

DECRU®



■ ■ ■ **ADMINISTRATION GUIDE**

DataFort FC-Series
Version 2.1

security

DataFort Administration Guide for S-Series DataFort

Copyright © 2003-2006 Decru, Inc. All rights reserved.

Part number: 30-000282 A0 (v. 020206_FC2.1))

Model Numbers: FC520, FC525, FC1020

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

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/>)."

TRADEMARK NOTICE

Decru®, Decru DataFort™, Cryptainer™, CryptoShred™, Lifetime Key Management™ software, 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.

LASER WARNING

Warning: Class 1 Laser product.

Attention : Produit laser de classe 1

Warnung: Laserprodukt der Klasse 1

FCC DECLARATION OF CONFORMITY

NAME AND MODEL NUMBER:	Decru DataFort Model FC520, FC525, FC1020
RESPONSIBLE PARTY (IN USA):	Decru, Inc.
ADDRESS:	275 Shoreline Drive, Suite 450, Redwood City, CA 94065
TELEPHONE:	650-413-6700

INSTRUCTION TO THE USER

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.

POWER SUPPLY NOTICE

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



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

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

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

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

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

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

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

OPPMERKSAMHET: Apparatet må kun tilkoples jordet stikkontakt.

POWER SUPPLY NOTICE FOR 2U DATAFORT



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

Note to 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 usages 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.



CONTENTS

Chapter 1 Introduction	12
About the Decru DataFort Security Appliance	12
DataFort Feature Licenses	12
Components of the Decru Security System	13
Encryption	13
Common Criteria Compliance	13
Hardened Architecture	13
CryptoShred Feature	13
Compartmentalization of Functions	14
Key Management	14
Lifetime Key Management Software	14
Configuration Database	14
Authentication Layers	14
DataFort Users	15
Security Domain	15
Installation Requirements	16
Conventions Used in this Manual	17
Chapter 2 Planning the Network Configuration	18
Planning the Security Domain	18
Decru DataFort Capacity	18
Installation Considerations	19
Failover Support in a Cluster	19
IPsec in a Cluster	19
Switch Connections in a Cluster	20
Updating Devices	20
Secure Network Practices	20
Maintaining Configuration Database Backups	20
Sending Recovery Cards to Escrow	20
Planning Remote Security Logging	21
Removing the System Card	21
Recommended Network Configurations	22
Planning Data Backup and Restoration	26
Backup Methods	26
Chapter 3 DataFort Initialization	28
Collecting Network Information	28
Completing Network Preparation	29
Preparing the Management Station	29
Setting Up the Lifetime Key Management Server	30
Management Interfaces	31

Contents

Installing Decru DataFort Appliances	32
Selecting a Location	32
Rack Mounting	32
Connecting the Decru DataFort	34
System Card Insertion	34
Rear Panel Network Connections	34
Power Connection	37
Assigning the DataFort IP Address	37
Setting the IP Address Using the LCD	37
Setting the IP Address Using the Serial Console	39
Running the Setup Wizard	40
Start the Wizard	40
Connect to Head of Cluster	41
Sign License Agreement	42
Recover From Database	43
Create Administrator	44
Configure Cluster Recovery Schema	45
Introduce Cluster Members	47
Add Licenses	49
Network and Certificates	50
Add Recovery Card	51
Apply Settings	54
Complete Wizard	56
Logging into DataFort	57
Before Creating Cryptainers	59
Checking Cluster State	59
Configuring Remote Logging	59
Starting LKM	60
Configuring Tape Settings	60
Creating Additional Administrators	60
Verifying System Version	60
Determining the Defense Setting	60
Restoring a DataFort	61
Chapter 4 DataFort Administration	62
Administrator Roles	62
Account Administration	64
Adding an Administrator	64
Requiring Authorization for Login	67
Changing the Administrator Password	68
Removing an Administrator	69
Changing a Card Association	69
DataFort Management Interfaces	70
Connecting to the DataFort WebUI	70
Connecting to the DataFort Command Line Interface	72

Contents

DataFort Front Panel LCD	74
Serial Console	75
DataFort Settings and Status	77
Viewing Settings in the WebUI	77
Security Preparedness and Response	79
Automatic and Manual Responses	79
Restoring Data and Normal Operation	79
Powering Up and Shutting Down	80
Chapter 5 Storage Administration	81
Cryptainer Creation	81
Cryptainer Creation Using Collections	81
Cryptainer Creation Without Collections	89
SAN Topology Page	90
DataFort WebUI Icons	91
Host Management	92
Host Collection Menu	92
Host Menu	93
Edit Host Page	94
Cryptainer Management	95
Cryptainer Collection Menu	95
Cryptainer Menu	96
Edit Cryptainer Page	97
Storage Management	98
Storage Collection Menu	98
Storage Device Menu	99
LUN Menu	99
Tape Menu	101
Tape Management	102
Tape Pool Collection Menu	102
Tape Pool Menu	103
Tape Device Menu	103
Edit Pool Page	104
ACL Learning	105
Managing Tape Settings	105
Pool Settings and Defaults	106
Tape Settings	106
Managing SAN Storage Settings	107
Virtualization Settings	107
Setting Single or Multi ID Mode	107
Restoring a Cryptainer	109
Chapter 6 Key Administration	110
Managing Trustees	110

Trustee Scenarios	110
Setting Up Trustees	111
Importing and Exporting Keys	117
Configuring Management Security Settings	118
Setting Security Certificates	119
Setting a Local Security Certificate	119
Setting a Certificate Authority Signed Certificate	122
Managing Licenses	124
Managing Recovery Officers and Recovery Cards	125
Replacing a Recovery Card	125
Changing a Recovery Card Password	127
Smart Card Reset	128
Chapter 7 Backup Administration	129
Saving Configurations to Lifetime Key Management Software	129
Configuring Backups to LKM	129
Backing Up the Configuration to LKM	130
Key Purging	131
Downloading Configurations to a Remote Location	133
Chapter 8 Physical Security Administration	134
Managing DataFort Defense Responses	134
Defense Triggers and Responses	134
DataFort Defense Setting	135
Changing the Defense Setting	135
Clearing a Defense Alert	136
CryptoShred Button States	137
System Card CryptoShred	137
Configuring and Viewing Logs	138
DataFort Log Storage Guidelines	138
Decru Signed Syslogd (DSS)	138
Configuring Log Storage	139
Windows Event Logging	140
Setting Up Syslog	141
Viewing the Log	142
Verifying Signed Log Messages	143
Zeroizing the Decru DataFort	144
Zeroizing After Setup	144
Zeroization Using the DataFort WebUI	144
Zeroization Using the CLI	145
Zeroization Using the Serial Console	146
Chapter 9 Cluster Administration	147
Cluster Management	147
Maintaining the Cluster Quorum	147
Cluster-Wide Management via WebUI	148
Checking the Cluster State	148

Contents

Adding and Removing Cluster Members	150
Changing the IP Address of a Clustered DataFort	151
Replacing a DataFort in a Cluster	151
Recovering a Cluster	152
Resolving a Cluster Conflict	152
Chapter 10 Machine Administration	154
System Configuration	154
Date and Time	154
Network Settings	154
SNMP Settings	154
Upgrading DataFort	155
Chapter 11 CLI Administration	156
Using the CLI	156
Connecting to the CLI	156
CLI Help	156
Administration Commands	157
Administrator Roles	157
Cluster Management	158
System Properties and Log Management	159
Verifying System Logs	160
Stack Trace Settings	161
Network Management	161
Backup Management	161
Storage Management Commands	162
Disk Commands	162
Host Commands	164
Cryptainer Commands	165
Turning on Metadata Support	167
Fibre Channel Kernel Commands	167
Chapter 12 Troubleshooting	168
Front Panel LEDs	168
Hardware Issues	169
Network Connections and Management Interfaces	169
Smart Cards	172
Storage Network	173
Clusters	174
Decru DataFort Operation with EMC	175
Symmetrix	175
CLARiiON	175
Decru DataFort Operation with Linux	176
Multiple LUNs	176

Contents

Failover	176
Resync Speed	176
Decru DataFort Operation with Solaris	177
Migrating MetaTool Volumes to a DataFort	177
Veritas Volume Manager	179
Decru DataFort Operation with Legacy Encrypted Tapes	180
Decru DataFort Operation with Tivoli and STK Drives	180
Decru DataFort Operation with LT02 Serialized Commands	180
Appendix I Command Line Interface Quick Reference	181
Using the CLI	181
CLI Syntax	181
CLI Help	181
CLI Command Overview	182
Top Level Commands	182
Device Commands	182
Disk Commands	183
FC Site Commands	183
FCC Cryptainer Commands	183
Host Commands	184
KFC Commands	184
Pool Commands	184
Tape Commands	185
CLI Formatting Commands	185
Help Command	185
Quit Command	185
Active-Role Commands	185
Authorize Command	185
Password Command	185
Role Commands	186
User Commands	186
Whoami Command	186
Trustee Commands	186
Network Commands	186
Key Management Commands	186
LKM Management Commands	187
Cluster Commands	187
Database Commands	187
System Commands	187
Appendix II Specifications	189
Supported Systems	189
Specifications	190

Contents

Appendix III Partial List of ISO Country Codes	193
Appendix IV Glossary	194
Index	198

■ ■ ■ ■ 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 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.

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 the web-based management interface (the DataFort WebUI). All key security administration tasks, including those necessary to manage cluster members, can be accessed from a single workstation.

DATAFORT FEATURE LICENSES

The FC-Series DataFort is licensed for use in environments with disk and/or tape storage. Disk features will not be available to customers with DataFort appliances licensed only for tape and vice versa. DataFort appliances with licenses for both disk and tape will allow access to all features. Clustering is also controlled by licenses issued by Decru for each DataFort appliance, or each customer site.

COMPONENTS OF THE DECRU SECURITY SYSTEM

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

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 during the encryption process. 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 is a Common Criteria EAL 4+ product. 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 the Decru support website.

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. The pick-resistant lock on the chassis is intended to keep the DataFort closed at all times. Whenever a DataFort management interface is accessed, tamper status is checked. DataFort can be configured to respond to a detected intrusion in a number of ways.

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).

Cryptainers are managed by DataFort administrators, but DataFort separates the ability to manage stored data from the ability to read data from a storage device. This means an administrator does not necessarily have access to the data that they manage. 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 Domain Key, shared by the members of a DataFort cluster. The Domain 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 SOFTWARE

Decru's Lifetime Key Management (LKM) software stores encryption keys used by multiple DataFort appliances. This software 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. Three types of smart cards are shipped with every DataFort: the System Card, Admin Card and Recovery Cards.

System Card

Each DataFort has a unique System Card which is used 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).

Admin Card	The Admin Card is used to authenticate communication between the administrator and DataFort. After it has been configured, an Admin Card can be used to manage one DataFort appliance, a cluster, or multiple separate DataFort appliances, depending on company policy.
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 belongs to 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.
Management Station	Decru supplies a smart card reader and software which convert a Windows PC into a Management Station. This provides a dock for smart cards, including the Admin Card, which allows the PC to make a secure connection to DataFort and apply smart card authentication to DataFort management.

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 system. Other administrators can be created that are able to execute a more limited set of functions, targeting specific administration tasks. Every administrator is authenticated with a login name and password. Additionally, administrators can be authenticated 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. Administrator types are further described in this guide.
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.

SECURITY DOMAIN

Security Domains are defined by sets of Recovery Cards. The deployment of DataFort appliances and 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 recreate a DataFort Disaster Recovery Key and 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
- 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 Cards, Admin Cards and Recovery Cards
- USB smart card reader, or readers
- Decru product licenses
- Slide rail mounting kit including hardware and instructions (included in the DataFort package)
- DataFort Documentation and Software CD-ROM. The documentation and software CD contains software necessary for DataFort operation, such as the smart card reader driver.
- 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.
- 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. If using an NTP server for time synchronization, have the appropriate NTP time server information for each dedicated IP address to be used during installation.
- Recovery schema. Determine what the recovery schema will be for this DataFort or DataFort cluster. See [DataFort Initialization](#) for more information about this decision.

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 so that it is stored in encrypted form. When data is read, it is decrypted by DataFort before reaching 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 will also add a Management Station (for initial DataFort configuration and for ongoing administration tasks) and a Lifetime Key Management server to the Ethernet portion of the network. This chapter summarizes topics to consider when planning DataFort network installation.

- [Planning the Security Domain](#)
- [Decru DataFort Capacity](#)
- [Installation Considerations](#)
- [Secure Network Practices](#)
- [Planning Data Backup and Restoration](#)

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 that share 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.

DECRU DATAFORT CAPACITY

Before installing DataFort, review current and near-future 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 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 per DataFort	7	Each DataFort supports 7 virtual devices. The number of virtual devices a cluster can support is equal to 7 times the number of DataFort appliances in the cluster. You may have 7 virtual devices and 7 virtual hosts per DataFort.

TABLE 1: DATAFORT CAPACITY (CONTINUED)

Device	Number	Explanation
Virtual hosts per DataFort	7	Each DataFort supports 7 virtual hosts. The number of virtual hosts a cluster can support is equal to 7 times the number of DataFort appliances in the cluster. The total number of virtual devices and virtual hosts together per DataFort cannot exceed 7.
Non-virtualized hosts	32	32 non-virtualized hosts are supported per 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	255	Port Mapping (one Cryptainer per LUN). 255 Cryptainers are supported per virtualized storage device.
Cryptainers on the primary port	254	LUN Mapping (LUN 0 is reserved). 254 Cryptainers are supported per DataFort cluster, regardless of the number of DataFort appliances in the cluster.
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.

INSTALLATION CONSIDERATIONS

In order to encrypt data moving to storage, DataFort separates the network into a cleartext and a ciphertext portion. Hosts are connected to the cleartext side, while storage devices are connected to the ciphertext side. 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.

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 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 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.

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.

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, 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](#)

MAINTAINING CONFIGURATION DATABASE BACKUPS

For maximum security and recoverability, keep database backups up to date, and use Decru's Lifetime Key Management software to store encryption keys.

- Use DataFort functions to save frequent backups of the configuration database to a specified location. Retain at least three of the most recent configurations in a remote location.
- Configure DataFort to send backups to Decru's Lifetime Key Management (LKM) software.

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 Disaster Recovery Key Archives (created using Decru's Lifetime Key Management software). 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/availability trade-off when determining whether to leave the System Card inserted in a running DataFort.

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.

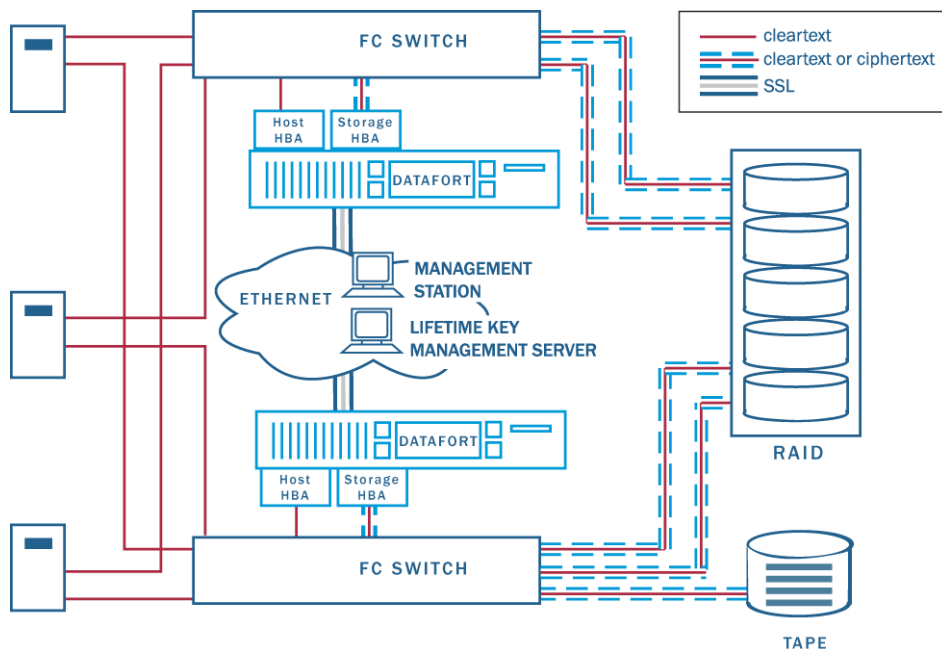


Figure 1: A DataFort cluster with two FC switches showing redundant paths

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.

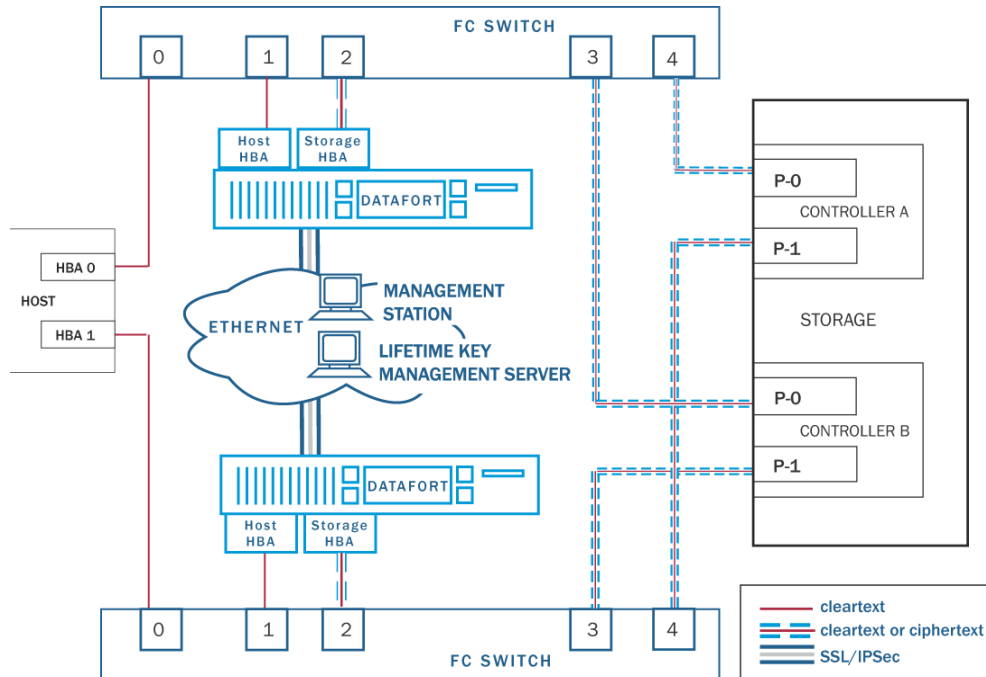


Figure 2: Fabric attached configuration

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.

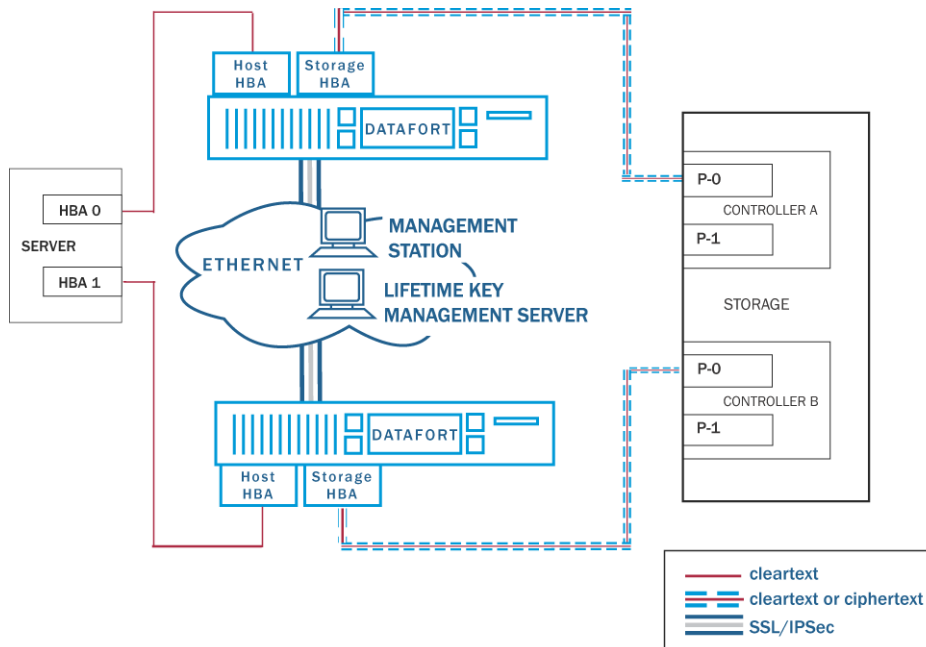


Figure 3: In-line configuration

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.

