DECRU®
A NetApp Company



ADMINISTRATION GUIDE

DataFort E-Series
Version 3.1

security

DataFort Administration Guide for E-Series DataFort

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

Part number: 30-000309 (v. 112706_E_3.1)

Model Numbers: E510/E515

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

TRADEMARK NOTICE

Decru®, Decru DataFort™, Cryptainer™, CryptoShred™, Lifetime Key Management™, the Decru logo and/or any Decru products or services referenced herein are trademarks and/or service marks of Decru, Inc. and may be registered in certain jurisdictions. All other product names, company names, marks, logos and symbols are trademarks or registered trademarks of their respective owners.

JRE and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Copyright© 2005 Sun Microsystems, Inc. All Rights Reserved.

This software is provided “AS IS,” without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SUN MICROSYSTEMS, INC. (“SUN”) AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Portions of this product are derived from FreeBSD, which is copyrighted by FreeBSD.

Copyright © 1994-2003 FreeBSD, Inc. All rights reserved.

Software derived from copyrighted material of FreeBSD is subject to the following license and disclaimer:

Redistribution and use of the software in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE FREEBSD PROJECT “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FREEBSD PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young.

This product includes software developed by the OpenSSL project for use in the OpenSSL Toolkit.

This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/.

Copyright © 2001 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name “Carnegie Mellon University” must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact:

   Office of Technology Transfer
   Carnegie Mellon University
   5000 Forbes Avenue
   Pittsburgh, PA 15213-3890
   (412) 268-4387, fax: (412) 268-7395
   tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/).”

Notices and Warnings

Power Supply Notice

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



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

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

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

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

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

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

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

OPPMERKSAMHET: Apparatet må kun tilkoples jordet stikkontakt.

Dual Power Supply Notice



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

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

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

Lithium Battery Notice for Service Personnel

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

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

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

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

Rack Mounting

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

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

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

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

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

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

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

CONTENTS

Chapter 1 Introduction **15**
About the Decru DataFort Security Appliance 16
Components of the Decru Security System 16
Encryption 16
Common Criteria Compliance 16
Hardened Architecture 16
CryptoShred Feature 17
Compartmentalization of Functions 17
Key Management 17
Lifetime Key Management Solutions 17
Configuration Database 17
Authentication Layers 18
DataFort Users 18
Security Domain 19
Installation Requirements 19
Conventions Used in this Manual 20

Chapter 2 Planning the Network Configuration **21**
Planning the Security Domain 22
Decru DataFort Capacity 22
Installation Considerations 24
Virtual Server Names and IP Addresses 24
End-User Access 24
Failover Support in a Cluster 24
Load Balancing in a Cluster 25
IPsec in a Cluster 25
Switch Connections in a Cluster 25
Secure Network Practices 26
Maintaining Configuration Database Backups 26
Sending Recovery Cards to Escrow 26
Planning Remote Security Logging 26
Removing the System Card 27
Preparing for Manual Security Responses 27
Placing DataFort in the Network 28
Workgroup Placement 29
Cluster Failover Network Topology 31
Configuring Switches for Failover 31
Planning Data Backup and Restoration 32
Snapshot Support 32
SnapMirror™ Support 32
NDMP Support 32

Chapter 3 Preparing to Install DataFort 33
Collecting Network Information 34
Preparing the Management Station 34
Management Station Security 35
Enabling TLS 35
Running the Installer 35
Setting Up Lifetime Key Management 36
Adding the DataFort Domain Access User 36
DataFort Windows Domain Access User 37
DataFort LDAP User 37

Chapter 4 DataFort Appliance Installation 38
Notices and Warnings 39
Power Supply Notice 39
Dual Power Supply Notice 39
Lithium Battery Notice for Service Personnel 39
Perchlorate Present 39
Rack Mounting the DataFort Appliance 40
Selecting a Location 40
Rack Mounting 40
Connecting the Decru DataFort Appliance 41
System Card Insertion 41
Rear Panel Network Connections 41
Power Connection 43
Assigning the DataFort IP Address 44
Setting the IP Address Using the LCD 44
Setting the IP Address Using the Serial Console 45
Powering Up and Shutting Down 46

Chapter 5 Initializing DataFort Appliances 47
About the Setup Wizard 48
Setup Wizard Functions 48
About Smart Cards and Readers 48
Initializing a Standalone DataFort or DataFort Cluster 49
Connect to Head of Cluster 51
Sign License Agreement 51
Recover From Database 52
Create Administrator 52
Configure Cluster and Recovery Schema 52
Network Settings 55
Add Licenses 57
Network and Certificates 58
Insert Recovery Card 59
Apply Settings 60
Logging into Appliances Using DMC 60

Adding a Member to a Cluster 61
Log in to Head of Cluster 61
Cluster and Recovery Schema 61
Network Settings 62
Add Licenses 63
Network and Certificates 63
Insert Recovery Card 63
Apply Settings 63

Chapter 6 DataFort Management Interfaces 65
Management Interfaces Overview 66
SecureView 67
Security Policies 67
Online Help 67
Connecting to the DataFort WebUI 68
Using the DataFort WebUI 68
Connecting via WebUI 68
Quick Links and Status 69
Connecting via WebUI using Dual Authorization 70
Connecting to the DataFort Command Line Interface 71
Using the CLI 71
Connecting via Standard CLI 71
Connecting via Secure CLI 71
Connecting via CLI using Dual Authorization 72
Connecting to CLI via WebUI 72
Accessing the Decru Management Console 73
Serial Console 74
Connecting the Serial Console Port 74
Logging in to the Serial Console Port 74
Configuring IP Settings 74
Clearing IP Settings 74
Zeroizing DataFort 75
DataFort Front Panel LCD 75
SNMP Settings 76

Chapter 7 DataFort Admin Roles and Account Administration 77
Administrator Roles 78
Account Administration 81
Adding an Administrator 81
Requiring Authorization for Login 84
Changing the Administrator Password 85
Removing an Administrator 87
Changing a Card Association 87

Chapter 8 Before Creating Cryptainers **88**
Checking Cluster State 89
Configuring Remote Logging 89
Starting LKM 89
LKM Server 89
LKM Appliance 89
Creating Additional Administrators 89
Verifying System Version 90
Determining the Defense Setting 90

Chapter 9 NAS Storage Administration **91**
Understanding DataFort Domains 92
File Servers and Domains 92
User Authentication and Domains 92
Domain Types and Subtypes 92
User Mapping and DataFort Domains 94
Userless Domains 94
Preparing to Create a NAS Cryptainer 95
Create CIFS Shares 95
Create NFS Exports 96
Creating a NAS Cryptainer 96
Connect to the DataFort WebUI 96
Servers & Portals 96
Add a Domain 97
Add a Server 98
Add a Share 99
Add a Virtual Server 100
Virtualize a Share 101
Add a Cryptainer 101
Cryptainer Ownership 102
Creating a NAS Cryptainer From a Home Directory 103
Creating a NAS Cryptainer Using Specialty Administrators 103
Managing Secure NAS Storage 104
Managing Domains 104
Deleting a Domain 104
Managing Servers 105
Editing a Server 105
Managing Shares 106
Options When Adding a Cryptainer 106
Managing Cryptainers 107
Adding Virtual Servers 108
Managing Virtual Servers 109
Editing a Virtual Server 111
Managing Virtual Shares 111
Restoring a Cryptainer 112

Chapter 10 iSCSI Storage Administration **113**
Preparing to Create an iSCSI Cryptainer 114
Setting up Groups 114
Using iSNS 114
Preparing to Create Cryptainers Using SnapDrive 114
Creating an iSCSI Cryptainer 115
Adding an iSCSI Portal 115
Virtualizing the Portal 117
Adding a CIFS share for Snap Drive Support 118
Adding an Initiator 118
Encrypting a Cryptainer 120
Configuring an Initiator 121
Configuring DataFort to Support MPIO 122
Managing Secure iSCSI Storage 123
DataFort WebUI Icons 123
Managing Portals 124
Managing Virtual Servers and iSCSI Routes 125
Managing Targets and LUNs 126
Managing Cryptainers 126
Managing Initiators 127
Restoring an iSCSI Cryptainer 128

Chapter 11 User Administration **129**
Managing Groups and Users 130
Adding Users 130
Searching for Users 130
DataFort Groups 132
Group Review 132
Managing Cryptainer ACL 134
Cryptainer ACL 134
ACL Capture and ACL Sync 135

Chapter 12 Accessing Secure Data **137**
CIFS Data Access 138
CIFS Data Access Example 138
NFS Data Access 140
NFS Data Access Example 140
Migrating Data 141
Secure Existing Data Using Initial Encryption 141
Secure Existing Data by Copying 141
CIFS User Registration 142
Registering the User's Windows Password 142
Registering the User's DataFort Password 143
Changing User Passwords 144

End-User Cryptainer ACL Management 146
End-User Login to DataFort CLI 147
HTTP Data Access 148
Web Access 148
WebDAV 149
Changing Web Configuration Using the DataFort CLI 149
FTP Data Access 150
FTP Home Directory 150
TFTP Data Access 151
TFTP Commands 151
Sample TFTP Configuration 151

Chapter 13 Key Administration 152
Managing Trustees 153
Trustee Scenarios 153
Setting Up Trustees 153
Importing and Exporting Keys 159
Managing DataFort Defense Responses 162
Defense Triggers and Responses 162
DataFort Defense Setting 162
Changing the Defense Setting 163
Clearing a Defense Alert 164
CryptoShred Button States 165
System Card CryptoShred 165
Setting Security Options 166
Choosing a Configured Security Level 166
Customizing a Security Level 167
Configuring IPsec 170
Supported Clients and Authentication Methods 170
Adding a Kerberos Rule for Windows Clients 170
Kerberos Authentication without IPsec 171
Adding a Preshared Secret Rule for Clients 172
Relevant System Properties 172
IPsec Configuration for Windows Clients 173
IPsec Configuration for Solaris Clients 173
Managing Recovery Officers and Recovery Cards 175
Replacing a Recovery Card 175
Changing a Recovery Card Password 177
Smart Card Reset 178

Chapter 14 Backup Administration 179
Saving Configurations to Lifetime Key Management Software 180
Configuring Backups to LKM Software 180
Backing Up the Configuration to LKM 181
Key Purging 182
Downloading Configurations to a Remote Location 183

Chapter 15 Physical Security Administration **184**
Setting Date and Time 185
Configuring and Viewing Logs 185
DataFort Log Storage Guidelines 185
Decru Signed Syslogd (DSS) 186
Configuring Log Storage 186
Windows Event Logging 186
Setting Up Syslog 188
Viewing the Log 189
Verifying Signed Log Messages 192
Zeroizing the Decru DataFort 193
Zeroizing After Setup 193
Zeroization Using the DataFort WebUI **193**
Zeroization Using the CLI 194
Zeroization Using the Serial Console 195
Emergency Serial Console Port Access 195

Chapter 16 Cluster Administration **196**
Cluster Management 197
Cluster-Wide Management via WebUI 197
Checking the Cluster State 197
Adding and Removing Cluster Members 198
Checking Failover Status 198
Recovering a Cluster from Failover 199
Changing Configurations in a Cluster 200
Replacing a DataFort in a Cluster 202
Recovering a Cluster 202
Resolving a Cluster Conflict 203
Setting Cluster Properties With the CLI 204
Configuring Cluster Members for STP 204
Cluster Crypto Failover Command 205
Auto Giveback 205
Reviewing the Cluster Load Balance 205

Chapter 17 Machine Administration **206**
Network Settings 207
Upgrading DataFort 207
Setting Security Certificates 208
Setting a Local Security Certificate 208
Setting a Certificate Authority Signed Certificate 211
Managing Licenses 213
SNMP Settings 214
Enabling SNMP 214
SNMP Configuration 214

Chapter 18 DataFort Appliance Settings and Status **216**
Viewing Settings in the WebUI 217

Chapter 19 Decru Management Console Functions **219**
Appliance Management 220
License and Administration Management 223
Logging Configuration 225
Decru Management Console Menus 226

Chapter 20 CLI Administration **229**
Using the CLI 230
Connecting to the CLI 230
CLI Help 230
Administration Commands 231
Administrator Roles 231
Cluster Management 232
System Properties and Log Management 233
Verifying System Logs 234
Stack Trace Settings 235
Network Management 235
Backup Management 235
CLI Management for NFS Cryptainers 236
NFS Administration Example 236
Manage Domains 236
Manage Servers 238
Manage Shares 238
Manage Cryptainers 239
Group Review 242
CLI Management for Multi-Protocol Cryptainers 243
Multi-Protocol Administration Example 243
Set DataFort Properties 243
Manage Domains 243
Manage Servers 244
Manage Shares 245
Manage Cryptainers 246
CLI Management for CIFS Cryptainers 248
CIFS Administration Example 248
Manage Domains 248
Manage Servers 249
Manage Shares 249
Manage Users and Groups 250
Manage Cryptainers 250
CLI Management for iSCSI Cryptainers 251
iSCSI Administration Example 251
Create Cryptainer 251

Restoring a Cryptainer 252
Special Commands 253
Cryptainer Aliases 253
Port Forwarding 253
IPsec Configuration and Management 254
WebUI Display 254
VLAN Tagging 255

Chapter 21 Troubleshooting 256
Restoring a DataFort 257
Front Panel LEDs 258
Power Supply LEDs 258
Network Connections and Management Interfaces 259
CIFS Cryptainers 261
NFS Cryptainers 263
iSCSI Cryptainers 265
Clusters 266
Smart Cards 267
Hardware Issues 267

Appendix I Command Line Interface Quick Reference 268
Using the CLI 269
CLI Syntax 269
CLI Help 269
CLI Command Overview 270
Top Level Commands 270
iSCSI commands 271
KFC Commands 271
Disk commands 271
CIFS Commands 271
Cryptainer Commands 271
Forwarding Commands 272
HTTP Commands 272
FTP Commands 272
iSNS commands 272
IPsec Commands 272
NFS Commands 273
Server Commands 273
Share Commands 273
TFTP Commands 273
Virtual Interface Commands 274
Virtual IP Commands 274
VLAN Commands 274
Virus Scanning Commands 274
CLI Formatting Commands 274

Help Command 275
Quit Command 275
Active-Role Commands 275
Authorize Command 275
Domain Commands 275
Group Commands 275
Password Command 276
Role Commands 276
User Commands 276
Whoami Command 276
Trustee Commands 276
Network Commands 276
Key Management Commands 277
LKM Management Commands 277
Cluster Commands 277
Database Commands 277
System Commands 278

Appendix II DataFort Virus Scanning 279
Considerations Before Configuration 280
Steps Before You Begin 280
Configuring DataFort for Virus Scanning 281
Registering AV Scanner with DataFort 282
Notes for Virus Scanning 283

Appendix III Specifications 285
Supported Systems 286
Specifications 287

Appendix IV Partial List of ISO Country Codes 289

Appendix V Glossary 290

Appendix VI Regulatory and Certifications 294
FCC B Declaration of Conformity 295
European Union 295
Canadian ICES-003 295
VCCI Class A Statement 296
CE Statement 296

Index 297

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 targets or directories 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 client, 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 E-Series DataFort appliances. This introduction includes the following sections:

- About the Decru DataFort Security Appliance
- Components of the Decru Security System
- Installation Requirements
- Conventions Used in this Manual

About the Decru DataFort Security Appliance

When installed between clients and file servers or initiators and targets, DataFort encrypts data en route to storage, and decrypts it as it is read by clients or initiators without impact on the existing network structure. Network clients can access their own Cryptainer vaults, storing data the same way they normally would on the network, but with the added protection of encryption.

Disk space is allocated from shared volumes without requiring that the volumes be reconfigured, and access control for network users is fully supported. Standard installation places DataFort appliances in a clustered configuration on a single network, with all encryption key and access control information shared securely between the cluster members.

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

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 clients or initiators 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.

DataFort appends 512 bytes of data to each file header, and may also append 16 additional bytes. This small addition allows DataFort to track key information on a per-file basis.

Common Criteria Compliance

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

Hardened Architecture

DataFort hardware and software were designed from the ground up for optimal security. At the heart of the system is Decru's Storage Encryption Processor (SEP), a hardware engine which enables Gigabit-speed, full-duplex encryption. The SEP is fully protected within the DataFort chassis, which is equipped with tamper-resistant features to protect all sensitive key material stored inside the appliance. An optional 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 NAS or iSCSI environment, a Cryptainer can consist of a directory on a file server or an iSCSI target (managed on the IP network by its iSCSI node name), a CIFS share or an NFS mount point.

Cryptainers are managed by the storage administrator, but DataFort separates the ability to manage stored data from the ability to read data from a storage device. This means the administrator who maps secure storage on the network does not necessarily have access privileges to the data. Data is secure no matter where it is stored, or who manages the storage.

Key Management

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

Each Cryptainer is associated with its own encryption key, which is required to encrypt and decrypt the stored data. Each encryption key used for a Cryptainer is in turn encrypted by a Parent Key, shared by the members of a DataFort cluster. The Parent Key is encrypted by a Master Key, unique to each DataFort. This Master Key, generated at the time DataFort is initialized, is used to decrypt and encrypt key material for safe storage and backup.

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

Lifetime Key Management Solutions

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

Configuration Database

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

Authentication Layers

DataFort incorporates smart cards into network management, backup and recovery procedures. This provides a second layer of authentication beyond username and password credentials. 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 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 An Admin Card adds additional optional authentication to the communication between administrator and DataFort. Admin Cards can be used for one or appliances (including a cluster or separate appliances).

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. The reader provides a dock for the smart cards.

DataFort Users

DataFort administrators are responsible for configuration and maintenance of DataFort on the network. Other users include network clients who will access Cryptainers managed by DataFort, and the Recovery Officers who are issued Recovery Cards.

DataFort Administrators DataFort can be managed by several types of administrators. A Full Administrator can complete all operations necessary to set up, manage and maintain the DataFort appliance. Other administrators 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.

Client User The client user has read and write access to specified data. This user is authenticated by the existing client login mechanism as well as DataFort-verified security parameters.

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 allow recovery of encrypted data, no single administrator or employee can bypass the system's security.

Installation Requirements

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

- Decru DataFort Appliance
- DataFort Documentation and Software CD-ROM. The documentation and software CD contains software necessary for DataFort operation, such as the smart card reader driver and Decru Management Console installer.
- Custom RJ45 to DB9 adapter and Category 5 cable for a serial connection
- AC power cord or cords appropriate for DataFort model
- DataFort smart cards, including System, Admin and Recovery Cards
- USB smart card reader
- Decru product licenses
- Slide rail mounting kit including hardware and instructions (included in the DataFort package)
- Network cables. Have the requisite number of network cables, of appropriate lengths.
- Network switch ports. Determine which Ethernet switch ports you will be using to connect the DataFort appliances to your network. The switch ports connecting DataFort to your network should be set to "Auto/Auto". The use of any other setting can affect management performance.
- IP address, Subnet mask and Default Gateway. Each DataFort will require one dedicated IP address. Know what the appropriate subnet mask and appropriate default gateway will be for each dedicated IP address to be used during installation.
- DataFort name. Establish what resolvable system name will be assigned to each DataFort being installed. Associating the specific IP addresses with their associated system names in your DNS configuration prior to installation will simplify IP resolution.
- DNS information. Have the appropriate DNS information (DNS suffix, primary DNS server IP address, secondary DNS server IP address) for each IP address to be used during installation.
- NTP address. Have the appropriate NTP time server information for each dedicated IP address to be used during installation. If you are not using an NTP server for time synchronization then this information is not required.
- Recovery schema. Determine what the recovery schema will be for the DataFort appliance or DataFort cluster. The recovery schema determines how many Recovery Cards and their associated owners must be present for sensitive data recovery operations.

Conventions Used in this Manual

The following typographic conventions are used in this manual:

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

2 Planning the Network Configuration

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

Complete installation in the enterprise positions DataFort between clients/initiators and file servers/targets, and will also add a Management Station (for initial DataFort configuration and for ongoing administration tasks) and a Lifetime Key Management server or appliance to the client side 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
- Placing DataFort in the Network
- 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 sharing user access and administrative oversight. Each Security Domain is associated with a set of Recovery Officers and Recovery Cards.

A company might establish Security Domains such as “HR data,” “CEO home directory,” “Customer transactions” or “Source code,” with each Security Domain protected by one or more DataFort appliances. Because each Security Domain is defined by a set of Recovery Cards and associated Recovery Officers, no single administrator, employee or group of unauthorized employees 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 capacity needs and divide network storage traffic across multiple DataFort appliances accordingly. Keep in mind the limitations outlined in Table 1.

Table 1: DataFort Capacity

Item	Number	Explanation
Number of DataFort appliances in a cluster	2	A DataFort cluster can support up to 2 appliances in the NAS/iSCSI environment.
NAS Domains	8	The limit on domains managed by DataFort appliance or cluster.
NAS Users	20,000	Total users is 20,000, 10,000 of which can be concurrent users. The limit on users, groups and membership relations applies to the number of imported users (users that have explicit access to Cryptainers served by DataFort) and not total users in the environment. Imported users include: • Users that are granted access to a Cryptainer. • Users that are members of a group with access to a Cryptainer. • Users who register with DataFort.
NAS Groups	1,000	
NAS Membership relations	30,000	To calculate the number of membership relations in a domain, take the sum, over all groups in the domain, of the number of members in that group. If two distinct groups contain the same member, then that member should be counted twice.
iSCSI Groups	512	The limit on iSCSI groups managed by DataFort appliance or cluster.
iSCSI Initiators	2048	The limit on iSCSI initiators managed by DataFort appliance or cluster.
iSCSI LUNs on a Single Target	2048	One Cryptainer per LUN is supported.

