group of tape pools, as defined by the DataFort administrator. The parameter is a text string, up to 31 characters.
<prop_name>	Name of a logging facility configuration property (see Table 4).
<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 DataFort that denied or allowed the information flow
<user>	Name of user that changed 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 DataFort logs, the administrator may select multiple storage locations. Whenever a new log message is generated, it is written to storage location(s) as configured for the log the message belongs to. The following storage options are available:

Temporary storage Logs stored in the temporary storage location are written to RAM within the DataFort 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 DataFort appliance configuration database.

Remote storage The DataFort 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 DataFort appliance appends a signature to the exported log message.

Table 32: Default Log Storage Locations

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

Log Presentation

- Temporary Logs
- Database Logs
- Remote Logs

Temporary Logs

The administrator may view log messages stored in RAM by issuing the **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 outputted log messages include:

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

Database Logs

The administrator may view log messages stored in the database using either the CLI interface, or the WebUI interface.

- Viewing database logs via CLI
- Viewing database logs via WebUI

Viewing database logs via CLI

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

Log messages are listed in the following format:

```
<SEQ> <DATE> <CAT> <MESG>
```

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

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

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

- <16.[4,3,2,1,0]>: High priority Security Log
- <16.[7,6]>: Low priority Security Log
- <17.[1,0]>: Operations 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 Prioirty Security Log.
- -<19.6> Low Priority security log. <19.*> is different from <16.*> messages in that the <19.*> messages are also available in CC mode.

<MESG> is the log message.

Viewing database logs via WebUI

The administrator may view log messages stored in the database from the **System Info > Log** pane of the DataFort WebUI.

All outputted log messages include:

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

Remote Logs

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

```
<PRI> <TIME> ' ' <MESG>
```

<PRI> contains a syslog facility and severity indication as specified in the syslog RFC. DataFort logs map to syslog facilities and severities.

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

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

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

```
<134>Mar  4 13 :49:36 boxmanager: Administrator WebUI login
from 10.10.10.10 succeeded 'admin' (sess id: 298053632)
```

Table 33: DataFort event and priority correspondence to syslog facility and severity

DataFort 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

TABLE 33: DATAFORT EVENT AND PRIORITY CORRESPONDENCE TO SYSLOG FACILITY AND SEVERITY

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

The administrator may configure the DataFort to sign log messages. See Configuring and Viewing Logs on page 152 for information. The configuration option is available separately for each DataFort log. If configured, metadata and signature fields are appended to the exported log message:

```
<PRI> <TIME> ' ' <MESG> '[' <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 DataFort log. The global sequence number is the message sequence number with respect to all DataFort generated logs. Note that the DataFort maintains sequence numbers across power cycles.

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

```
<MESG> ' [' <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

DataFort 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

DataFort 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 34: Space allowances for temporarily stored DataFort log message

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

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

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.

Audit Configuration

The DataFort audit function may be configured using either the WebUI or the WebCLI.

- WebUI audit configuration
- WebCLI audit configuration

WebUI audit configuration

WebUI configuration of the audit function is performed using the **General > Configure Log Pane** pane of the WebUI.

WebCLI audit configuration

CLI configuration of the audit function is performed by setting the logging system properties.

Table 35: Audit configuration database properties

Property	Log association
sys.proc.syslogd.conf.sec_major	High Priority Security Log
sys.proc.syslogd.conf.sec_minor	Low Priority Security Log
sys.proc.syslogd.conf.op_error	Operations Alert Log
sys.proc.syslogd.conf.op_warning	Operations Warning Log
sys.proc.syslogd.conf.op_info	Operations Informational Log
sys.proc.syslogd.conf.op_trace	Operations Debug Log
sys.proc.syslogd.conf.perf_major	High priority performance log
sys.proc.syslogd.conf.perf_minor	Low priority performance log

The syntax for syslogd properties specifies a comma separated list. The maximum number of destination parameters that may be specified is 4 (this does not include the “sign” parameter). If additional parameters are specified, the input is considered invalid and the audit configuration will not be changed.

Table 36: Audit function WebCLI configuration list parameters

Audit function configuration list parameter	Description
!db	If present in the comma separated list, logs of this type will use the database storage location.
@<hostname>	If present in the comma separated list, logs of this type will be forwarded to a remote syslog host, as indicated by the <hostname> parameter. Note, the DataFort will resolve hostnames before allowing the configuration change to occur. Multiple hosts may be specified in separate comma separated list entries.