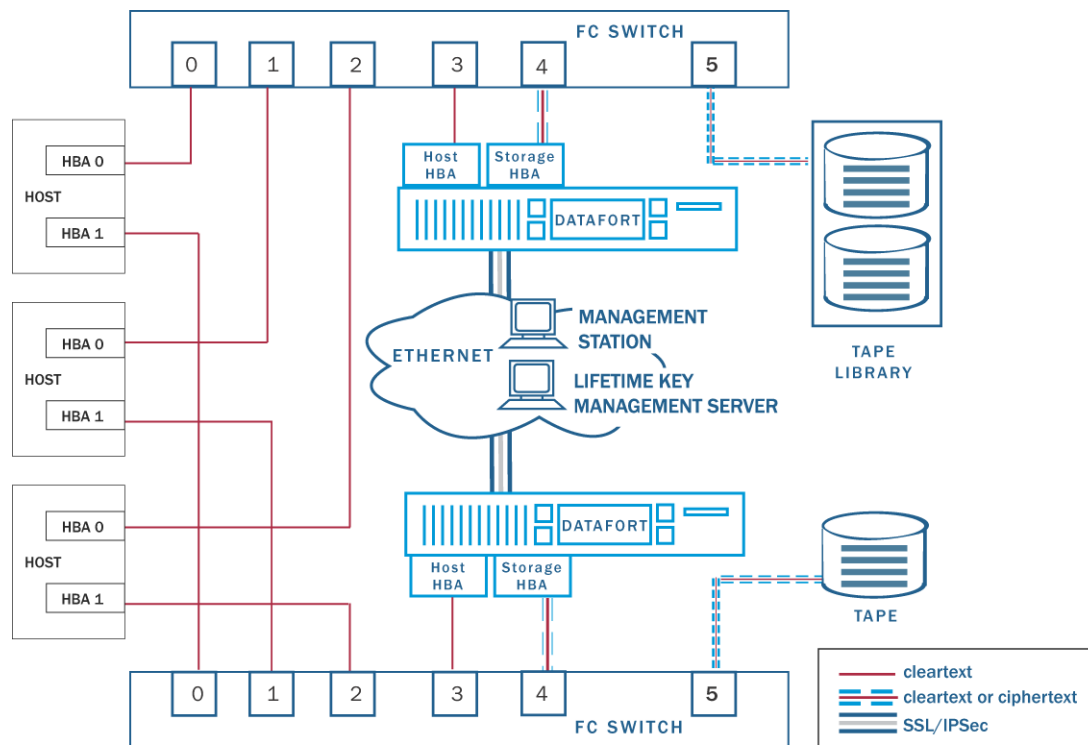


Figure 4: A DataFort cluster with two FC switches sending encrypted and cleartext data to tape

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 2: BACKUP METHODS

Backup Method	DataFort Solution
LAN-based — The data flows from the application server to the backup server by LAN. The backup server writes data to tape.	To encrypt backups, configure the network so that data flows from the backup server through DataFort to tape.
LAN-free by Client — The bulk of the data flow occurs between the application server and the tape library.	DataFort encrypts data as it is sent to tape.
Client-free — The bulk of the data flow is between the back-end disk array through the backup server and to the tape library. In this case the data server is freed from performing the backup.	If the primary data is not encrypted or there is no reason to prevent the backup server from reading cleartext, place DataFort between the backup server and tape. Data 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.

TABLE 2: BACKUP METHODS (CONTINUED)

Backup Method	DataFort Solution
Server-free — The bulk of the data flow goes directly from the disk array to the tape library. This topology is supported through the use of the SCSI extended copy command, or in some cases vendor proprietary features.	Server-free backup/restore technology is currently immature. This topology is supported through the use of the SCSI extended copy (xcopy) command, or similar vendor proprietary features. Currently DataFort does not support the xcopy SCSI command for Server-free environments. However, a backup server operating <i>behind</i> the DataFort can use xcopy to copy encrypted data from disk to tape. In this case too, the backup/restore operations are done at the block level.

SAN Mirroring

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



3 DATAFORT INITIALIZATION

This chapter provides background and instructions for installing a standalone or clustered DataFort for the first time. Initialization of a new DataFort appliance creates the first Full Administrator for that DataFort or DataFort cluster.

DataFort is initialized from the Management Station, and since this initial setup 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. Key operations necessary in order to get DataFort up and running include:

- [Collecting Network Information](#)
- [Completing Network Preparation](#)
- [Installing Decru DataFort Appliances](#)
- [Connecting the Decru DataFort](#)
- [Running the Setup Wizard](#)
- [Logging into DataFort](#)

It is recommended that necessary information about the network be collected before beginning DataFort installation, and that decisions about the data recovery setting and defense setting also be made in advance, according to your organization's security policy. Check [Installation Requirements](#) on page 16 before beginning installation.

COLLECTING NETWORK INFORMATION

It may be necessary for the DataFort administrator to gather information from other individuals before installing DataFort appliances. The following information is required:

Information Needed When [Running the Setup Wizard](#)

[DataFort IP Information](#) as determined when [Assigning the DataFort IP Address](#)

- IP address
- Subnet mask
- Gateway

[DataFort Network Information](#)

- Hostname for DataFort
- DNS suffix (if DNS is used)
- DNS server IP addresses (if DNS is used)
- Security Certificate information including country code (see [Partial List of ISO Country Codes](#))

[Cluster Member Information](#)

- IP addresses of all DataFort cluster members
- User-defined IPsec secret

- Purchased cluster licenses for all cluster members or customer site
- Data Recovery Setting, including number of cards needed for quorum and the names and passwords associated with those Recovery Cards

Information Needed When [Completing Network Preparation](#)

- Remote syslog server IP address
- Lifetime Key Management server IP address
- Names and roles of alternate and additional administrators

COMPLETING NETWORK PREPARATION

Before installing DataFort on the network, perform the following operations:

- [Preparing the Management Station](#)
- [Setting Up the Lifetime Key Management Server](#)

PREPARING THE MANAGEMENT STATION

DataFort setup and management require that smart cards from the provided set be inserted into the smart card reader installed on the Management Station. The DataFort Setup Wizard will be installed on the Management Station by running the installer from the DataFort CD.

Management Station Requirements

The Management Station must be a Windows PC with a CD drive and USB port. (If no USB port is available, a serial smart card reader is available from Decru.) The Management Station requires one of the following:

- Microsoft Windows 2000 Professional/Server
- Microsoft Windows XP
- Microsoft Windows Server 2003
- Microsoft Windows NT 4.0 (SP6a or greater)

With any of these operating systems, the DataFort WebUI requires Internet Explorer version 6.0 (SP1 recommended) or greater, and either Microsoft JVM or Sun JRE 1.4.2.08. The DataFort smart card reader installer installs Sun JRE 1.4.2.08.

A workstation running Unix and SSH (secure shell) can be used for some aspects of DataFort management. However, the Windows PC described above is still needed for essential DataFort management operations, including running the Setup Wizard used to configure a new DataFort.

Management Station Security

The Management Station should be current on security patches and have unnecessary services disabled or removed. Logons should be limited to authorized administrators, with no remote management enabled. The Management Station should not be used to browse untrusted websites or run unverified code. For password security, it is good practice not to set Internet Explorer to auto-fill or cache usernames and passwords.

Installing the Smart Card Reader and DataFort Setup Wizard

It is required that the installer be run on the Management Station before DataFort can be configured. This installer includes the driver for the smart card reader as well as the DataFort Setup Wizard. Use of the smart card reader and wizard are both required for initial setup of DataFort appliances.

1. Insert the provided DataFort CD-ROM into the CD drive of the selected Windows PC. The main index page of the CD will appear (if not, open the index.htm file on the CD).
2. Click the DataFort Installer link.
3. Read the installation instructions, then click the installer link. The installer will prompt for the model number of the smart card reader. This can be found by looking at the bottom of the smart card reader (for example, M/N: GemPC413-SL or GemPC USB-SL).
4. When prompted, connect the smart card reader to the Management Station.
5. Choose Yes when prompted to reboot the PC.

Note: This installer updates the configuration of the Sun JVM installation. If you install Sun JVM at a later time, it could cause the DataFort WebUI to stop functioning. To avoid this possibility, run the smart card installer again after you install Sun JVM.

SETTING UP THE LIFETIME KEY MANAGEMENT SERVER

Decru's Lifetime Key Management (LKM) software is designed to run on a network server, providing a solution for managing and archiving key information for multiple DataFort appliances. When set up to use LKM, DataFort sends updates to the designated LKM server automatically.

Before configuring DataFort, set up the LKM Server. Install LKM software on a designated server, using the installer and instructions on the DataFort CD. Make sure the server is up and its IP address is reachable from the Ethernet network. Instructions for enabling automatic updates to LKM are provided in [Chapter 7](#).

DataFort supports automated configuration backups to four LKM servers.

About the LKM Server

See the [LKM Administration Guide](#) for a complete list of requirements. Keep in mind the following:

- LKM software should not be run on the Management Station. The LKM server should be a separate, dedicated server.
- The LKM station must be dedicated to LKM use. No other process must be allowed to run on this station, as any hostile local processes may issue destructive commands to the server database.
- The LKM server should be assigned a static IP address that is reachable by the entire DataFort cluster at all times. All cluster members will use the same instance of LKM software.
- The LKM server should run Windows 2000 Server or Windows Server 2003 (recommended), or be a dedicated workstation running Windows 2000 or Windows XP.

MANAGEMENT INTERFACES

DataFort setup involves assigning network settings to the DataFort and then running the Setup Wizard. After initial setup is complete, a DataFort administrator uses a secure connection to the DataFort WebUI to complete configuration. The management interfaces available to the DataFort administrator are summarized in the following table.

TABLE 3: MANAGEMENT INTERFACES

Interface	Description	Usage
Secure Sockets Layer (SSL)	A secure HTTP (HTTPS) connection to the DataFort WebUI via a web browser running on the Management Station. Can be configured to require smart card authentication as well as the administrator password. See Connecting to the DataFort WebUI .	Primary method for creating and managing Cryptainers, DataFort settings, users, etc. The only interface for managing smart cards.
Secure Shell (SSH)	A secure shell connection to DataFort CLI (command line interface) via secure shell client. Can be configured to require smart card authentication as well as the administrator 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 system 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 address, gateway and subnet mask. Zeroize DataFort when other interfaces are not available.
LCD	The DataFort front panel displays messages. The 2U DataFort appliance front panel also functions as an interactive touch screen.	View DataFort status and throughput information at a glance. Use 2U DataFort touch panel buttons to enter initial IP settings and get more 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.	View DataFort status via SNMP tool. No secure information is permitted over this protocol (read only, no set commands).

INSTALLING DECRU DATAFORT APPLIANCES

For each new DataFort added to the network, make sure the following steps are performed:

- [Selecting a Location](#)
- [Rack Mounting](#)
- [Connecting the Decru DataFort](#)
- [Assigning the DataFort IP Address](#)
- [Running the Setup Wizard](#)

SELECTING A LOCATION

DataFort's design allows for easy installation in an EIA standard 19" rack or on a desktop. When installing the unit in an equipment rack, select a location that meets the following requirements:

- 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 +35°C (41°F to 95°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 DATAFORT, DO NOT LIFT OR CARRY THE UNIT BY THE FRONT PANEL. THE FRONT PANEL IS INTENDED TO BE AN EASILY DETACHABLE COMPONENT AND IS NOT DESIGNED TO CARRY PRODUCT WEIGHT.

RACK MOUNTING

Appropriate hardware is provided with the DataFort appliance in order to mount it in an EIA standard 19" rack. Follow instructions provided in the DataFort package to mount the slide rails to the sides of DataFort, and attach the rail mounts to the rack. Then slide DataFort 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.

CONNECTING THE DECRU DATAFORT

Insert the System Card into the slot on the front panel, then connect DataFort to the network in the following order:

- [Rear Panel Network Connections](#)
- [Power Connection](#)
- [Assigning the DataFort IP Address](#)

SYSTEM CARD INSERTION

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.

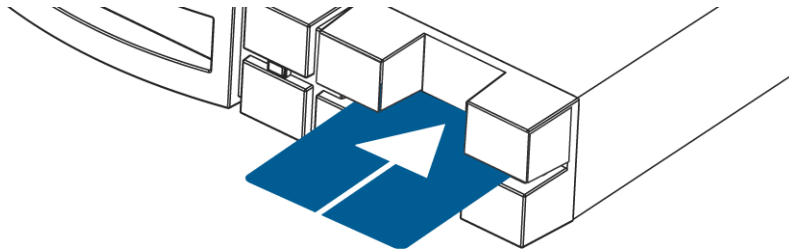


Figure 5: The front panel slot housing the System Card on a 1U DataFort

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.

REAR PANEL NETWORK CONNECTIONS

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

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

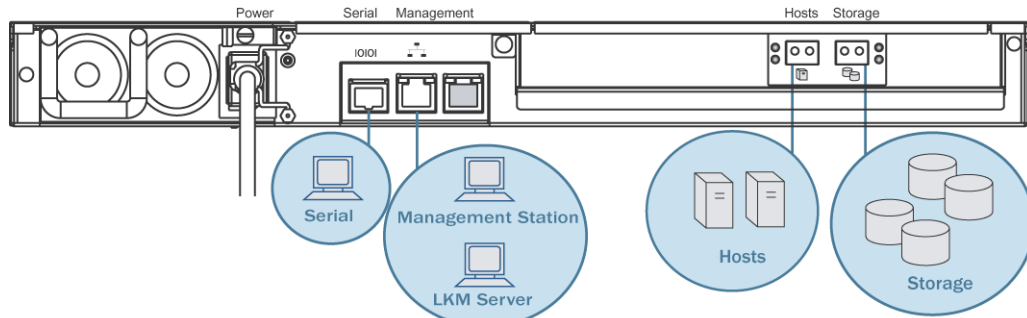


Figure 6: Rear panel connections 1U DataFort

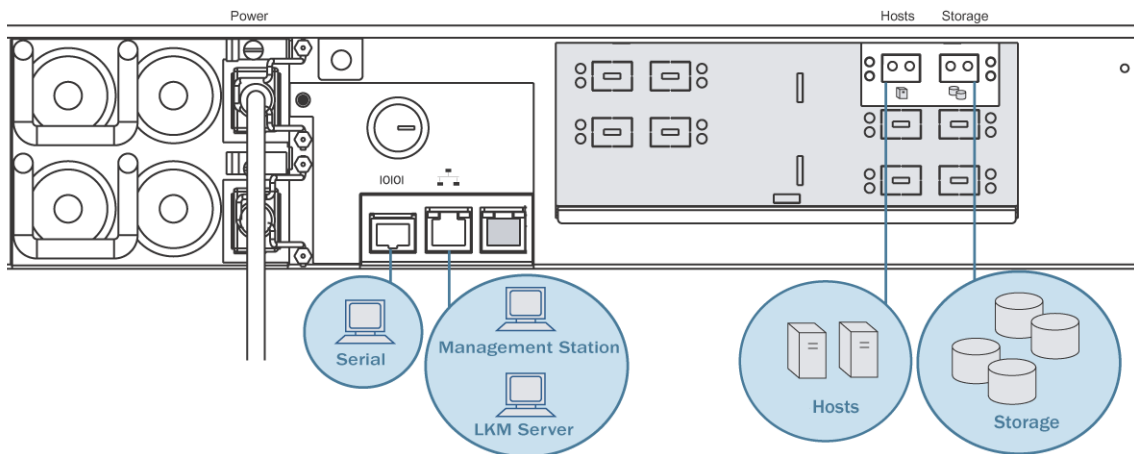


Figure 7: Rear panel connections 2U two-port DataFort

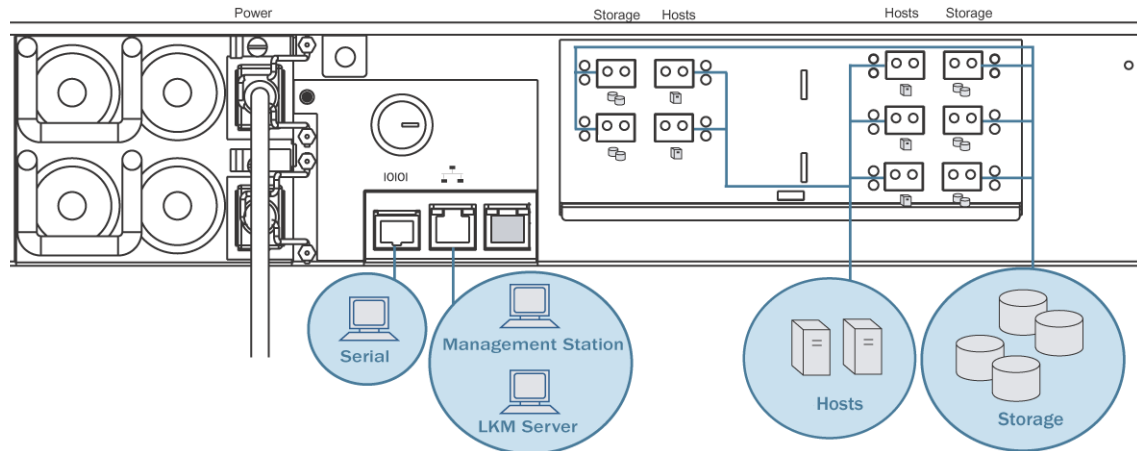


Figure 8: Rear panel connections 2U ten-port DataFort

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.

- The LKM server should also be connected to this network segment.

Fibre Channel Connection

DataFort features distinct interfaces for connecting to the network. A Host HBA provides an interface for unencrypted data sent from hosts, and a Storage HBA provides an interface 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 HBA to a FC fabric including network hosts.
2. Use a FC cable to connect each Storage HBA to a FC fabric including network storage devices.

Connecting DataFort to a Fibre Channel switch that supports the establishment of zones is recommended. Use zoning to separate Storage HBAs and storage devices from Host HBAs and hosts. Separate switches can also be used to divide the host and storage zones.

Note: DataFort dual HBAs are NL-Ports. Some switches do not support NL-Ports. DataFort can be configured to support such switches, but without an NL-Port, some DataFort storage management features will not be available.

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'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.

POWER CONNECTION

The DataFort appliance is equipped with one or two replaceable power supply/fan modules depending on whether the DataFort is a 1U or 2U model. Power supplies can be easily 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.

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.

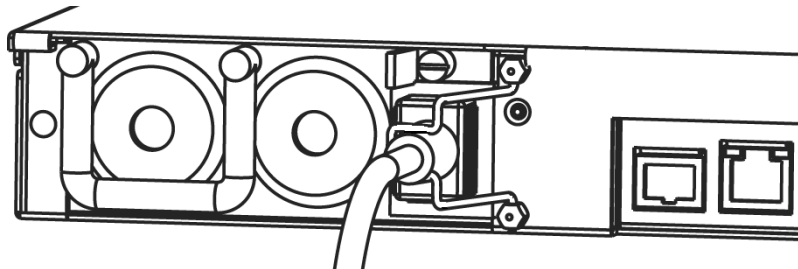


Figure 9: Power cord secured by the wire retaining clamp

2. When the cord or cords are connected, DataFort will power on automatically.
3. Wait two to three minutes while DataFort powers up. When the LCD messages are completed, DataFort is ready for initialization.

ASSIGNING THE DATAFORT IP ADDRESS

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

2U DataFort

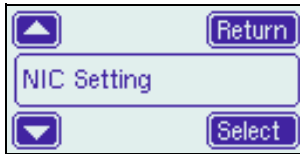
Assign the DataFort IP settings using the touch-sensitive buttons on the front panel LCD as described in [Setting the IP Address Using the LCD](#), or the serial console port, as described in [Setting the IP Address Using the Serial Console](#). The LCD can only be used to configure IP settings for an 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. The screen shows the NIC Setting entry. (If not, touch either the up or down arrow to scroll the menu to the correct entry.)



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



6. When you have 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) on the workstation connected to the serial port (see [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. The serial console menu offers the following options:

```
1. Configure Network Interface - not configured
   IP Address                  : (not set)
   Netmask                    : (not set)
   Default Gateway Address    : (not set)
2. Ping Default Gateway
3. Save and Exit
-----
C. Clear Current Settings
Z. Zeroize DataFort
Q. Quit
```

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

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

RUNNING THE SETUP WIZARD

Run the Setup Wizard from the Management Station. This wizard can be used to do the following:

- Set up a new standalone DataFort.
- Set up a new cluster. All cluster members should be initialized and connected to the network before beginning.
- Join a new DataFort to an existing cluster.
- Set up a new DataFort with an existing configuration (restore a configuration).

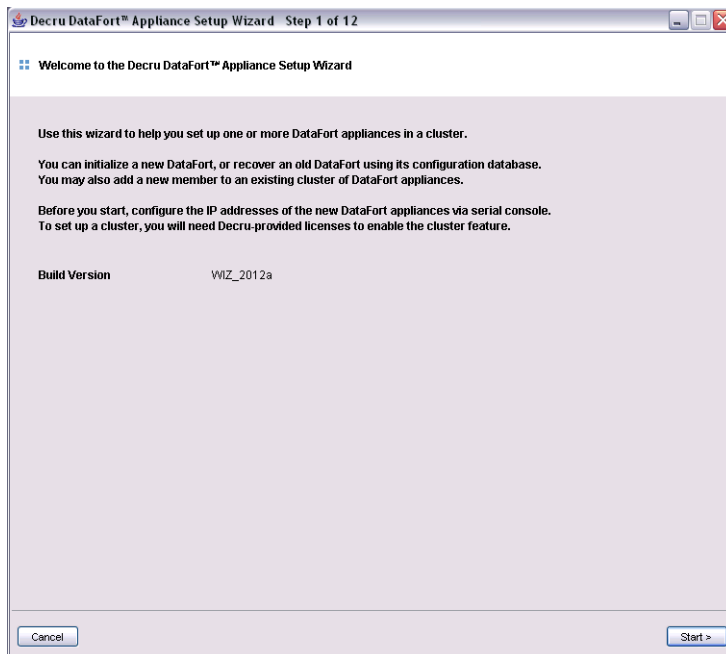
Consider the following when running the wizard:

- Security settings established during this procedure will 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 28.
- The Setup Wizard cannot be run through Windows Terminal Services or Remote Desktop.