TABLE 1: DATAFORT CAPACITY (CONTINUED)

Item	Number	Explanation
iSCSI Targets	256	The limit on iSCSI targets managed by DataFort appliance or cluster.
Servers/VLANs	32	The limit on storage devices managed by DataFort appliance or cluster.
Cryptainers/Shares	1,500	If the number of Cryptainers exceeds capacity, an additional DataFort cluster may be added to manage a subset of the Cryptainers that the existing cluster is managing. A recommended installation for a large network divides the network into sections, with a DataFort or DataFort cluster for each section.
Cryptainer Keys per Cluster	4500	Once more than 4500 keys have been generated for a cluster by creating or rekeying Cryptainers, keys should be purged from the system upon backup.

Installation Considerations

In order to encrypt data moving to storage, DataFort separates the network into cleartext and ciphertext portions. Clients and initiators are connected to the cleartext portion, while file servers and targets are connected to the ciphertext portion. Separate NICs are available on DataFort to make these connections. DataFort appliances can be installed as standalone appliances, or as members of a cluster. Clustered DataFort appliances share critical configuration information to provide failover and load balancing support for the network.

Decide whether DataFort appliances will be standalone or clustered. If clustered, decide which DataFort in the cluster will be the primary DataFort for each server (plan Load Balancing in a Cluster). Prepare for failover configuration by assigning VRIDs for Failover Support in a Cluster. Decide which file servers will house encrypted data, and devise a naming plan for virtual servers (assign Virtual Server Names and IP Addresses). The topics that follow summarize major installation considerations.

Virtual Server Names and IP Addresses

File servers are added to the DataFort configuration database so that DataFort can export shares on those servers as Cryptainers. Clients view file servers through DataFort, which virtualizes the data stored on the servers. In an iSCSI configuration, targets are added to the configuration database so that target LUNs can be exported as Cryptainers.

When servers and targets are added to DataFort in order to host Cryptainers, they are assigned virtual IP addresses and names. This allows DataFort to virtually present the stored data to network clients and initiators. Determine the IP addresses or domain names that will be used in advance of setting up DataFort. It is recommended that the network administrator make a list of the servers and targets that will be exported through DataFort, and determine a naming scheme that works best for the enterprise.

End-User Access

End users access Cryptainers the same way they access any ordinary share, according to Access Control List (ACL) settings. As soon as a new Cryptainer is created for a user, the Cryptainer can be used to store data. If an existing share is made into a Cryptainer, or if existing data is moved from an ordinary share to a Cryptainer, end users need to access that share through DataFort. Determine the best method for introducing DataFort to the environment before creating Cryptainers.

Decru recommends creating a virtual server that has the name of the real server, and then renaming the real server. This allows DataFort to export the server names already in use, which will mean no changes are necessary on the client side. It also prevents clients from attempting to access the server shares directly. Alternatively, a virtual server can be created with a new name, and clients can refer to the new name. In this case no modifications are necessary on the server side, but clients will have to begin using the new names in order to access their data.

Failover Support in a Cluster

Clustered DataFort appliances provide failover support, allowing a functioning DataFort to take over operations for a failed DataFort. When a file server is added to the DataFort configuration database, it is associated with one DataFort in the cluster as its primary DataFort. The primary DataFort handles the data for that server, but shares information about the server with a secondary DataFort. Should file serving operations on the primary DataFort be compromised for any reason, the secondary DataFort in the cluster will take over.

VRIDs for Cluster Members

DataFort clusters use an application-level heartbeat to monitor the liveness of cluster members. Decru uses the VRRP (Virtual Router Redundancy Protocol) packet format for that heartbeat. The DataFort administrator must obtain a block of exclusive, sequential VRIDs from the network administrator—one for each cluster member.

Note: A unique VRID (a valid number in the range 0-255) is required for each DataFort appliance.

The network administrator should assign these VRIDs based on the VRIDs that other network devices are using. (Note that the VRRP protocol itself is not implemented in a DataFort cluster.)

Load Balancing in a Cluster

Decru recommends that the administrator decide how to distribute servers and targets between clustered DataFort appliances before adding them to a DataFort cluster. The most important consideration is data throughput. A recommended configuration splits the servers and targets into groups which are balanced in terms of load. Each group is assigned to a different DataFort as primary. It is important to remember that if one DataFort fails, the remaining DataFort appliances in the cluster will serve the combined load of the cluster.

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

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 switch, attempt to connect each DataFort to a separate blade or line card of the switch. For some switch makes and models, individual line cards can be upgraded or swapped out without impacting other line cards, and therefore without impacting the rest of the cluster.

Where possible, connect both the Clients NIC and the File Servers NIC of each individual DataFort to the same switch. Connecting a clustered DataFort's Clients and File Servers NIC to two different switches may (if one of the two switches fails) lead to degradation or increased convergence time in the application-level failover between cluster members.

A recommended topology includes the following elements:

- Two distribution-layer switches, each with its own connection to a backbone switch.
- A redundant switch-to-switch link between the two distribution-layer switches.
- A cluster of two DataFort appliances. One DataFort appliance with both Clients NIC and File Servers NIC connected to one of the two switches, the other DataFort appliance with both NICs connected to the other switch.
- Ideally, clustered file servers, with two heads: one head connected to one switch, and one head connected to the other switch.

Secure Network Practices

Determine the desired level of security for your environment before installing DataFort. For a high-security environment, plan an installation that includes not only DataFort appliances and a Management Station, but also a Lifetime Key Management server or appliance, a location for storing remote logs and database backups, and the use of an escrow service for smart card and password storage. Consider the following recommended procedures for a highly-secure network installation.

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

Maintaining Configuration Database Backups

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

- 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 the latest configuration database backup to Decru's Lifetime Key Management (LKM) software automatically, or use an LKM appliance.

Sending Recovery Cards to Escrow

Each DataFort or DataFort cluster is configured with a data recovery schema setting that determines the minimum number of Recovery Cards required for data recovery to take place. There are several ways in which Recovery Cards can be configured, depending on the security policy of the enterprise. It is possible to use a different set of Recovery Cards for each DataFort cluster, or a single set of Recovery Cards for all DataFort appliances in the company.

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

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

Planning Remote Security Logging

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

Removing the System Card

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

Preparing for Manual Security Responses

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

The defense setting determines a DataFort appliance's automatic response to physical intrusion. See Defense Triggers and Responses on page 162 for details. In an emergency, there are also manual steps that can be taken to suspend DataFort encryption and decryption operations.

Table 2: Manual Security Responses

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

Placing DataFort in the Network

The following examples illustrate two key aspects of planning DataFort network design: placing DataFort within the network in order to maximize data security, and considering standalone deployment versus high-availability cluster deployment.

If all of the clients DataFort will serve are in one department or workgroup, the most secure deployment is to place the DataFort standalone appliance or cluster as close as possible to the client users. Placing DataFort close to clients will minimize the exposure of cleartext data to network eavesdropping or other plaintext attacks.

If DataFort can be installed on the same IP subnet as all clients, simple IP-based access checks on the network routers servicing the workgroup can be used to restrict access to DataFort to IP addresses within the workgroup. The protected data can reside either on file servers local to the workgroup, or on central corporate servers.

Client Co-location

The following diagram illustrates an installation where all authorized access to secured data is from within a single department or workgroup.

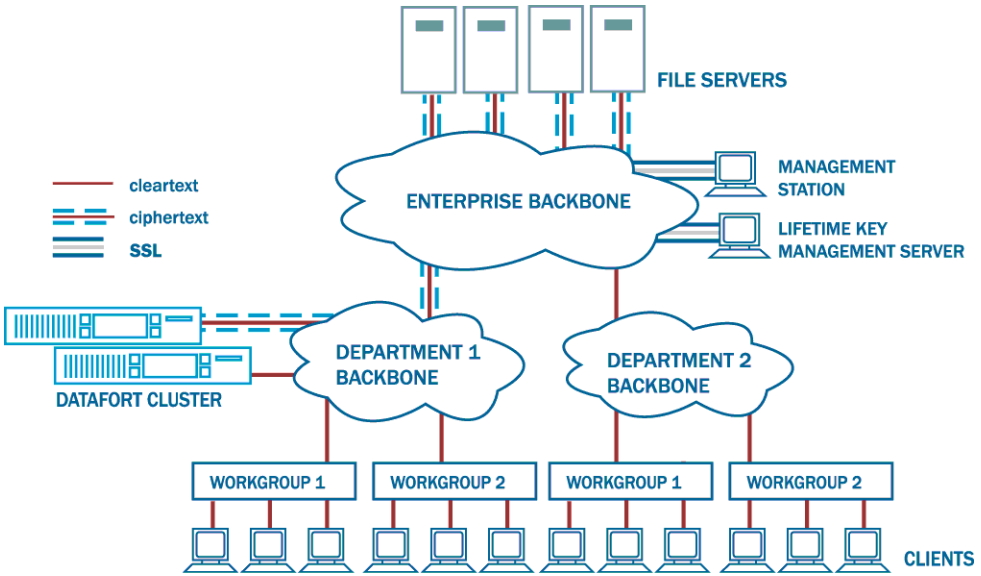


Figure 2-1: Cluster connected to a single department of the enterprise

Server Co-location

If DataFort cannot be placed close to the authorized clients because the clients are distributed throughout the organization, the most practical solution is to co-locate DataFort with the file servers.

This deployment scenario has the disadvantage that cleartext data being accessed by authorized users is visible throughout the organization's network, where it may be vulnerable to eavesdropping or

other attacks. Customers choosing this deployment scenario may wish to deploy IPsec to protect data in transit between DataFort and authorized client machines. Note that DataFort IPsec to client machines is a separately-licensed option.

The following diagram shows a deployment scenario where authorized users of data secured by DataFort are scattered throughout the entire organization. For example, DataFort may be protecting sensitive financial and budgetary data, which is accessed by the managers of individual workgroups within each department.

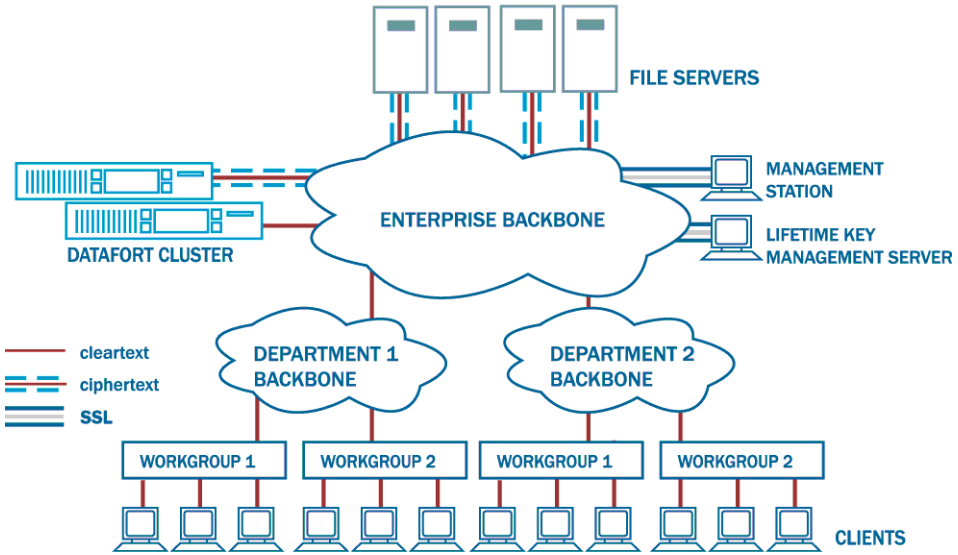


Figure 2-2: Cluster connected to the enterprise backbone

WORKGROUP PLACEMENT

In a basic installation DataFort, network clients and file servers are all connected to the same subnet. DataFort also supports a network configuration which straddles two different networks. In this configuration, file servers can be located on the client or file server side of the network.

Simple Workgroup Deployment

The simplest DataFort deployment places both the Clients NIC and File Servers NIC of the DataFort (cluster or standalone) on the same subnet as all of the clients. Not only does the DataFort IP-based ACL restrict access to only legitimate clients, but the workgroup router can stop external users from forging client IP addresses. An advantage of this deployment is that DataFort installation is transparent to the rest of the organization.

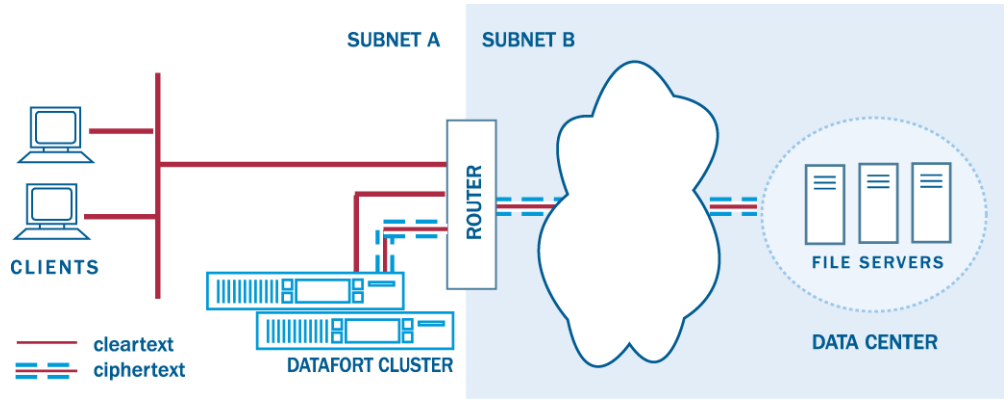


Figure 2-3: Simple deployment

Secure Enclave Deployment

A secure enclave is a subgroup protected from the rest of an organization by a firewall. Connecting the DataFort Clients NIC to one subnet, and the File Servers NIC to another subnet places DataFort inside an already-secured workgroup with a network firewall, separating it from the rest of the organization. This deployment is a natural choice for a subgroup with access to data shared by an external party.

In an installation where DataFort is spanning the boundary between the secure workgroup on the one hand and the corporate file server on the other (in the data center), clients can access extremely sensitive data while the data is protected outside of the secure enclave by DataFort. Traffic to corporate file servers does not impact the firewall device.

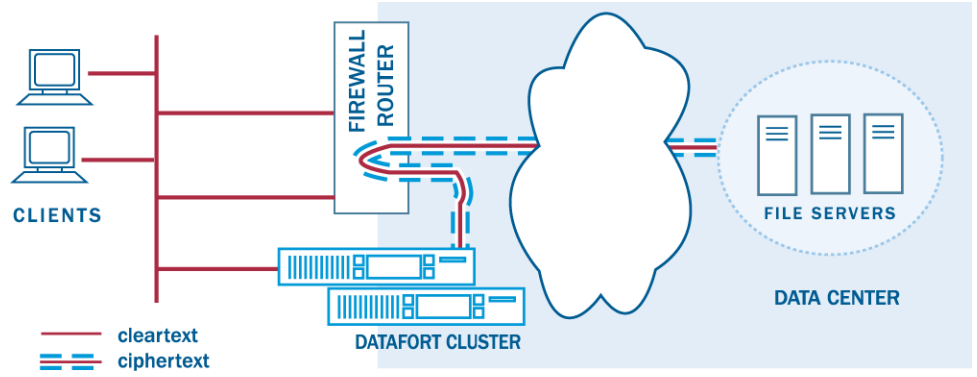


Figure 2-4: Secure enclave deployment

Cluster Failover Network Topology

For enterprises where high availability is crucial, a cluster of DataFort appliances should be deployed. The cluster ensures data availability if a network component fails. To maximize data availability, plan the exact topology carefully, linking redundant DataFort appliances, switches and file servers.

The following diagram shows a recommended topology which guarantees data availability in the case of any single failure, by combining a file server cluster, a DataFort cluster and redundant switch links. It can also survive multiple failures, provided there is no more than one failure per layer of network components. (Layers are indicated in the following diagram by shaded blocks.)

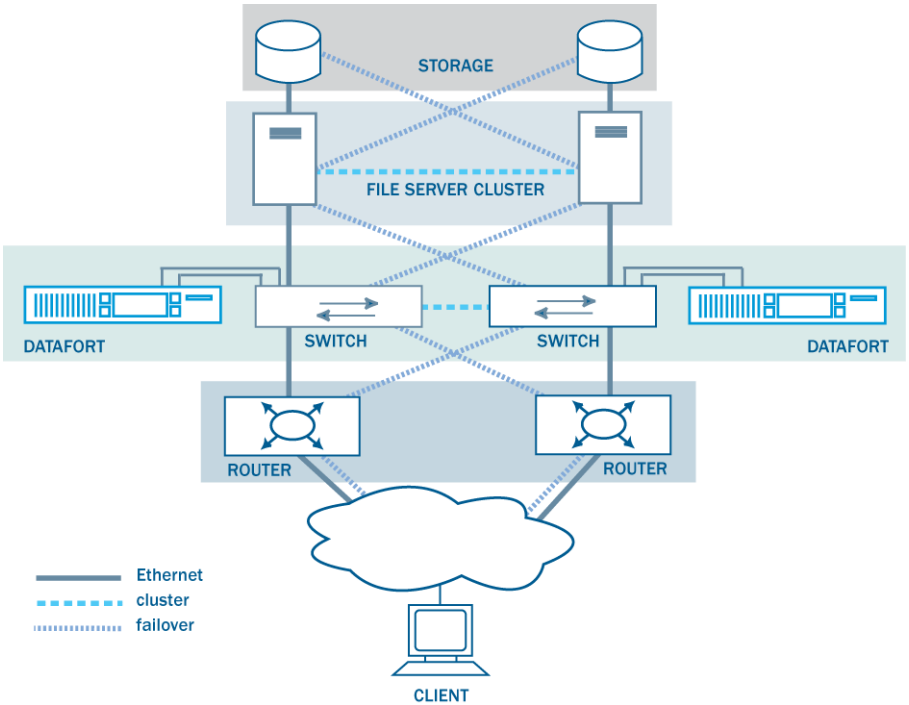


Figure 2-5: Failover paths in a DataFort cluster

Configuring Switches for Failover

Ethernet switch behavior affects how quickly a DataFort cluster can failover or resume file serving operations after a loss of network connectivity. Ethernet switches usually implement spanning-tree protocol (STP). STP requires that a switch impose a holddown period when a link is detected on a previously disconnected Ethernet port. This allows spanning-tree advertisements to stabilize (in case the link is connected to another switch when it comes back up), and may delay forwarding traffic on the new link for up to 60 seconds.

DataFort does not implement spanning-tree, therefore the best practice is to disable the spanning-tree holddown period altogether on switches connected to the DataFort network (Cisco calls this disabling Portfast™; other vendors use different terminology).

Note: If STP holddown cannot be disabled for some reason, DataFort must be configured with an estimate of the delay. See Configuring Cluster Members for STP on page 204.

Always set the DataFort holddown to match the observed delay between link-up events and the switch actually forwarding network traffic to and from DataFort. Inconsistency between the holddown property setting and the true switch holddown time can lead to unnecessary failover events (some tens of seconds each) once all cluster members have full network connectivity.

Planning Data Backup and Restoration

DataFort supports secure backup and restore capabilities in storage networks. In a data backup configuration, Decru recommends that DataFort be placed *in front of* the primary backup/restore components in the storage network so that the main data path between the data server, data mover and tape library does not pass through DataFort. This is done for several reasons:

- The data is encrypted once—to the primary disk.
- The bulk backup/restore traffic does not have to flow through DataFort.
- Data from the servers is already encrypted, allowing for secure backups and restores.

As DataFort sits in front of the backup and restore system components, the data being backed up and restored is always encrypted, and is always accessed in the same way by the backup software. Therefore, normal backup operations remain the same. When restores are made to the same Cryptainer from which the data was backed up, no changes are required in the restore method.

Note: In order to work with a backup/restore system that depends on file access by filename (e.g. restoring a single file), use the option to leave filenames unencrypted at the time Cryptainers are created.

Snapshot Support

DataFort works in snapshot environments where the virtual copy of the file system is made to the same disks—in this case, the Cryptainer. If the snapshot is not on the same physical set of disks, the administrator must copy the data to the original Cryptainer before being able to access the file in non-encrypted form.

SnapMirror™ Support

As snapshots do not protect against physical problems such as block or disk failure, administrators may choose to copy file systems to another disk or location. NetApp® SnapMirror™ technology enables snapshot data to be mirrored to a remote filer.

The remote filer can be located anywhere across a LAN or WAN. In the event that a primary filer fails, DataFort can use the remote filer instead. As with snapshots, no specific DataFort configuration is required for use in this situation. After failure of a primary filer, the administrator typically configures the secondary filer to assume the role of primary filer, either manually or automatically. DataFort automatically sees the secondary filer as the correct filer to use, and since the data is already encrypted with the appropriate key, users may continue to access the data without interruption.

NDMP Support

DataFort works with NDMP (Network Data Management Protocol) when the network is configured so that DataFort is in front of the backup/restore components. All NDMP devices are able to function as necessary behind DataFort.

3 Preparing to Install DataFort

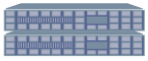
It is recommended that necessary information about the network be collected before beginning DataFort installation, and that decisions about administration, data recovery and defense settings be made in advance, according to your organization's security policy.

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

- Collecting Network Information
- Preparing the Management Station
- Setting Up Lifetime Key Management
- Adding the DataFort Domain Access User

Once DataFort is installed, the appliance is managed using the DataFort management interfaces. See the Management Interfaces Overview on page 66 for a list of interfaces and their uses.

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

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

Collecting Network Information

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

DataFort Network Information

- Resolvable hostname for DataFort Appliance
- DNS suffix and DNS server IP address (if DNS is used)
- DataFort Management IP address, Subnet Mask and Gateway. This is the IP address of the DataFort Client Side NIC connected to the client side of the network, and also serves as the management interface. This is initially set when Assigning the DataFort IP Address.
- DataFort File Server Side NIC IP address, Subnet Mask and Gateway. This is the address of the DataFort NIC connected to the file server side of the network.