TABLE 36: AUDIT FUNCTION WEBCLI CONFIGURATION LIST PARAMETERS (CONTINUED)

$<filepath>	If present in the comma separated list, logs of this type will be stored to a temporary file in a ram based file system. Valid options for <filepath> include: • /var/log/security • /var/log/operation • /var/log/performance • /var/log/audit (E-Series product only) If a configuration is specified using a filepath not in the previous list, the audit function configuration will not be changed. Note that any of the previous filepaths may be specified for any syslog property.
sign	If present in the comma separated list, logs of this type will be signed by the DataFort, before export to a remote syslog host. The parameter has no effect on the audit function if no remote hosts are specified. Specifying the sign parameter with no log storage destinations is not a valid input, and the audit configuration will not be changed.
disabled	If present in the comma separated list, logs of this type will be disabled. Specifying the disable option with any other parameters is not a valid input, and the audit configuration will not be changed.

Appendix III Port IDs

The FC-Series DataFort 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	DataFort 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	WebUI, WebCLI, 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

- Mgmt/Client, Storage means DataFort 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
	Web browser	Microsoft Internet Explorer 6.0 or greater for Windows 2000/Windows Server 2003/Windows XP
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

- DataFort FC520 Specifications
- DataFort FC525 Specifications
- DataFort FC1020 Specifications

Table 3: DataFort FC520 Specifications

Item	Detail	Specification
Hardware	Rack mountable	Standard 19" EIA rack (2U height)
	Weight	12.8 kg (28.3 lbs)
	Size	43.2 cm (17") W x 48.2 cm (19") D x 8.9 cm (3.5") H
	Security	SEP FIPS Level 3 Physical Security, Tamper Evident Label, Intrusion Detection Circuit
	Network Ports	2 FC HBAs for storage network connectivity
	Management Port	1 10/100/1000Base-T Ethernet port
	Serial Port	RJ45 serial console port
	Power Supply	Two, Redundant / Hot-Swappable / Universal Input 100-240V ~47-63 Hz, 5A
	LED	Power status, network activity
	LCD	Liquid Crystal display with touch-panel capability
	Smart Card	1 internal smart card reader
Environment	Temperature	Operating Temperature: 5°C to 40°C (41°F-104°F) Storage Temperature: -10°C to 60°C (14°F-140°F)
	Humidity	Operating Humidity: 85% RH at 40°C
Regulatory Compliance	EMC	United States FCC Class B Canada ICES-003 Class B Japan VCCI Class A Korea RRL Class B EU Community CE (EN55022 Class B, EN55024, EN61000-3-2 Class A, & EN61000-3-3) Australia/New Zealand AS/NZS 3548 Class B China CCC Taiwan BSMI International IEC 60950-1
	Safety	United States UL 60950-1 Canada CSA 60950-1 Japan IEC 60950-1 EU Community EN6095, TUVR 2845 China CCC International CB: IEC 60950-1

TABLE 4: DATAFORT FC525 SPECIFICATIONS

Item	Detail	Specification
Hardware	Rack mountable	Standard 19" EIA rack (1U height)
	Weight	10.4 kg (22.9 lbs)
	Size	43.2 cm (17.00") W x 4.4 cm (1.73") H x 53.3 cm (21.0") D
	Security	Chassis: Pick-resistant Medeco lock, intrusion detection
	Network Ports	1 Dual Port HBA for storage network connectivity
	Management Port	1 10/100/1000Base-T Ethernet port
	Serial Port	RJ45 serial console port
	Power Supply	Universal: 100-240V/3A, 50/60 Hz
	LED	Power Status
	LCD	Character Display, 20 Characters by 2 Lines
	Smart Card	1 internal 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 35°C
Regulatory Compliance	EMC	United States FCC Class B Canada ICES-003 Class B Japan VCCI Class A Korea RRL Class B EU Community CE (EN55022 Class B, EN55024, EN61000-3-2 Class A, & EN61000-3-3) Australia/New Zealand AS/NZS 3548 Class B China CCC Taiwan BSMI International IEC 60950-1
	Safety	United States UL 60950-1 Canada CSA 60950-1 Japan IEC 60950-1 EU Community EN6095, TUVR 2845 China CCC International CB: IEC 60950-1