START THE WIZARD

The DataFort installer will have placed the smart card reader and Setup Wizard on the Management Station (see [Preparing the Management Station](#) on page 29).

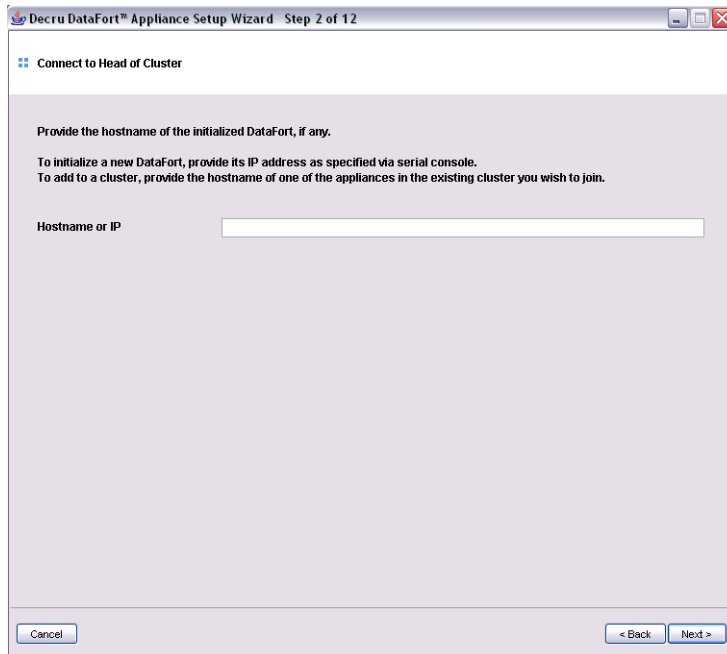
1. On the Management Station, select **Start > Programs > Decru > DataFort Wizard**.



2. Click Start.

CONNECT TO HEAD OF CLUSTER

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



Decru DataFort™ Appliance Setup Wizard Step 2 of 12

Connect to Head of Cluster

Provide the hostname of the initialized DataFort, if any.

To initialize a new DataFort, provide its IP address as specified via serial console.
To add to a cluster, provide the hostname of one of the appliances in the existing cluster you wish to join.

Hostname or IP

Cancel < Back Next >

1. Enter the IP address or resolvable hostname of the standalone DataFort or the cluster head:

Standalone DataFort

Enter the IP address or the hostname for the DataFort as determined when it was initialized.

First DataFort in cluster

Enter the IP address or the hostname for the DataFort as determined when it was initialized.

Additional DataFort in cluster

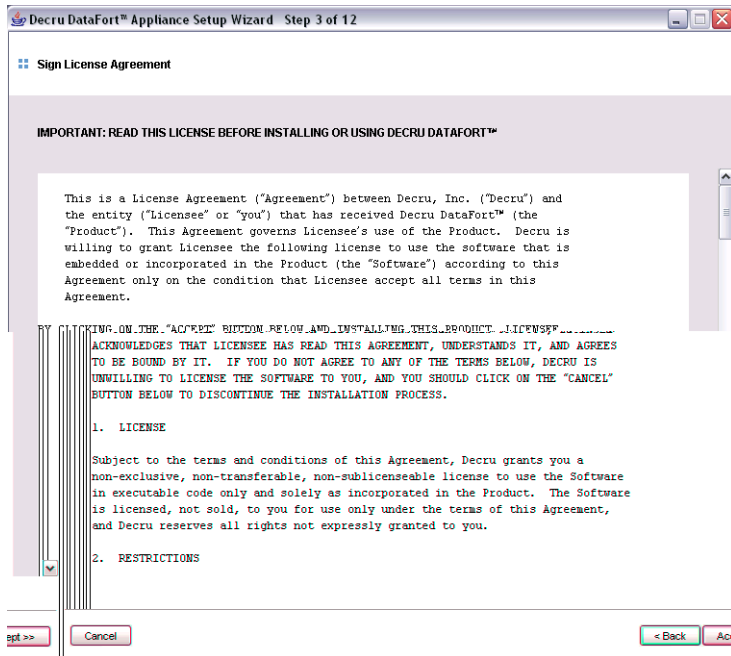
Enter the IP address or the hostname of the first DataFort in the cluster.

Note: If the wizard has been run before on this Management Station, previously entered IP information will have been cached and will appear in the field.

2. Click Next.

SIGN LICENSE AGREEMENT

Agree to the license terms to continue the wizard.



1. Read the license agreement.
2. Click Agree 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. If not, skip to the next screen using the Next button.

Decru DataFort® Appliance Setup Wizard Step 4 of 12

Recover from Database (Optional)

Identify the path to the configuration database for the DataFort appliance you wish to restore.
Leave the field blank if you wish to initialize a new DataFort.

Path to Configuration Database

1. Enter the path to the existing database, or leave the field empty if this DataFort will not use an existing configuration.
2. Click Next.

CREATE ADMINISTRATOR

Create an administrator for this DataFort. This administrator will be a Full Administrator, and will have management privileges for the entire cluster.

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.

Decru DataFort™ Appliance Setup Wizard Step 5 of 12

Create Administrator

Specify an administrative username and password.

Username

Password (8 characters minimum)

Confirm Password

Cancel < Back Next >

1. Enter a username for the administrator.
2. Enter and confirm a password for the administrator. Passwords may be composed of upper and lower case characters, numbers and punctuation marks. Select a password consisting of at least 8 valid, randomly-chosen characters.

This name and password will be used every time the administrator logs in to DataFort. Record this information for future reference.

3. Click Next.

CONFIGURE CLUSTER 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.

- [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. If there is an existing cluster, the recovery schema will already be selected.

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.

CAUTION: The recovery schema is permanent for the entire cluster. Plan the setting according to the security policy of your organization.

Decru DataFort™ Appliance Setup Wizard Step 6 of 12

Configure Cluster and Recovery Schema

The Recovery Schema determines the quorum of Recovery Cards required during data recovery. This Recovery Schema selection will be permanently set upon clicking Next.

Cluster size is the desired total number of DataFort appliances in the cluster.

IPsec Shared Secret is required for communication within a cluster.

Recovery Schema: 2 out of 5

Cluster Size: Standalone

Shared Secret: (8 characters minimum)

Confirm Secret:

Cancel < Back Next >

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.

CAUTION: DATA RECOVERY SETTINGS CANNOT BE CHANGED AFTER YOU CONTINUE TO THE NEXT STEP OF THE WIZARD.

Setting the Cluster Size

Select standalone or cluster size.

Standalone

Select Standalone for a standalone DataFort. Another DataFort can still be added in the future to create a cluster.

Cluster

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. It is also possible to add a DataFort to an existing cluster.

Enter an IPsec secret for the cluster members to share, and confirm the password. This password is shared by cluster members to ensure secure communication across the IPsec channel. Use a strong password, 8 or more characters, including letters, digits and punctuation.

Decru DataFort™ Appliance Setup Wizard - Step 6 of 12

Configure Cluster and Recovery Schema

The Recovery Schema determines the quorum of Recovery Cards required during data recovery. This Recovery Schema selection will be permanently set upon clicking Next.

Cluster size is the desired total number of DataFort appliances in the cluster.

IPsec Shared Secret is required for communication within a cluster.

Recovery Schema: 2 out of 3

Cluster Size: 2

Shared Secret: ***** (8 characters minimum)

Confirm Secret: *****

Cancel < Back Next >

2. Click Next to proceed.

INTRODUCE CLUSTER MEMBERS

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 Cluster Size was set in the previous step, a set of fields will appear for each cluster member.

Standalone Network Settings

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

Decru DataFort™ Appliance Setup Wizard Step 7 of 12

Introduce Cluster Members

Specify network information for each cluster member.

Click Next after the Crypto Module is done initializing.

Hostname 1	zippy1
IP Address 1	10.101.22.84
Netmask 1	255.255.248.0
Gateway 1	10.101.20.1
FC Site 1	<auto-detect>

1. Enter a hostname for this DataFort.
2. The IP address, Netmask and Gateway set for the Management NIC will appear. (These were set when [Assigning the DataFort IP Address](#) on page 37.)
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.
4. Click Next.

Cluster Network Settings

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

Decru DataFort™ Appliance Setup Wizard Step 7 of 12

Introduce Cluster Members

Specify network information for each cluster member.
Click Next after the Crypto Module is done initializing.

Hostname 1: zippy1
IP Address 1: 10.101.22.84
Netmask 1: 255.255.248.0
Gateway 1: 10.101.20.1
FC Site 1: <auto-detect> [Customize...](#)

Hostname 2:
IP Address 2:
Netmask 2:
Gateway 2:
FC Site 2: <auto-detect> [Customize...](#)

☐ Send requests to security manager

[Cancel](#) [< Back](#) [Next >](#)

The IP Address, Netmask and Gateway set for the Management NIC of the first DataFort will appear.

For each additional DataFort, enter the following:

1. Enter a hostname.
2. Enter an IP Address, Netmask and Gateway.
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.

ADD LICENSES

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.

Decru DataFort™ Appliance Setup Wizard Step 9 of 12

Network and Certificate

Provide cluster-wide network information (optional).

DNS Suffix

DNS Search Path(s)

DNS 1

DNS 2

Specify values for the self-signed certificate.

Country

State

City

Organization

Organization Unit

Email

Cancel < Back Next >

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).

Provide cluster-wide network information (optional).

DNS Suffix

DNS Search Path(s)

DNS 1

DNS 2

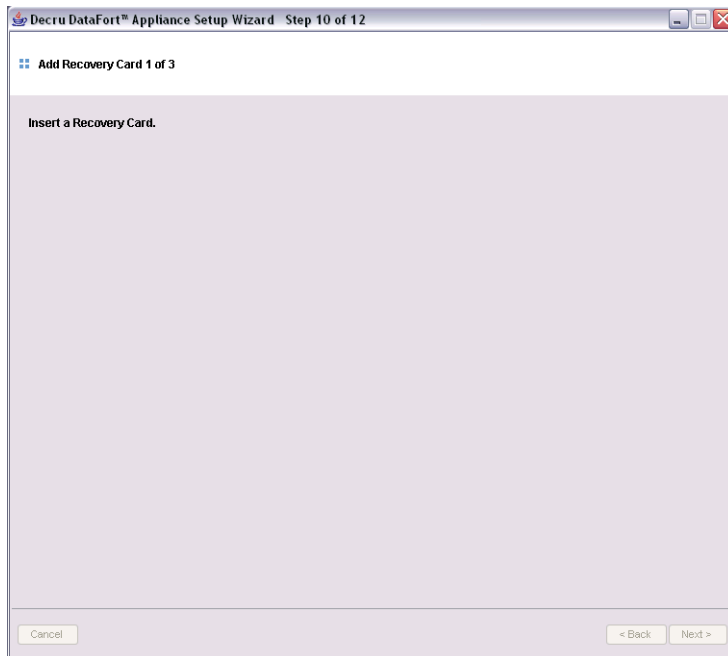
Certificate

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

1. Enter 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 193.
2. Enter the rest of the required information about your location.
3. Click Next.

ADD 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.
Uninitialized Card: If the card is uninitialized, DataFort will provide a default card label and Security Domain. The Recovery Officer responsible for this card should replace the default settings with the card label, the name of the Security Domain and enter a password as determined by the security policy of the organization.
Initialized Card: If the card has already been initialized, DataFort will load the card label and Security Domain into the wizard and prompt for the password. The Recovery Officer responsible for this card should enter the password into the field provided.

2. The Recovery Officer responsible for this card should enter the required information into the provided fields.
 - Strong passwords are an important part of the overall security of the system. Passwords may be composed of upper and lower case characters, numbers and punctuation marks. Please select a password consisting of at least 8 valid, randomly chosen characters.
 - The Security Domain entered for the first card in the set will be applied to the entire set of Recovery Cards.

Decru DataFort™ Appliance Setup Wizard Step 10 of 12

Add Recovery Card 1 of 3

Authenticate this Recovery Card.

Card ID 09000000ds2e1462a1678b2a9111ec2a0a0cccd8

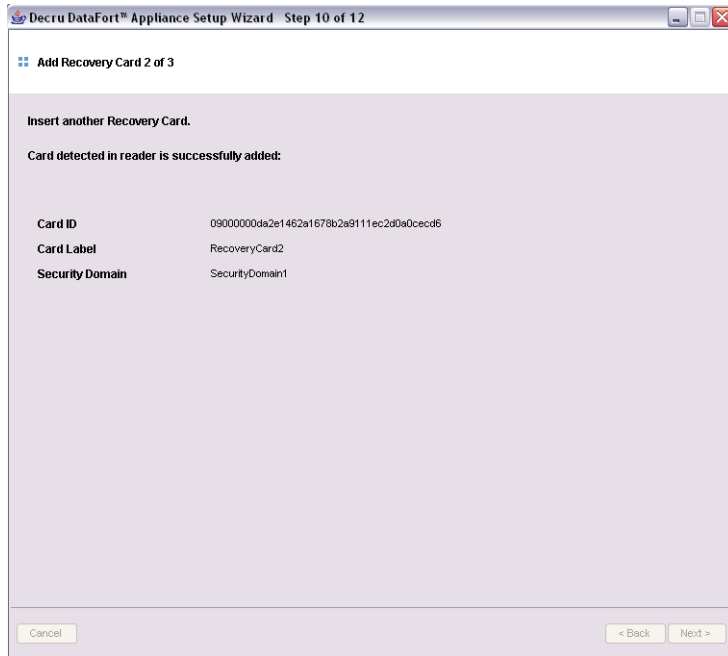
Card Label RecoveryCard2

Security Domain SecurityDomain1

Current Password

Cancel < Back Next >

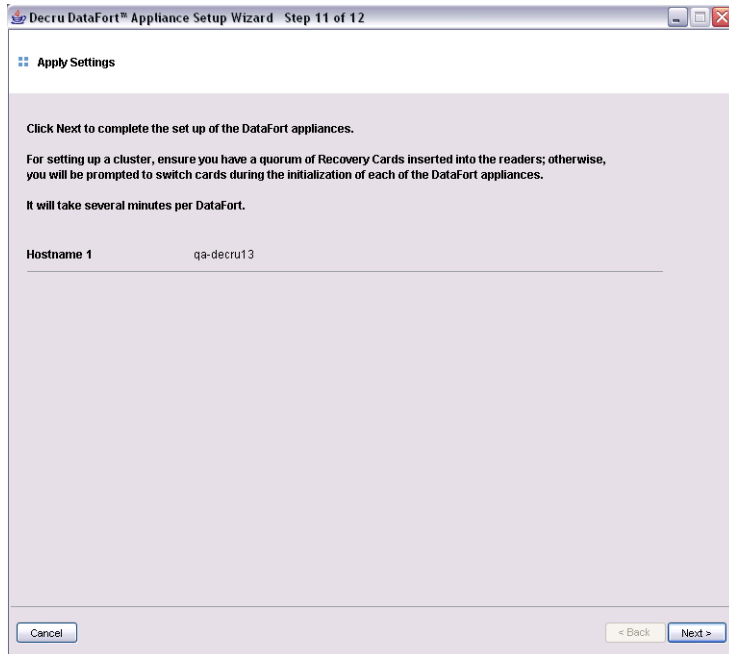
3. Repeat the previous steps for all the cards specified by the recovery schema. These cards will be used for all DataFort appliances in this Security Domain.



4. When all cards have been introduced, click Next.

APPLY SETTINGS

Click Next to apply the settings to all DataFort appliances that are being configured using the wizard. Note that for a cluster, you will be prompted to insert the quorum of Recovery Cards.



1. Click Next.
2. 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.

The screenshot shows a window titled "Decru DataFort™ Appliance Setup Wizard Step 11 of 12". The window has a standard Windows-style title bar with minimize, maximize, and close buttons. Below the title bar, the text "Apply Settings" is displayed with a small icon. The main content area has a light purple background and contains the following text:

Click Next to complete the set up of the DataFort appliances.

For setting up a cluster, ensure you have a quorum of Recovery Cards inserted into the readers; otherwise, you will be prompted to switch cards during the initialization of each of the DataFort appliances.

It will take several minutes per DataFort.

Below the text, there are two rows of input fields:

Hostname	Value
Hostname 1	qa-decru15
Hostname 2	qa-decru16

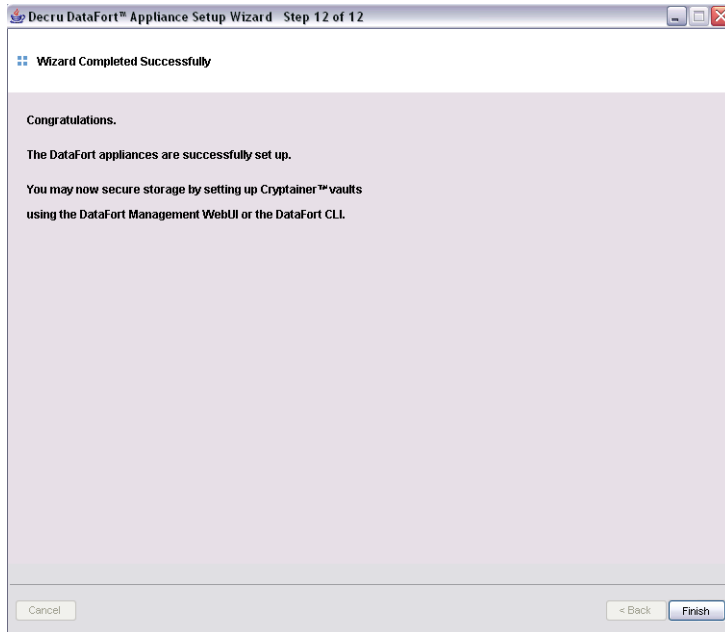
At the bottom of the main content area, there is a progress bar and the text "Send requests to security manager".

The bottom of the window contains three buttons: "Cancel", "< Back", and "Next >".

3. After the settings have been applied, click Next.

COMPLETE WIZARD

When the wizard is complete, the final screen appears.



1. Click Finish.

LOGGING INTO DATAFORT

After the wizard is complete, log into the DataFort WebUI.

1. Open Internet Explorer on the Management Station.
2. Enter <https://> and the IP address or hostname assigned to DataFort. (Be sure to enter https.)

A message appears about the security certificate issued by Decru.



3. Click Yes to proceed.

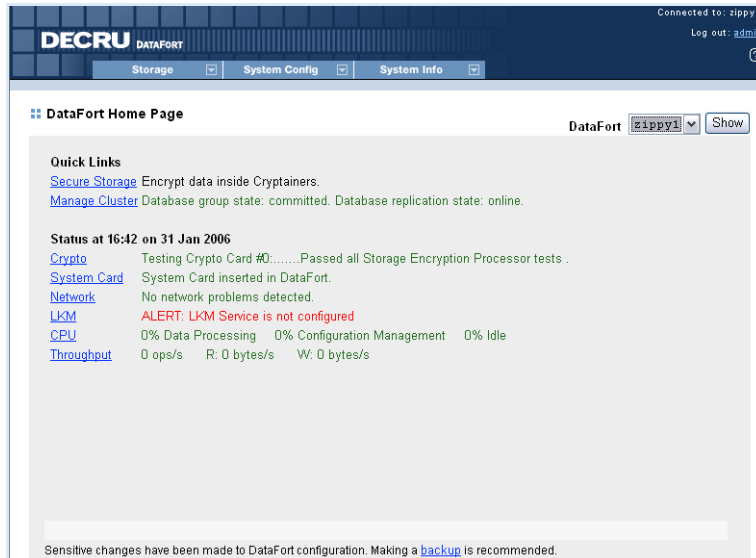
Internet Explorer will display a security warning before loading the Decru applet for the first time. By agreeing to load the applet you are allowing the Management Station to display the DataFort WebUI in Internet Explorer.



4. Click Yes to proceed.
The DataFort Login page appears.
5. Log in to DataFort with the username and password provided set during the wizard. See [Create Administrator](#) on page 44.

6. Click Log In.

The DataFort Home page is displayed whenever 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** 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 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
- 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 136.

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. Only that page will be displayed. Once you navigate off that page, you are returned to the original WebUI.

BEFORE CREATING CRYPTAINERS

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.

Note: The DataFort configuration can be modified using the DataFort WebUI, with the exception of the data recovery schema. If you discover that this schema is incorrect, you will have to zeroize the DataFort. See [Zeroizing After Setup](#) on page 144. If DataFort must be zeroized, it is best to do so before creating Cryptainers, forming a cluster or managing any data.

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

- [Checking Cluster State](#)
- [Configuring Remote Logging](#)
- [Starting LKM](#)
- [Configuring Tape Settings](#)
- [Creating Additional Administrators](#)
- [Verifying System Version](#)
- [Determining the Defense Setting](#)

These and other management operations are performed using the WebUI. For login instructions, see [Connecting to the DataFort WebUI](#) on page 70. 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.

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 [Cluster Management](#) on page 147 for information about the meaning of various cluster states.

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 138 for details.

STARTING LKM

Decru's Lifetime Key Management software runs on a network server, where it stores encryption keys used by multiple DataFort appliances. For information about setting up the Lifetime Key Management server, see [Setting Up the Lifetime Key Management Server](#) on page 30.