Cluster Member Information

- IP addresses or resolvable domain names of all DataFort cluster members
- User-defined IPsec secret for IPsec in a Cluster
- Quorum of Recovery Cards and associated user names and passwords
- Purchased Decru licenses for all cluster members
- Sequential block of VRIDs for Cluster Members (one for each cluster member)
- Virtual Server Names and IP Addresses
- Domain information including domain name and DataFort domain access user information (see Adding the DataFort Domain Access User)
- Remote syslog server IP address
- Lifetime Key Management solution (one of the following):
  - LKM Server with fixed IP address
  - LKM Appliance

Preparing the Management Station

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

Smart cards from the provided set must be inserted into the smart card reader connected to the Management Station during the wizard. The Management Station is also used to access management interfaces for the DataFort appliance.

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

TABLE 3: MANAGEMENT STATION REQUIREMENTS

Management Station Requirements	
Windows operating system (one from list)	Windows XP Service Pack 2
	Windows 2000 Pro/Server Service Pack 4
	Windows 2003 R2 Service Pack 1
Browser for DataFort WebUI	Internet Explorer version 6.0 (Service Pack 1) or greater. TLS must be enabled.
	Microsoft JVM or Sun JRE 1.4.2.08. (DataFort installs Sun JRE 1.4.2.08.)
Hardware requirements	2Ghz
	1GB RAM
	4GB free hard drive space
	An available USB port for the smart card reader from Decru (If no USB port is available, a serial smart card reader is available from Decru.)
	A CD drive for installing software

MANAGEMENT STATION SECURITY

The Management Station should be current on security patches and have unnecessary services disabled or removed. The Management Station should not be used to browse untrusted web sites or run unverified code. Logons should be limited to authorized administrators, with no remote management enabled.

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

ENABLING TLS

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

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

RUNNING THE INSTALLER

The Decru installer must be run on the Management Station before a DataFort or LKM appliance can be configured. This installer will place the Decru Management Console (DMC) and smart card reader driver on the Management Station. Both the smart card reader and DMC are required for initial setup of all Decru appliance types.

1. Insert the CD provided by Decru into the Management Station.

   The CD will run automatically if autorun is on.
2. Click the installer link.

3. When prompted by the File Download screen to open or save the file, click the Open button to open the file.
4. Follow the prompts to start the installer.
5. Read and accept the terms of the license agreement.
6. Select the model number of your smart card reader. The model number can be found on the underside of the smart card reader (i.e. GemPCUSB-SL).
7. Select "Yes, I want to restart my computer now" and click Finish to complete installation.

Setting Up Lifetime Key Management

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

Decru's Lifetime Key Management appliance

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

If you are using an LKM appliance, set up the appliance using the Management Console as described in the *LKM Appliance Administration Guide*.

Decru's Lifetime Key Management software

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

If you are using LKM software, install the software on a designated server. Make sure the server is up and its IP address is reachable from the Ethernet network before configuring DataFort appliances. Instructions for enabling automatic updates to LKM servers are provided in Chapter 14.

Adding the DataFort Domain Access User

Before using DataFort to create Cryptainers on NAS servers, add a special user for DataFort domain access to the Windows or LDAP domains in which DataFort will be used. In a Windows domain, this user enables CIFS access, allowing DataFort to explore Windows domains, discover available servers and query them for shares, as well as synchronize lists of users and groups with that of the domain controller. In an LDAP domain, this user enables synchronization of users and group memberships from an LDAP server.

DataFort Windows Domain Access User

Use Windows Administration Tools to create a Windows user for DataFort access.

> **Note:** The DataFort domain access user is a special user for DataFort use only. It does not impact file access, and it cannot be used to access Cryptainers. A Cryptainer is accessed according to end-user credentials.

- The domain access user's password should be set with no expiration date, and should not contain spaces. The user name and password for the domain access user are both limited to 30 characters. Record the name and password of this user, as it will be required when adding the domain to the DataFort configuration database.
- A DataFort domain access user should be created in every domain the DataFort will serve.

DataFort LDAP User

In order for DataFort to access an LDAP server, a special user account must be added to the server. The same username and password combination that is used by DataFort to access Windows domains is also used to access LDAP servers.

Place this user either at the top level of the LDAP directory or underneath the "ou=People" level. The user can be of object class inetOrgPerson or NIS. Make sure that the user has its "uid" attribute defined to be the name of the DataFort domain access user. Set the user's password to be the same as the password of the DataFort domain access user, using the "userPassword" attribute.

> **Note:** If you want DataFort to authenticate with your LDAP server via Kerberos, add this user as a principal in your Kerberos domain. Use the same username and password. Keep in mind that Kerberos principal names are case-sensitive.

4 DataFort Appliance Installation

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

- Rack Mounting the DataFort Appliance
- Connecting the Decru DataFort Appliance
- Assigning the DataFort IP Address
- Powering Up and Shutting Down

Consider the listed Notices and Warnings when installing the appliance.

Notices and Warnings

Power Supply Notice

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



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

Dual Power Supply Notice



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

Lithium Battery Notice for Service Personnel

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



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

Perchlorate Present

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

Rack Mounting the DataFort Appliance

Perform the following steps to install the appliance:

- Selecting a Location
- Rack Mounting
- Connecting the Decru DataFort Appliance
- Assigning the DataFort IP Address

Selecting a Location

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

- Make sure the ambient temperature around the unit (which may be higher than the room temperature) is within the limit specified for the unit:
  - Operating Temperature: +5°C to +40°C (41°F to 104°F)
  - Storage Temperature: -10°C to +60°C (+14°F to 140°F)
- Make sure there is sufficient air flow around the unit. Do not block air flow to fans.
- Make sure electrical circuits are not overloaded - consider the nameplate rating of all the connected equipment, and make sure you have overcurrent protection.
- Make sure the equipment is properly grounded.
- Make sure no objects are placed on top of the unit.
- Do not block access to the front panel smart card slot, LEDs or LCD panel.
- Allow access to rear panel ports and power supplies.
- Avoid dusty or damp locations.



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

Rack Mounting

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



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

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

Connecting the Decru DataFort Appliance

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

- System Card Insertion
- Rear Panel Network Connections
- Power Connection

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.

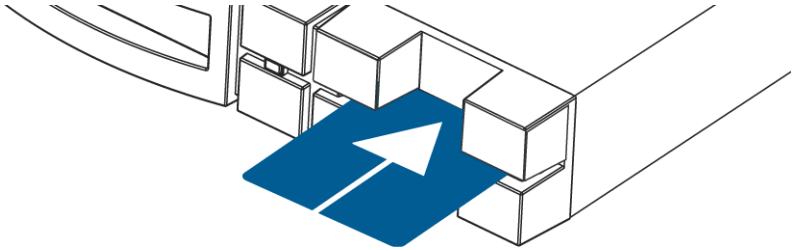


Figure 4-6: The front panel slot housing the System Card on a 1U DataFort

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 rear panel ports as described in the following sections:

- Ethernet Connection
- Serial Console Port

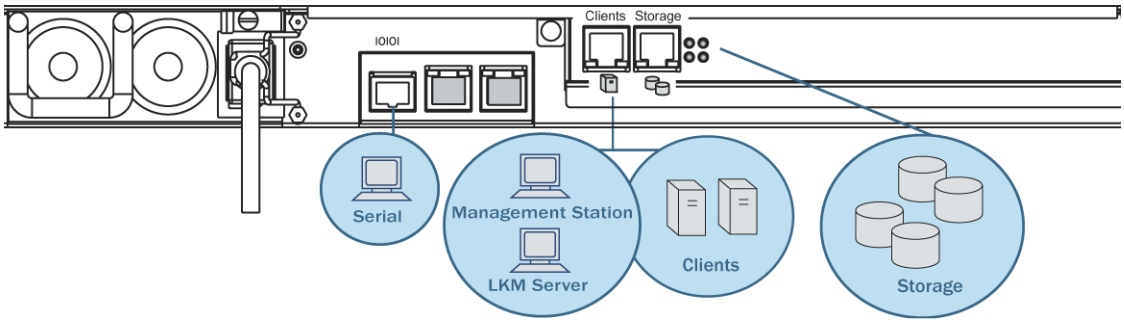


Figure 4-7: Rear panel connections 1U DataFort

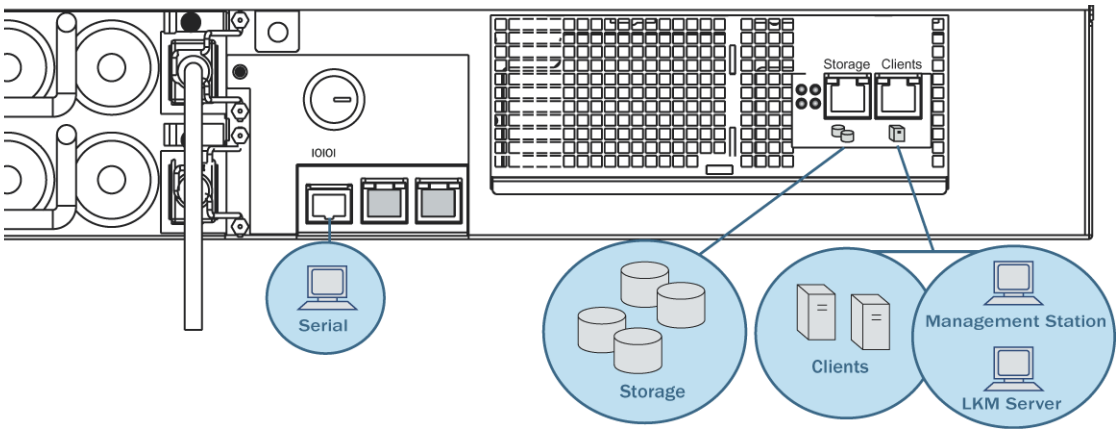


Figure 4-8: Rear panel connections 2U DataFort

Ethernet Connection

DataFort features two distinct interfaces for connecting to the network. The Clients NIC provides an interface for unencrypted data (clients and initiators), and the Storage NIC provides an interface for encrypted data (file servers and targets). Icons on the DataFort indicate which port is which. Port label coloration indicates black for encrypted data flow, and silver for cleartext data. In a network which separates clients and file servers into separate subnets, connect the File Servers NIC to the segment where file servers reside, and the Clients NIC to the segment where clients reside.

File Servers NIC

- Connect the DataFort File Servers NIC to the subnet where file servers and or targets reside using a Category 5 Ethernet cable.

Clients NIC

- Connect the DataFort Clients NIC to the client subnet where clients and or initiators reside using a Category 5 Ethernet cable.

- The PC being used as a Management Station should also be connected to this network segment.
- The LKM server or appliance should also be connected to this network segment.

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.

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

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

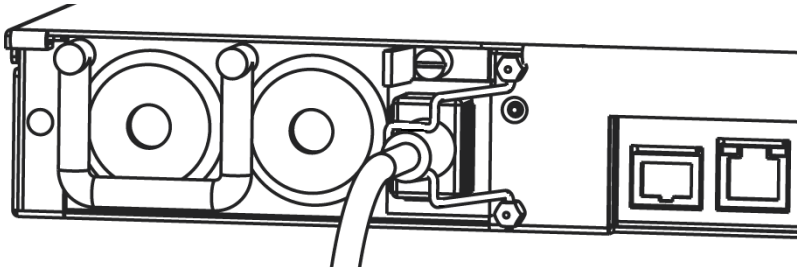


Figure 4-9: Power cord secured by the wire retaining clamp

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

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

3. Proceed to the step of Assigning the DataFort IP Address.

   Note: Leave DataFort powered on for normal operation. See Powering Up and Shutting Down on page 46 for instructions on powering off the appliance.

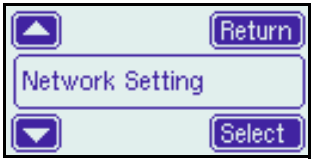
Assigning the DataFort IP Address

Assigning an IP address for the DataFort Clients/Management NIC is required so that setup can be completed from the Management Station. Follow instructions to assign the IP address 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 Network Setting entry. (If not, touch either the up or down arrow to scroll the menu to the correct entry.)



3. Touch the Select button.
4. Touch the Edit button. The screen displays a keypad of numbers, and selectable fields for the Clients NIC 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 Clients NIC address, touch Next. The touch panel screen displays a keypad of numbers, and selectable fields for the Clients NIC 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 Clients NIC- 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 Clients NIC.
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.

Powering Up and Shutting Down

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

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

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

Power DataFort on	Connect each provided power cord to a DataFort power port. Then connect the cord to an AC power source. The appliance will power on automatically.
Power DataFort off temporarily	Use the power button located on the rear panel next to the power supply. To temporarily power off DataFort, depress the recessed power button until the system turns off. This may take up to five seconds.
Power DataFort off permanently	Unplug all power cords from the AC power source. Always back up the configuration database before powering off DataFort (as described in the administrative chapters of this guide).

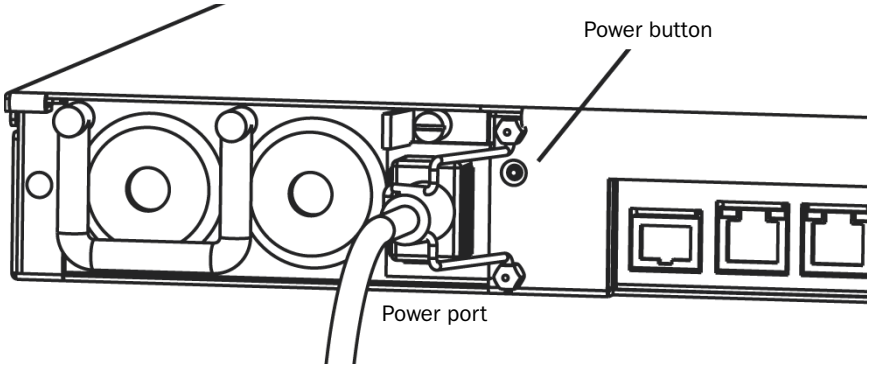


Figure 4-10: Rear panel power port and button on 1U appliance

5 INITIALIZING DATAFORT APPLIANCES

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

Note: Only the Decru Management Console Setup Wizard can set up new appliances. Once appliances have been set up, they can be managed using the DMC, the DataFort WebUI and the DataFort CLI.

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 19 before beginning installation.

Complete the procedures outlined in the following topics to initialize a DataFort appliance:

- About the Setup Wizard
- Initializing a Standalone DataFort or DataFort Cluster
- Logging into Appliances Using DMC
- Adding a Member to a Cluster

About the Setup Wizard

Consider the following when running the wizard:

- Initialization of a new DataFort appliance creates the first Full Administrator for that DataFort or DataFort cluster.
- 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 34.

Setup Wizard Functions

The Setup Wizard allows an administrator to complete the following procedures:

- Set up a new standalone appliance. The appliance must be initialized and connected to the network before beginning. See Initializing a Standalone DataFort or DataFort Cluster on page 49.
- Set up a new cluster. All cluster members must be initialized and connected to the network before beginning. Initializing a Standalone DataFort or DataFort Cluster on page 49
- Add a new member to an existing cluster. A standalone appliance must already be set up and the new member initialized and connected to the network before beginning. See Adding a Member to a Cluster on page 61.
- Set up a new appliance or cluster with an existing configuration (restore a configuration). See Restoring a DataFort on page 257.

About Smart Cards and Readers

The setup process will require the presence of Recovery Cards and the Recovery Officers responsible for those cards. Setting up an appliance requires that cards be inserted into the smart card reader connected to the Management Station.

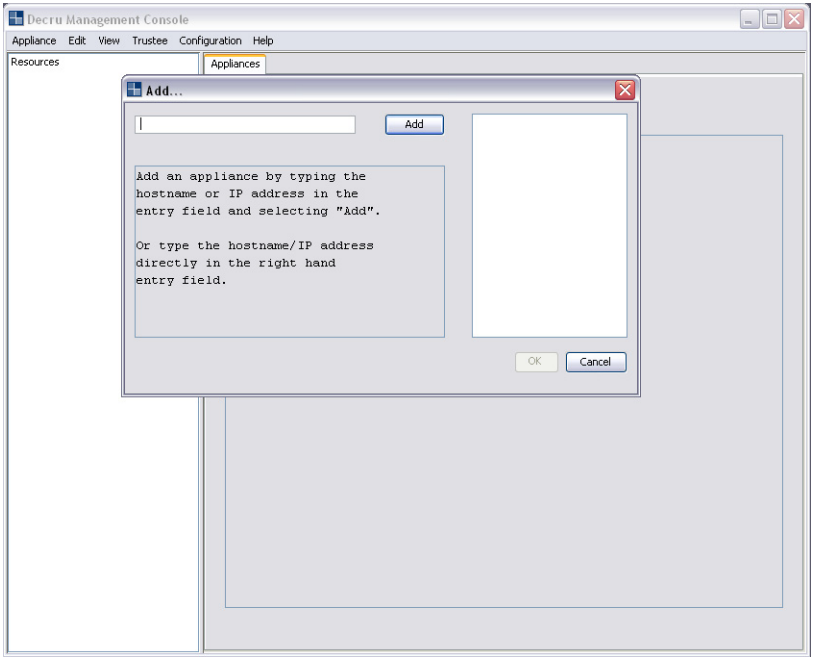
You can choose to connect multiple smart card readers to the Management Station, thereby making it possible to complete the wizard without having to switch cards. For example, if the quorum is 2 out of 5 cards for the cluster and two card readers are connected, both required Recovery Cards can be inserted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

INITIALIZING A STANDALONE DATAFORT OR DATAFORT CLUSTER

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

   DMC will start.

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

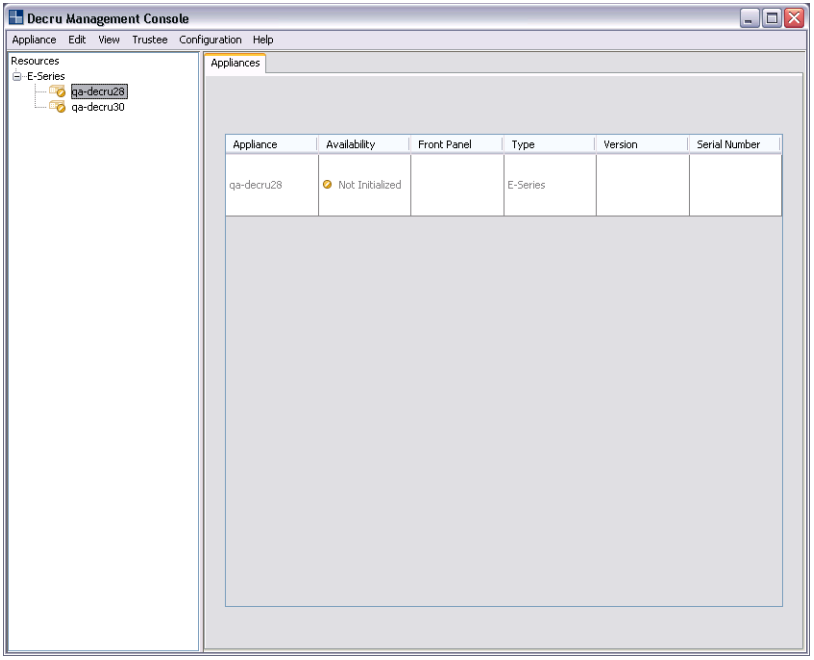


2. Enter the IP address or hostname of all appliances that will be set up.

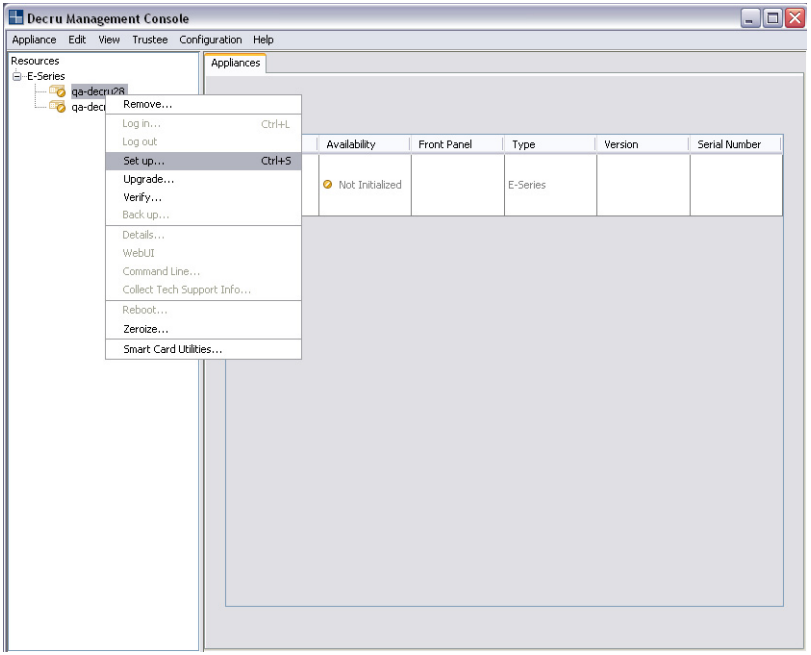
   More than one appliance can be added on this screen: enter the IP address or hostname for each appliance in the single field provided and click Add after each, or add all IP addresses or hostnames directly into the pane on the right side of the screen.

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

   The added appliances will appear in the DMC.



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



The Welcome page of the Wizard appears.

6. Click Start.

Connect to Head of Cluster

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

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

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

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

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

Sign License Agreement

Agree to the license terms to continue the wizard.

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

Recover From Database

Use this page of the wizard ONLY if this DataFort will replace a previously existing DataFort and a configuration database from that previous DataFort will be used to configure this new DataFort. For information about this feature, see Restoring a DataFort on page 257.

- Skip the Recover from Database screen by clicking Next.

Create Administrator

Create an administrator for this appliance. 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.

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 special characters. Note that double quotes and backslashes are not permitted. Select a password consisting of at least 8 valid, randomly-chosen characters.