TABLE 5: DATAFORT FC1020 SPECIFICATIONS

Item	Detail	Specification
Hardware	Rack mountable	Standard 19" EIA rack (2U height)
	Weight	34.3 lbs (15.6 kg)
	Size	43.2 cm (17.00") W x 8.8 cm (3.46") H x 53.2 cm (20.95") D
	Security	Chassis: Pick-resistant Medeco lock, intrusion detection
	Network Ports	10 FC HBAs for storage network connectivity
	Management Port	1 10/100/1000Base-T Ethernet port
	Serial Port	RJ45 serial console port
	Power Supply	2 Universal: 100-240V/6A, 50/60 Hz, Hot swappable
	LED	Power status, network activity
	LCD	Liquid Crystal display with touch-panel capability
	Smart Card	1 internal smart card reader
Environment	Temperature	Operating Temperature: 5°C to 40°C (41°F-104°F) Storage Temperature: -10°C to 60°C (14°F-140°F)
	Humidity	Operating Humidity: 85% RH at 35°C
Regulatory Compliance	EMC	Canada ICES-003 Class B United States FCC Class B Japan VCCI Class B 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 International CISPR 22 Class B
	Safety	Canada CSA 60950 United States UL 60950 Japan IEC60950 A4 European Community EN60950, TUV International IEC 60950

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

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

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

European Union

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

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

CANADIAN ICES-003

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

Cet appareil numerique de la classe A respecte toutee les exigences du Regiements sur le material brouilleur du Canada.

VCCI Class A Statement

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.

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

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:

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

The following harmonized standards have been applied

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

Appendix VII 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 devices, total system redundancy is increased, decreasing the probability 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.

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

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 via the DataFort WebUI.

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 deployed DataFort appliances.
smart cards	Credit card-sized devices with embedded microchips used by DataFort for authentication procedures.
SNMP	Simple Network Management Protocol. A protocol for network management and monitoring of network devices.
SSH	Secure Shell or Secure Socket Shell. A command interface and protocol used for remote access to a computer. SSH communication with the remote computer is encrypted.
SSL	Secure Sockets Layer. A protocol providing secure message transfer over the Internet. Used to secure transmission of data via web browsers.
Storage Encryption Processor (SEP)	DataFort's hardware encryption/decryption engine, which enables gigabit-speed, full duplex encryption.
System Card	A smart card provided by Decru which inserted at the front panel of DataFort for boot-up to enable DataFort encryption services. The System Card may be removed during normal operation to prevent unauthorized use of DataFort upon reboot.
Trustee	A trustee is a remote DataFort with which a trust relationship has been formed, allowing exportable Cryptainer Keys to be shared. A trustee may import from or export to a trustee.
Trustee Acceptance Package (TAP)	The second message between DataFort 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 120
ACL Learning 119
Active IO limit per appliance 23
Adding and Removing Cluster Members 166
Admin Card 18, 19, 269
  associate with administrator 87
administrator 19, 269
  add 85
  associate card 87
  associate with Admin Card 87
  change password 89
  change the card association 90
  delete profile 90
  dual authorization, login 74
  login to CLI 75
  login to WebUI 72
  new 92
  number recommended 85
  require login authorization 88
  roles outlined 83
  Security Administrator 127, 144, 150
  specialty administrator, create 86
administrator roles 83
administrator roles, CLI 201
AES 16, 269
alert, clearing 137
appending ciphertext 117
appending cleartext 117
ARP table 205
associate Admin Card with administrator 87
Atape 235
authentication 18, 269
authorization for login 88
authorizing administrator 88
Auto-detected pools 120

B

backup
  DataFort configuration 27, 144
  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 269

C

Category 5 cable 20, 47
certificates
  Management Station to DataFort 175
certificates lost after zeroization 158
change password
  administrator 89
change password, Recovery Card 142
changing media type 213
chassis 17, 269
  intrusion 135
ciphertext 16, 269
ciphertext and cleartext 25, 103, 269
CLARiiON 226
clear all DataFort settings 158
clear an intrusion (defense alert) 137
clear smart cards 143
cleartext 16, 103, 111, 121, 269
cleartext Cryptainer 103
cleartext pools 121
cleartext tape 29
CLI 75
  command help 200, 238
  commands and admin roles 201
  connect from SSH client 75
  disk management 206
  general information 200, 238
  help 242
  host management 208
  login 75
  permissions 199
  Quick Reference 237
  quit 242
  system commands 203, 244
  time-out 238