After the LKM server is configured, and its IP address specified using the DataFort WebUI, DataFort will send a backup copy of the most recent configuration database to the LKM server automatically approximately every hour, adding current key and Cryptainer information to the LKM archive.

To allow DataFort to automatically back up its configuration database to the LKM server for key storage, configure DataFort LKM settings.

- 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 129. All LKM settings are propagated across cluster members, therefore it is sufficient to enter LKM settings once for each cluster.

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 license controlling tape features is installed on DataFort.

- 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. See [Cryptainer Creation](#) on page 81 for instructions.

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 [DataFort Administration](#). The Full Administrator can create these administrators after completing the Setup Wizard.

- 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 64 for instructions.

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.

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 134.

RESTORING A DATAFORT

If a standalone DataFort is lost, a saved configuration database from that DataFort can be used to configure a new DataFort. The recovered DataFort will then be able to retrieve data that was encrypted using the previous DataFort.

The wizard is used to give 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.

Note: 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 [Replacing a DataFort in a Cluster](#) on page 151. 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.
 - The minimum set of Recovery Officers and Recovery Cards as determined by the recovery schema of the cluster.
 - A new or zeroized DataFort.
 - 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 37.
 2. Run the wizard.
 3. At the Recover from Database page (see [Recover From Database](#) on page 43), browse to the saved configuration database.
 4. 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.
 5. Complete the wizard.



■ ■ ■ ■ 4 DATAFORT ADMINISTRATION

This chapter provides instructions for adding a DataFort administrator and connecting to DataFort management interfaces used to complete administrative tasks. It includes general information about the following topics:

- [Administrator Roles](#)
- [Account Administration](#)
- [DataFort Management Interfaces](#)
- [DataFort Settings and Status](#)
- [Security Preparedness and Response](#)
- [Powering Up and Shutting Down](#)

ADMINISTRATOR ROLES

All DataFort administration tasks can be carried out by the 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, the 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 (creating a Cryptainer is such a procedure).

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

TABLE 4: 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 DataFort Initialization. The Full Administrator can complete all administrative tasks including: • DataFort Initialization • Account Administration • Storage Administration • Key Administration • Backup Administration • Physical Security Administration • Cluster Administration • Machine Administration
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, as well as the ability to create or delete a Cryptainer as described in Storage Administration. Key Administrator tasks include: • Managing Licenses • Managing Trustees as well as importing and exporting exportable keys • Purging keys upon backup to LKM as described in Key Purging • Managing Cryptainers as described in Storage Administration • Configuring Management Security Settings • Setting Security Certificates • 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: • Managing DataFort Defense Responses • 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

TABLE 4: ADMINISTRATOR ROLES AND PRIVILEGES

Role Name	Privileges
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: • System Configuration • Upgrading DataFort
Read-Only Administrator	A Read-Only Administrator can view all DataFort settings (see DataFort 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:

- DataFort administrators should be highly trusted individuals in your organization.
- At least two Full administrators should be associated with each DataFort or DataFort cluster. Associating more than one Admin Card with a DataFort is recommended.
- 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

A Full Administrator or an Accounts Administrator must be logged in to the WebUI to add an administrator. See [Connecting to the DataFort WebUI](#) on page 70 for login instructions.

1. From the WebUI, select **System Config > System Users > Administrators**.
Administrators known to this DataFort are listed.

Manage Administrators Cluster-wide

Administrators

Administrator	Fullname	Role	Has Card
admin	admin	san-admin	y

Buttons: Add... Edit... Delete Refresh Associate Card Authorize Login

2. Click Add.

Manage Administrators : Add

Username

Password (8-30 chars)

Confirm Password

Fullname

Role ☒ Read Only ☐ Specialty ☐ Full Admin

Buttons: Apply Cancel

3. Enter the name of the new administrator, and a password for that administrator. Strong passwords are an important part of the overall security of the system. Passwords may be composed of upper and lower case characters, numbers and punctuation marks. Select a password consisting of at least 8 valid, randomly chosen characters.
4. Confirm the password.
5. Enter a full name for the administrator.
6. Select the type of administrator you want to create. See [Administrator Roles](#) on page 62 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 67 for more information.

Note: Full Admins 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 the 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.

Manage Administrators : Add

Username:

Password (8-30 chars):

Confirm Password:

Full Name:

Role: ☐ Read Only ☒ Specialty ☐ Full Admin

☐ Key ☒ Security ☐ Accounts ☐ Storage ☐ Backup ☐ Machine

7. Click Apply.

Manage Administrators Cluster-wide

<u>Administrator</u>	<u>Fullname</u>	<u>Role</u>	<u>Has Card</u>
321	321321321	san-storage-admin	n
Security Admin	Security Admin	san-security-admin	n
admin	admin	san-admin	y

8. Select the newly created administrator from the list.

9. 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.
10. 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, all administrators can log in to DataFort without additional authorization. A newly added administrator automatically becomes a member of the authorizer group unless the authorizer privilege is revoked.

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 administrator with full login privileges at all times: a Full Administrator not requiring prior authorization.

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, 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.

Create an Administrator Requiring Authorization

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

Manage Administrators : Edit security administrator

Fullname:

Login: ☐ Direct ☒ Requires Prior Authorization

Role: ☒ Specialty ☐ Full Admin

☒ Security ☐ Storage ☐ Machine

Change Password:

Current:

New:

Confirm:

4. Select the Requires Prior Authorization button.
5. Click Apply.

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

Note: To remove the requirement for login authorization, access the same page, 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.
3. Click Edit.

4. Enter the current password for the administrator.
5. Enter the new password and confirm the entry. Strong passwords are an important part of the overall security of the system. Passwords may be composed of upper and lower case characters, numbers and punctuation marks. Select a password consisting of at least 8 valid, randomly chosen characters.
6. Click Apply.
The password will be changed.

REMOVING AN ADMINISTRATOR

It may be desirable to delete an administrator profile. After an administrator has been deleted from a DataFort's list of known administrators, the DataFort or DataFort cluster will

DATAFORT MANAGEMENT INTERFACES

After setup, the primary management interfaces for DataFort are the DataFort WebUI and DataFort CLI (command line interface). Some setup and management functions are also available from the serial console. DataFort appliances equipped with a front touch panel LCD offer an additional management interface. See the [Management Interfaces](#) table on page 31.

Security policy settings determine whether an Admin Card is required for logging in to the WebUI or CLI. 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 118.

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.

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, as described in [Configuring Management Security Settings](#) on page 118.

Using the DataFort WebUI

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

- To return to the Home page from any other page of the WebUI, click the Decru logo.
- Click the onscreen ? icon to view online help.
- 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 hostname assigned to DataFort. (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. If Secure Web is in effect, insert an Admin Card that is associated with a valid administrator for this DataFort.
5. Enter the username and password that was set for the administrator.
6. Click No if Windows offers to store password information.
7. Click Log In.

When authentication is complete, the DataFort Home page is displayed. Choose management commands from the links or pull-down menus on the Home page.

Connecting via WebUI using Dual Authorization

By default, all valid administrators can log in to DataFort without additional authorization. If this privilege is revoked for a given administrator (see [Requiring Authorization for Login](#) on page 67) that administrator will require the presence of an authorizing administrator in order to log in to DataFort. 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), and enters username and password.
5. Click Log In.
6. Choose **System Config > System Users > Administrators**.
7. In the Known Administrators panel, select the administrator requiring authentication and click Authorize Login.
8. The administrator with authorization privileges should log out of the WebUI by clicking the Log out link at the top of the screen.
9. 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.

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 118. Secure CLI requires that a session-specific password be furnished via the WebUI before the administrator can log in.

Using the CLI

- See [Using the CLI](#) on page 181 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 is designed to provide the same level of authentication for CLI login as is required for secure WebUI login, requiring 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.

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 70.
2. Click the button: Obtain a One Time Password for the CLI.

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

DataFort Login

DataFort Hostname: DataFort

Administrative Username:

Password:

Action: ☒ Login to the WebUI ☐ Obtain a One Time Password for the CLI

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 valid administrators can log in to the CLI without additional authorization. If this privilege is revoked for a given administrator (see [Requiring Authorization for Login](#) on page 67) that administrator will require the presence of an authorizing administrator in order to log in to the CLI. 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, which is accessed by directly connecting to the DataFort via SSH, as described in [Connecting via Standard CLI](#) on page 72.

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

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

DATAFORT FRONT PANEL LCD

After setup, the DataFort front panel LCD displays messages and a bar ew1Loei:ew1Ld)-76(mi-6.d1(d a ta(h)-1(e)6.1(rf)0.1(t

TABLE 6: READ/WRITE RATE DISPLAY ON 1U DATAFORT APPLIANCES

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

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.

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.

Connecting the Serial Console Port

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.

1. Attach the provided RJ45 to DB9 adapter to the Category 5 cable.
2. Connect the DB9 end of the cable to the serial console port of a workstation or a serial switch.
3. Connect the RJ45 end of the cable to the serial console port (marked **IOIOI**) on the DataFort.
4. Open a serial console (such as HyperTerminal) on the workstation.
5. Set the new connection with the following properties:
 - Speed - **9600**
 - Data bits - **8**
 - Stop bits - **1**
 - Parity - **None**
 - Hardware or no flow control

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. The main serial console menu is displayed after login from the serial console.

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. The serial console menu offers the following options:

```
1. Configure Network Interface - not configured
   IP Address                  : (not set)
   Netmask                    : (not set)
   Default Gateway Address    : (not set)
2. Ping Default Gateway
3. Save and Exit
-----
C. Clear Current Settings
Z. Zeroize DataFort
Q. Quit
```

2. Select option **1**, and 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 154.

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 to an uninitialized state. See [Zeroizing the Decru DataFort](#) on page 144 for general information, and [Zeroization Using the Serial Console](#) on page 146 for details.

Emergency Serial Console Port Access

If all Admin Cards and passwords for a DataFort are lost, it will not be 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 will allow the DataFort to be zeroized so it can be reset for future use.

1. Insert the Recovery Card into the DataFort front panel slot.
2. Log in to the serial console using the card label and password of that Recovery Card.
The main serial console menu will appear.

DATAFORT 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 139.

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.

SECURITY PREPAREDNESS AND RESPONSE

Administrators can prepare for emergencies by observing [Secure Network Practices](#), including maintaining regular configuration database backups. If these practices are followed, complete recovery is possible after a threat that suspends DataFort operation, weakens security, or disables DataFort entirely.

AUTOMATIC AND MANUAL RESPONSES

The DataFort defense setting determines the automatic response to evidence of physical intrusion. See [Collecting Network Information](#) on page 28.

In an emergency, there are manual steps that can be taken to suspend DataFort encryption and decryption operations:

- **Pressing the CryptoShred button** (available in some DataFort models) With the Basic defense setting, pressing the CryptoShred button suspends encryption and decryption immediately. With the Medium or High defense setting, encryption keys are also deleted.
- **Removing the System Card followed by shutdown** For DataFort models without a CryptoShred button, removing the System Card and powering off DataFort stops encryption and decryption immediately (see [System Card CryptoShred](#) on page 137). Note that removing the System Card alone does not stop DataFort operation.

RESTORING DATA AND NORMAL OPERATION

After an intrusion has been detected or the CryptoShred button has been pressed, the DataFort defense setting determines the requirements for resuming normal operation.

- With Basic Level defense, a Full Administrator can reset DataFort (see [Clearing a Defense Alert](#) on page 136). If the CryptoShred button was pressed, it must be released before the administrator can complete the reset (see [CryptoShred Button States](#) on page 137).
- With Medium and High Level defense, DataFort must be zeroized and then restored (see [Restoring a DataFort](#) on page 61). DataFort recovery requires using the Setup Wizard, Recovery Officers, and a saved configuration database. If the CryptoShred button was pressed, it must be released before recovery (see [CryptoShred Button States](#) on page 137).

After removal of the System Card and shutdown (System Card CryptoShred), resumption of normal operations depends on the availability of the System Card.

- 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](#) on page 61.

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.

To power DataFort on, first 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. For normal operation, leave DataFort powered on continuously, with the System Card in the card slot.

DataFort can be switched off temporarily using 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 power DataFort off permanently, unplug all power cords from the AC power source.

Note: Always back up the configuration database before powering off DataFort. This is the same routine backup you should do after making any configuration changes.

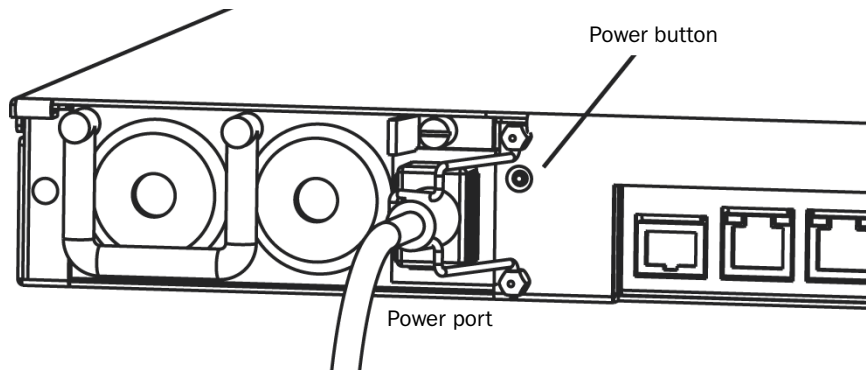


Figure 10: Rear panel power port and button

■ ■ ■ ■ 5 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 as described in [Chapter 3](#).

A Full or Storage Administrator can perform all of the functions outlined in this chapter.

- [Cryptainer Creation](#)
- [Host Management](#)
- [Cryptainer Management](#)
- [Storage Management](#)
- [Tape Management](#)
- [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.

CRYPTAINER CREATION

Use the SAN Topology page of the 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 90 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. The following section gives an example of basic Cryptainer creation using the DataFort WebUI.

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

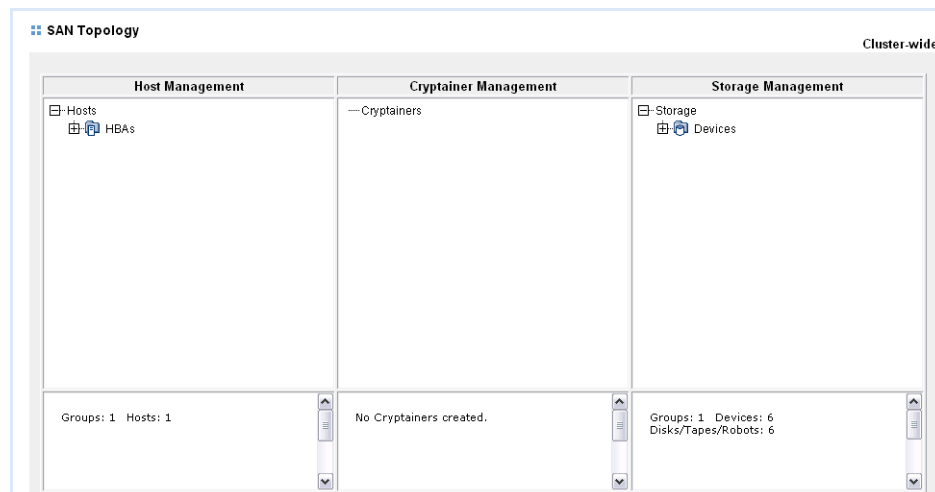
CRYPTAINER CREATION USING COLLECTIONS

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

- [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 a Storage Administrator must log in to the WebUI to create Cryptainers. See [Connecting to the DataFort WebUI](#) on page 70 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.

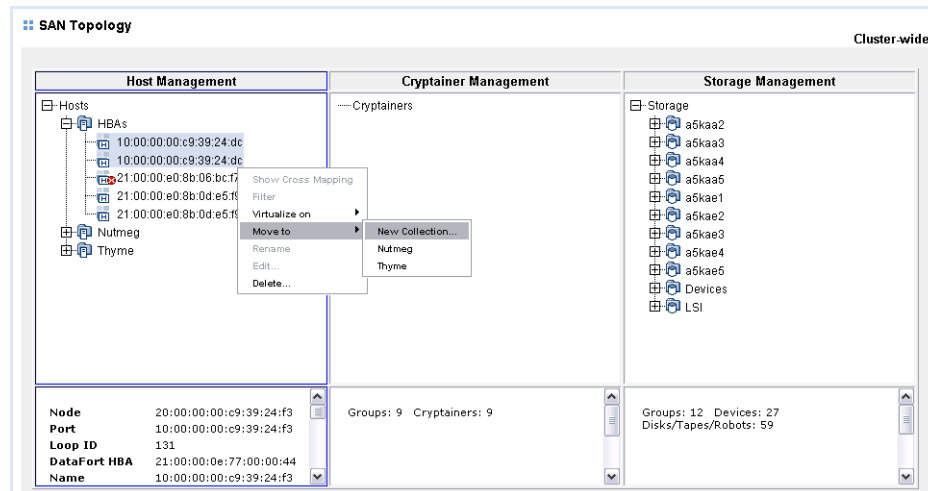
Create a Collected Host

In a standard high-availability 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.

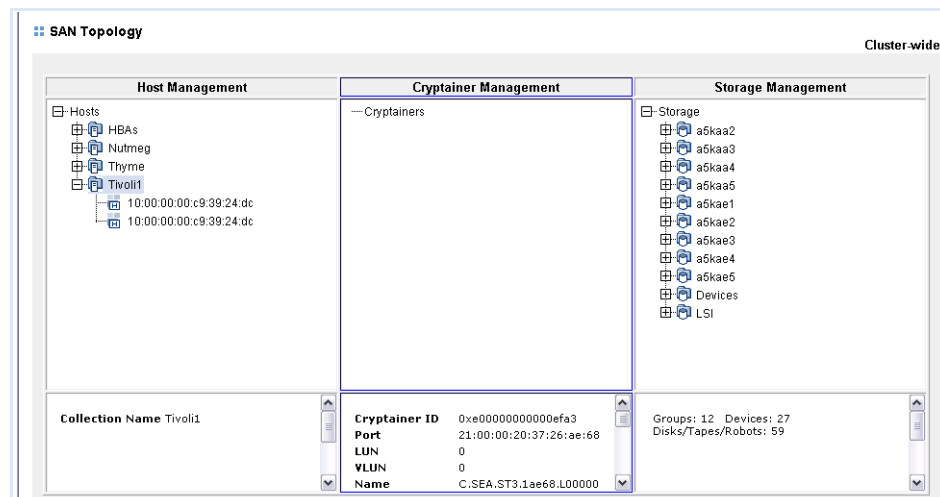
1. Multiple-select host instances by control or shift-clicking them in the Host Management pane.

Note: All collections must consist of devices with the same Node WWN.

2. Right-click to view the [Host Collection Menu](#) and select **Move to > New collection...**

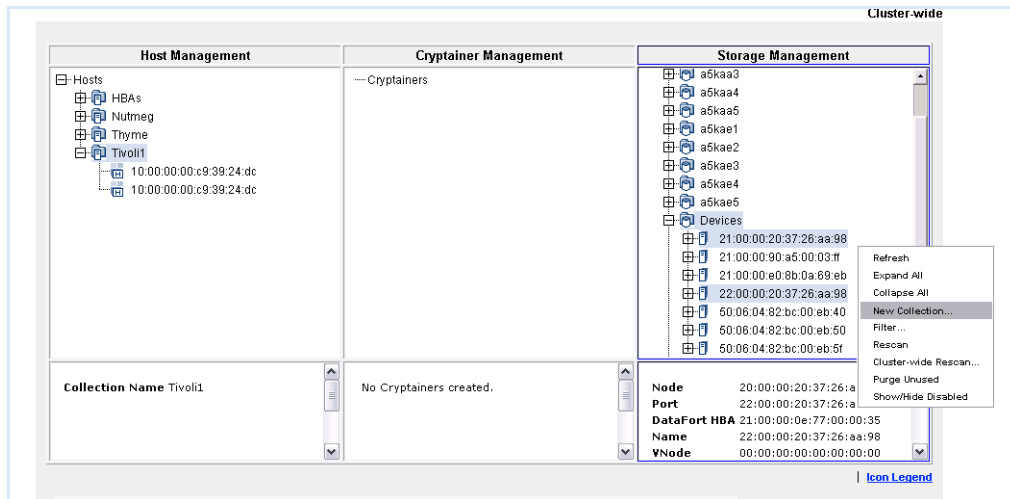


- Enter a name for the collection and click OK. The new collection appears in the WebUI.



Create a Collected Storage Device

- 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.
- Right-click to view the [Storage Collection Menu](#) and select **Move to > New collection...**

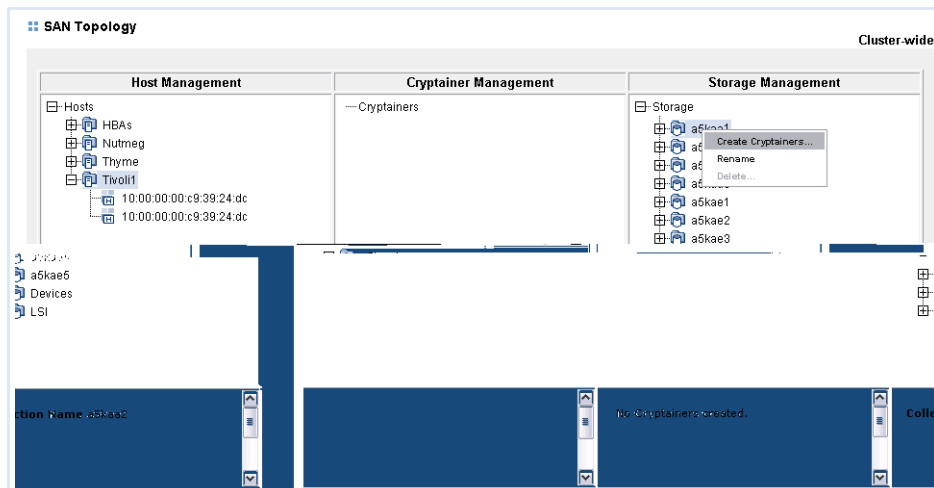


- Enter a name for the collection and click OK. The new collection appears in the WebUI.