   Note: Record login information carefully. You will not be able to manage the appliance without it. This name and password will be used every time the administrator logs in to the appliance using any DataFort management interface.
3. Click Next.

Configure Cluster and Recovery Schema

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

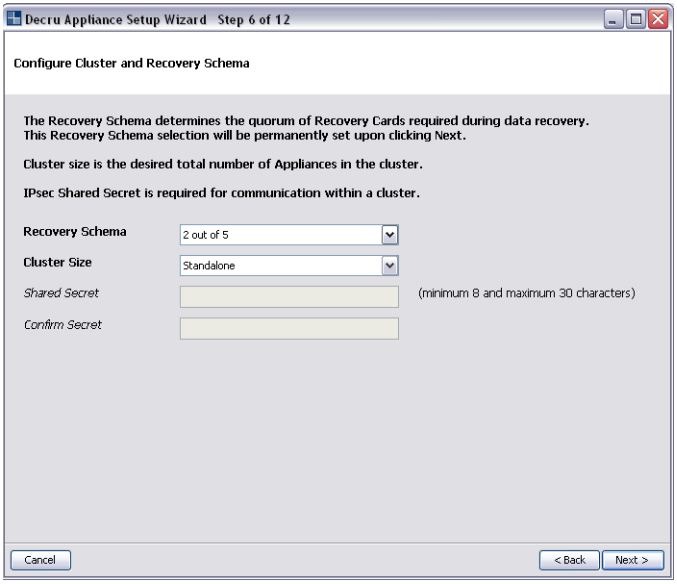
Note: The recovery schema is permanent. Plan the setting according to the security policy of your organization before completing the wizard.

- Setting the Recovery Schema
- Setting the Cluster Size

Setting the Recovery Schema

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

2 out of 5 is the recommended data recovery setting, in which any 2 of the 5 Recovery Cards that are initialized during DataFort setup are required to complete a recovery procedure. Each card should be given to a different individual, so that two people must be present for any data recovery to occur. In this scenario, two cards may be sent to escrow for safekeeping. If needed, the number of people required for a recovery operation can be expanded by having one person in physical possession of a Recovery Card and another person know the password for the card. For more about options when managing smart cards, contact Decru.



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

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

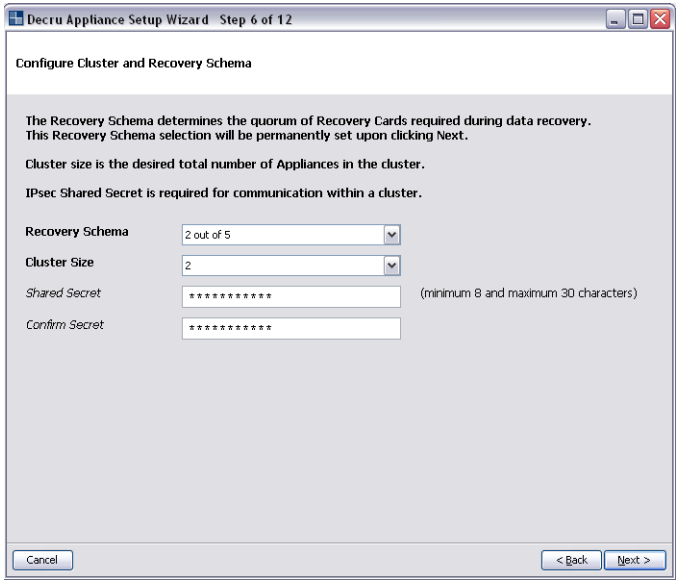
Setting the Cluster Size

2. Select standalone or cluster size.

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

Cluster Size—Select a Cluster Size of 2 from the Cluster Size menu if this is the first DataFort in a cluster, or if this is a DataFort joining a standalone appliance in order to form a cluster.

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



3. Click Next to proceed.

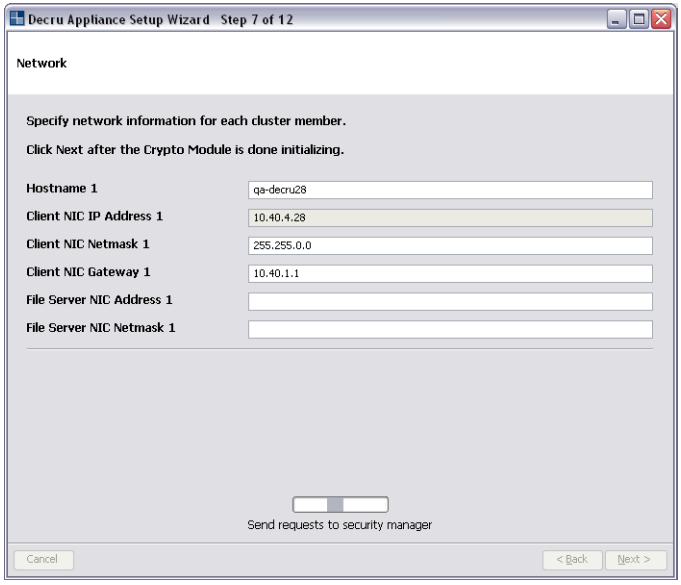
NETWORK SETTINGS

Enter the appropriate network settings.

- If Standalone was selected in the previous step, only one set of fields 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. See Cluster Network Settings.

Standalone Network Settings

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



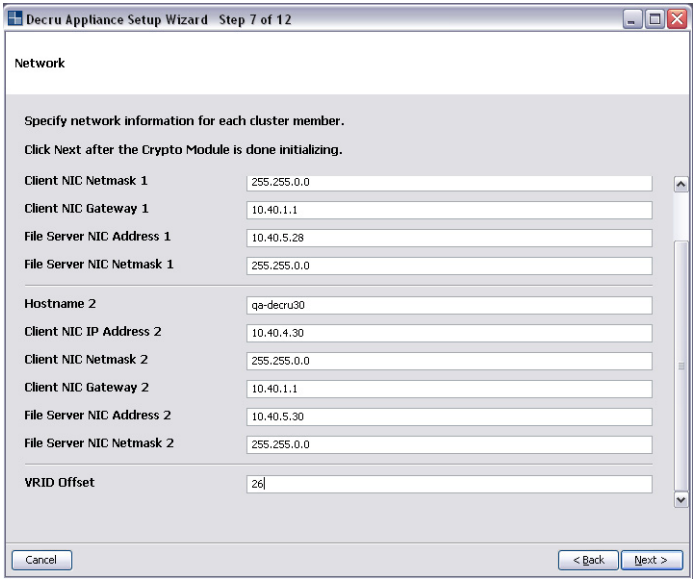
1. Enter a hostname for this DataFort.

   The IP address, Netmask and Gateway set for the Clients NIC will appear. (These were set when Assigning the DataFort IP Address on page 44.)

2. Enter an IP address and Netmask for the File Servers NIC.
3. Click Next.

Cluster Network Settings

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



1. Enter a hostname for the first DataFort.

   The IP Address, Netmask and Gateway set for the Clients NIC of the first DataFort will appear. (These were set when Assigning the DataFort IP Address on page 44.)

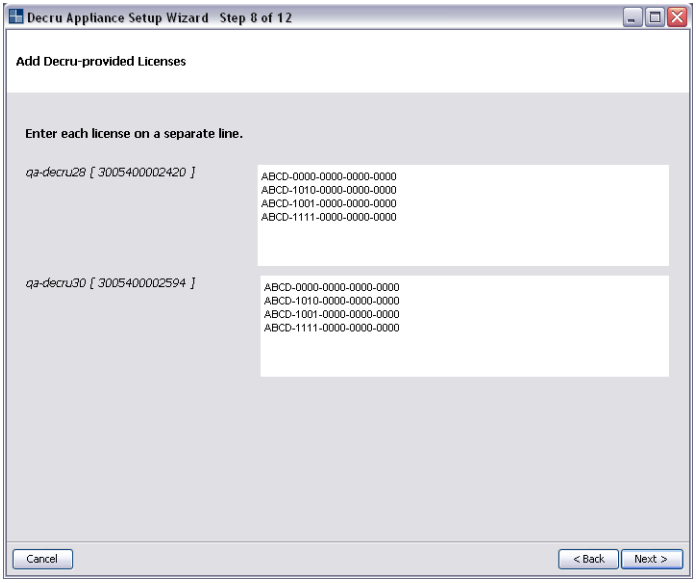
2. Enter an IP Address and Netmask for the File Servers NIC of the first DataFort.
3. Enter a hostname for the second DataFort.
4. Enter IP Address, Netmask and Gateway information for both the Clients NIC and the File Servers NIC of the second DataFort.
5. VRID Offset: Enter the first VRID in the sequential block assigned by the network administrator (see VRIDs for Cluster Members on page 25).

   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.

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

ADD LICENSES

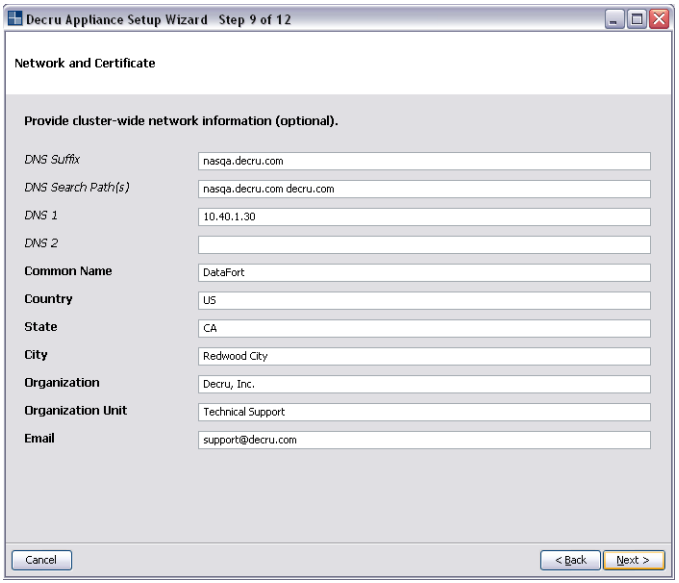
Make sure that each DataFort which will be in the cluster has a license that supports the same features. Site-wide licensing is also available, which allows the same licenses to be used for all appliances in the cluster.



1. Enter the license key provided by Decru for each feature for each appliance.
   - To enter multiple licenses enter each license and then press Enter on the Management Station keyboard to start a new line for the next license.
   - If site licenses are in use, the same licenses should be entered for each DataFort.
2. Click Next.

NETWORK AND CERTIFICATES

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



DNS

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

Certificate

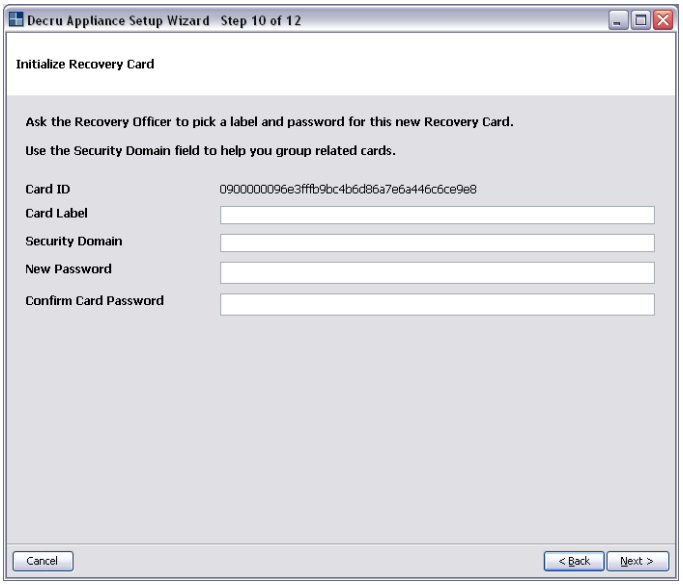
Configure DataFort to accept a self-signed security certificate to improve security for the SSL communication between the Management Station and DataFort.

1. Enter a name for the appliance.
2. Enter the country code for your location. The country code is limited to two characters in length. For the United States, enter **US**. Other codes are listed in Partial List of ISO Country Codes on page 289.
3. Enter the rest of the required information about your location.
4. Click Next.

INSERT RECOVERY CARD

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

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



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

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

Initialized Card — If the card has already been initialized, the card label and Security Domain will load into the wizard and you will be prompted for the password. The Recovery Officer responsible for this card should provide this information.

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

Security Domain information from the first card will be entered automatically. You may change it if you want the card grouped differently.

5. Repeat the previous steps for all the cards specified by the recovery schema.

Apply Settings

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

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

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

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

When the wizard is complete, the appliance is ready to be managed by the Decru Management Console or DataFort WebUI. See Chapter 6 for a list of DataFort management interfaces.

- The DataFort WebUI provides complete management tools for a DataFort appliance or cluster. After the wizard is complete, you can close DMC and log into the WebUI to manage DataFort. Continue with DataFort Management Interfaces on page 65.
- The Decru Management Console offers a sub-set of the appliance management options available in the DataFort WebUI. To use the DMC, log into the appliance as described below. Continue with DataFort Management Interfaces on page 65.

Logging into Appliances Using DMC

Log into each appliance after adding it to DMC as described in Initializing a Standalone DataFort or DataFort Cluster on page 49.

1. Select an appliance in the DMC Resources pane and choose the **Appliance > Log in** menu item.
2. Enter the administrator name and associated password at the Login page.
3. Click OK.

   If the correct credentials were entered the status of the appliance will change to online. See Decru Management Console Functions on page 219 for more information about using DMC.

Adding a Member to a Cluster

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

- You will need the cluster quorum of Recovery Officers with their cards, and the shared secret of the cluster.

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

   DMC will start.

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

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

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

   The added appliance will appear in the DMC.

6. From the Resources pane, right-click a existing member of the cluster and choose Set up.

   Note: Do not select the DataFort that will be added. Select an existing member of the cluster.

   The Welcome page of the Wizard appears.

7. Click Start.

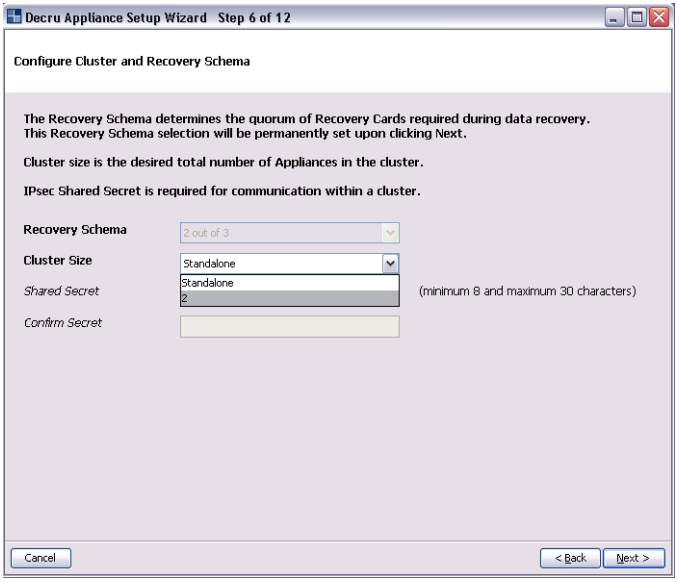
Log in to Head of Cluster

You will be prompted to trust the certificate from DataFort and log in to the appliance.

1. Trust the certificate when prompted.
2. Enter the administrator name and password set for the standalone appliance being joined by the new appliance to form the cluster.
3. Click OK.

Cluster and Recovery Schema

You will not be able to modify the Recovery Schema, as it has already been set for the cluster.



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

NETWORK SETTINGS

Enter the network settings for the appliance the will be added to the cluster.

1. Enter a hostname.
2. Enter IP Address, Netmask and Gateway information for both the Clients NIC and the File Servers NIC of the second DataFort.
3. VRID Offset: Enter the first VRID in the sequential block assigned by the network administrator (see VRIDs for Cluster Members on page 25).

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

Add Licenses

1. Enter the license key provided by Decru for each feature for each appliance.

   To enter multiple licenses enter each license and then press Enter on the Management Station keyboard to start a new line for the next license.

   If site licenses are in use, the same licenses should be entered for each DataFort.

2. Click Next.

Network and Certificates

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

DNS

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

Certificate

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

1. Enter a name for the appliance.
2. Enter the country code for your location. The country code is limited to two characters in length. For the United States, enter **US**. Other codes are listed in Partial List of ISO Country Codes on page 289.
3. Enter the rest of the required information about your location.
4. Click Next.

Insert Recovery Card

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

1. Insert the first Recovery Card into the Management Station's smart card reader. Smart cards must be fully inserted into the reader. If a card is not recognized, re-insert it for better contact.
2. The Recovery Officer responsible for this card should enter the required information into the provided fields.
3. Click Next.
4. Repeat the previous steps for all the cards specified by the recovery schema.

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 to apply the settings to all appliances that are being configured using the wizard.
2. Insert the quorum of Recovery Cards. If one smart card reader is in use, the cards will need to be inserted and removed as indicated by the wizard.

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

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

When the wizard is complete, the appliance is ready to be managed by the Decru Management Console or DataFort WebUI. See Chapter 6 for a list of available management interfaces.

- The DataFort WebUI provides complete management tools for a DataFort appliance or cluster. After the wizard is complete, you can close DMC and log into the WebUI to manage DataFort. Continue with DataFort Management Interfaces on page 65.
- The Decru Management Console offers a sub-set of the appliance management options available in the DataFort WebUI. To use the DMC, log into the appliance as described below. Continue with DataFort Management Interfaces on page 65.

6 DataFort Management Interfaces

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

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

Management Interfaces Overview

After initial setup is complete, a DataFort administrator can use management interfaces to configure and manage the appliance. The management interfaces available to the DataFort administrator are summarized in the following table.

Table 4: Management Interfaces

Interface	Description	Usage
• Secure Sockets Layer (SSL) • Transport Layer Security (TLS)	A secure HTTP (HTTPS) connection to the DataFort WebUI via a web browser running on the Management Station. Can be configured to require smart card authentication in addition to the administrator password. See Connecting to the DataFort WebUI.	Primary method for creating and managing Cryptainers, DataFort settings, users, etc.
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 in addition to 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 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).
Decru Management Console (DMC)	A Java tool used for setup and management of LKM and DataFort appliances. DMC provides a centralized management interface for all appliances in an installation.	The only way to set up an appliance using the Setup Wizard. The only management interface for the LKM appliance. Provides some additional management functions for DataFort appliances.
	A limited DMC is shipped with each DataFort appliance. The full DMC product supports SecureView.	
	SecureView feature of Management Console	Enables many-at-once control of LKM and DataFort appliances. Requires SecureView license on all appliances that will be managed simultaneously.

SECUREVIEW

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

To facilitate management of multiple appliances using SecureView, add the same administrator (with the same name and password) to all appliances. This will make it possible to select, log into and manage all appliances at once.

SECURITY POLICIES

Security policy settings determine whether an Admin Card is required for logging in to the WebUI or CLI of an appliance. By default, DataFort is set not to require an Admin Card for WebUI or CLI access. To turn on Secure Web or Secure CLI (which require the presence of an Admin Card to log into DataFort), customize the security policy as described in Management Security Settings on page 169.

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. Fro more about administrator types, see Chapter 7.

ONLINE HELP

Use the Decru Management Console to access online help for the DataFort appliance. Using the Help menu, use DMC to open an online version of the administrative guide for the appliance selected in the console. See Decru Management Console Menus on page 226 for details about the DMC Help menu.

Connecting to the DataFort WebUI

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

Using the DataFort WebUI

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.
- 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. To login for User Registration, see CIFS User Registration on page 142.

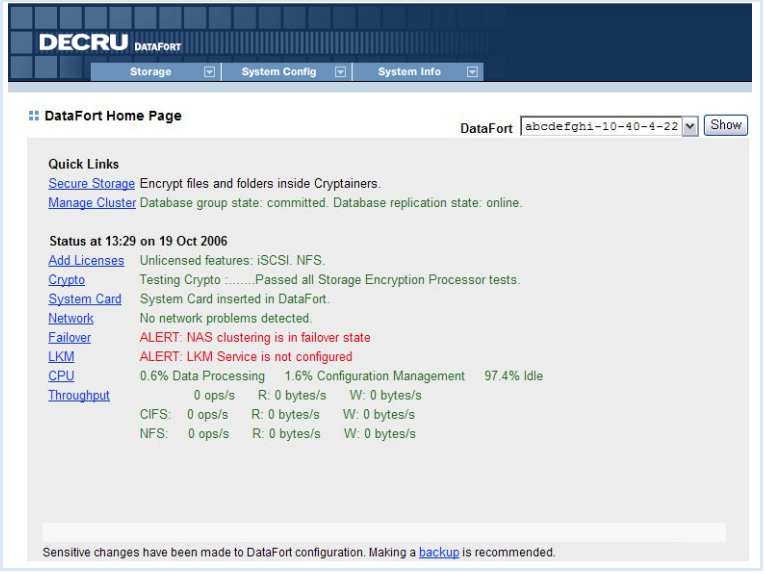
1. From Internet Explorer on the Management Station, enter **`https://`** followed by the IP address or resolvable hostname assigned to DataFort. (Be sure to enter https.)

   Note: TLS 1.0 must be enabled as described in Preparing the Management Station on page 34.
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 Yes to proceed.

   The DataFort Login page appears.
8. Enter the username and password set during the wizard and click Log In.

   The DataFort Home page is displayed after running a Setup Wizard, and after that, 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 Servers and Portals
D+I Initiators and Targets
D+B Back Up Configuration
D+L Log
D+C LCD
D+W WebCLI

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

Quick Links and Status

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

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

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

Note: If the DataFort defense response has been triggered, a warning will appear on the Home page. DataFort will not accept any management commands in this state. To address this warning, see Clearing a Defense Alert on page 164.

Cluster Member Access

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

Connecting via WebUI using Dual Authorization

By default, all valid administrators can log in to DataFort without additional authorization. If this privilege is revoked for a given administrator 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 Management Security Settings on page 169. 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 269 for information about CLI online help.
- As a security measure, the CLI times out after 10 minutes of inactivity.