top level commands 239
turn off Secure Web 219
WebUI access 77
CLI documentation 200, 238
CLI login with dual authentication 76
cluster 269
change to standalone 166
commands, CLI 244
forming, after initial setup 166
IPsec tunnel 26
management 162
management using CLI 202
network diagram 29, 32
recovery guidelines 168
remove member 166
replace an offline member 166
requirements 166
resolving conflict 165
restore previous configuration 168
state 164, 165
state after wizard 92
switch connections, planning 26
cluster configuration 26
cluster conflict 165
cluster disable command 202, 220, 225
cluster quorum 166, 202
cluster size 162
cluster troubleshooting 220, 225
cluster-wide operations 164
Common Criteria 16
configurable security levels 139
configuration database 18, 270
applied to new DataFort 215
backup to LKM 94, 145
backup using WebUI 149
changes synchronized in cluster 26
commands, CLI 244
contents 144
event log capacity 152
purging unused keys after backup 147
size 148
used for recovery 215
create a Cryptainer 113, 114
Cross Mapping 107, 108, 110, 111, 114, 117
Cryptainer 270
before creating 91
defined 17
management with WebUI 110
management, with WebUI 112
rekey with CLI 210
restore 126
Cryptainer collections 96
Cryptainer creation and management 96
Cryptainer creation, with WebUI 96
Cryptainer encryption after creation 103
Cryptainer encryption key 17
Cryptainer ID 112, 126, 206, 211
Cryptainer Key ID 115
Cryptainer Management Menu 110
Cryptainer management with CLI 209
Cryptainer Management with WebUI 112
Crypto Copy 207
Crypto Copy with CLI 207
Crypto Copy with WebUI 115
cryptographic test 185
CryptoShred 17, 138
CryptoShred button 17, 135, 136, 137
states 137

D

data
encryption 17
data size when encrypted 16
DataFort
administrators 184
assigning IP settings 48
capacity 23
CLI, connecting to 75
cluster 26
Defense Setting 135
emergency shutdown 138
in SAN 29
licenses 60, 180
recovery 215
Recovery Officers 184
restoring a previous configuration 215
specifications 259
troubleshooting 214
upgrading 174
users 19
WebUI, connecting to 72
where installed 16, 29
zeroizing 158
DataFort CD-ROM 20
DataFort CLI 75, 270
login 75

DataFort CLI Reference Guide 199, 237
DataFort HBAs 259, 260, 261
DataFort hostname limitations 36
DataFort media type 213
DataFort Throughput 184
DataFort WebUI 72, 270
  login 72
DCS
  administrator roles 201
Decru licenses 60, 180
Decru Management Console 19, 186
  menus 186
Decru MIB 81, 181
Decru Signed Syslogd (DSS) 152
defense
  alert, clearing 137
  response 135
  triggers 135
Defense Setting
  changing after setup 135
  summary 135
defense setting 28, 135
deleted Cryptainer
  purge unused keys 147
  restoration 126
disabling a cluster member 202
disk
  management with CLI 206
  management with WebUI 113
  rescan 206
DMC 19, 186
documentation 20
dual authentication login, CLI 76
dual authentication login, WebUI 74
dual authorization 74, 76, 88

E

EMC 226
emergency shutdown 138
emergency zeroization via serial console 160
Enabling SNMP 181
enabling TLS 37
encryption 16
escrow service 27
Ethernet cable 20
event logs 152
exportable key 100, 115

F

failover 26, 269, 270
fan modules, replacing 222
FC Site settings 58, 59, 66
FC switch
  in network diagram 29, 32
feature licenses 60
Fibre Channel 15, 29
Fibre channel cables 20
Fibre channel switch ports 20
front panel
  display 80
  LCD used to assign IP address 48
  LED 216
  System Card slot 44
Front Panel Dual LEDs - 2U 216
Front Panel LEDs - 1U 216
full database 148

G

Global Default Pool 121
grant host access to Cryptainer
  CLI 210

H

hardware maintenance 222
HBA (host bus adapter)
  Host HBA, connecting to FC network 46
  Hosts 25
  Storage 25, 46
Home page
  returning to 72
Host Default Pools 121
Host HBA
  interface for unencrypted data 46
Host Icons 107
Host Management Menu 107
Host Virtualization enabled 124
Host Virtualization with CLI 208
hostname limits for DataFort 36
Hosts
  managing with CLI 208
  Managing with WebUI 107
  supported platforms 258