Create a Cryptainer

- 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.

Note: All collections must consist of devices with the same Node WWN.



The Create Cryptainer page appears.

SAN Topology : Create Cryptainer

Devices within the collection will automatically be mapped as alternate paths.

Mapping

☒ Port Mapped (Virtual Ports)

☐ LUN Mapped (Primary Port) ort)

Host of Masked LUNS

Assign Key

☒ On

☐ Off

Exportable

☐ On

☒ Off

Port Forwarding

☐ On

☒ Off

(Optional)
(For empty disks
only)

Apply

Cancel

2. Select the settings for the Cryptainer on this device. See [Options When Creating a Cryptainer](#).

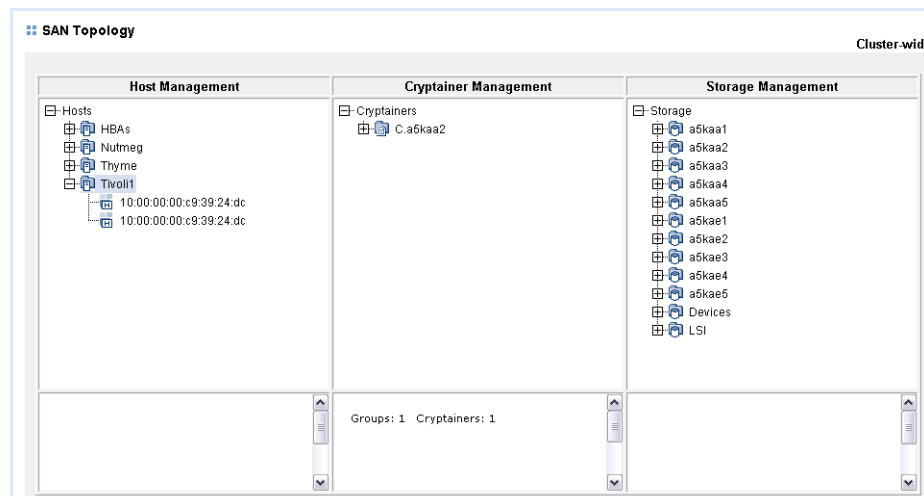
Options When Creating a Cryptainer

The following options are available when creating a Cryptainer. With the exception of initial encryption, the effects of these settings cannot be reversed after the Cryptainer has been created.

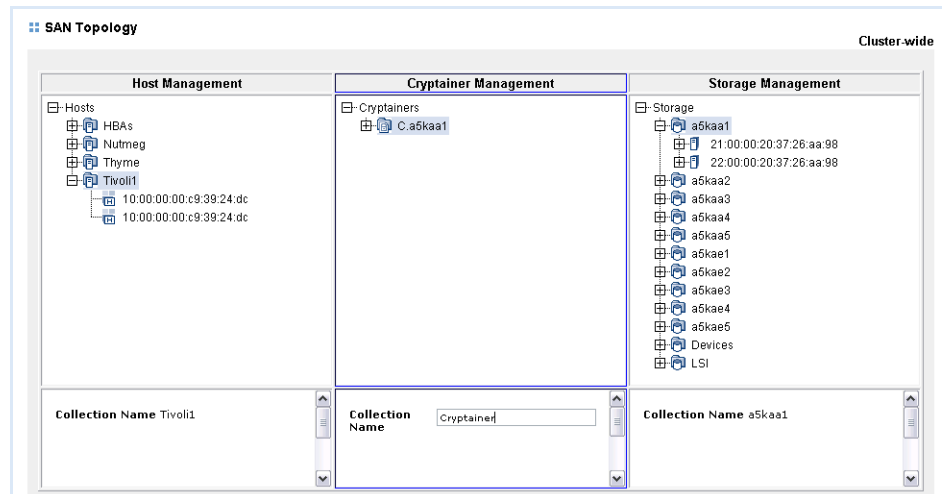
Port Mapped	Port Mapping, which presents the LUN of the storage device to the host, is recommended when creating Cryptainers on an enterprise storage target. This method of mapping will preserve the LUN assignments of the target by creating a virtual port which DataFort maps to the actual storage port 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	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 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	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 Host Management for more about virtualizing hosts.

Initial Encryption	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 Cryptainer Management for more about data encryption.
Exportable	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 for more about trustees.
Port Forwarding	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.

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



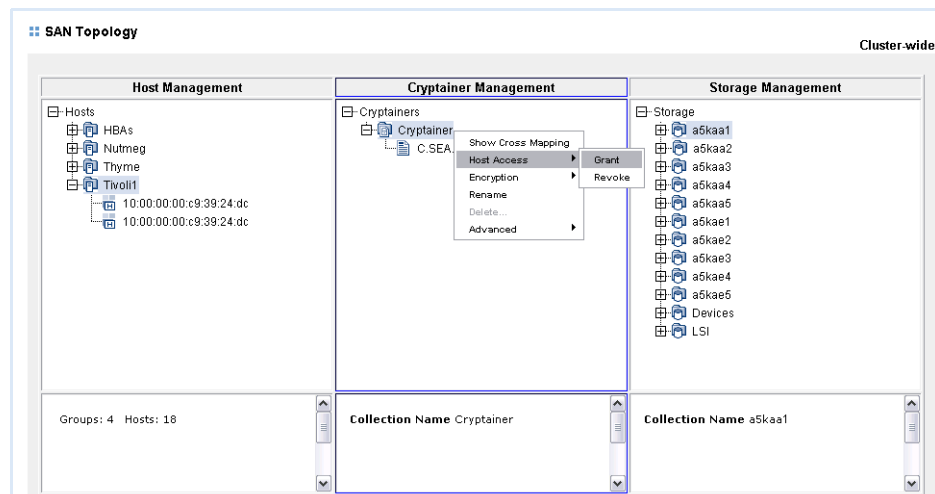
2. To change the name of the Cryptainer, right-click it and select Rename. The name field will open in the lower pane.



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

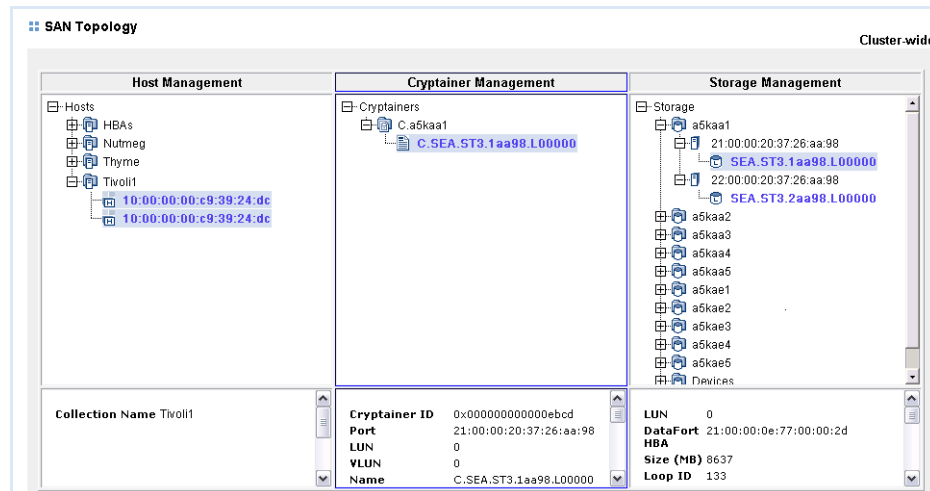
Assign Permissions to a Cryptainer

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.

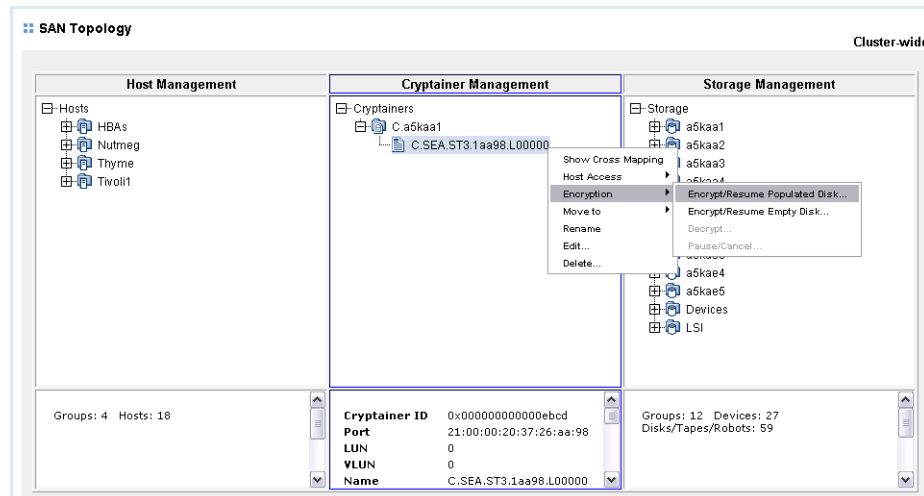


Bold text indicates the storage location of the Cryptainer and which host has access.

Encrypt Cryptainer Data

Cryptainers created on disk can be encrypted after creation. If a Cryptainer is created with [Initial Encryption](#) off, it will be cleartext until rekeyed. The [Cryptainer icon](#) will indicate whether encryption is on or off.

- 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 will be 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 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:

- [Host Management](#)
- [Cryptainer Management](#)
- [Storage Management](#)

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 7: 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 !	Metadata and/or 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	

HOST MANAGEMENT

DataFort offers Port Locking and Host Authentication features 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 or refresh the pane view and add a new host or collection of hosts.
Host Collection Menu	Right-click a collected host to use the menu to manage all host instances together. See Host Collection Menu .
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 .

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 Tape Management 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.

SAN Topology : Edit Host 21:00:00:e0:8b:05:1d:55

Name

Label of Default Pool

Port Lock Mode ☐ On ☒ Off

RAID Admin Mode ☐ On ☒ Off

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	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	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. In order for DataFort to grant the host access to the RAID device, a cleartext Cryptainer must be created on that device.

CRYPTAINER MANAGEMENT

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 .

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 > Remove .
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 Pause/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.
Advanced	Advanced > Metadata (disk only): When a Cryptainer is created for a LUN, it is assigned key material for encrypting and decrypting data stored there. This key material is the metadata of the Cryptainer, which uniquely identifies the key associated with the LUN. This metadata is always stored in the configuration database of the DataFort as well as with an LKM server if one is configured. Forcing metadata ON will allow DataFort to write this metadata to a block of the LUN when a Cryptainer is created, regardless of what is already on the disk. This can be useful when restoring data.

CRYPTAINER MENU

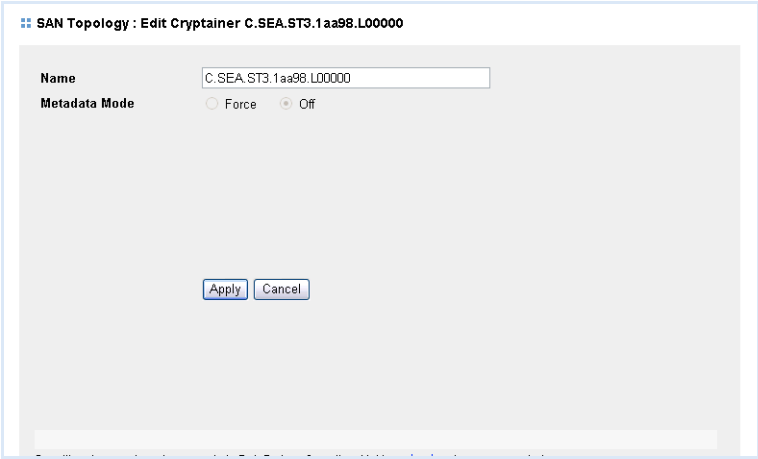
Right-click a Cryptainer to view the Cryptainer level menu. Use this menu to manage individual Cryptainers.

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 > Remove .
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 Pause/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 the Name and Metadata 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 allows the Name and Metadata mode and Host Authentication to be set on the selected Cryptainer.



Name	Change the name of the Cryptainer.
Metadata Mode	(Disk only) Forces Metadata ON for this Cryptainer. When a Cryptainer is created for a LUN, it is assigned key material for encrypting and decrypting data stored there. This key material is the metadata of the Cryptainer, which uniquely identifies the key associated with the LUN. This metadata is always stored in the configuration database of the DataFort as well as with an LKM server if one is configured. Forcing metadata on will allow DataFort to write this metadata to a block of the LUN when a Cryptainer is created, regardless of what is already on the disk. This can be useful when restoring data.

STORAGE MANAGEMENT

The Storage Management pane features the following elements:

Storage Pane Menu	Right-click in the Storage pane to use the top level menu. The menu offers options to modify or refresh the pane view and add a new collection of storage devices.
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 Tape Menu	Right-click a tape device to view the tape level menu. See Tape 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 .

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 85. 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 85. 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 whitespace 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 85.
Paths	Select the storage device and choose Show Alternate Paths to view all paths to the device. 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 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 110.
Import key	Import key allows a Cryptainer key for this LUN to be imported from a trustee. See Managing Trustees on page 110.
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.

TAPE MENU

While tape devices are managed with the **Storage > Manage Tapes** page, there are right-click menu options for tape devices on the SAN Topology page. Expand a storage device view to see its tape devices. Right-click a device to view the tape menu.

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.
Paths	Show Alternate Paths will display all mappings to the device. Select the storage device and choose Show Alternate Paths to view all paths to the device.
	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.
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.
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.

TAPE MANAGEMENT

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 105.
Tape Pool Collection Menu	Right-click a collection of tapes to use the collection menu. See Tape Pool Collection Menu on page 102. 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 103.
Individual Tape Device Menu	Right-click a tape device to view the device level menu. See Tape Device Menu on page 103.
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 .

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.
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 > Remove .
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 105.
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 110.

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. Once ACL Learning is on, clicking the onscreen ACL Learning is on link will bring up the [Tape Settings](#) page. See [Managing Tape Settings](#) on page 105. 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 general settings for the DataFort, including default settings for pools and tapes. These settings will determine how tapes and pools that are auto-detected are managed by default. Note that this page will only appear 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](#)

Tape Settings

Cluster-wide

Pool Settings and Defaults

Cleartext Default

☒ OFF - Auto-detected Pools will be encrypted

☐ ON - Auto-detected Pools will be cleartext

Default Pool Policy

☐ Pool - A key with no expiration is generated per pool

☒ Tape - A key is generated per tape

Tape Key Lifespans

0

Years

Default Read/Write Span (Use 0 for No expiration)

0

Years

Default Key Lifespan

Key Export

☐ OFF - Pool Keys will not be exportable

☒ ON - Pool Keys will be exportable

Tape Settings

ACL Learning

☐ OFF - Local ACL is enforced

☒ ON - All host accesses go through and are recorded in the local ACL

Compression

☐ OFF - Even if requested by hosts, data will not be hardware compressed

☒ ON - If requested by hosts, data will be hardware compressed before it is encrypted

Apply

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 represents the span in days that the key may be used for reading. Lifespan can be specified in days, months, weeks or years. Note that 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 110.

TAPE SETTINGS

Tape settings determine whether ACL learning and compression are on or off by default. By enabling compression DataFort may 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.

Turning ACL Learning on allows DataFort to record ACLs. When on, DataFort will monitor backup activity on the network and record which devices have access to storage.

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

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.

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 only or tape and disk

It is recommended that virtualization be ON for the Host HBA, and OFF for the Storage HBA on a DataFort in most tape or tape and disk 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 only

It is recommended that virtualization be ON for both the Host HBA and Storage HBA of a DataFort in most disk-only 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

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.
 - 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.

SAN Storage Settings

Cluster-wide

Virtualization Settings: requires DataFort(s) reboot

Host

☒ OFF - Do not virtualize on the host side
☐ ON - Virtualize up to 7 storage devices on the host side

Storage

☒ OFF - Do not virtualize the storage side
☐ ON - Virtualize up to 7 host devices on the storage side

Apply

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.

6 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 Licenses](#)
- [Managing Recovery Officers and Recovery Cards](#)

Any administrator can reset smart cards using the WebUI:

- [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 Cryptainer, tape and pool 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. Data is protected via Cryptainers, 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. 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.
- Files and information will need to be provided by the main site administrator so that the remote site administrator can import the trust package.

Main Site Initiation and TEP Creation

1. From the WebUI of the main site DataFort, select **System Config > Security > Manage Trustees**. Any current trustees will appear.



2. Click Initiate to start the process of creating a trustee relationship. The Initiate page will appear.
3. Enter the trustee name (this is what the trustee will be called locally).
4. The Self Name is what the remote DataFort will see when importing this TEP. Enter a name that the remote DataFort administrator will recognize.

Manage Trustees : Initiate

Initiate a new Trust Relation between two clusters by downloading a Trust Establishing Package (TEP).

Trustee Name

Self Name

NOTICE: Creating Trust Establishing Package for download...

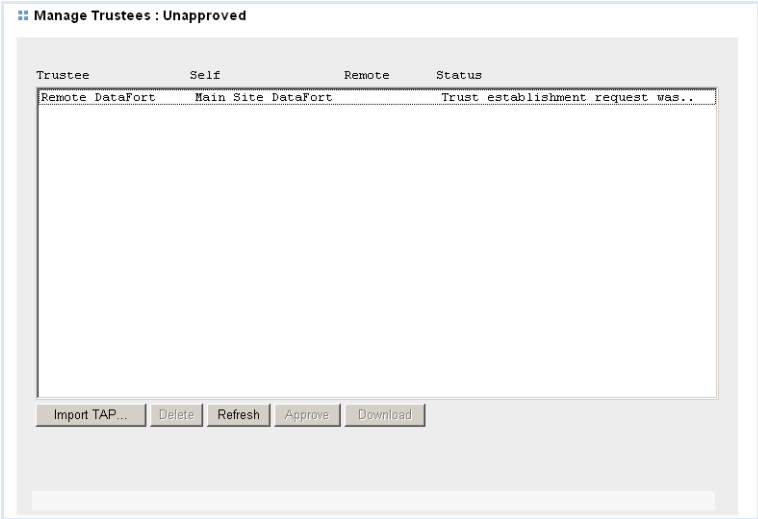
5. Click Generate TEP This will create a TEP and pop up a download file dialog. Download the file, saving it in an accessible location.
6. The TEP file needs to be transferred in some way to the remote DataFort site (for example via email).
7. The administrator of the main site can look up the verifier by clicking the Unapproved Trustee pending link on the Manage Trustees page.

Manage Trustees Cluster-wide

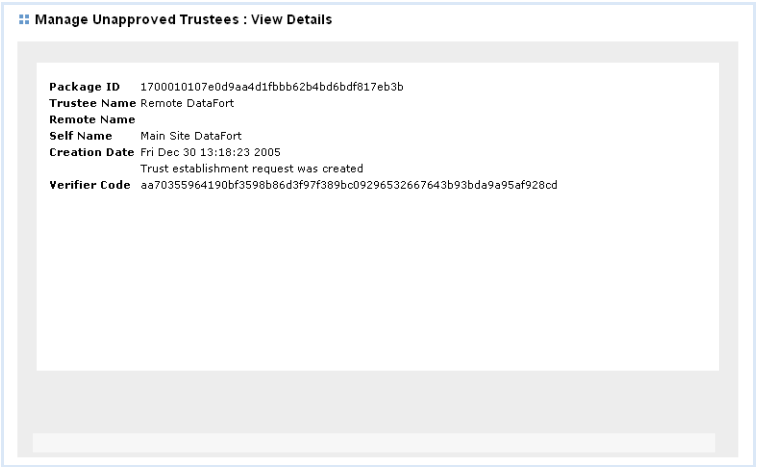
Trustees	Creation Time	ID

NOTICE: There are [unapproved trustees](#) pending.

- 8. Click the link to open the unapproved trustee page.



- 9. Double-click the unapproved trustee.



The verifier is listed on the View Details screen.

- 10. The main site administrator should relay the verifier to the remote site administrator.

Remote Site Importing TEP and Generating TAP

The remote site administrator should have the TEP file and the verifier from the main site administrator.

11. Once the TEP file is received at the remote site, it can be imported. From the WebUI of the remote DataFort, select **System Config > Security > Manage Trustees** and click Import TEP.

The screenshot shows a web interface titled "Manage Trustees : Import Trust Establishing Package". It contains two main sections:

1. Upload the Trust Establishing Package (TEP) from the remote Trustee Relation Initiator.

This section has a "Trust Package" label followed by a text input field, a "Browse..." button, and an "Upload" button.

2. Verify and approve the imported Trust Package using Recovery Cards:

This section has four input fields: "Initiator Name", "Verifier Code", "Trustee Name", and "Self Name". Below these fields are two buttons: "Verify & Approve..." and "Cancel".