Connecting via Standard CLI

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

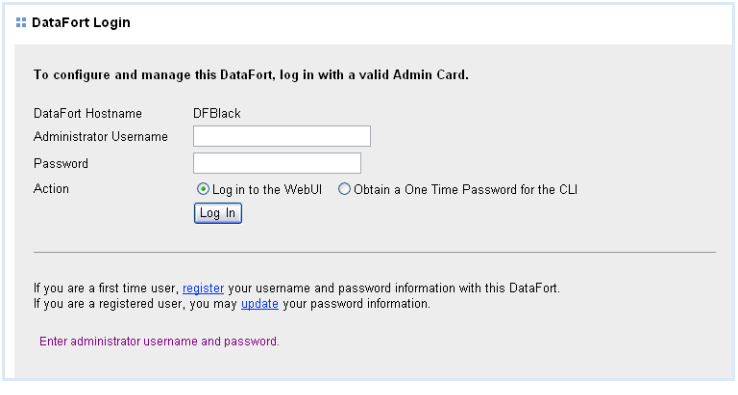
1. Open an SSH client on a workstation connected to the same network as the DataFort.
2. Enter the IP address or hostname assigned to DataFort.
3. In the terminal window, enter the administrator login name and password.

Connecting via Secure CLI

Secure CLI requires that an administrator present an Admin Card as well as a username and password. The smart card authentication requires log in to the WebUI via the Management Station. A temporary CLI login password is generated, which can be used to log in to CLI from an SSH client.

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 68.
2. Click the button: Obtain a One Time Password for the CLI.

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



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

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

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

Connecting via CLI using Dual Authorization

By default, all valid administrators can log in to the CLI without additional authorization. If this privilege is revoked for a given administrator 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.

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

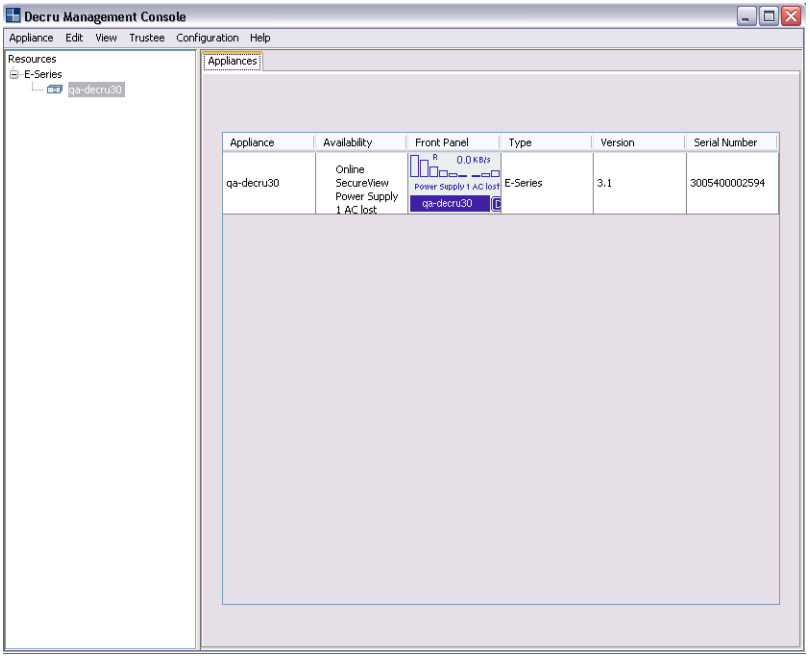
  Note: WebCLI does not support the following features: command history, command line editing and completion, output paging and context-sensitive help.

ACCESSING THE DECRU MANAGEMENT CONSOLE

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

- Choose **Start > Programs > Decru > Decru Management Console** from the Management Station. Any appliances which have been added to DMC will appear.
- See Decru Management Console Menus on page 226 for a description of the menu options.

Some menu options initiate operations which are described only in the *Lifetime Key Management Administration Guide*.



Serial Console

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

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.

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

Configuring IP Settings

1. At the shell prompt, log in using the default administrator name and password (note that these entries are space and case sensitive):
   - Login: **user**
   - Password: **MTKNMTKN**

   The main menu will appear.
2. Select option **1**, and set an IP address, subnet mask and default gateway for the Clients NIC.
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 207.

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 Zeroization Using the Serial Console on page 195 for details. If the Admin Card has been lost, see Emergency Serial Console Port Access on page 195.

DATAFORT FRONT PANEL LCD

After setup, the DataFort front panel LCD displays messages and a bar graph showing data read and write rates. If the DataFort is equipped with a touch-sensitive panel, onscreen buttons will provide more options, including the ability to access more information about an error and configure the IP settings on an uninitialized DataFort.

The left side of the graph indicates the rate (in bytes per second) at which DataFort reads data, or decrypts encrypted data. The right side of the graph depicts the rate at which DataFort writes, or encrypts data. The read/write display differs according to the type of DataFort LCD:

- Read/Write Rate Display on 2U DataFort Appliances
- Read/Write Rate Display on 1U DataFort Appliances

TABLE 5: READ/WRITE RATE DISPLAY ON 2U DATAFORT APPLIANCES

Bar Display	Rate (per second)
1 bar	1 - 5K
2 bars	5K - 50K
3 bars	50K - 500K
4 bars	500K - 5MB
5 bars	5MB - 50MB
6 bars	50MB and up

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

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

Touch Panel Onscreen Buttons

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

Menu The Menu button opens a scrollable menu with access to network settings and DataFort information (including software version and serial number). Use the up and down arrows to navigate the menu options, touching the Select button to access more information about the selected topic, and the Return button to return to the previous screen.

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

Details When an error message appears, the Details button becomes visible on the LCD. Touching the button displays more information about the current error, and suggested steps to take to correct the error.

SNMP Settings

DataFort supports both MIB II and the read-only private Decru MIB. The Decru MIB is included on the DataFort CD. It provides standard MIB-II as well as Decru MIB messages. All Decru MIBs are read-only for security reasons. See Machine Administration on page 206 for details.

7 DataFort Admin Roles and Account Administration

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

- Administrator Roles
- Account Administration

ADMINISTRATOR ROLES

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

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

- Full Administrator
- Accounts Administrator
- Storage Administrator
- Key Administrator
- Security Administrator
- Backup Administrator
- Machine Administrator
- Read-Only Administrator
- User 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 speciality administrator can also be created. It may be useful for example to have several combined Machine, Storage and Key Administrators, but leave the Security and Account roles for a few highly-trusted individuals. See Administrator Roles and Privileges on page 79 for details.

TABLE 7: ADMINISTRATOR ROLES AND PRIVILEGES

Role Name	Privileges
Full Administrator	The Full Administrator sets up each DataFort or DataFort cluster for the first time by running a setup wizard as described in Initializing DataFort Appliances. The Full Administrator can complete all administrative tasks including: • Initializing DataFort Appliances • Account Administration • NAS Storage Administration • iSCSI Storage Administration • User 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 servers, VIPs, shares, initiators and targets which are required in order to create Cryptainers. (Note that actual Cryptainer creation must be performed by a Full or Key Administrator.) Storage Administrator tasks are described in NAS Storage Administration and iSCSI 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 described in NAS Storage Administration and iSCSI Storage Administration. Key Administrator tasks include: • Managing Trustees as well as importing and exporting exportable keys • Purging keys upon backup to LKM as described in Key Purging • Managing Cryptainers as described in NAS Storage Administration and iSCSI Storage Administration • Managing DataFort Defense Responses • Setting Security Options • Configuring IPsec • Managing Recovery Officers and Recovery Cards
Security Administrator	A Security Administrator is responsible for applying physical security-related settings to DataFort appliances as described in Physical Security Administration. Security Administrator tasks include: • Setting Date and Time • Configuring and Viewing Logs • Zeroizing the Decru DataFort

TABLE 7: ADMINISTRATOR ROLES AND PRIVILEGES (CONTINUED)

Role Name	Privileges
Backup Administrator	A Backup Administrator is responsible for managing backups of the configuration database, including those to LKM. Backup Administrator tasks described in Backup Administration include: • Saving Configurations to Lifetime Key Management Software • Downloading Configurations to a Remote Location
Machine Administrator	A Machine Administrator is responsible for managing system properties and non-security sensitive cluster operations. This administrator can change local network settings. Machine Administrator tasks described in Machine Administration include: • Network Settings • Upgrading DataFort • Setting Security Certificates • Managing Licenses • SNMP Settings • The Machine Admin can also add cluster members as described in Cluster Administration.
Read-Only Administrator	A Read-Only Administrator can view all DataFort settings (see DataFort Appliance Settings and Status) and can view status and logs, but cannot modify settings.
User Administrator	A User Administrator is responsible for managing NAS users and groups, domains and access control for data managed by DataFort. This administrator can perform functions described in User Administration including: • Managing Groups and Users • Group Review • Managing Cryptainer ACL and syncing server and DataFort ACLs.

ACCOUNT ADMINISTRATION

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

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

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

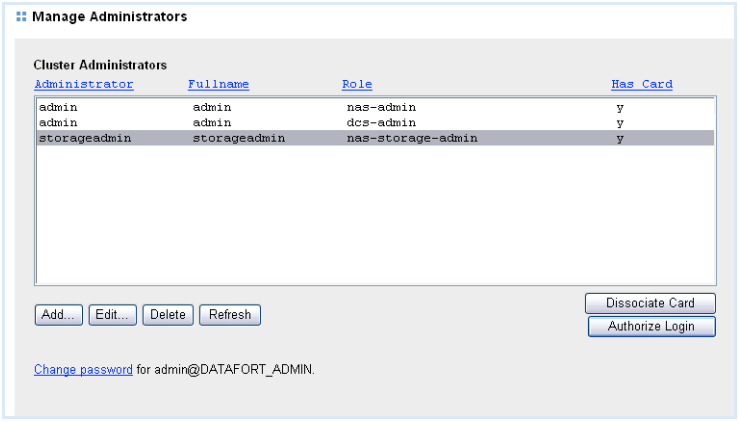
- Adding an Administrator
- Requiring Authorization for Login
- Changing the Administrator Password
- Removing an Administrator
- Changing a Card Association

ADDING AN ADMINISTRATOR

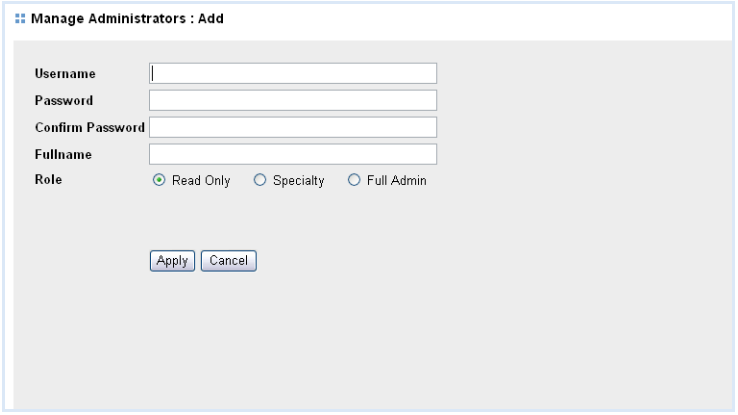
A Full Administrator or an Accounts Administrator must be logged in to the WebUI to add an administrator. See Connecting via WebUI on page 68 for login instructions.

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

   Administrators known to this DataFort are listed.



2. Click Add.



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.

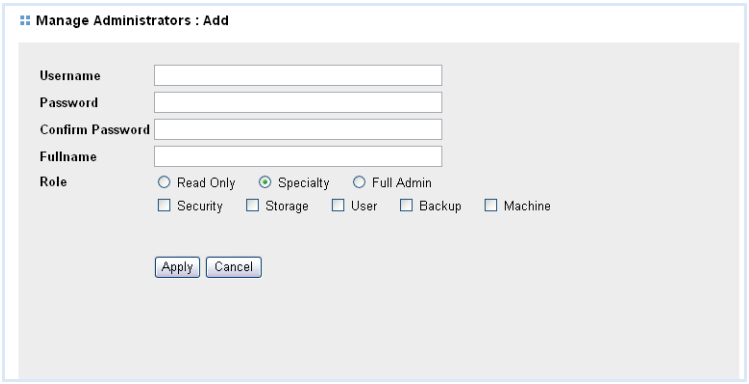
   Passwords may be composed of upper and lower case characters, numbers and special characters. Note that double quotes and backslashes are not permitted.

   Select a password consisting of at least 8 valid, randomly chosen characters.

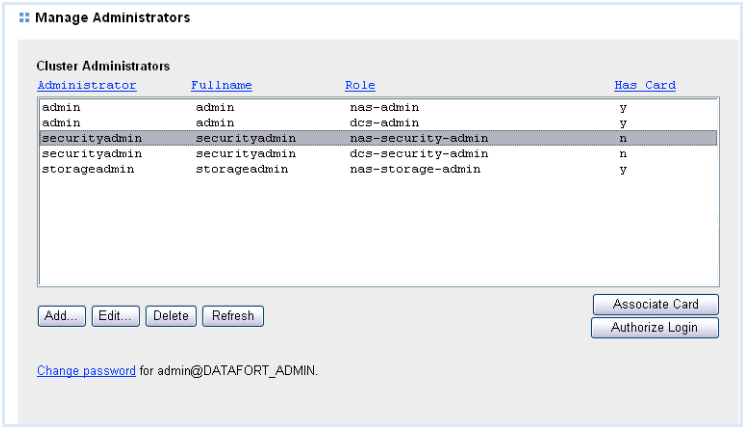
4. Confirm the password.
5. Enter a full name for the administrator.
6. Select the type of administrator you want to create. See Administrator Roles on page 78 for details. You can also require that an administrator be authenticated before being able to log in to DataFort. See Requiring Authorization for Login on page 84 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.



7. Click Apply.



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 and click Associate Card.

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

Requiring Authorization for Login

By default, 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 Full Administrator not requiring prior authorization at all times.

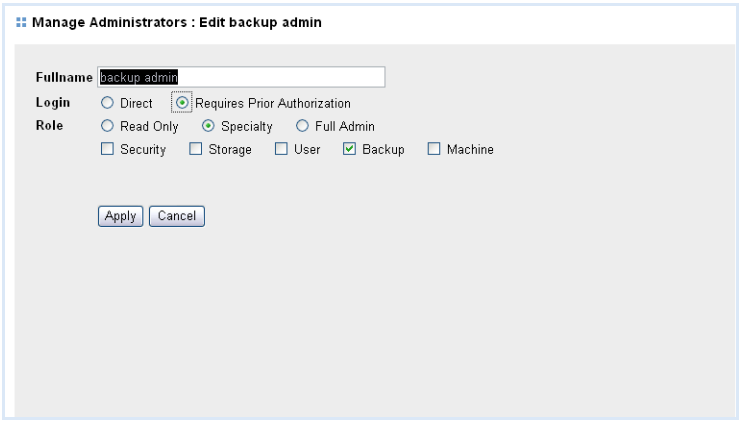
Protecting Against Insider Attacks

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.



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

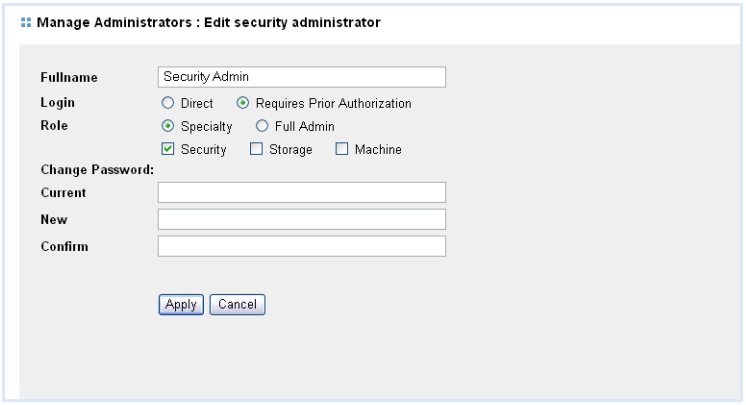
   Now this administrator will need authorization to log in to the DataFort. See Connecting via WebUI using Dual Authorization on page 70 for authorizing WebUI login, and Connecting via CLI using Dual Authorization on page 72 for authorizing CLI login.

   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.

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

   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 no longer authenticate that administrator. A Full Administrator or an Accounts Administrator can delete an administrator.

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

Changing a Card Association

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

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

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

8 Before 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.

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

- Checking Cluster State
- Configuring Remote Logging
- Starting LKM
- Creating Additional Administrators
- Verifying System Version
- Determining the Defense Setting

These operations are performed using the WebUI. For login instructions see Connecting to the DataFort WebUI on page 68. Note that the Decru Management Console (DMC) can also be used to perform some of these operations. See Chapter 19 for DMC menu options.

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 Checking the Cluster State on page 197 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 185 for details.

Starting LKM

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

Before configuring DataFort, set up the LKM management solution. See Setting Up Lifetime Key Management on page 36.

LKM Server

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

- From the WebUI, click the LKM link or choose **System Config > Recovery > LKM Settings**.
- Set the LKM server information for automatic backup. See Saving Configurations to Lifetime Key Management Software on page 180. All LKM settings are propagated across cluster members, therefore it is sufficient to enter LKM settings once for each cluster.

LKM Appliance

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

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 Admin Roles and Account Administration.

- 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 81 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 162.

9 NAS Storage Administration

This chapter includes instructions for using the DataFort WebUI to manage NAS Cryptainers, the backbone of a storage network secured by DataFort appliances. NAS and iSCSI storage management functions share many menus and features. For iSCSI Cryptainers, see iSCSI Storage Administration.

A Full Administrator is assumed to have completed installation and preparation of DataFort appliances. A Full Administrator can perform all of the functions outlined in this chapter. If specialized administrators are in use, keep in mind that while a Storage Administrator can complete most tasks leading up to the creation of a Cryptainer, only a Full or Key Administrator can actually assign data an encryption key by creating a Cryptainer.

Whether or not specialized administrators are in use, the process of creating Cryptainers requires that shares or exports existing on file servers be introduced to DataFort for export as encrypted data.

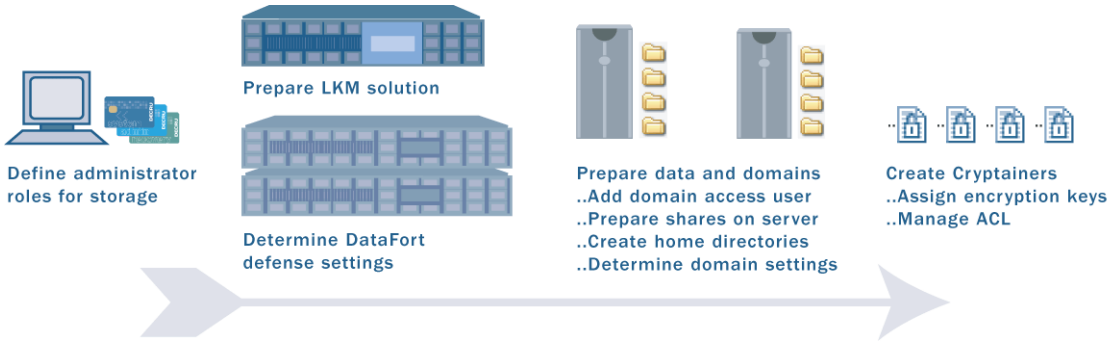


Figure 9-11: Overview of the workflow for creating NAS Cryptainers

NAS storage administration involves the following:

- Understanding DataFort Domains
- Preparing to Create a NAS Cryptainer
- Creating a NAS Cryptainer
- Creating a NAS Cryptainer From a Home Directory
- Creating a NAS Cryptainer Using Specialty Administrators
- Managing Secure NAS Storage
- Restoring a Cryptainer

Understanding DataFort Domains

To create NAS Cryptainers, introduce domains and file servers (where data will be stored) to DataFort, and select shares on those servers to be exported as Cryptainers. It is important to understand DataFort support for domains during this process. DataFort offers options for working with domains, including controls for how DataFort syncs information with a domain controller.

DataFort associates the following with a domain:

- a collection of users and groups that are members of the domain
- a domain controller that maintains information about the current users and groups in the domain
- a collection of file servers that are members of the domain, or that perform user authentication against the domain controller
- a domain name, used for reference and sometimes for protocol-specific communication with the domain controller
- a DataFort Domain Access User name and password, used by DataFort for communicating with the domain controller and with file servers belonging to the domain (see Adding the DataFort Domain Access User on page 36)
- DataFort also supports Userless Domains on which it does not enforce access restrictions.

File Servers and Domains

When file servers are added to DataFort in preparation for creating Cryptainers, they are associated with a specific domain. The name of the domain chosen, and the DataFort Domain Access User name and password associated with that domain, are the credentials that DataFort will use to communicate with the file server when performing operations such as Cryptainer creation.

For Windows, the domain chosen for a file server does not have to be the actual domain in which that file server resides. However, the file server will still need to accept the domain name, the access user name, and the password of the domain chosen during an authentication request by DataFort.

User Authentication and Domains

The domain associated with a file server is also used to help authenticate NFS and CIFS users when they attempt a connection to a file server through DataFort. For CIFS, a user is first verified locally by DataFort to make sure that user exists in the domain. DataFort can be configured to require that users register in order to access their data through DataFort. If user registration is required, DataFort also checks that the password supplied by the user matches the one registered for that user.

For NFS, the domain of the virtualized file server and the user's UNIX UID are used to identify the NFS user. This is done so that DataFort can support more than one NFS domain, and thus support NFS file servers that use different authentication (for example, NIS) domains.

Domain Types and Subtypes

Adding domains is part of the Cryptainer creation procedure. When adding a domain that will encompass UNIX users and groups and NFS file servers, an NFS domain should be added. When adding a domain that will encompass Windows/CIFS users and groups and CIFS servers, a CIFS domain should be added.