I

Icon Legend 105, 106, 107, 110, 113, 116
Icons

host 107
installation
in rack 42
planning 25
precautions v, 43
requirements 20
International Organization for Standardization (ISO) 178, 262
Internet Explorer 258
for accessing WebUI 72
intrusion detection 135, 137
IO limit 23
IP address 20
DataFort, assigning 48
DataFort, current 184
preserve during zeroization 159
IP settings
assigning from LCD 48
assigning from serial console 79
changing, with WebUI 173
DataFort, assigning from serial console 49
IPsec 26, 270
ISO 262
IT power systems iv, 41

J

JBOD 206, 208, 270

K

key 270
encryption key 17
escrow 27
Key Purging 145
key, chassis 135

L

LCD 80, 185
assigning DataFort IP settings 48
bar graph 80
buttons 80
touch panel interface 70
web page 185
LED 216
LEDs
power supply 217
legacy cleartext tape 29
licenses 20, 180
managing 180
lifespan of tape keys 118, 121
Lifetime Key Management (LKM) 17, 270
limited administrator 88
Limits
Cryptainers on the primary port 23
LUNs on a single device 23
Non virtualized hosts 23
Number of DataFort appliances in a cluster 23
Virtual devices per DataFort 23
Virtual hosts per DataFort 23
Lithium battery v, 41
LKM 27, 145
server saves latest configuration backup 27
server, specifying settings in WebUI 94, 145
LKM appliance setup 39, 94
LKM servers
number supported 145
LKM software setup 39
LKM using SSL 146
login
CLI 75
CLI, dual authorization 76
requiring authorization 88
WebUI 74
WebUI, dual authorization 74
logs, DataFort 152
configuring storage location 153
Decru Signed Syslogd (DSS) 152
filtering 156, 184
guidelines 152
syslog mapping table 155
temporary file mapping 156
viewing, with WebUI 156
Loop ID 211
lost Recovery Card 140
LUN Mapping 23, 100, 104, 113, 114

M

Manage Tapes 116
Management Console installation 38
Management Port
connecting to Ethernet network 46
Management Station 18, 270
Management Console installer 38
requirements 258
Management Station requirements 37
Management Station security 37

manual assignment of keys 212
map a Cryptainer with WebUI 114
mapping a device 207
mapping a device with CLI 207
Master Key 17, 271
media type 213
metadata 152
MetaTool 228
MIB 81, 181, 271
mixed-mode tape mode 123
mounting DataFort in rack 42
Multi ID 124, 125
Multi ID mode 125
  non NL-ports 124
multi-appliance management 186
multiple DataFort appliances in cluster 26

N

NAS 15
network
  connection to DataFort ports 44
  diagram, SAN 25, 29, 32
  information needed for setup 36
  manage, with CLI 205
  planning backup and restore 33
  settings, changing 173
Network Attached Storage (NAS) 15
network commands, CLI 205
Network switch ports 20
NL-Port 124
NTP time server 20

O

online help 71, 198

P

Parent Key 17
password
  administrator, changing 89
  one-time, CLI 75
  Recovery Card, changing 142
Password and Label Limitations 62
pool display 116
pools and tapes 120
  settings 120
port
  FC ports 46
  Management 46
Port Lock 109
port locking
  switches supported 108, 109
Port Mapping 23, 100, 104, 113, 114, 271
power
  precautions iv, 41
power button 50
power cord 20
power down DataFort 50
power supply
  LEDs 217
  notice iv, 41
  replaceable 222
powering down 50
powering up 50
protect against insider attacks 88
purging encryption keys 148
purging keys 147

Q

quorum 19, 27, 140, 141, 143, 220, 225, 271

R

rack installation 42
rack mounting kit 20
RAID Admin 109
Recovery Card lost 140
Recovery Card replacement 140
Recovery Cards 18, 140, 271
  change password 142
  replacement procedure 140
Recovery Officers 19, 271
  required for forming cluster 168
  required for replacing DataFort 167, 215
  required for replacing Recovery Card 128, 140
  required for Setup 52
Rekeying a Cryptainer
  CLI 210
Remote Desktop 72, 219
remove all host access to a Cryptainer
  CLI 210
Removing a Cryptainer
  CLI 210
replacing a Recovery Card 140
replacing an offline cluster member 166
requiring login authorization 88
reset DataFort 158

reset smart cards 143
reset System Card 221
restore a Cryptainer 126
restore a deleted Cryptainer. 115
restore a previous DataFort configuration 215
restore, planning 33
RJ45 to DB9 adapter 20, 47