12. Browse to the location of the file and click Upload. Once uploaded, the Initiator name will be updated with the self label assigned to the TEP. The administrator at the data recovery site should make sure the TEP is the correct one to import.
13. The remote site administrator should check with the main site administrator that the verifier matches the initiator name.
14. At the Import Trust Establishing Package page, the remote site administrator should type in the verifier, trustee name and the Self Name, which will be displayed to the main site administrator when receiving the TAP.

Manage Trustees : Import Trust Establishing Package

1. Upload the Trust Establishing Package (TEP) from the remote Trustee Relation Initiator.

Trust Package

2. Verify and approve the imported Trust Package using Recovery Cards:

Initiator Name: Main Site DataFort

Verifier Code: 55964190b3598b86d397389bc09296532667543b93bda9a95af928cd

Trustee Name:

Self Name:

NOTICE: TrustPackage imported. Please verify and approve the package.

15. Click Verify and Approve. DataFort will add the TEP and start a Data Recovery Card approval process. DataFort will prompt for Recovery Cards and passwords in order to verify the remote DataFort and approve the TEP.
16. Once the TEP is approved, a TAP will automatically be generated and a download file dialog will appear. Save the file in an accessible location.
17. The remote site administrator should transfer the TAP to the main site administrator.

Main Site Importing TAP

18. Upon receiving the TAP, the main site administrator should access the Manage Trustees page and click the Unapproved Trustee pending link on the page.

Manage Trustees Cluster-wide

Trustees	Creation Time	ID
Remote DataFort	Fri Dec 30 13:46:18 2005	160000013f5831f1be16b705123b..

NOTICE: There are [unapproved trustees](#) pending.

19. The Manage Unapproved Trustees page appears.

Trustee	Self	Remote	Status
Remote DataFort	Main Site DataFort	Main Site..	Trust authorization was created

Import TAP... Delete Refresh Approve Download

20. Click Import TAP

Manage Trustees : Unapproved : Import Trust Accepting Package

1. Upload the Trust Accepting Package (TAP) from the remote Trustee Relation Responder.

Trust Package

2. Verify and approve the imported Trust Package using Recovery Cards:

Responder Name

Verifier Code

21. Browse to the TAP file and click Upload. The responder name will be displayed, and the main administrator should contact the data recovery administrator for the verifier.
22. Once the verifier is obtained and entered, clicking Verify & Approve launches a Data Recovery Card authorization process.
23. When approval is complete, a trustee relationship has been created.

Note: Imported keys and trustees are replicated in a cluster. A trustee added on one DataFort should be able to export and import keys to all the cluster members in the remote trustee's cluster.

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.

CONFIGURING MANAGEMENT SECURITY SETTINGS

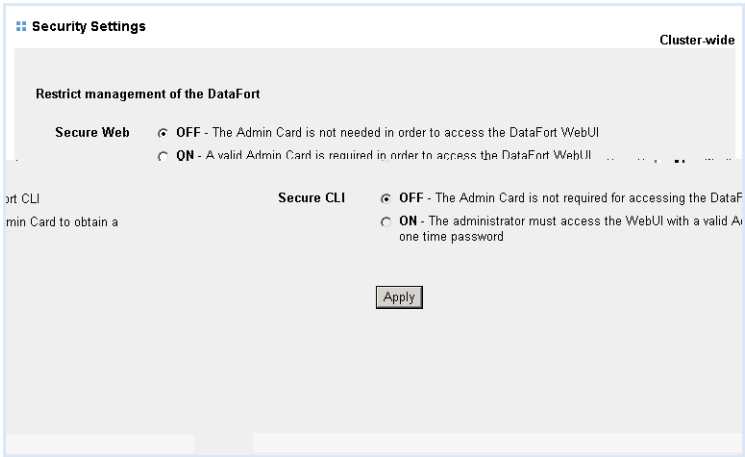
DataFort offers configurable levels of security for DataFort management interfaces.

- 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.



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 122. 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.

SETTING A LOCAL SECURITY CERTIFICATE

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

The local certificate is self-signed.		
Valid From	Jun 6 01:00:05 2003 GMT	
Valid Till	Jun 5 01:00:05 2006 GMT	
Common Name	Issued To	Issued By
Country	DataFort	DataFort
State / Province	US	US
City / Town	CA	CA
Organization Name	Redwood City	Redwood City
Organization Unit	Decru, Inc.	Decru, Inc.
Contact Email	Technical Support	Technical Support
	support@decru.com	support@decru.com

2. Click Use Self-Signed.

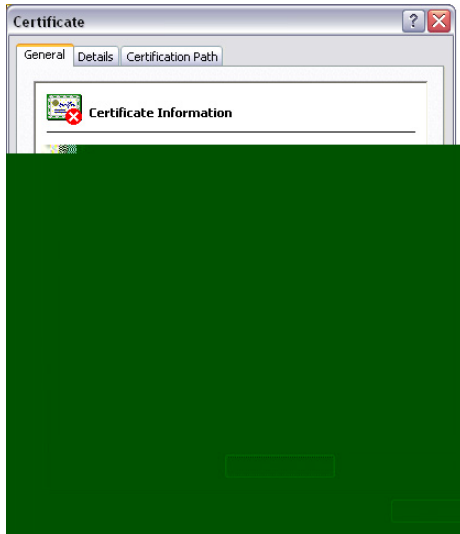


The DataFort hostname will appear in the Common Name field. The Common Name must be the hostname or IP address of this DataFort. If a hostname is used, it must be resolvable by DNS.

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 193.

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**.

DataFort Certificate DataFort poly Show

The local certificate is self-signed.

Valid From	Jun 6 01:00:05 2003 GMT
Valid Till	Jun 5 01:00:05 2006 GMT

Common Name	DataFort	Issued To	DataFort	Issued By	DataFort
Country	US		US		US
State / Province	CA		CA		CA
City / Town	Redwood City		Redwood City		Redwood City
Organization Name	Decru, Inc.		Decru, Inc.		Decru, Inc.
Organization Unit	Technical Support		Technical Support		Technical Support
Contact Email	support@decru.com		support@decru.com		support@decru.com

Use Self-Signed... Use CA-Signed...

2. Click Use CA-Signed.

DataFort Certificate : Request & Set DataFort poly Show

1. Generate a signing request, and submit the request to a Certificate Authority.

Common Name	olympia	[Generated Request]
Country Code		
Province/State		
City/Town		
Organization Name		
Organization Unit		
Contact Email		

Generate Request

2. Paste the signed request from the Certificate Authority below and set as certificate.

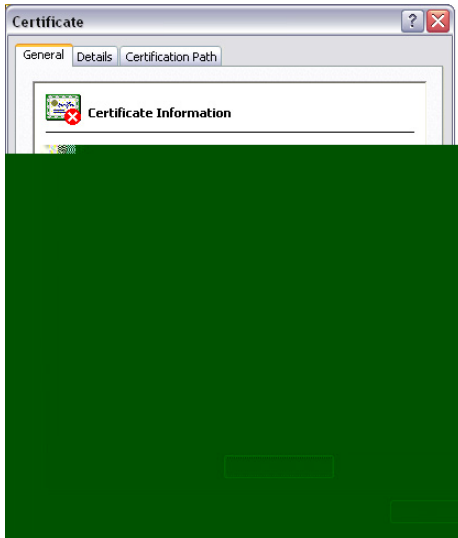
Set as Certificate Cancel

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 193.

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; instead you will see a valid certificate message.

MANAGING LICENSES

DataFort features (such as clustering) 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.

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.

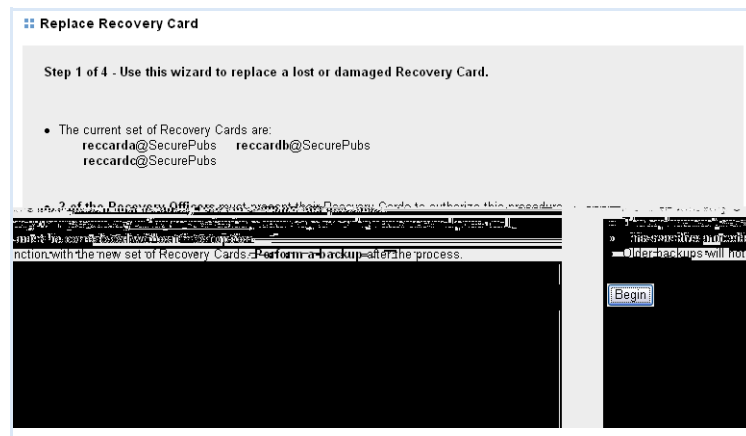
Note: Card replacement procedures are sensitive, and should not be interrupted by any other configuration or activity.

Card replacement procedures require:

- A replacement card (uninitialized or initialized).
- The required Recovery Officers and their Recovery Cards. 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 create a new Recovery Card.

REPLACING A 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.

Replace Recovery Card

Step 2 of 4 - Mark the Recovery Card to be replaced.

Known Recovery Cards

Label	Security Domain	Card ID
reccarda	SecurePubs	0900000048de53bc3ae10c52cfc0ab3ba7eb9a82
reccar db	SecurePubs	090000007ac343cfaea4225cd5d26ab8451a2886
reccar dc	SecurePubs	09000000942c8759f682dee01061ce123c0b9d25

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**.

Recovery Officers

This page allows Recovery Officers to change the passwords on their Recovery Cards.

Recovery Schema	2 out of 3
Recovery Cards	reccarda@SecurePubs reccardb@SecurePubs reccardc@SecurePubs

Please insert a Recovery Card, load its properties and enter the passwords.

Card Label

Security Domain

Current Password

New Password (8 - 30 characters)

Confirm Password

2. Insert the card for which the password will be changed into the Management Station smart card reader. Strong passwords are an important part of the overall security of the system. New passwords should be 8 or more characters, and include letters, digits and punctuation marks.
3. Click Load.
4. Enter the existing password.
5. Enter the new password.
6. Click Change.

SMART CARD RESET

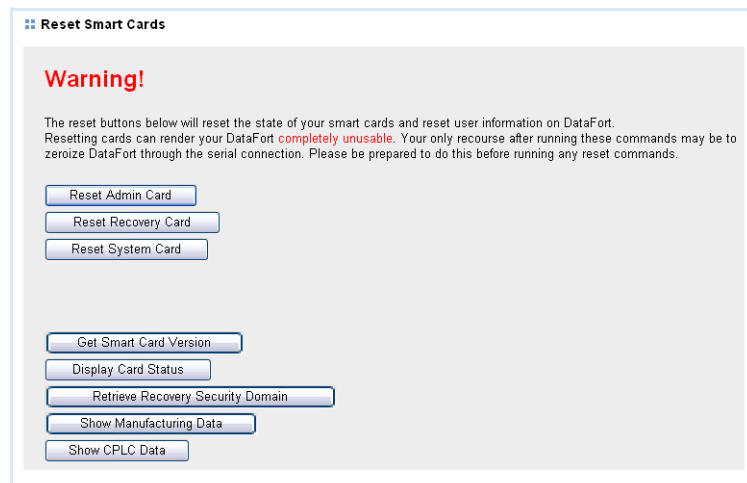
It is possible to completely reset a smart card using a special DataFort Reset Smart Cards page. This page also allows the administrator to check smart card versions and status.

CAUTION: 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.

The DataFort configuration database contains all relevant information about the secure network including information about Cryptainers, storage, hosts and administrators. 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.

SAVING CONFIGURATIONS TO LIFETIME KEY MANAGEMENT SOFTWARE

It is good practice to automate backups of key data to Decru's Lifetime Key Management software. The LKM software will manage keys and Cryptainer information 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 used for Cryptainers, tapes and pools, even if the original keys are purged from DataFort or the source DataFort is decommissioned. Keys are encrypted while in transit to the LKM server. 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, DataFort will back up the configuration database to LKM 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.

CONFIGURING BACKUPS TO LKM

Us.6(e) e this procedure to set up regular automatic backups. DataFort se pportse to four s.6(e) ervrse r the LKM system. Backups will be sent all LKM serve1(er)TJ22.8723 0 TD0.0014 ToX.0035 Two(s)-7.1(at)-4.8(the)-7.1(same) 1.in to the WebUe1(I, an)-5.8(d cho)-5.8(yaffs) -Reco very > LKM Settings.

2. Enter a label and description that will identify this DataFort in the LKM interface.

Lifetime Key Management (LKM) Settings

DataFort

Decru recommends the use of the LKM system to archive encryption keys for data restoration.

This unique label will be used to identify this particular DataFort in the LKM system.

Label

Description (Optional)

DataFort will automatically back up its configuration database to the LKM server(s) specified below. (Cluster-wide)

IP Address	Port	Using SSL
10.20.22.230	15362	0
10.20.23.19	15362	0
10.20.23.25	15362	0
10.40.3.185	15362	0

3. Click Add.
4. Enter the IP address of the LKM 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.
If you prefer to send backups over an SSL connection, skip to [Backups over SSL](#).
6. Click Apply.

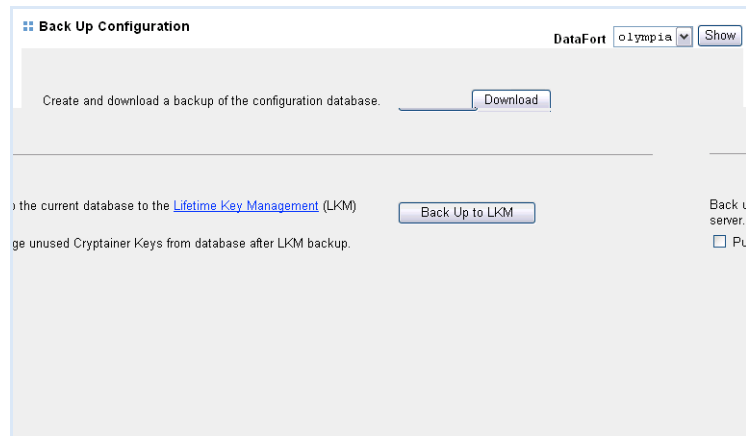
Backups over SSL

1. To configure DataFort to communicate with the LKM server across a secure SSL connection, select the Using SSL Connection button.
2. Enter and confirm a shared secret. The shared secret can be any string of up to 32 characters, including spaces.
3. As soon as possible, plan to enable SSL and enter the same shared secret into the LKM UI. Until this is done, secure (SSL) backups to the LKM server will not proceed.
4. Click Apply.

BACKING UP THE CONFIGURATION TO LKM

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 Cryptainers 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 8](#) on page 132 outlines the relationship between tape settings and key generation. See [Managing Tape Settings](#) on page 105 for information about tape settings.

TABLE 8: 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**.

The screenshot shows a web interface titled "Back Up Configuration". At the top right, there is a "DataFort" label, a dropdown menu showing "olympia", and a "Show" button. The main content area has a light gray background. It contains the text "Create and download a backup of the configuration database." followed by a text input field and a "Download" button. Below this, there is a section with the text "Back up the current database to the [Lifetime Key Management \(LKM\)](#)" and a "Back Up to LKM" button. To the right of this section, there is a "Back server" label and a checkbox labeled "Force". Below the checkbox, there is a line of text: "Delete unused Cryptainer Keys from database after LKM 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.

■ ■ ■ ■ 8 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:

- [Managing DataFort Defense Responses](#)
- [Configuring and Viewing Logs](#)
- [Zeroizing the Decru DataFort](#)

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. |
| 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 136).
- 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 can be restored to a previous configuration.

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 extended periods), DataFort may not detect or signal a physical intrusion.

CAUTION: 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 9. If in doubt, choose the Basic level.

TABLE 9: 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

To change the defense setting after setup:

1. From the WebUI, choose **System Config > Security > Defense Settings**.
2. Select the level of desired defense.

Note: Only a Full Administrator can change the defense setting. After setup the defense level can be raised but not lowered.

3. Click Apply.

Defense Settings

During a defense-triggering event*, DataFort will stop processing in order to protect secured data. Certain procedures will then be required for restoring normal operation.

Important: Choose the Basic Level if unsure. Defense Settings can only be increased after they are set on this page.

Administrative Procedures for Recovery	
☒ Basic Level 	For all defense-triggering events, clear the alert and reboot DataFort.
☐ Medium Level 	For a low battery condition, clear the alert and reboot DataFort. For all other defense-triggering events, zeroize and restore DataFort from a backup configuration and a set of Recovery Cards.
☐ High Level 	For all defense-triggering events, zeroize and restore DataFort from a backup configuration and a set of Recovery Cards.

* **Defense-triggering events** :

- Physical intrusion to DataFort
- A low battery condition when switching on DataFort
- One touch of the physical CryptoShred button (available on some DataFort appliances)

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.

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 144. A new System Card will have to be initialized. DataFort can be restored to the last configuration that was downloaded or backed up.

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)

It is recommended that logs be stored in more than one location. See [Recommended Configuration](#) on page 139 for an example of a secure logging configuration.

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**.

Logging Configuration Cluster-wide

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

Source	Priority	Location				Signed
		Temporary	Database	Remote Logging Host	Event Log Host	
Security	Low (6)	☒	☒	☒ 10.101.11.49	☐	☐
	High (4)	☒	☒	☒ 10.101.11.49	☐	☐
Operations	Trace (7)	☒	☒	☒ 10.101.11.49	☐	☐
	Information (6)	☒	☒	☒ 10.101.11.49	☐	☐
	Warning (4)	☒	☒	☒ 10.101.11.49	☐	☐
	Error (1)	☒	☒	☒ 10.101.11.49	☐	☐
Performance	Low (6)	☒	☒	☒ 10.101.11.49	☐	☐
	High (4)	☒	☒	☒ 10.101.11.49	☐	☐

1. 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.
2. 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**.

Source	Priority	Location			Event Log Host	Signed
		Temporary	Database	Remote Logging Host		
Security	Low (6)	☒	☒	☒ 10.10.21.49	☐	☒
	High (4)	☒	☒	☒ 10.10.21.49	☐	☒
Operations	Trace (7)	☒	☒	☒ 10.10.21.49	☐	☒
	Information (6)	☒	☒	☒ 10.10.21.49	☐	☒
	Warning (4)	☒	☒	☒ 10.10.21.49	☐	☒
	Error (1)	☐	☒	☒ 10.10.21.49	☐	☒
Performance	Low (6)	☒	☒	☒ 10.10.21.49	☐	☒
	High (4)	☒	☒	☒ 10.10.21.49	☐	☒

Buttons: Apply, Reset, Edit User...

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

This information will be used for Windows Event Logging.

Domain:

User:

Password:

Confirm Password:

Buttons: Apply, Cancel

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 10](#) shows the Descriptive Name, System Property Name, Syslog Facility and Level mapping for DataFort logs.

TABLE 10: 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 11](#) describes the mapping for temporary logs.

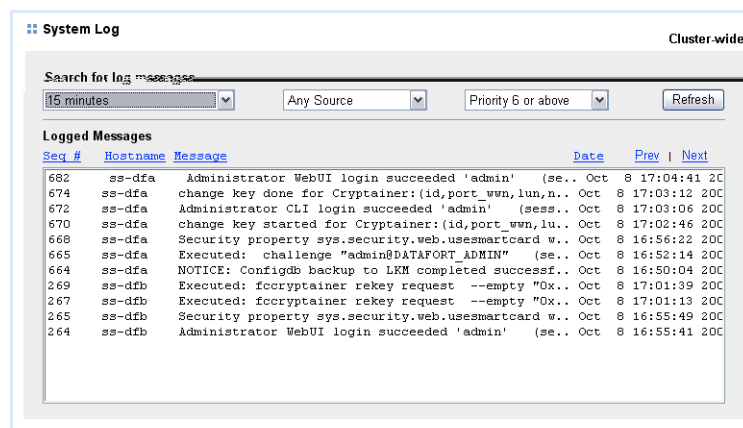
TABLE 11: TEMPORARY LOG MAPPING

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, 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 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

Verify the correctness of the log by ensuring that the 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 139) 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 160.

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.

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 an LKM server, 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.

Zeroization using the WebUI is described below. If login to the DataFort WebUI is impossible, zeroization can be performed using the CLI or serial console. This is described in the following section.

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

ZEROIZING AFTER SETUP

If after running the Setup Wizard, you discover that the initial configuration is incorrect, or you must zeroize for some other reason, it is best to do so before creating Cryptainers. Log into the WebUI and complete steps to zeroize as described below. If necessary, you may also need to reset smart cards initialized during the Setup Wizard, as described in [Configuring and Viewing Logs](#) on page 138.

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.

1. From the WebUI, choose **System Config > Security > Zeroize**.
2. If it is desirable to preserve the IP address assigned to DataFort, leave the Keep DataFort IP address box checked.

Zeroize DataFort **qa-decru16** Show

Secured data will not be readable by DataFort "qa-decru16" after zeroization.

Details

Zeroizing the DataFort appliance "qa-decru16":

- Deletes cryptographic key material from the SEP
- Deletes cryptographic key material from and resets application state of the System Card
- Deletes configuration data

Decryption of secured data will not be possible via the DataFort appliance unless the Recovery Wizard is run. Recovering this DataFort appliance requires a backup of the configuration database and the presence of 2 Recovery Officers and their Recovery Cards.

Steps

Click 'Zeroize'. The DataFort appliance "qa-decru16" will reboot after zeroization. Set the DataFort network configuration after reboot. (See Admin Guide.)