For each CIFS and NFS domain added to the DataFort configuration database, a subtype needs to be chosen. Subtypes include LDAP, NIS, Windows, Local and Userless domains. The subtype specifies the type of domain controller that the domain will use, and therefore how DataFort will learn about users and groups in the domain.

Table 8 describes the domain and subtype combinations supported by DataFort. Creating a NAS Cryptainer on page 96 includes steps required to add the domain and subtype combinations.

TABLE 8: DOMAINS AND SUBTYPES

Type	Subtype	Description	Instructions to Add Domain
CIFS	Windows	This is the most common choice for CIFS/ Windows environments.	Add a Domain. Specify the Windows domain name when adding the domain.
	Windows Domain-less Environment	If a Windows environment consists of file servers that are not members of any Windows domain, a file server may be added to DataFort as a domain.	Add a Domain. Specify the NetBIOS name of the file server as the domain name. Once this domain is added, DataFort will be able to query the file server for information about its local user and group accounts. Add the file server as a member of this domain. See Add a Server.
	LDAP	The domain controller for this domain is an LDAP server. DataFort supports the LDAP server schemas inetOrgPerson and NIS. Once the domain is added, users with LDAP accounts can access CIFS file servers through DataFort.	Add a Domain. Since these users have no actual Windows accounts to use for authentication against the file server, DataFort User Mapping and Use Local ACL should be turned ON. See User Mapping and DataFort Domains and File Server Security Settings.
	NIS	The domain controller for this domain is an NIS server. Once the domain is added, users with NIS accounts can access CIFS file servers through DataFort (by mapping a drive using Windows).	Add a Domain. Since these users have no actual Windows accounts to use for authentication against the file server, User Mapping should be turned ON. See User Mapping and DataFort Domains and File Server Security Settings.
	Userless	Use this subtype to have DataFort encrypt data in Cryptainers and permit access without performing its own access checks.	Add a Domain. Add the file server in that domain. Virtualize shares from the file server on a VIP that is in that domain. See Userless Domains.

TABLE 8: DOMAINS AND SUBTYPES (CONTINUED)

Type	Subtype	Description	Instructions to Add Domain
NFS	NIS	NIS is a common choice for NFS/UNIX environments that use NIS (YP) for user and group accounts.	Add a Domain. The domain controller for this domain is an NIS server.
	LDAP	Use LDAP for NFS/UNIX environments that use an LDAP server to store their user and group account information.	Add a Domain. Add the LDAP server as the domain controller.
	Local	Choose Local for NFS/UNIX environments where there is no domain controller to query.	NFS users and groups must be added manually to the DataFort. An NFS domain of some other subtype may be converted to this subtype to disable automatic user/group imports from the domain.
	Userless	Use this subtype to have DataFort encrypt data in Cryptainers and permit access without performing its own access checks.	Add a Domain. Add the file server in that domain. Virtualize shares from the file server on a VIP that is in that domain. See Userless Domains.

USER MAPPING AND DATAFORT DOMAINS

When the DataFort User Mapping feature is turned on, DataFort will perform all access to the file server on behalf of the connected user using the credentials of the DataFort Domain Access User (see Adding the DataFort Domain Access User on page 36.) See File Server Security Settings on page 168 for more information about User Mapping.

Commonly, CIFS domains with LDAP or NIS subtypes are used in conjunction with the User Mapping feature. This allows DataFort users with LDAP or NIS accounts to access Cryptainers on CIFS file servers, even though these users have no actual Windows accounts.

In order for User Mapping to work in an NFS domain, the domain has to have a properly set domain access user which might not be required otherwise.

USERLESS DOMAINS

Userless domains make it possible for DataFort to encrypt data at rest without performing any separate access checks and without the need to manage user accounts. A userless domain normally contains one user: its access user.

Userless domains are useful when enforcing ACLs is not a priority. If you do not want to track and manage users or access control privileges, a userless domain is preferable. With a userless domain any newly created users can have Cryptainer access immediately without involving an administrator.

For a server in a DataFort userless domain, access requests to any Cryptainer are routinely granted without any checks. Users accessing those Cryptainers do not have to be known to DataFort. The recommended configuration is for the virtual server and the corresponding real server to be in the same userless domain. The actual server may be in a regular domain, and may be enforcing user-based access controls. If you do not want to manage users, set up the server so that it does not enforce access control.

Preparing to Create a NAS Cryptainer

To create a Cryptainer, the DataFort administrator introduces an existing share to DataFort. This requires that the server on which the share is located be in a domain to which DataFort has access. DataFort will proxy servers that are added to the configuration database, exposing a virtual server name (or IP address) to network clients. The virtual server will be presented to clients as if it were the actual server. Set up new network shares for users so that the shares can be exported by DataFort as Cryptainers. See Create CIFS Shares and Create NFS Exports for guidelines.

Note: See Migrating Data on page 141 for tips on encrypting existing cleartext data.

Create CIFS Shares

Keep the following in mind when creating CIFS shares that will become Cryptainers:

- Create shares on servers in domains that can be accessed by DataFort, and therefore can be added to the DataFort configuration database.
- The DataFort domain access user must exist in the same domain as the servers that are added (see Adding the DataFort Domain Access User on page 36).
- When a share is created on the file server, right-click the share, select Sharing and Security, and make sure the share is set up to be shared.
- Edit share permissions so that the DataFort domain access user has full control, and other users have the appropriate permissions. Users must have permission according to both share and file/folder ACLs. Verify access control permissions for shares according to the operating system file permissions before they are introduced to DataFort for export as Cryptainers.
- The network administrator should follow standard procedures to set up shares for clients on network servers. DataFort can manage any share created on a server in a known domain. Access control settings for Cryptainers are established using end-user's credentials, and are subject to any further limitations imposed by CIFS security levels.
- Shares can be empty before they become Cryptainers, or they can contain data. A Cryptainer created from an empty share can have data copied or written to it after creation. By default, existing data within a share will not be encrypted at the time the Cryptainer is created. See Options When Adding a Cryptainer on page 106 for choices when creating a Cryptainer.
- A Cryptainer can be created at the share level or in a directory within the share (sub-share level). For sub-share level Cryptainers, the specified directory must not exist, but parent directories need to be present. For example, to create a Cryptainer at \\server\share\crypt, there must not be a directory named "crypt" in \\server\share. There is an exception to this rule when creating a Cryptainer with initial encryption on.
- It is recommended that shares which will become Cryptainers be created with a dollar sign ($) at the end of the share name. Shares ending with a dollar sign are hidden from user browsing on the file server, which discourages attempts to access shares directly on the server, and encourages users to access the share as it is presented through DataFort.
- DataFort supports the creation of home directories. Use the home set command to assign homes to users who will then see only their home directories when connecting to the server through DataFort. See Creating a NAS Cryptainer From a Home Directory on page 103.

Create NFS Exports

Keep the following in mind when creating NFS exports that will become Cryptainers:

- From the operating system you are using to administer NFS, create exports (file locations for sharing purposes) on network servers, and set permissions.
- It is recommended that the server hostname be changed and that the old hostname be used by DataFort to re-export secured data. This way clients can mount the same server and share as before, and have their data encrypted and decrypted transparently.
- Shares can be empty before they become Cryptainers, or they can contain data. A Cryptainer created from an empty share can have data copied or written to it after creation. By default, existing data within a share will not be encrypted at the time the Cryptainer is created. See Options When Adding a Cryptainer on page 106 for choices when creating a Cryptainer.
- It is recommended that Unix user volumes be hard-mounted. (BSD is automatically set to hard mount. Solaris and Linux users must specify hard as an option for mounting.)
- A Cryptainer can be created at the share level, which will require that the root user be granted access to that share in order to mount it for its owner, or a Cryptainer can be created at the subshare level (inside of a share to which its owner has access) which allows root to mount the share without requiring root access to the Cryptainer.

Creating a NAS Cryptainer

DataFort supports the creation of CIFS, NFS and multi-protocol (CIFS and NFS) Cryptainers. To transform an existing share into a Cryptainer, complete the following steps:

- Add a Domain
- Add a Server
- Add a Share
- Add a Virtual Server
- Virtualize a Share
- Add a Cryptainer

A Full Administrator can complete all tasks necessary to create a Cryptainer. If only specialized administrators are in use, a User, Storage and Key Administrator will be needed. See Creating a NAS Cryptainer Using Specialty Administrators on page 103.

Connect to the DataFort WebUI

1. Log in to the WebUI from the Management Station.
2. Select **Storage > Servers & Portals** from the WebUI menu, or click the Secure Storage link on the Home page of the WebUI.

Servers & Portals

Use the Real Elements and Virtual Elements panes of the Servers & Portals page to manage the secure network. The Real Elements side of the page displays the Domains tree: domains, servers and shares that have been added to the DataFort database, as well as Cryptainers that have been created on the servers.

The Virtual Elements side of the page displays the DataFort or DataFort cluster in the configuration, as well as virtual representations of the actual servers (virtual servers) and shares that have been virtualized so that they can be exported as Cryptainers.

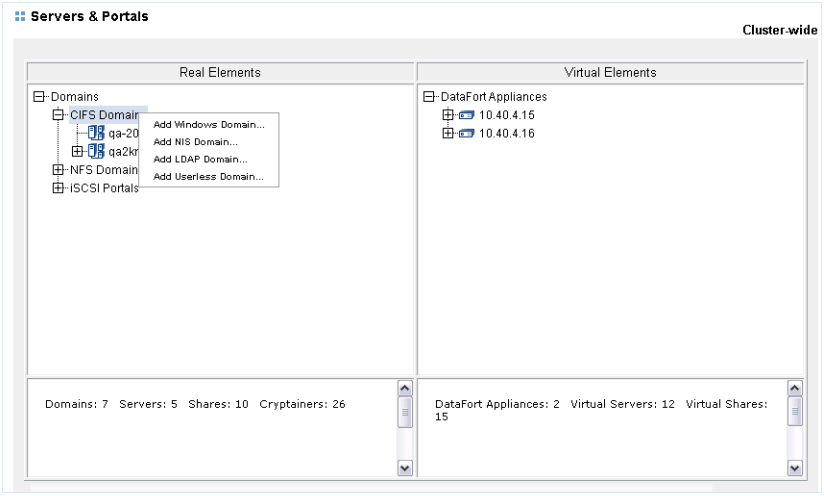
Each onscreen pane provides the following tools for managing the storage network:

Right-click menus	Right-click each device or group of devices for menu options.
Lower information pane	Detailed information about the selected device appears in the lower pane.
Multiple device select	Select multiple devices by shift-clicking or control-clicking them on screen. The maximum number of devices that can be selected at once is 255.

ADD A DOMAIN

Only a Full Administrator or User Administrator can add or remove domains.

1. At the Servers & Portals page, right-click the Domains entry for the correct type of domain (CIFS or NFS) in the Real Elements pane.
2. Select the subtype of domain you want to add. See Understanding DataFort Domains on page 92 for information.



3. Enter the required information to Add a CIFS Domain or Add an NFS Domain. For multi-protocol support, be sure to add a domain that includes a multi-protocol server. Note that:
   - Unlike CIFS domains, NFS domains enforce case-sensitivity on user and group names.
   - It is possible to use the same name for the full name and NetBIOS name of a single domain. The same name may not be used for the full name of two domains, the NetBIOS name of two domains or the NetBIOS name of one domain and the full name of another domain.

Add a CIFS Domain

1. Add a Windows, NIS, LDAP or Userless domain. See Understanding DataFort Domains on page 92 for information. Enter the required information for the domain.
2. Enter the name and password of the DataFort domain access user (see Adding the DataFort Domain Access User on page 36) into the Access Username fields.
3. Click Apply.

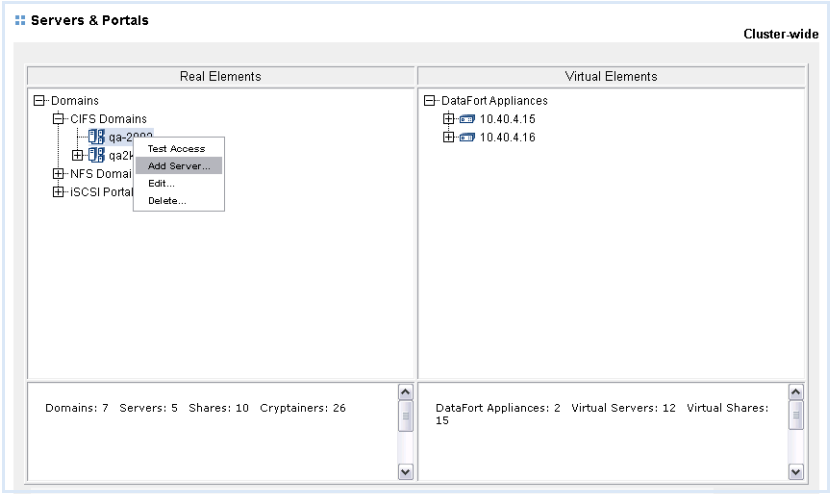
Add an NFS Domain

1. Add a NIS, LDAP, Local or Userless domain. See Understanding DataFort Domains on page 92 for information. Enter the required information.
2. For an NIS or Local domain, add the root user (User ID 0, 0) for that domain at the same time.

   DataFort requires the root user to mount exports and create Cryptainers on file servers. Other users are imported from the NIS automatically as Cryptainers are created for them. Since the root user is not part of the domain, it must be added to the DataFort manually.

Add a Server

1. Select the domain the server should be added to:
   - CIFS or NFS: Right-click a domain in the Domains tree of the DataFort WebUI.
   - Multi-protocol: Multi-select an NFS and a CIFS domain (select the first domain, then hold down the Control key and select the next domain) and then right-click. Once added, the server will appear in both the CIFS Domains and NFS Domains trees.
2. Choose Add Server from the right-click menu.

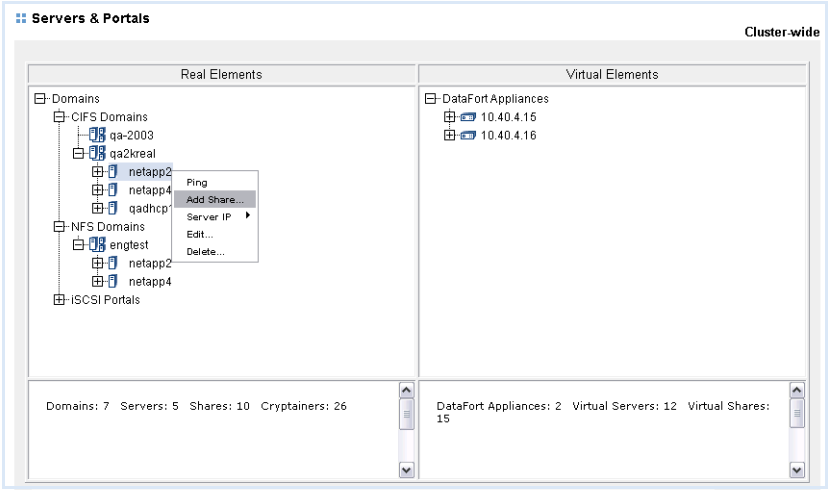


   The Add Server page for the selected type of domain (CIFS, NFS or Multi-Protocol) will appear.
3. Enter a hostname for the server. Enter an IP address as well if needed.

4. For NAS, iSCSI Access should be Off.
5. Assign an interface for the server. By default, servers are assumed to be on the file server side of the network (connected to the DataFort File Servers NIC). However DataFort also supports a network configuration that includes file servers on the client side of the network.
   - If the server is on the file server side of the network, leave the File Servers button selected.
   - If the server is on the client side of the network select the Clients button.
6. Click Apply.

ADD A SHARE

1. Add a share from the server:
   - CIFS or NFS: Right-click a server in the Domains tree.
   - Multi-protocol: Multi-select both instances of the server, then right-click.
2. Select Add Share.



3. Enter names or make selections to add one or more shares.
   - CIFS or NFS: Add a share by entering its name, or add several shares by selecting them in the onscreen list of Discovered Shares. Select multiple devices by shift-clicking or control-clicking them on screen.
   - Multi-protocol: Add a share by entering its CIFS and NFS name, or select the share in the Discovered CIFS Shares and Discovered NFS Shares panes.

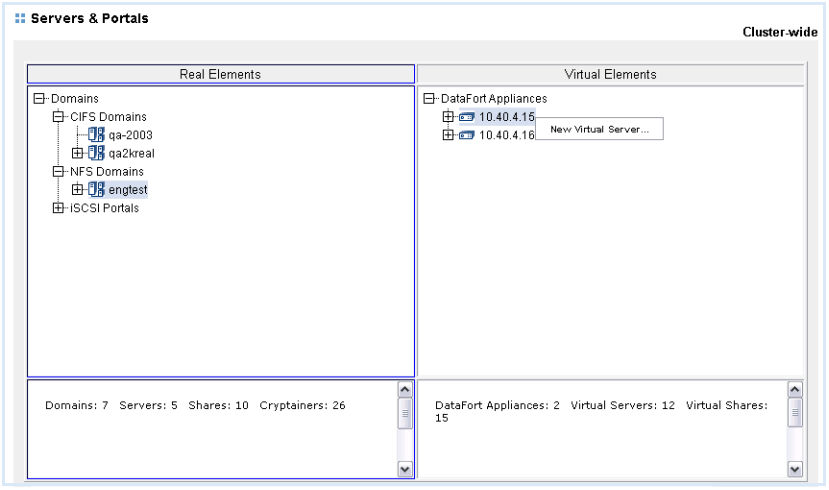


4. Click Add.

   The share will appear in the Real Elements pane.

ADD A VIRTUAL SERVER

1. Right-click a DataFort in the Virtual Elements pane.
2. Select New Virtual Server.



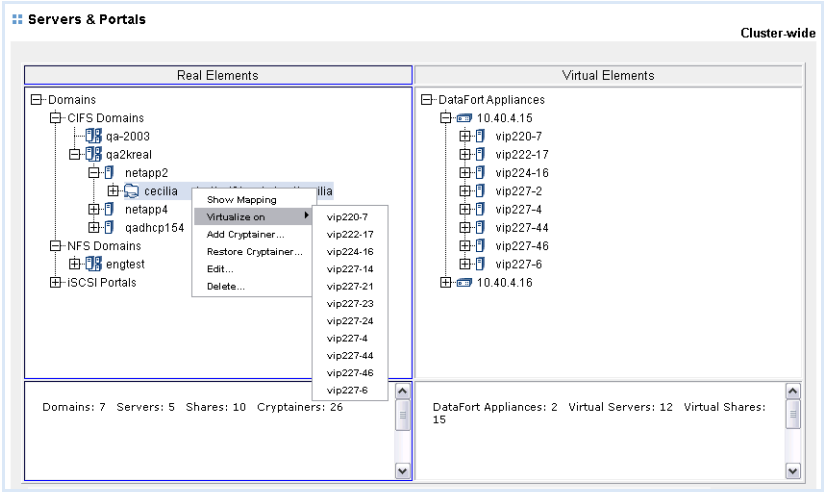
3. Enter a hostname for the server. Enter an IP address as well if needed.
4. From the CIFS and/or NFS Domain pull-down menus, select the domain to associate with the virtual server.

5. Turn Floating ON to support failover. See Adding Virtual Servers on page 108 for more about this setting.
6. Click Apply.

VIRTUALIZE A SHARE

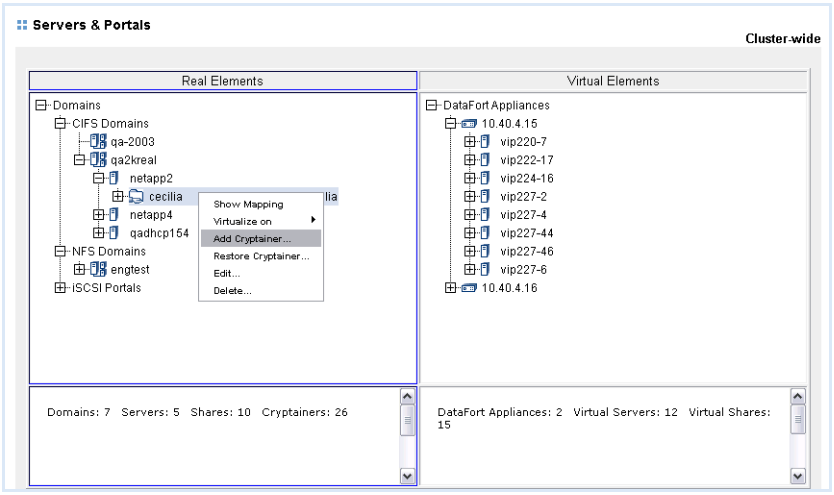
Icons for shares that have not been virtualized are shaded darker than virtualized shares.

1. Virtualize the share:
   - CIFS or NFS: Right-click the share from the Real Elements pane.
   - Multi-protocol: Right-click either the CIFS or the NFS representation of the share to create a virtual share for both CIFS and NFS.
2. From the right-click menu, select Virtualize on, and select the virtual server on which to virtualize the share.



ADD A CRYPTAINER

1. In the Real Elements pane, select the share or shares to add. Shift-click or control-click to select multiple shares.
   - For a CIFS or NFS share, right-click the share, and select Add Cryptainer.
   - For a multi-protocol share, right-click one instance of the share, and select Add Cryptainer.



2. Choose the Cryptainer options. See Options When Adding a Cryptainer on page 106 for more information.
3. In the Path field:
   - If only one share was selected, you may edit the path field.
   - If multiple shares are selected, you may create only share-level Cryptainers.
4. In the Cryptainer Owner field:
   - You may specify an owner for the Cryptainer(s) being created. This owner may be an administrator, an NFS or CIFS group, or an NFS or CIFS user.
   - If you leave the field blank, the administrator logged in to the WebUI (or CLI) when the Cryptainer is created becomes the owner.
   - For NFS and multi-protocol Cryptainers, if an administrator is the owner, DataFort will use the root UID when creating the Cryptainer.
   - For CIFS and multi-protocol Cryptainers, if an administrator is the owner, DataFort will use the CIFS domain access user to sync ACLs and will set the domain access user as the owner in the Windows Security Descriptor.
5. Click Apply.