S

SAN 15
  network diagram 25, 29, 32
  supported hosts and storage devices 258
SAN Storage Settings 124
SAN Topology page 96, 105
secret share 271
Secure CLI 71, 139
  login 75
Secure Web 71, 72, 139
  turn on and off via CLI 219
SecureView 19, 70
Security Administrator 127, 144, 150
Security Certificate 175
  Certificate Authority Signed, installing 177
  self-signed, installing 175
Security Domain 19, 272
  planning 25
Security Policy
  planning 27
Security Settings 139
security, implementing and maintaining 25
Sensors 185
SEP 17, 185, 272
serial console 79
  assigning DataFort IP settings 49
  clearing IP Settings 79
  connecting serial port 46, 79
  emergency access 160
  menu options 79
  zeroizing DataFort 79
serial number 185
servicing DataFort 222
shutting down 50
Single ID 124, 125
Single ID mode 124, 125
size of data when encrypted 16
size of the configuration database 148
smart card reader 18, 20
Smart Card Reset 143, 152
smart cards 20, 272
  checking versions and status 143
  reset procedure 143
  summary 18
  troubleshooting 221
SNMP 181, 272
  MIBs 181
  setting with WebUI 182
  turning on and off 181
  version 182
software CD-ROM 20
Solaris 228
specialized administrators 83
specifications 257
SSH 70, 272
  CLI access 75, 76, 200
SSL 146, 272
stack trace 205
Standard CLI 75
standard rack mount 42
status and settings 183
Storage Area Network (SAN) 15
storage device collection 98
storage devices 258
Storage Diagnostics 184
Storage Encryption Processor (SEP) 17
Storage HBA
  connecting to FC network 46
  interface for encrypted data 46
Storage Management Menu 113
storage management with CLI 206
supported platforms 258
switch connections in a cluster 26
Symmetrix 226
syslog, syslogd (syslog daemon) 152, 155
System Card 18, 272
  inserting 44
  removing, in emergency 138
  resetting 221
System Config menu (WebUI)
  General, Upgrade 174
  Network, IP Settings 173
  Network, SNMP Agent 182
  Recovery, Backup 149
  Recovery, Replace Recovery Card 140
  Security, Zeroize 159
  System Users 184
  System Users, Administrators 92

view settings 184
System Info menu (WebUI)
Status 185
Status, Log 156, 184
system properties, CLI 203
System Requirements 258
system users 184

T

TAP 128, 197
tape key 118, 121
deletion 118, 121
expiration 118, 121
lifespan 118, 121
tape pool types 120
Tape Settings
access from ACL Learning link 119
access from Tape Management page 116
tapes
manage with WebUI 116
ten port DataFort 162
ten port DataFort rear panel 46
TEP 128, 197
Terminal Services 72, 219
time and date
setting from WebUI 151
time servers 151
time-out
CLI 75
serial session 79
WebUI 72
trap 182
troubleshooting 214
network connections 218
smart cards 221
trustee 115
Trustee Acceptance Package 128, 197
Trustee Establishment Package 128, 197
Trustees 128
types of keys recovered during a restore 158

U

updating hosts in a Microsoft operating system 25
upgrading DataFort 174
USB 20

V

Verifying System Logs 204
Veritas 230
virtualization settings 124
Multi ID 125
Single ID 125
virtualize a host, CLI 208

W

WAN 26
WebCLI 77
WebUI
accessing 72
device grouping 105
device information pane 105
keyboard shortcuts 73
login 72
login with Secure Web 72
multiple device selection 105
required display setting 72
right-click menus 96
time-out 72
WebUI access to cluster members 164
WebUI login with dual authentication 74
Windows event logging 154
Windows Event Viewer 154
WWN configuration 58, 59, 66
WWNs
assigning an override setting 58, 59, 66

Z

zeroization without admin card 160
zeroizing DataFort 158
using serial console 160
using WebUI or CLI 159
zones 46