☒ **Keep DataFort IP addresses**

Zeroize...

3. Click Zeroize.
4. Type the provided code into the popup box to verify that you want to zeroize this DataFort.
5. When a message appears informing you of the system reboot, click OK.
6. Close the browser.
DataFort will reboot.
7. 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 38.
8. 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. Log in to the CLI with a valid administrator username and password.
2. 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.
3. Enter the command again, followed by the code.
`system zeroize [confirmation-value]`
4. Wait while the System Card is reset, and the DataFort reboots.

5. If they were not preserved, reassign the DataFort IP settings as described in [Assigning the DataFort IP Address](#) on page 38.
6. 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. Connect the serial console port (see [Connecting the Serial Console Port](#) on page 75).
2. Log in to the serial console with a valid administrator username and password.
3. To zeroize DataFort, enter option **Z**.
4. Enter a confirmation code when prompted.
The DataFort will reboot.
5. Assign the DataFort IP settings. See [Assigning the DataFort IP Address](#) on page 37.
6. After the DataFort has been assigned IP settings, complete the configuration by running the Setup Wizard.



9 CLUSTER ADMINISTRATION

A cluster is created using the Setup Wizard. See [Chapter 3](#) for instructions on completing the wizard. Note that standalone DataFort appliances cannot be joined together to form a cluster.

A 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.

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. Cluster management tasks include:

- [Maintaining the Cluster Quorum](#)
- [Adding and Removing Cluster Members](#)
- [Replacing a DataFort in a Cluster](#)
- [Recovering a Cluster](#)
- [Resolving a Cluster Conflict](#)

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.

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 12 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.

TABLE 12: CLUSTER QUORUM EXAMPLES

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

TABLE 12: CLUSTER QUORUM EXAMPLES (CONTINUED)

Number of DataFort Appliances in Cluster	Required Number of Online DataFort Appliances
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.

IP Settings

Hostname:

DNS Suffix: (Optional)

DNS Search Path(s): (Optional)

DNS 1: (Optional)

DNS 2: (Optional)

Gateway:

DataFort: Show

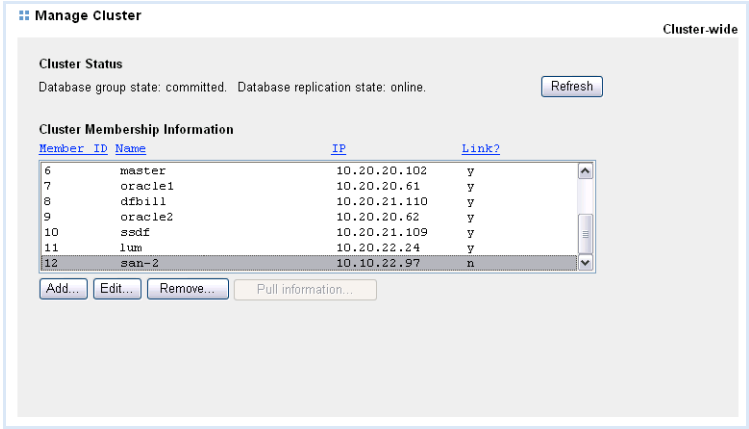
- poly
- df1
- df4
- db
- peg
- past
- master
- oracle1
- dfbill
- oracle2

CHECKING THE CLUSTER STATE

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**.

Use the Manage Cluster page to add, edit or delete cluster members. See [Adding and Removing Cluster Members](#), [Replacing a DataFort in a Cluster](#) and [Recovering a Cluster](#) for details on using the WebUI to manage the cluster.

Note: See [Cluster Management](#) on page 158 for information on using the CLI to manage clusters, including the ability to disable cluster members if necessary.



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 13 for a description of cluster states.

TABLE 13: 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. See Resolving a Cluster Conflict .	

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 3](#) 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. See [Maintaining the Cluster Quorum](#) for details. 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 158.

Adding a Cluster Member

Keep the following in mind when adding new DataFort appliances to 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 144.
- 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 members would 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 Administrator can run the wizard and add a cluster member.
- Adding a cluster member to an existing cluster or a standalone DataFort is just like creating a cluster from the outset.

Removing a Cluster Member

A DataFort 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.
5. Cluster status will be aborted/recover until the change to the cluster has been completed.

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 150.

1. Log in to the WebUI of DataFort 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.

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. Click Add. To leave the shared secret unchanged, click Next. To change the shared secret for the cluster, enter it and click Set.
 5. Click Add. In the popup window, enter the IP address of the member that will be added. Click OK.
 6. Click Next.
 7. Make a note of the instructions on the page, and click OK.
 8. Log out of the WebUI of the online DataFort.
 9. Replace the removed DataFort with the new, uninitialized DataFort.
 10. Assign an IP address to that DataFort as described in [Assigning the DataFort IP Address](#) on page 37 and connect the new DataFort to the network.
 11. 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. See [Introduce Cluster Members](#) on page 47.

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 144).

- 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 [Replacing a DataFort in a Cluster](#) on page 151. 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. See [Assigning the DataFort IP Address](#) on page 37.
 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.
 4. Add the second DataFort during the wizard.

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.

Manage Cluster

Cluster wide

Cluster Status

Database group state: committed. Database replication state: conflict.

Refresh

Cluster Membership Information

Member	ID	Name	IP	Link?
0		df-2b	10.20.22.96	y
1		tire	10.20.21.87	y
2		df-2a	10.20.22.144	y

Add...

Edit...

Remove...

Pull information...

Sensitive changes have been made to DataFort configuration. Making a [backup](#) is recommended.

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.”



■ ■ ■ ■ 10 MACHINE ADMINISTRATION

A Full Administrator or specified Machine Administrator can complete all the procedures described in this chapter. Machine administration includes tasks that allow system properties to be set and DataFort upgrades to be executed:

- [System Configuration](#)
- [Upgrading DataFort](#)

SYSTEM CONFIGURATION

You can review and reset system settings at any time using the System Configuration options of the WebUI. The System Config menu in the WebUI allows access to the following:

- [Date and Time](#)
- [Network Settings](#)
- [SNMP Settings](#)

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.

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.

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. The Decru MIB tree is available from Decru.

Supported version SNMPv1, SNMPv2c.

Supported tools Generally available SNMP tools can be used to query SNMP MIBs.

Supported MIBs Standard MIB-II (Internet MIB) as described in RFC 1157.
Private Decru MIB.

Enabling and Disabling SNMP

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.

SNMP Configuration

The following MIBs can be configured using the SNMP Settings 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.

1. To set the SNMP connection to DataFort for use with SNMP tools such as HP OpenView, choose **System Config > Network > SNMP Agent**.
2. Enable SNMP using the radio button.
3. Enter the System Location. The System Location field is a string that describes the location of the system (the DataFort).
4. In the System Contact field, enter the contact information for the person responsible for managing SNMP.
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.
8. Click Apply.

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.

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.

■ ■ ■ ■ 11 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. Frequently used procedures are described in this chapter, including:

- [Administration Commands](#)
- [Storage Management Commands](#)

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 181 of this guide.

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. 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 72). 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](#)
- [Cluster Management](#)
- [System Properties and Log Management](#)
- [Stack Trace Settings](#)
- [Network Management](#)
- [Turning on Metadata Support](#)

ADMINISTRATOR ROLES

Use the CLI to find out which administrators can execute particular CLI commands. Some commands are limited to a specialty administrator or a Full Administrator. The roles are:

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

1. Log in as the 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. With the CLI you must grant these properties explicitly. Substitute the role name (from the list above) for `<group>`.

1. Log in to the CLI as a Full Administrator.
2. To create an administrator for a single DataFort:

```
user add <group> <username>
```

3. To create an administrator that is replicated to cluster partners:

```
user add --replicate <group> <username>
```

CLUSTER MANAGEMENT

The following commands are useful when managing clusters.

cluster status Shows the status of a DataFort cluste

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 utilities 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 <mesg>`
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) [AAAAAEAAAAFAAAAgUpQA== 3NKQ18/
5r3x6n+Rw]

system log verify "boxmanager: Executed: share virtual add --ip
\"his\" \\\\\\\his\\\\\\chi \"nas-hiro1\" (sess id: 228933632)
[AAAAAEAAAAFAAAAgUpQA== 3NKQ18/5r3x6n+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 [AAAAAEAAAAHAAAnCruPg==
5uKW37o/jlF5t+VT]"
```

This returns:

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

Execute the verification procedure again to check sequence validity:

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

This returns:

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

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 leak 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](#)[Cryptainer Commands](#)
- [Fibre Channel Kernel Commands](#)

A list of top-level commands can be found in the [Command Line Interface Quick Reference](#).

DISK COMMANDS

To perform storage device management commands, first execute the `disk list` command to get necessary information such as the `<node-wwn>` `<port-wwn>` `<lun>` of the device.

<code>disk list</code>	Generates a list of all storage devices and their status on the cluster. Options include query offset and limit, hidden disk, host port WWN, node-wwn, disk node WWN, port-wwn, disk port WWN, disk LUN, disk name, Cryptainer id, disk with no associated Cryptainer, WWN of the DataFort HBA which discovered the disk and name of the DataFort that has paths to the disk(s).
<code>disk rescan</code>	Rescans the fabric for disks. This command may be needed to update recent changes to disks.
<code>disk remove</code>	Enter the device parameters into the command to remove it from the configuration database: <code>disk remove <port-wwn> <lun></code> . Options include specifying the host port WWN, the WWN of the DataFort HBA which discovered the disk and the name of the DataFort that discovered the disk.
<code>disk rmall</code>	Enter the device parameters into the command: <code>disk rmall <port-wwn></code> . All devices associated with the indicated WWN will be removed from the configuration database. There is also an option to indicate the host port WWN.
<code>disk blink</code>	Enter the disk parameters into the command: <code>disk blink <host-port-wwn> <lun> on off</code> . If the value is set on, the LED on the selected disk 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 <code>disk rescan</code> command.
<code>disk map</code>	To add a second path to an existing Cryptainer, first find the Cryptainer ID using the <code>fcery list</code> command. Enter device and Cryptainer parameters: <code>disk map <port-wwn> <lun> <cryptainer-id></code> . There is also an option to indicate the host port WWN.
<code>disk rmap</code>	Execute the <code>disk rmap</code> command to remove the path to the Cryptainer, using the same device and Cryptainer parameters: <code>disk rmap <port-wwn> <lun> <cryptainer-id></code> . 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 rmmmap <primary-port-wwn> <alternative-port-wwn>
```

Replacing a Device Maintaining Cryptainer Mapping

This command maps a device's Cryptainer keys to a new device.

1. Use the `fccryptainer list` command to list the Cryptainers in the system. Identify the Cryptainer-ID of the Cryptainer to be replaced.
2. Use `disk list --cryptainer-id <cryptainer-id>` to retrieve the old node-WWN, port-WWN, LUN on which the Cryptainer was created originally.

Note: In a cluster, remove the secondary path (use the `disk rmmmap` command) before replacing the device. Remap the new secondary path information to the replaced device.

3. Use `disk list` to retrieve the `<new-node-wwn>` `<new-port-wwn>` `<new-lun>` parameters for the replacement (new) device.
4. Execute the `disk replace` command with the device information:

```
disk replace <old-port-wwn> <old-lun> <new-port-wwn> <new-lun>
```

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.

<code>host list</code>	Generates a list of all hosts and their status on the cluster.
<code>host rescan</code>	Rescans the cluster, forcing a loop reset on the Host side of the fabric. This command may be needed to update recent changes to hosts.
<code>host add</code>	Enter information about the host that will be added: <code>host add <node-wwn> <port-wwn> <name></code> .
<code>host remove</code>	The indicated host will be removed from the configuration database: <code>host remove <port-wwn></code> .

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, use `sys prop set`:

```
sys prop set dfc.isp.max_host_vp 7
```

```
sys prop 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.

CRYPTAINER COMMANDS

To perform Cryptainer management commands, first execute the `fccryptainer list` command to get necessary information about Cryptainers in the configuration database. Note that `fccryptainer` can be shortened to `fccry`. Note that some commands are only applicable to disk and not to tape drives.

<code>fccryptainer list</code>	View all Cryptainers hosted by the cluster. Options include offset and limit, host port WWN, disk node WWN, disk port WWN, disk LUN, WWN of the DataFort HBA with a path to the Cryptainer, name of the DataFort that discovered the disk where the Cryptainer is located, Cryptainer ID, or Cryptainers not accessible from host port or node WWN.
<code>fccryptainer path</code>	Lists all paths to Cryptainers. Options include offset and limit, host port WWN, disk node WWN, disk port WWN, disk LUN, WWN of the DataFort HBA with a path to the Cryptainer, name of the DataFort that discovered the disk where the Cryptainer is located, Cryptainer ID, or Cryptainers not accessible from host port or node WWN.
<code>fccryptainer perm list</code>	Lists permissions on all Cryptainers. Options include offset and limit, host node WWN, host port WWN, disk node WWN, disk port WWN, disk LUN and Cryptainer ID.
<code>fccryptainer rekey list</code>	Lists all rekey jobs with status.
<code>fccryptainer rekey request</code>	Request a rekey job: <code>fccry rekey request <cryptainer-id></code> . Options include indicating that data will be decrypted, that the Cryptainer is empty, block access to the Cryptainer, the WWN of the DataFort HBA which should do the rekey and the name of the DataFort to be used to do the rekey.
<code>fccryptainer rekey notify</code>	Reactivate a stalled or stopped rekey job (activate all new or changed key requests).
<code>fccryptainer add</code>	Use the command to add a Cryptainer, specifying disk information and mapping options: <code>fccry add <map-type> <port-wwn> <lun></code>. Indicate <code>map-type</code> as <code><lunmap portmap></code>. Options include a description, the option to create a cleartext Cryptainer (assigning no key), create a Cryptainer that can be exported to trustees, enter the start and end LBA for unencrypted region to allow for partial encryption, indicate the host port WWN, forward port WWN. Specify that the Cryptainer be added as cleartext (unencrypted) with the <code>nokey</code> option (disk Cryptainers only): <code>fccry add --nokey <map-type> <port-wwn> <lun></code>.
<code>fccryptainer createall</code>	Use the command to automatically create one Cryptainer per LUN in a multi-disk target. Specify disk information and mapping type: <code>fccry createall <map-type> <port-wwn></code> . Options are the same as when using <code>fccry add</code> .

<code>fccryptainer clone</code>	Reuses one Cryptainer's key for another Cryptainer, creating a new Cryptainer for a copied LUN. Specify Cryptainer information: <code>fccry clone <cryptainer-id> <map-type> <port-wwn> <lun></code> . Options include description, host port WWN and forward port WWN.
<code>fccryptainer remove</code>	This command removes the keys and access associated with a Cryptainer from the configuration database: <code>fccry remove <cryptainer-id></code> . Use the <code>[-f, --force]</code> option to attempt to remove the Cryptainer without prompting for confirmation. A removed Cryptainer can be restored as long as the storage device on which it was created remains. To aid in recovery, record the port WWN and LUN number of the Cryptainer before removal. Note that DataFort stores information about Cryptainers, even deleted Cryptainers, indefinitely unless they are purged when saved to LKM.
<code>fccryptainer rmall</code>	Remove all Cryptainers from the configuration database. Use the <code>[-f, --force]</code> option to attempt to remove all Cryptainers without prompting for confirmation.

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 `rval` command:

`fccry rval access <cryptainer-id>`

TURNING ON METADATA SUPPORT

When a Cryptainer is created for a LUN, it is assigned a key for encrypting and decrypting data stored there. This key is the metadata of the Cryptainer. If metadata is on, DataFort also writes this metadata to a block of the LUN when a Cryptainer is created. This command is available for Cryptainers created on disk only.

In circumstances where the Cryptainer Key ID associated with a LUN cannot be identified from either the configuration database of the DataFort or the LKM server, the administrator can use the metadata written on the LUN to restore Cryptainer.

1. Use the **fccry set** command to turn metadata support on:

```
fccry set [-d, --descrip <descrip>] [--metadata <metadata>]
<cryptainer-id>
```

Set metadata options to **on** or **force**. Forcing metadata on will allow DataFort to write metadata, regardless of what is already on the disk.

Note: Metadata is off for cleartext Cryptainers until they are rekeyed (encrypted).

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). 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.



12 TROUBLESHOOTING

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

- [Front Panel LEDs](#)
- [Hardware Issues](#)
- [Network Connections and Management Interfaces](#)
- [Storage Network](#)
- [Clusters](#)
- [Smart Cards](#)

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](#)

FRONT PANEL LEDs

Depending on the type of chassis, the DataFort front panel features one or two bi-colored LEDs that signal the status of DataFort, as summarized in the tables below.

TABLE 14: 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 15: 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

TABLE 15: FRONT PANEL LEDs - 1U (CONTINUED)

Color	Behavior	Indication
Red	Solid	Network error, no traffic
Red	Blinking	Error found, with traffic

HARDWARE ISSUES

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

CAUTION: THERE ARE NO SERVICEABLE PARTS INSIDE THE DATAFORT. DO NOT OPEN THE CHASSIS.

NETWORK CONNECTIONS AND MANAGEMENT INTERFACES

[Table 16](#) contains troubleshooting tips for the network and management connections to DataFort.

TABLE 16: 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 turn 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.

TABLE 16: NETWORK CONNECTIONS AND MANAGEMENT INTERFACES (CONTINUED)

Problem	Possible Cause and Solution
Cannot connect to IP address	• Check that IP settings were set and saved after initialization. See Assigning the DataFort IP Address. • Make sure the DataFort IP address is reachable on the network from the Management Station.
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, but messages will appear about this condition. • For a DataFort that has not been configured, switch DataFort off, and re-insert the System Card before switching it back on. Make sure the System Card is inserted all the way into the front panel slot, with gold contacts facing up and to the back of the slot. • 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.
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. • If Secure Web is turned on, a valid administrator name and Admin Card are needed when logging in. • If Secure Web is on, Terminal Services or Remote Desktop cannot be used to 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 and Connecting via WebUI using Dual Authorization.
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.
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.

TABLE 16: NETWORK CONNECTIONS AND MANAGEMENT INTERFACES (CONTINUED)

Problem	Possible Cause and Solution
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: <code>system property get sys.security.web.usesmartcard</code> to check the setting. A setting of <code>1</code> requires the Admin Card in order to log in to the WebUI; <code>0</code> disables the requirement. If necessary, enter: <code>system property set sys.security.web.usesmartcard 0</code> 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 <code>kfc sync</code>. Reload the WebUI.

SMART CARDS

[Table 17](#) contains troubleshooting tips for working with smart cards.

TABLE 17: 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.
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: <code>system property set sys.security.web.usesmartcard 0</code> 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.
Lost Recovery Card	• Assemble a quorum of Recovery Officers and replace the Recovery Card.
Smart card errors appear	• Use an eraser to clean the metal contact on the smart card.

STORAGE NETWORK

[Table 18](#) includes troubleshooting tips for the storage network.

TABLE 18: STORAGE NETWORK

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. • 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.
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.
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.

CLUSTERS

[Table 19](#) includes troubleshooting tips for cluster management issues.

TABLE 19: 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 <code>cluster stat</code> on each of the members in the cluster. • If there are two members that are not communicating, disable both of them and then bring them back one at a time, making sure that the cluster forms with each addition. Use the <code>cluster disable</code> 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 <code>cluster disable</code> command to remove an offline member from the cluster and redefine the number of members required for the quorum.
Cluster goes into standalone mode during rekey	If a clustered DataFort is put into standalone mode during a rekey, and the Cryptainer being rekeyed had a path to the DataFort that left the cluster, 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.

DECURU 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 `vcmfnd` 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.

DECURU 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

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/rdisk/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/rdisk/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 to do so:

```
# 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 LT02 SERIALIZED COMMANDS

If a backup or restore to an LT02 tape drive fails and the drive returns CheckCondition, Aborted Command and Overlapped Command Attempted (0x4e/0x00), set the following system property (while there is no data I/O):

```
sys prop set dfc.serialize_storage_cmds true
```



■ ■ ■ ■ 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 72. 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

- 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 `?` to view the top level commands.