   The Cryptainer will appear under its share in the Real Elements pane. See Managing Cryptainers on page 107 for more about Cryptainer menu options.

Cryptainer Ownership

Note the following permissions and restrictions on Cryptainer ownership:

- CIFS Cryptainers cannot be owned by NFS users.
- NFS Cryptainers cannot be owned by CIFS users.

- There is only one owner of a Cryptainer, but the Cryptainer owner may be a group.
- DataFort keeps track of the Cryptainer owner, who has the right to change the Cryptainer's ACL.
- For CIFS Cryptainers, the owner field is synced with the corresponding owner in the Windows Security Descriptor. Syncing occurs on Cryptainer creation, ACL sync, and ACL capture. See User Administration for more about Cryptainer ACLs.

Creating a NAS Cryptainer From a Home Directory

If you want to create CIFS home directories for users in a domain, follow these steps:

1. Create shares to be used as home directories for these users on a server in the domain. These should be shared home directories on the server (each directory is a separate share).
2. Following the steps outlined in Creating a NAS Cryptainer on page 96, use the WebUI to create share-level Cryptainers in each shared home directory, all virtualized on the same VIP.
3. Log into the CLI and using the `user home set` command, set each user's home directory as the appropriate share.

```
user home set <user or domain> <path>
```

Creating a NAS Cryptainer Using Specialty Administrators

In order to create a Cryptainer using only speciality administrators but no Full Administrators, the specialty administrators will need to log into DataFort to complete specific tasks. The Storage Administrator specializes in adding and deleting servers, shares and VIPs, the User Administrator has the power to add domains, and the Key Administrator can actually create the Cryptainer.

Table 9 outlines which administrators will need to log into DataFort to complete each part of the process that will complete Cryptainer creation.

Table 9: Administrator Roles and NAs Cryptainer Creation

Administrator Type	Task
User or Full Administrator	Add a Domain
Storage or Full Administrator	Add a Server
Storage or Full Administrator	Add a Share
Storage or Full Administrator	Add a Virtual Server
Storage or Full Administrator	Virtualize a Share.
Key or Full Administrator	Add a Cryptainer

Managing Secure NAS Storage

Use the Servers & Portals page to manage the secure NAS. NAS storage administration tasks include:

- Managing Domains
- Managing Servers
- Managing Shares
- Managing Cryptainers
- Managing Virtual Servers
- Editing a Virtual Server

Managing Domains

Right-click a domain in the Real Elements pane to see domain management options.

Table 10: Domain Menu Options

Menu Selection	Purpose
Edit Users (NFS only)	DataFort imports user, group and membership information from domains automatically every 30 minutes. Use the Edit menu to add a user such as the root user to the NFS domain (see Add an NFS Domain). If this is an NIS or LDAP domain, users that are added or removed will be cleared/restored during the next synchronization, except for users that have a UID less than or equal to a pre-set number. (The maximum UID is set in the property `user.domain.max.system.uid`; UIDs are checked against this value before they are purged.) Typically a user with UID 0 needs to be added to every NFS domain because NFS mounting is usually done by the user "root" on the client, which has UID 0.
Test Access (CIFS only)	Test DataFort access to this domain.
Add Server	Add a Server found in this domain. The Add Server page for the type of domain you have selected will appear. See Add a Server for instructions.
Edit	CIFS: Change domain settings including domain controller, NetBIOS and domain access username and password.
	NFS: Change domain settings including NIS Server, root username and password.
Delete	Remove the domain. You must first remove any servers that are in the domain. See Deleting a Domain.

Deleting a Domain

In order to delete a domain, the servers in that domain must be deleted as well. A domain can be deleted so that all Cryptainers in that domain are also deleted, or so that Cryptainers are preserved.

Delete a Domain and Cryptainers

1. Delete all Cryptainers existing in servers in that domain. See Managing Cryptainers on page 107.
2. Delete all shares existing in servers in that domain. See Managing Shares on page 106.
3. Delete all servers in that domain. See Managing Servers on page 105.
4. Edit associated VIPs and change association in the pull down menu from the associated domain to datafort_admin. See Editing a Virtual Server on page 111.
5. Right-click the domain and select Delete.

Delete a Domain while Preserving Cryptainers

1. Revoke any “change permissions” access that users from this domain have to existing Cryptainers. If for a certain Cryptainer only users from this domain have “change permissions” access, you need to grant “change permissions” access to a user from a different domain first.
2. Make sure there are no servers or virtual servers that use this domain (either as a CIFS or NFS domain). If there are, you have to set their domain to a different one. See Managing Servers on page 105 and Managing Virtual Servers on page 109.
3. Delete the domain.

Managing Servers

Right-click a server in the Real Elements pane to see server management options.

Table 11: Server Menu Options

Menu Selection	Purpose
Ping	Test DataFort access to this server.
Add Share	Add a share for Cryptainer creation. See Add a Share for instructions.
Server IP	Add: Add a server IP address to the DataFort configuration. DataFort can use multiple server IP addresses when communicating with a server, in order to get better performance from the server. For example, if a server has two NICs, each with a different IP address, the administrator can allocate some shares for access over one IP address, and some for access over the other. See Add a Server for more about the information needed when adding a server.
	Resolve: If the IP address of the server has changed, use the Resolve menu option to update the information for that server in the DataFort configuration.
Edit	Change server attributes including IP address, domain, iSCSI access and DataFort interface. See Editing a Server.
Delete	Delete server. The shares on that server must be deleted first. See Managing Shares.

Editing a Server

The Edit Server page is designed to be used when an attribute of a server changes. The Edit Server web page should not be used when switching to a different server (a different physical computer) with a different set of shares. If the physical server requires changing, delete the server and add it again.

Options when editing a server include:

Hostname Enter or change the hostname of a server.

CIFS and NFS Domains Select the CIFS or NFS domain for the server from the drop-down menus. If the server is a multi-protocol server, select the NFS domain and the CIFS domain from the drop-down menus.

iSCSI Access OFF for a NAS only server.

IP address Indicate the IP address of the server. To update the server IP address after changing it at the server itself, change the IP address information here.

On Interface File servers can reside on the File Servers or Clients side of the DataFort. Click the radio button to indicate which side the server is on. File Servers is the default setting. Change the default only if the Clients NIC is on a separate subnet and the real server resides on that separate subnet.

Managing Shares

Right-click a share in the Real Elements pane to see share management options.

Table 12: Share Menu Options

Menu Selection	Purpose
Show Mapping	Shows the location of any Cryptainers created from this share.
Virtualize on	Gives the option to virtualize the share on available virtual servers in preparation for creating a Cryptainer. See Virtualize a Share for details.
Add a Cryptainer	Gives the option to add a Cryptainer on the selected share. See Add a Cryptainer and Options When Adding a Cryptainer for details.
Restore Cryptainer	Restore a deleted Cryptainer. See Managing Virtual Shares for instructions.
Edit	Edit share: change CIFS name, NFS name, or both names.
Delete	Delete a share from the database. The original share remains on the server.

Options When Adding a Cryptainer

Options when adding a Cryptainer include:

Filename Encryption By default, filenames within Cryptainers are not encrypted, in order to support backups and data restoration: only file contents are encrypted, leaving filenames in plaintext. In an extremely secure environment, it may be desirable to also encrypt filenames by turning Filename Encryption on.

Data Encryption By default, data within Cryptainers is encrypted. To leave the contents of a Cryptainer in cleartext (unencrypted) form, turn Data Encryption off. This will allow DataFort to manage the access control for the shares without requiring that the data in the share be encrypted. Turn off Data Encryption if you want to use DataFort only to strengthen the ACL on a share, not to encrypt its contents. Or turn Data Encryption off if you do not want to encrypt data that existed before DataFort was installed in the environment. When Data Encryption is off, the Cryptainer icon will appear in the WebUI without the lock image. To encrypt the data later, use the Rekey Cryptainer feature described in Managing Cryptainers.

Require IPsec To require clients to use IPsec to connect to this Cryptainer, turn Require IPsec on. Note that IPsec must be enabled on the virtual server hosting this Cryptainer. See Configuring IPsec on a Virtual Server.

Initial Encryption By default, Initial Encryption is off. To encrypt cleartext data that is added to the Cryptainer automatically, turn Initial Encryption on. This allows you to add data to a share directly on the server and then create a Cryptainer which will encrypt the contents of the share.

Managing Cryptainers

Right-click a Cryptainer in the Real Elements pane to see Cryptainer management options. If there are more than 300 Cryptainers under a share, the Cryptainer list is truncated. Extra nodes are replaced by the overflow placeholder "All..." Double-click All to see the remaining shares, batch by batch. On the overflow pages, menu actions are replaced by action buttons (Edit CIFS, Edit NFS, Delete).

Table 13: Cryptainer Menu Options

Menu Selection	Purpose
Access Control	ACL: To grant access to a Cryptainer to a user or group, select the user or group, check the appropriate boxes (read/write/change permissions), and click Apply. You can set the owner of the Cryptainer by selecting the user and clicking Set Owner. You can sync the Cryptainer ACL with the ACL on the server. See ACL Sync and ACL Preview.
	IP Restriction: Use to restrict access to the Cryptainer from specified IP addresses. See Setting Cryptainer IP Address Restriction.
IPsec	Choose Required to require IPsec when a client connects to the Cryptainer. Note that IPsec must first be set up on the virtual server hosting the Cryptainer. See Setting Cryptainer IPsec Restriction.
Rekey	A Cryptainer can be rekeyed at any time using the Rekey feature. Rekeying changes the Cryptainer key used to encrypt the contents of the Cryptainer. Use the menu options to Start or Cancel a rekey job. To view current rekey jobs, select Current Jobs. Do not make any changes to the configuration while the Cryptainer is being rekeyed. Note that rekeying must be resumed manually if stopped. See Rekeying Cryptainers.
Export Key	Export the key for this Cryptainer to a trustee. See Importing and Exporting Keys for details.
Delete	Delete removes the Cryptainer from the configuration database. No users will be able to access the Cryptainer unless it is restored. Restoration is possible if the source data remains on the file server. See Managing Virtual Shares.

Note: See Options When Adding a Cryptainer on page 106 for Cryptainer creation options.

ACL Sync and ACL Preview

You can view user and group permissions on a Cryptainer. For CIFS Cryptainers, you can also review the current server ACL and sync the DataFort ACL with the server ACL. If Use Local ACL is on, you must confirm newly added users or groups using ACL Sync before new users can access Cryptainers.

1. Right-click a Cryptainer and choose **Access Control > ACL**.

   The ACL window lists users and groups with access to the selected Cryptainer. This is the Cryptainer ACL saved in the DataFort configuration database.

2. Click Sync (CIFS Cryptainers only).

DataFort accesses the server, reads the ACL and displays it in the Preview Sync window.

3. Click Confirm to update the DataFort ACL with the ACL of the server.
4. Click Refresh to re-read the ACL from the server. Click Cancel if you do not want to sync the DataFort ACL (that is, you do not want to accept changes).

Note: A Cryptainer owner can modify the ACL of the Cryptainer. See Cryptainer ACL on page 134.

Setting Cryptainer IP Address Restriction

Cryptainer access can be restricted to clients within a specified IP address range. Use the Servers & Portals page to view and set Cryptainer IP access control.

1. Right-click the Cryptainer that will only allow access from specified IP addresses.
2. Select **Access Control > IP Restriction**.
3. Click Add.
4. Enter the range of IP addresses that should be allowed access to the selected Cryptainer. For one client, enter the same IP address for the start and end of the range (as in: 10.10.20.100-10.10.20.100).
5. By default the access is Read and Write. Check the desired access setting (Read, Write, or both Read and Write).
6. Click Apply.

Setting Cryptainer IPsec Restriction

A particular Cryptainer can be configured to allow access only from clients connecting through IPsec.

1. First configure IPsec on the virtual server. See Configuring IPsec on a Virtual Server on page 109.
2. From the Servers & Portals page, right-click a Cryptainer and select **IPsec > Required**.

Rekeying Cryptainers

DataFort can encrypt or rekey existing files in the background, without taking data offline. If a Cryptainer is already encrypted, a rekey will apply a new encryption key to the data. If a Cryptainer was unencrypted at the time of the rekey, the rekey will encrypt the Cryptainer data for the first time.

1. Right-click the Cryptainer that will be rekeyed.
2. Select **Rekey > Start**.

   The status of a rekey job is show on the DataFort WebUI Home page. To view details, right-click the Cryptainer and choose **Rekey > Current Jobs**. While a rekey is in progress, a small rekey icon appears above the lock icon on the Cryptainer. In case of a rekey error, for example a file access error, encryption or rekeying stops and the rekey icon changes to an error icon.

Adding Virtual Servers

Right-click a DataFort in the Virtual Elements pane to add a new virtual server. Do not use the same virtual server for NAS and iSCSI storage. Options when adding a server include:

Virtual Hostname	Enter the hostname of a server.
IP address	Indicate the IP address of the server.

CIFS/ NFS Domain — Select the CIFS or NFS domain for the server from the drop-down menus. If the server is a multi-protocol server, select the NFS domain and the CIFS domain from the drop-down menus.

Floating — Set ON for NAS. The VIP is assigned to a VRID, so it will move with that VRID to whichever cluster member becomes the master of that VRID during NAS failover.

Set OFF for iSCSI. The VIP is assigned to a cluster member and it will always stay with that member. iSCSI VIPs should be of this type, because iSCSI redundancy is implemented via client-driven failover.

Managing Virtual Servers

Right-click a server in the Virtual Elements pane to see virtual server management options.

Table 14: Virtual Server Menu Options

Menu Selection	Purpose
Secure Access	Configure a secure IPsec connection to the server. See Configuring IPsec on a Virtual Server.
Certificates	Set CA Certificate: Set a root Certificate Authority (CA) certificate for the virtual server See Setting Virtual Server Certificates.
	Set Virtual Server Certificate: Set a certificate to authenticate the virtual server to a client. See Setting Virtual Server Certificates.
Move to	Move the virtual server to another DataFort IP address. This can be used when load balancing the network. See Load Balancing in a Cluster.
Edit	Edit Virtual Servers: change Virtual Hostname, IP address, Netmask, Domain, Floating, Primary DataFort, SMB Signatures settings and Joined CIFS Domain setting. See Editing a Virtual Server.
Delete	Delete virtual servers that are not hosting shares which have become Cryptainers.

Configuring IPsec on a Virtual Server

This option sets up the virtual server to support the IPsec requirement when clients connect to Cryptainers. Configuring IPsec consists of creating IPsec rules for each connection, with each rule specifying the authentication method and the IP addresses of the parties. IPsec must be configured on the client side as well as at DataFort.

A Full or Key Administrator can set IPsec restrictions on a virtual server. See Configuring IPsec on page 170.

Setting Virtual Server Certificates

The Certificate Authority (CA) certificate is used to authenticate clients on a specific virtual IP address (See Setting CA Certificate).

The Virtual Server certificate (self- or CA-signed) is used to authenticate the virtual IP address to clients (See Setting Virtual Server Certificate).

Setting CA Certificate

The web access feature allows the administrator to install a root Certificate Authority (CA) certificate for each virtual IP address (virtual IP). When this type of certificate is installed on a virtual IP, each client using the web access or WebDAV feature from that virtual IP will be required to present a certificate signed by the corresponding Certificate Authority. The DataFort administrator can obtain the root certificate from the Certificate Authority administrator.

1. Right-click the virtual server in the Virtual Elements pane.
2. Select **Certificates > Set CA Certificate**.
3. Paste a CA certificate provided by the Certificate Authority administrator into the provided panel.
4. Click Set as Certificate.

Setting Virtual Server Certificate

1. Right-click the virtual server in the Virtual Elements pane.
2. Select **Certificates > Set Virtual Server Certificate**.
3. Choose Use Self-Signed or Use CA-Signed.
4. Follow instructions to add the certificate.
   - If adding Self-signed, enter the required information and click Sign and Set Certificate.
   - If adding CA-signed, enter the required information into the fields provided and click Generate Request. When you receive the signed request, paste it into the box provided.
   - If adding CA-signed with a private key, enter the required information into the fields provided and click the import a private key link. Paste the key into the box provided and click Import.

Editing Virtual Servers to Support SMB Signatures

CIFS message signing (SMB signatures) provides security against session hijacking and man-in-the-middle attacks. CIFS message signing provides a signed MD5 hash of the message to prevent data modification or injection of new messages. The key is private and changes with each session.

- In order to enable CIFS message signing on the DataFort, User Registration must be on (see Domain Controller Security Settings on page 168 or Auto Import must be enabled for the user's domain (see Domain Menu Options on page 104).
- Before setting DataFort to support CIFS signatures, configure the clients and servers to use CIFS signatures. Message signing is disabled by default in most installations of Windows. See Windows documentation for commands to enable CIFS message signing.

1. Right-click the virtual server in the Virtual Elements pane and select Edit.
2. Select the SMB signature setting and click Apply.
   - If Client-side SMB Signatures are Disabled, message signing will not be enabled for communication with clients.
   - If Client-side SMB Signatures are Required, only clients that support signing will be allowed to connect.
   - If Server-side SMB Signatures are Disabled, message signing will not be enabled for communication with servers.
   - If Server-side SMB Signatures are Required, only servers that support signing will be allowed to connect.

Editing a Virtual Server

Right-click a virtual server in the Virtual Elements pane to edit the virtual server. Options include:

Virtual Hostname	Enter the hostname of a server.
IP address/Netmask	Indicate the IP address and netmask of the server.
CIFS/ NFS Domain	Select the CIFS or NFS domain for the server from the drop-down menus. If the server is a multi-protocol server, select the NFS domain and the CIFS domain from the drop-down menus.
Floating	Set ON for NAS. The VIP is assigned to a VRID, so it will move with that VRID to whichever cluster member becomes the master of that VRID during NAS failover. Set OFF for iSCSI. The VIP is assigned to a cluster member and it will always stay with that member. iSCSI VIPs should be of this type, because iSCSI redundancy is implemented via client-driven failover.
Primary DataFort	Indicate which DataFort is the primary for this server. This DataFort will serve the VIP unless there is a failover to the other cluster member.
Client-side/Server-side SMB Signatures	CIFS message signing (SMB signatures) provides security against session hijacking and man-in-the-middle attacks. This can be provided on the client or server side NIC of DataFort. See Editing Virtual Servers to Support SMB Signatures on page 110.
Joined CIFS Domain	For a Windows client using Kerberos to communicate with the VIP, it must join a CIFS domain. Select Yes in the Joined CIFS Domain option. Enter the domain user and domain password in the fields that appear.

Managing Virtual Shares

Right-click a share in the Virtual Elements pane to see virtual share management options.

Table 15: Virtual Share Menu Options

Menu Selection	Purpose
Show Mapping	Shows the location of any Cryptainers created from the selected share.
Access via	Access via is used to set the access IP address for the share on the server. For example, on a multi-homed server with two IP addresses, you can specify which address DataFort should use to access a virtual share. You can also define two virtual shares that map to the same real share, but use the two different server IP addresses for accessing that real share. Select the server IP address that will be used for access, and then select the virtual share that will use the specified IP address for access. Right-click on the selected share, and choose Access via.
Move to	Move the virtual share to a different virtual server.
Edit	Change the virtualized share name, virtual hostname or hostname of server for virtual shares.
Delete	Delete virtual shares.

Restoring a Cryptainer

A Cryptainer that has been deleted from the configuration database can be restored. The restore procedure can be executed by a Full Administrator from any member of a DataFort cluster. The cluster must be the same one for which the Cryptainer was originally created. Note that if you are using LKM software to manage Cryptainer keys and the LKM server is on line, DataFort queries LKM for missing keys automatically.

The original encrypted data and .decru file must still be available to restore the Cryptainer. If necessary, copy the encrypted data including the .decru file to a share on a file server in a domain that has been added to the DataFort configuration database.

1. Verify that the DataFort domain access user has read access to the .decru file in the share to be restored.
2. If the file server where the share resides has not been added to the DataFort configuration database, access the Servers & Portals page of the WebUI, right-click the domain where the file server with the data resides and choose Add Server.
3. Right-click the server and choose Add Share to add the share to be restored.
4. Right-click the share and Virtualize the share on a virtual server.
5. Right-click the share and select Restore Cryptainer to restore it.
   - If only one share is selected, you can enter the path and owner.
   - If multiple shares are selected, there is no option to edit paths.
   - For CIFS Cryptainers, entering the owner is optional. If the owner is not specified, the administrator performing the restore becomes the owner.

A Cryptainer restore does not restore the Cryptainer ACL. After a Cryptainer is restored, the ACL is set on DataFort so that the administrator who performed the restore is given delete permission, the specified owner (or the administrator if no owner is specified) is given read, write, change and delete permissions, and the Storage Administrator is given delete permission.

6. Restore the CIFS Cryptainer ACL as follows:
   - If the ACL on the server has not changed from that on the original Cryptainer, sync the restored Cryptainer with the server ACL: On the Servers & Portals page, right-click the Cryptainer name and choose **Access Control > ACL**. (For multi-protocol Cryptainers, access the Cryptainer via its CIFS domain.) Click Sync. The Preview Sync page enables you to preview the new ACL read from the server, before saving it into the DataFort configuration database. Review the users and permissions, and click Confirm.
   - If the ACL on the server has changed, update it on the server and then sync the server and the DataFort as described above. The Preview Sync window will show the updated users and permissions on the server (if it does not, click Refresh) and you can confirm them.
7. There is no ACL Sync for NFS Cryptainers. Set up the ACL manually from the WebUI:
   - Choose **Access Control > ACL**.
   - Initiate a search among users and groups in one or more domains, or select Show All Users/Groups. Click Refresh.
   - Select the user or group to add to the ACL, check the appropriate permissions and click Apply.