<code>device...</code>	SAN storage device commands...	Device Commands
<code>disk...</code>	SAN disk commands...	Disk Commands
<code>fcsite...</code>	DataFort Fibre Channel site configuration commands...	FC Site Commands
<code>fccryptainer...</code>	SAN Cryptainer commands...	FCC Cryptainer Commands
<code>host...</code>	SAN host commands...	Host Commands
<code>kfc...</code>	SAN kernel commands.	KFC Commands
<code>pool</code>	SAN pool (tape) commands...	Pool Commands
<code>tape...</code>	SAN tape commands...	Tape Commands
<code>cli...</code>	Command line commands...	CLI Formatting Commands
<code>help +</code>	Command line usage help	Help Command
<code>quit</code>	Quit the current client session	Quit Command
<code>active-role...</code>	Active role commands...	Active-Role Commands
<code>authorize +</code>	Authorize admin login	Authorize Command
<code>password +</code>	Change user password	Password Command
<code>role...</code>	Role commands...	Role Commands
<code>user...</code>	User commands...	User Commands
<code>whoami</code>	Display effective user ID	Whoami Command
<code>trustee</code>	Trustees management commands...	Trustee Commands
<code>net...</code>	Network commands...	System Commands
<code>keyman...</code>	Key management commands...	Key Management Commands
<code>lkm...</code>	LKM management commands...	LKM Management Commands
<code>cluster...</code>	Cluster commands...	Cluster Commands
<code>db...</code>	Database administration commands...	Database Commands
<code>system...</code>	System commands...	System Commands

DEVICE COMMANDS

Type `device ?` to view the device commands

<code>group...</code>	Device group commands...
<code>list +</code>	List all storage devices
<code>map +</code>	Setup Paths from Primary storage device to an Alternative storage device
<code>rmmap +</code>	Remove Paths from Primary storage device to an Alternative storage device
<code>set +</code>	Set storage device settings

DISK COMMANDS

Type **disk ?** to view the disk commands

blink +	Blink a disk
cryptocopy...	Crypto Copy commands...
list +	List all disks in the configuration database
map +	Map a disk to a Cryptainer
metadata...	Disk metadata commands...
path +	List all paths to the disk
purge	Purge disks that are offline and have no Cryptainers
remove +	Remove a disk/LUN by its port WWN
replace +	Replace a disk
rescan	Force DataFort to rescan the fabric for disks
rmail +	Remove all LUNs of a disk
rmmmap +	Remove mapping of a disk to a Cryptainer
set +	Set disk settings
unhideall	Show all hidden disks

FC SITE COMMANDS

Type **fcsite ?** to view fcsite management commands.

list +	List all the FC sites in the configuration database
remove +	Delete the FC site settings for the specified DataFort
replace +	Make the local DataFort a replacement for the specified FC site
set +	Change the FC site settings for the specified DataFort

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

<code>rmall +</code>	Remove all Cryptainers from database
<code>set +</code>	Set Cryptainer settings

HOST COMMANDS

Type `host ?` to view host management commands.

<code>add +</code>	Add a host
<code>auth...</code>	Host WWN authentication commands...
<code>group...</code>	Host group commands...
<code>list +</code>	List hosts
<code>purge</code>	Purge hosts that are offline and have no permissions to Cryptainers
<code>remove +</code>	Remove a host
<code>rescan</code>	Force DataFort to rescan the fabric for hosts
<code>set +</code>	Set host settings
<code>unvirtualize+</code>	Unvirtualize a host
<code>virtualize+</code>	Virtualize a host

KFC COMMANDS

Type `kfc ?` to view fibre channel kernel commands.

<code>config</code>	Configure FC kernel
<code>list</code>	Display SAN kernel statistics
<code>sync</code>	Query the fabric to update the status of all devices
<code>util...</code>	SAN kernel utility commands...
<code>vp...</code>	SAN kernel virtual port commands...
<code>wwn...</code>	Fibre Channel primary port node/port WWN utils...

POOL COMMANDS

Type `pool ?` to view pool commands.

<code>add +</code>	Add a pool
<code>grant +</code>	Grant pool access to a host
<code>group...</code>	Pool group commands...
<code>key...</code>	Pool key commands...
<code>list +</code>	List pools
<code>perm...</code>	List pool permissions...
<code>remove +</code>	Remove a pool
<code>revoke +</code>	Revoke pool access from a host
<code>set +</code>	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.

<code>list +</code>	List roles
<code>path...</code>	Role path commands...

USER COMMANDS

Type `? user` to view user commands.

<code>add +</code>	Add a user account
<code>list +</code>	List all users in database
<code>remove +</code>	Remove a user from the database
<code>role...</code>	User role commands...
<code>set +</code>	Set user settings

WHOAMI COMMAND

Type `whoami` to see the current user ID.

<code>whoami</code>	Display effective user ID
---------------------	---------------------------

TRUSTEE COMMANDS

Type `trustee ?` to view trustee commands.

<code>delete +</code>	Remove trustee from the system
<code>keys..</code>	Trustee key export and import commands...
<code>list +</code>	List all the approved trustees in the system
<code>unapproved..</code>	Trust establishment commands for unapproved trustees...

NETWORK COMMANDS

Type `net ?` to view network management commands.

<code>apply +</code>	Apply network changes
<code>connection...</code>	Network connection administration commands...
<code>interface...</code>	Network interface commands...
<code>status +</code>	Display network status
<code>util...</code>	Network utilities...

KEY MANAGEMENT COMMANDS

Type `? keyman` to view key management commands.

<code>cryptainerkeys +</code>	Query Cryptainer Keys
<code>lkmkeys +</code>	LKM key management commands...
<code>masterkeys +</code>	Query Master Keys
<code>purgekeys</code>	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

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.

`backup +` Backup the configuration database
`begin` Begin a transaction
`commit` Commit the current transaction
`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 SPECIFICATIONS**

[Supported Systems](#) lists support for components of the DataFort system.

[Specifications](#) lists DataFort hardware specifications.

SUPPORTED SYSTEMS

Please visit the Decru website for the most up-to-date information about DataFort interoperability.

TABLE 1: SUPPORTED PLATFORMS

Item	Component	Requirement
Management Station	System Requirements	PC 32MB RAM 10MB free disk space Windows 2000/Windows XP Windows Server 2003 10Base-T Ethernet port Port for smart card reader (USB or serial)
	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.

SPECIFICATIONS

- [DataFort FC520 Specifications](#)
- [DataFort FC525 Specifications](#)
- [DataFort FC1020 Specifications](#)

TABLE 2: DATAFORT FC520 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	2 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 35°C (41°F-95°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

TABLE 3: 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 35°C (41°F-95°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/Canada FCC Class B Japan VCCI 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

TABLE 4: 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 35°C (41°F-95°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 IV 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 is encrypted by DataFort with a Cryptainer Key, using AES.
cryptography	The science of rearranging data by applying algorithms mathematically to combine cleartext and an encryption key. The resulting ciphertext appears to be random, but contains all of the original information.
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 software used to manage DataFort encryption keys and Cryptainer 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 106
- ACL Learning 105, 106
- Adding and Removing Cluster Members 150
- Admin Card 14, 15, 194
 - associate with administrator 67
- administrator 15, 194
 - add 64
 - associate card 67
 - associate with Admin Card 67
 - change password 68
 - change the card association 69
 - delete profile 69
 - dual authorization, login 71
 - login to CLI 72
 - login to WebUI 71
 - new 60
 - number recommended 64
 - require login authorization 67
 - roles outlined 62
 - Security Administrator 110, 129, 134
 - specialty administrator, create 66
- administrator roles 62
- administrator roles in CLI 157
- administrator roles, CLI 157
- Administrator types 66
- AES 13, 194
- alert, clearing 136
- appending ciphertext 103
- appending cleartext 103
- ARP table 161
- associate Admin Card with administrator 67
- authentication 14, 194
- authorization for login 67
- authorizing administrator 67
- Auto-detected pools 106

B

- backup
 - DataFort configuration 129
 - topologies 26
- Backup Methods 26

- backup, data
 - Client-free 26
 - LAN-based 26
 - LAN-free by Client 26
 - planning 26
 - SAN Mirroring 27
 - Server-free 27
- backup, DataFort configuration 20
- battery iv
- block cipher 194

C

- Category 5 cable 16, 36, 75
- certificates
 - Management Station to DataFort 119
- change password, administrator 68
- change password, Recovery Card 127
- chassis 13, 194
 - intrusion 134
 - lock 13
- ciphertext 13, 194
- ciphertext and cleartext 19, 88, 194
- CLARiiON 175
- clear all DataFort settings 144
- clear an intrusion (defense alert) 136
- clear smart cards 128
- cleartext 12, 13, 19, 88, 95, 106, 194
- cleartext Cryptainer 88
- cleartext pools 106
- cleartext tape 22
- CLI 72
 - command help 156, 181
 - commands and admin roles 157
 - connect from SSH client 72
 - disk management 162
 - general information 156, 181
 - help 185
 - host management 164
 - login 72
 - permissions 156
 - Quick Reference 181
 - quit 185

- system commands 159, 187
 - time-out 181
 - top level commands 182
 - turn off Secure Web 171
 - WebUI access 74
 - CLI documentation 156, 181
 - CLI login with dual authentication 73
 - cluster 194
 - change to standalone 150
 - commands, CLI 187
 - forming, after initial setup 150
 - IPsec tunnel 19
 - management 147
 - management using CLI 158
 - network diagram 22, 25
 - recovery guidelines 152
 - remove member 150
 - replace an offline member 151
 - requirements 150
 - resolving conflict 152
 - restore previous configuration 152
 - state 149
 - state after wizard 59
 - switch connections, planning 20
 - cluster conflict 152
 - cluster disable command 158, 174
 - cluster quorum 150, 158
 - cluster size 147
 - cluster troubleshooting 174
 - cluster-wide operations 148
 - configurable security levels 118
 - configuration database 14, 195
 - applied to new DataFort 61
 - backup to LKM 60, 129
 - backup using WebUI 133
 - changes synchronized in cluster 19
 - commands, CLI 187
 - contents 129
 - event log capacity 138
 - purging unused keys after backup 131
 - save before power-down 80
 - size 131
 - used for recovery 61
 - create a Cryptainer 98, 99
 - Cross Mapping 92, 93, 95, 96, 99, 101, 103
 - Cryptainer 195
 - before creating 59
 - defined 14
 - management with WebUI 95
 - management, with WebUI 97
 - rekey with CLI 166
 - restore 109
 - Cryptainer collections 81
 - Cryptainer creation and management 81
 - Cryptainer creation, with WebUI 81
 - Cryptainer encryption after creation 88
 - Cryptainer ID 97, 109, 162, 167
 - Cryptainer Key ID 100, 101, 167
 - Cryptainer Management Menu 95
 - Cryptainer management with CLI 165
 - Cryptainer Management with WebUI 97
 - Crypto Copy 163
 - Crypto Copy with CLI 163
 - Crypto Copy with WebUI 100
 - cryptographic test 78
 - CryptoShred 13, 137
 - CryptoShred button 13, 79, 134, 135, 137
 - states 137
- D**
- data
 - data recovery schema 59
 - encryption 14
 - data size when encrypted 13
 - DataFort
 - administrators 78
 - assigning IP settings 37
 - back panel connections 34, 75
 - capacity 18
 - CLI, connecting to 72
 - cluster 19
 - Defense Setting 134, 135
 - diagram, back panel 34
 - emergency shutdown 137
 - in SAN 22
 - licenses 49, 124
 - Login page 57
 - management interfaces 70
 - new unit, necessary steps 32
 - recovery 61
 - Recovery Officers 78
 - restoring a previous configuration 61
 - specifications 190
 - troubleshooting 168
 - upgrading 155
 - users 15

- view settings 77
- WebUI, connecting to 70
- where installed 12, 22
- zeroizing 144
- DataFort CD-ROM 16
- DataFort CLI 72, 195
 - login 72
- DataFort CLI Reference Guide 156, 181
- DataFort HBAs 190, 191, 192
- DataFort Setup Wizard installation 29
- DataFort Throughput 78
- DataFort WebUI 70, 195
 - login 70
- date and time 154
- DCS
 - administrator roles 157
- Decru licenses 49, 124
- Decru MIB 154
- Decru Signed Syslogd (DSS) 138
- defense
 - alert, clearing 136
 - response 134
 - triggers 134
- Defense Setting
 - changing after setup 134
 - summary 135
- defense setting 59, 79, 134
- deleted Cryptainer
 - purge unused keys 131
 - restoration 109
- disabling a cluster member 158
- disk
 - management with CLI 162
 - management with WebUI 98
 - rescan 162
- disk license 12
- documentation 16
- dual authentication login, CLI 73
- dual authentication login, WebUI 71
- dual authorization 67, 71, 73

E

- EMC 175
- emergency shutdown 137
- encryption 13
- escrow service 20
- Ethernet cable 16
- event logs 138

- exportable key 86, 100

F

- failover 19, 194, 195
- fan modules, replacing 169
- FC Site settings 47, 48
- FC switch
 - in network diagram 22, 25
 - zoned 36
- feature licenses 49
- Fibre Channel 12, 22
- Fibre channel cables 16
- Fibre channel switch ports 16
- front panel
 - display 74
 - LCD used to assign IP address 37
 - LED 168
 - System Card slot 34
- Front Panel Dual LEDs - 2U 168
- Front Panel LEDs - 1U 168
- full database 131

G

- grant host access to Cryptainer
 - CLI 166

H

- hardware maintenance 169
- HBA (host bus adapter)
 - Host HBA, connecting to FC network 36
 - Hosts 19
 - Storage 19, 36
- Home page
 - returning to 70
- Host Default Pools 106
- Host HBA
 - interface for unencrypted data 36
- Host Icons 92
- Host Management Menu 92
- Host Virtualization enabled 107
- Host Virtualization with CLI 164
- Hosts
 - managing with CLI 164
 - Managing with WebUI 92
 - supported platforms 189

I

- Icon Legend 90, 91, 92, 95, 98, 102
- Icons

- host 92
- installation 28
 - in rack 32
 - planning 19
 - precautions 32
- Installation requirements 16
- International Organization for Standardization (ISO) 122, 193
- Internet Explorer 189
 - for accessing WebUI 70
 - for running setup wizards 57
- intrusion detection 134, 136
- IP address 16
 - DataFort, assigning 37
 - DataFort, current 78
 - preserve during zeroization 144
- IP settings
 - assigning from LCD 37
 - assigning from serial console 76
 - changing, with WebUI 154
 - DataFort, assigning from serial console 39
- IPsec 19, 195
- ISO 193
- IT power systems iii

J

- JBOD 162, 164, 195

K

- key 195
 - encryption key 13
 - escrow 20
- Key Purging 129
- key, chassis 134

L

- LCD 74, 78
 - assigning DataFort IP settings 37
 - bar graph 74
 - buttons 75
 - ready for initialization 37
 - touch panel interface 31
 - web page 78
- LED 168
- LEDs
 - power supply 169
- legacy cleartext tape 22
- licensed features 12

- licenses 12, 16, 124
 - managing 124
- lifespan of tape keys 104, 106
- Lifetime Key Management (LKM) 14, 195
- limited administrator 67
- Limits
 - Cryptainers on the primary port 19
 - LUNs on a single device 19
 - Non virtualized hosts 19
 - Number of DataFort appliances in a cluster 18
 - Virtual devices per DataFort 18
 - Virtual hosts per DataFort 19
- Lithium battery iv
- LKM 20, 129
 - secondary server support 30
 - server IP 30
 - server saves latest configuration backup 20
 - server setup 60
 - server, requirements 30
 - server, specifying settings in WebUI 60, 129
- LKM servers
 - number supported 30, 129
- LKM using SSL 130
- login
 - CLI 72
 - CLI, dual authorization 73
 - requiring authorization 67
 - WebUI 57, 71
 - WebUI, dual authorization 71
- Login page 57
- logs, DataFort 138
 - configuring storage location 139
 - Decru Signed Syslogd (DSS) 138
 - filtering 78, 142
 - guidelines 138
 - syslog mapping table 141
 - temporary file mapping 142
 - verifying signed messages 143
 - viewing, with WebUI 142
- LUN Mapping 19, 85, 89, 98, 99

M

- Manage Tapes 102
- Management Port
 - connecting to Ethernet network 36
- Management Station 15, 195
 - for running setup wizards 57
 - requirements 29, 189

- map a Cryptainer with WebUI 99, 101
- mapping a device 163
- mapping a device with CLI 163
- Master Key 196
- metadata 138, 167
- metadata support
 - CLI 167
- MetaTool 177
- MIB 154, 196
- mounting DataFort in rack 32
- Multi ID 107
- Multi ID mode 107
 - non NL-ports 107
- multiple DataFort appliances in cluster 19

N

- NAS 12
- network
 - connection to DataFort ports 34
 - diagram, SAN 19, 22, 25
 - information needed for setup 28
 - manage, with CLI 161
 - planning backup and restore 26
 - settings, changing 154
- Network Attached Storage (NAS) 12
- network commands, CLI 161
- Network switch ports 16
- NL-Port 36, 107
- non NL-Ports 36
- NTP time server 16

O

- online help 70

P

- password
 - administrator, changing 68
 - one-time, CLI 72
 - Recovery Card, changing 127
- pool display 102
- pools and tapes 105
 - settings 105
- port
 - FC ports 36
 - Management 36
- Port Lock 94
- port locking
 - switches supported 93, 94

- Port Mapping 19, 85, 89, 98, 99, 196
- power
 - precautions iii
- power button 80
- power cord 16
- power down DataFort 80
- power supply
 - LEDs 169
 - notice iii
 - replaceable 169
- powering down 80
- powering up 80
- protect against insider attacks 67
- purging encryption keys 131
- purging keys 131

Q

- quorum 15, 20, 125, 126, 128, 174, 196

R

- rack installation 32
- rack mounting kit 16
- RAID Admin 94
- Recovery Cards 14, 125, 196
 - change password 127
 - replacement procedure 125
- Recovery Officers 15, 196
 - required for forming cluster 152
 - required for replacing DataFort 61, 151
 - required for replacing Recovery Card 111, 125
 - required for Setup 40
- Rekeying a Cryptainer
 - CLI 166
- Remote Desktop 40, 70, 170
- remove all host access to a Cryptainer
 - CLI 166
- Removing a Cryptainer
 - CLI 166
- replacing a Recovery Card 125
- replacing an offline cluster member 151
- requiring login authorization 67
- reset DataFort 144
- reset date and time 154
- reset smart cards 128
- restore a Cryptainer 109
- restore a deleted Cryptainer. 100, 101
- restore a previous DataFort configuration 61
- restore, planning 26

RJ45 to DB9 adapter 16, 36, 75

S

SAN 12

- network diagram 19, 22, 25
- supported hosts and storage devices 189

SAN Storage Settings 107

SAN Topology page 82, 90

secret share 196

Secure CLI 70, 118

- login 72

Secure Web 70, 118

- turn on and off via CLI 171

Security Administrator 110, 129, 134

Security Certificate 119

- Certificate Authority Signed, installing 122
- self-signed, installing 119

Security Domain 15, 197

- planning 18

Security Policy

- planning 20

Security Settings 118

security, implementing and maintaining 18

Sensors 78

SEP 13, 78, 197

serial console 75

- assigning DataFort IP settings 39
- clearing IP Settings 76
- connecting serial port 36, 75
- emergency access 77
- menu options 76
- zeroizing DataFort 77

serial number 78

servicing DataFort 169

Show Alternate Paths 101

shutting down 80

Single ID 107

Single ID mode 107

size of data when encrypted 13

size of the configuration database 131

smart card reader 15, 16

- installing 29
- port connection 29

Smart Card Reset 128, 138

smart cards 16, 197

- checking versions and status 128
- reset procedure 128

summary 14

troubleshooting 172

SNMP 154, 197

MIBs 155

setting with WebUI 155

turning on and off 155

software CD-ROM 16

Solaris 177

specialized administrators 62

specifications 189

SSH 29, 31, 197

CLI access 72, 73, 156

SSL 130, 197

stack trace 161

Standard CLI 72

standard rack mount 32

status and settings 77

Storage Area Network (SAN) 12

storage device collection 83

storage devices 189

Storage Diagnostics 78

Storage Encryption Processor (SEP) 13

Storage HBA

- connecting to FC network 36
- interface for encrypted data 36

Storage Management Menu 98

storage management with CLI 162

supported platforms 189

switch connections in a cluster 20

switching WebUI to cluster member view 59

Symmetrix 175

syslog, syslogd (syslog daemon) 138, 141

System Card 14, 197

inserting 34

removing, in emergency 137

System Config menu (WebUI)

General, Date/Time 154

General, Upgrade 155

Network, IP Settings 154

Network, SNMP Agent 155

Recovery, Backup 133

Recovery, Replace Recovery Card 125

Security, Zeroize 144

System Users 78

System Users, Administrators 60

view settings 78

System Info menu (WebUI)

- Status 78
- Status, Log 78, 142
- system properties, CLI 159
- System Requirements 189
- system users 78

T

- TAP 110
- tape key 104, 106
 - deletion 104, 106
 - expiration 104, 106
 - lifespan 104, 106
- tape license 12
- tape pool types 106
- Tape Settings
 - access from ACL Learning link 105
 - access from Tape Management page 102
- tapes
 - manage with WebUI 102
- ten port DataFort 147
- ten port DataFort rear panel 36
- TEP 110
- Termial Services 170
- Terminal Services 40, 70
- time and date
 - setting from WebUI 154
- time servers 154
- time-out
 - CLI 72
 - serial session 76
 - WebUI 70
- trap 155
- troubleshooting 168
 - network connections 169
 - smart cards 172
- trustee 100
- Trustee Acceptance Package 110
- Trustee Establishment Package 110
- Trustees 110

U

- updating hosts in a Microsoft operating system 20
- upgrading DataFort 155
- USB 16

V

- Verifying System Logs 160
- Veritas 179

- view DataFort settings 77
- virtualization settings 107
 - Multi ID 107
 - Single ID 107
- virtualize a host, CLI 164

W

- WebCLI 74
- WebUI
 - accessing 70
 - device grouping 90
 - device information pane 90
 - keyboard shortcuts 58
 - login 57, 71
 - login with Secure Web 71
 - multiple device selection 90
 - required display setting 70
 - right-click menus 81
 - time-out 70
- WebUI access to cluster members 148
- WebUI login with dual authentication 71
- Windows event logging 140
- Windows Event Viewer 140
- WWN configuration 47, 48
- WWNs
 - assigning an override setting 47, 48

Z

- zeroizing DataFort 144
 - after setup 59
 - using serial console 146
 - using WebUI or CLI 144
- zones 36