10 iSCSI Storage Administration

This chapter includes instructions for using the DataFort WebUI to manage iSCSI Cryptainers. A Full Administrator is assumed to have completed installation and preparation of DataFort appliances as described in previous chapters of this guide.

A Full Administrator can perform all of the functions outlined in this chapter. A specified Storage Administrator can perform most of them. NAS and iSCSI storage management functions share many menus and features.

If specialized administrators are in use, keep in mind that while a Full or Storage Administrator can complete most tasks leading up to the creation of a Cryptainer, only a Full or Key Administrator can actually assign data an encryption key, thereby creating a Cryptainer.

iSCSI storage administration involves the following:

- Preparing to Create an iSCSI Cryptainer
- Creating an iSCSI Cryptainer
- Managing Secure iSCSI Storage
- Restoring an iSCSI Cryptainer

Preparing to Create an iSCSI Cryptainer

When preparing to create iSCSI Cryptainers, follow these guidelines. Some preparations require logging into the DataFort CLI (see Connecting to the DataFort Command Line Interface on page 71).

Setting up Groups

Set up the LUN and Initiator Group on the target before importing portals and groups into DataFort. For example, create an Initiator Group and LUN using NetApp® management tools and map the drive from the initiator that will access the target the way you normally would for iSCSI storage.

DataFort does not support the encryption of existing data in iSCSI Cryptainers. All data existing on the disk prior to the creation of the Cryptainer will be rendered unreadable. DataFort only supports encryption of empty Cryptainers for iSCSI. If there is data on the storage device, it will be overwritten when the Cryptainer is created. Format the LUN before creating a Cryptainer.

Using iSNS

If iSNS is in use, assign the iSNS server name to DataFort and turn iSNS off at the server. DataFort will serve as the iSNS server. To enable iSNS through DataFort complete the following:

- Make sure iSNS on the target server is disabled.
- From the DataFort CLI, add the iSNS server:

```
isns server set <IP Address>
isns restart
```

- On the DataFort appliance, set up the iSCSI server, VIP, and initiator as described in Creating an iSCSI Cryptainer on page 115.

Preparing to Create Cryptainers Using SnapDrive

SnapDrive support requires that a specific command be executed at the DataFort CLI which sets all Cryptainers for newly discovered LUNs as encrypted. In addition, a CIFS share must be set up before creating a Cryptainer. This share will be assigned the same VIP as the iSCSI portal as described in Virtualizing the Portal on page 117.

Setting iSCSI SnapDrive Support

When using SnapDrive, the following command must be executed at the DataFort CLI before creating Cryptainers:

```
system property set dfc.iscsi_features 431
```

Note: To switch back to a completely non-SnapDrive environment execute:

```
system property set dfc.iscsi_features 175
```

Creating a CIFS Share

A CIFS share should have been set up for use with SnapDrive in advance. This share is added as part of the Cryptainer creation process.

CREATING AN ISCSI CRYPTAINER

Use the Real Elements and Virtual Elements panes of the Servers & Portals and Initiators & Targets pages of the DataFort WebUI to manage the network.

The Real Elements side of the Servers & Portals page displays the Domains tree which shows the iSCSI Portals added to the DataFort database. The Virtual Elements side of the Servers & Portals page displays the DataFort or DataFort cluster in the configuration, as well as virtual servers. The Initiators & Targets page offers the initiators, Cryptainer and Target management panes.

Each onscreen pane provides the following tools for managing the storage network:

Right-click menus	Right-click each device or group of devices for menu options.
Lower information pane	Detailed information about the selected device appears in the lower pane.
Multiple device select	Select multiple devices by shift-clicking or control-clicking them on screen. The maximum number of devices that can be selected at once is 255.

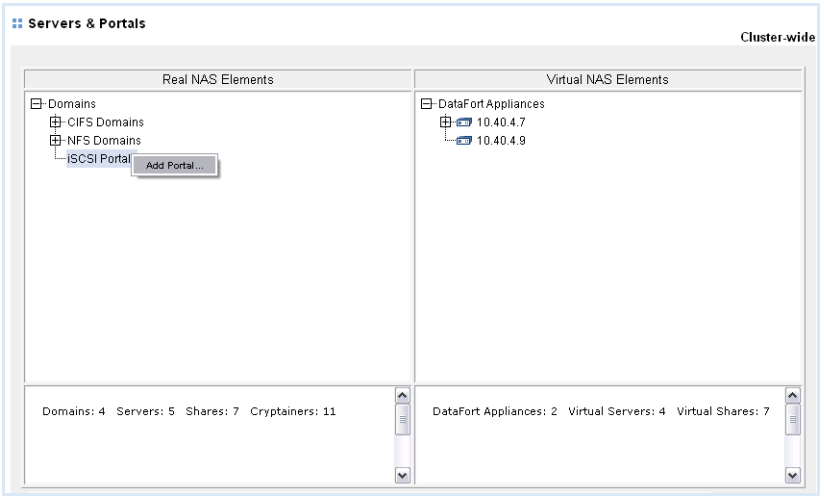
iSCSI Cryptainer creation steps include:

- Adding an iSCSI Portal
- Virtualizing the Portal
- Adding an Initiator
- Encrypting a Cryptainer
- Configuring an Initiator
- Configuring DataFort to Support MPIO

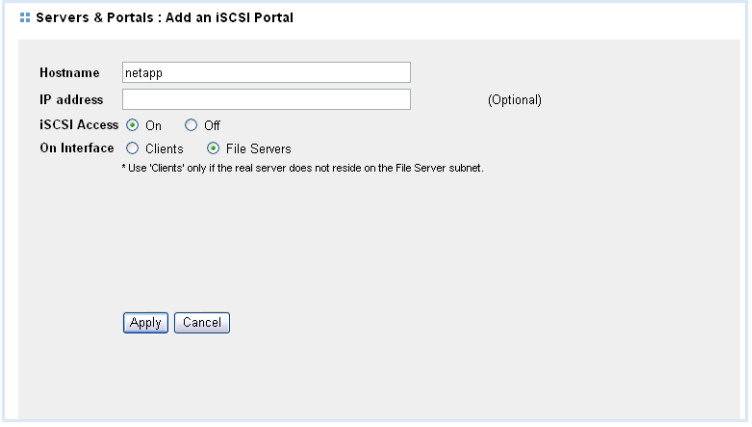
ADDING AN ISCSI PORTAL

1. Log in to the WebUI from the Management Station.
2. Select **Storage > Servers & Portals** from the WebUI menu, or click the Secure Storage link on the Home page of the WebUI.
3. Right-click the iSCSI Portals entry in the Real Elements pane and select Add Portal...

   An iSCSI portal is an IP address with which an iSCSI target is accessed via the TCP/IP network. More than one target can be accessed via a single portal (IP address). Similarly, a single target can be accessed via more than one portal.



4. Enter the hostname for the target. Be sure that iSCSI Access is turned on.



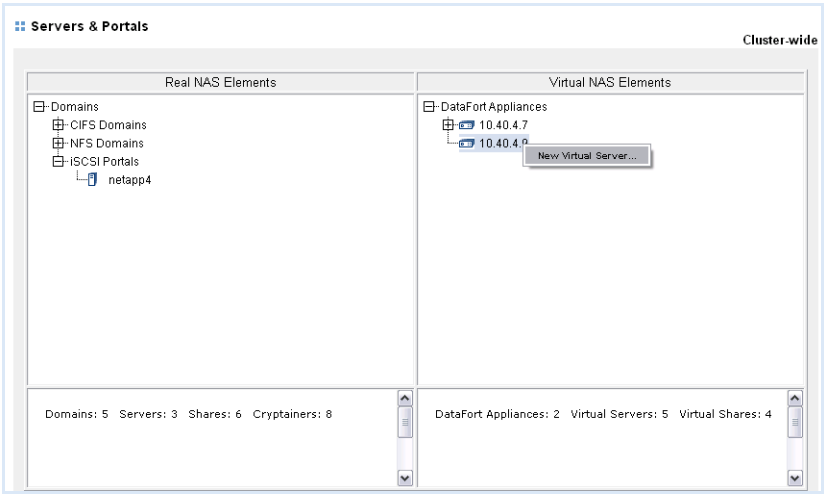
5. Click Apply.

   The target will appear in the Real Elements pane.

6. To support clustering in the iSCSI environment using Microsoft Multipath I/O (MPIO), add the second interface of the target. See Configuring DataFort to Support MPIO on page 122.

VIRTUALIZING THE PORTAL

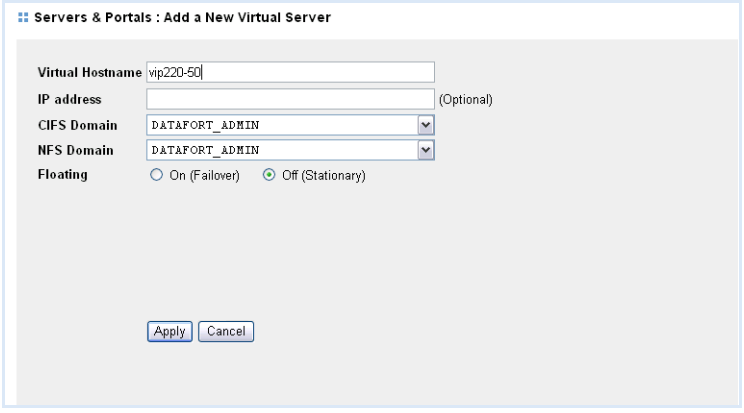
1. Right-click a DataFort appliance in the Virtual Elements pane and select New Virtual Server.



   The Add a New Virtual Server page appears.

2. Enter a name for the virtual server.
3. Select the button to turn Floating OFF. (See Adding Virtual Servers on page 108 for details). Do not serve iSCSI and NAS storage on the same virtual IP.

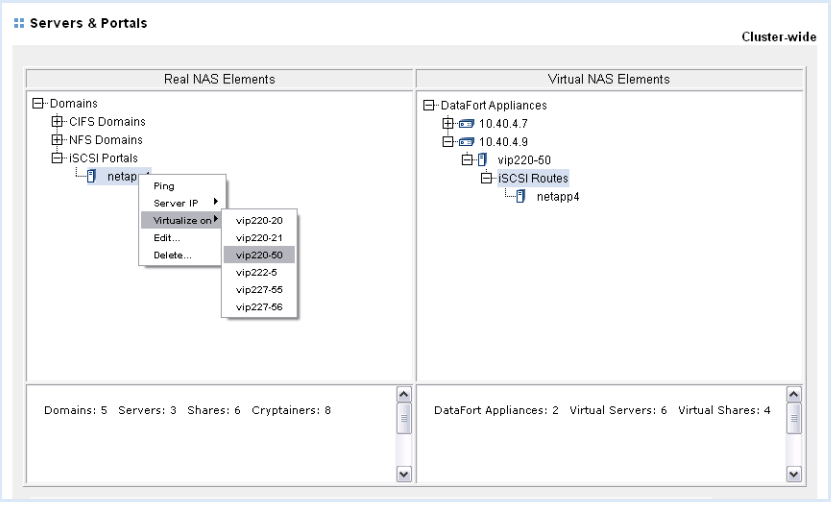
   Note: CIFS and NFS information is not needed.



4. Click Apply.

   The virtual server will appear in the Virtual Elements pane.

5. To support clustering in the iSCSI environment using Microsoft Multipath I/O (MPIO), add a second VIP for the second interface of the target. See Configuring DataFort to Support MPIO on page 122.
6. Right-click the iSCSI Portal and select the Virtual Server it will be virtualized on.



7. To support clustering, right-click the iSCSI Portal for the second target interface and select the Virtual Server it will be virtualized on.

Adding a CIFS share for SnapDrive Support

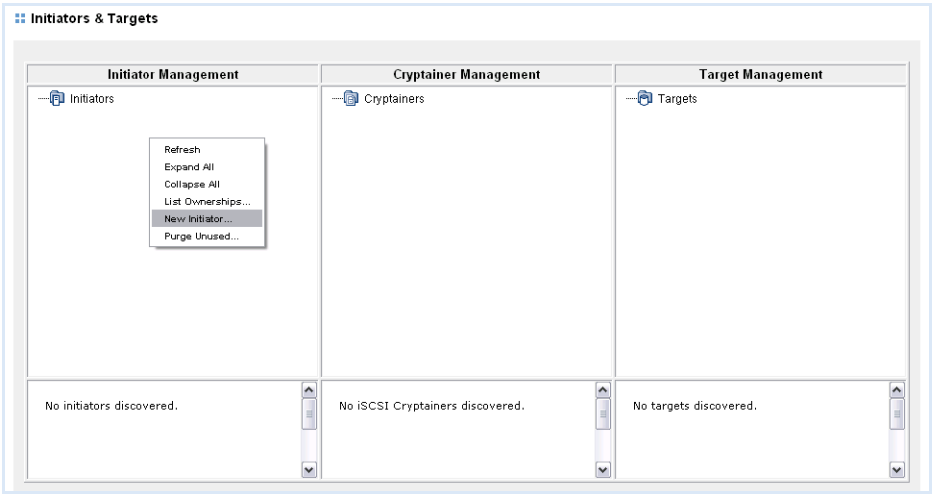
For SnapDrive support ONLY, complete the following steps before Adding an Initiator. For installations without SnapDrive, skip to the following section on Adding an Initiator.

1. Right-click the iSCSI Portal and select Add Share.
2. Add a share by entering its name, or add several shares by selecting them in the onscreen list of Discovered Shares. Select multiple devices by shift-clicking or control-clicking them on screen.
3. Click Add.

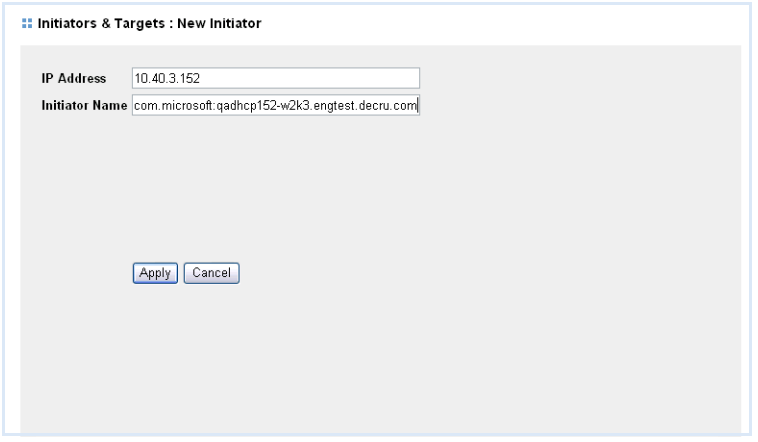
   The share will appear in the Real Elements pane.
4. Right-click the share from the Real Elements pane and select Virtualize on, and select the same virtual IP that the iSCSI Portal was virtualized on in Virtualizing the Portal on page 117.

Adding an Initiator

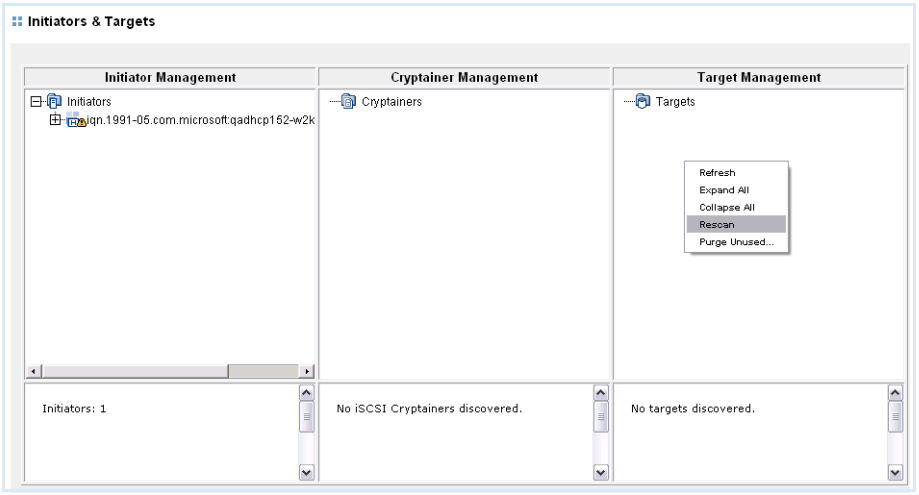
1. From the DataFort WebUI, access the DataFort **Storage > Initiators and Targets** page.
2. Right-click in the Initiator Management Pane and select New Initiator...



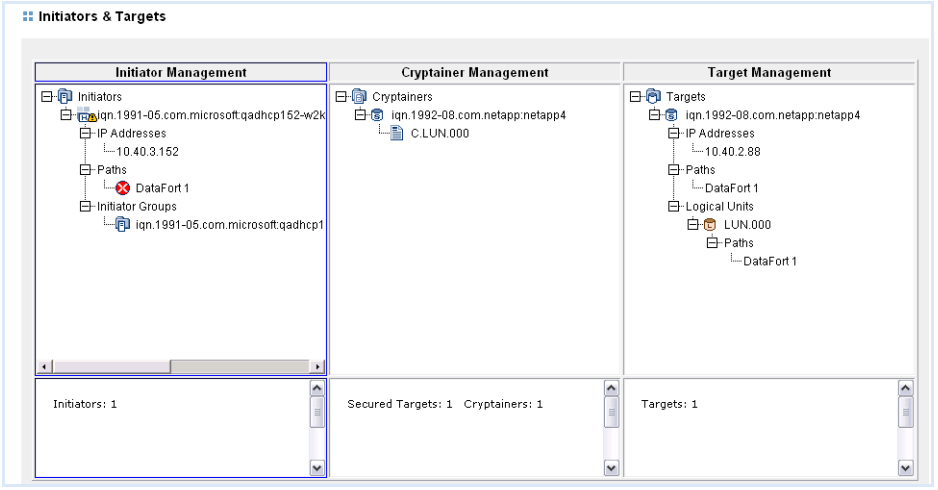
The New Initiator page will appear.



3. Enter the IP address and name for the initiator.
4. Copy the initiator node name from the iSCSI Initiator Properties panel and enter it into the Initiator name field.
5. Click Apply.
6. Right-click in the Target Management Pane and select Rescan.



After a few seconds the LUN will appear, and a Cryptainer will be created.



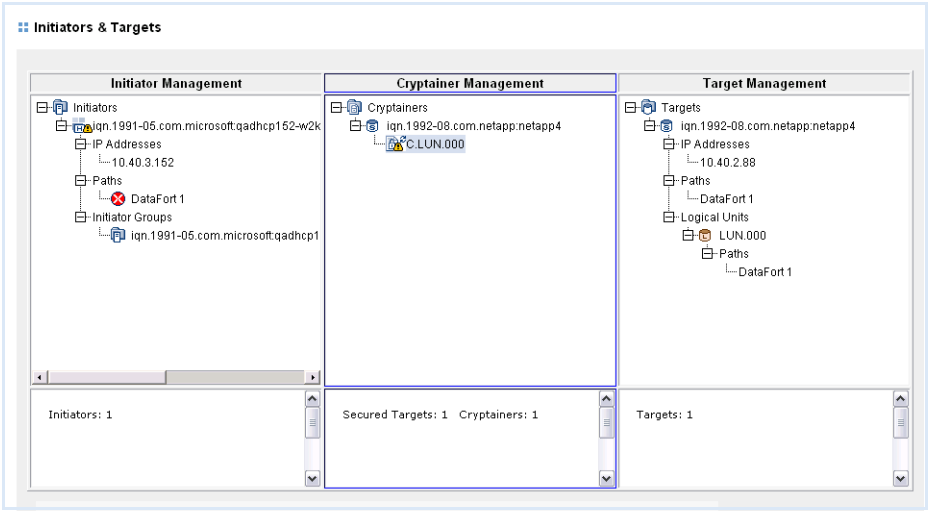
ENCRYPTING A CRYPTAINER

Note: This step is **not** required when using SnapDrive.

1. Expand the Cryptainer tree to view the Cryptainer icon.
2. Right-click the Cryptainer and select **Encrypt Empty**.

Note: DataFort only supports encryption of empty Cryptainers for iSCSI. If there is data on the storage device, it will be overwritten when the Cryptainer is created.

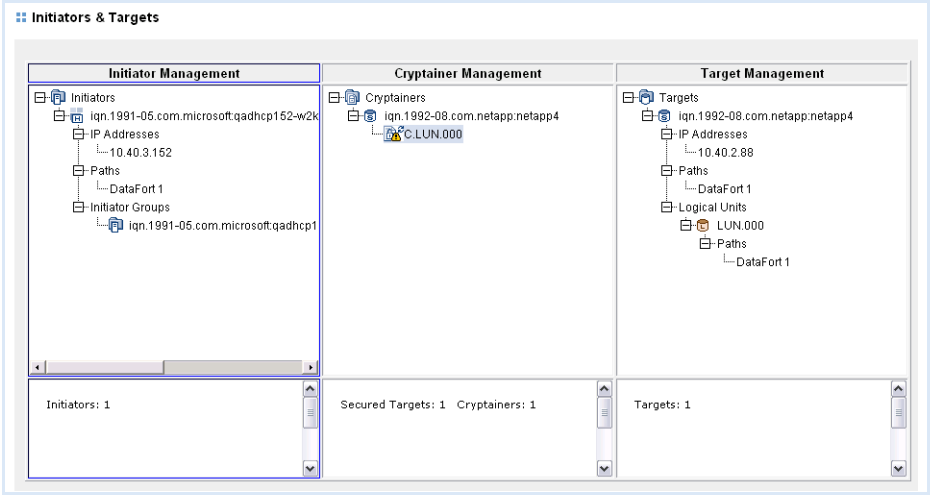
3. Agree to the warning by typing YES and clicking OK.



The icon will show that the Cryptainer is being encrypted.

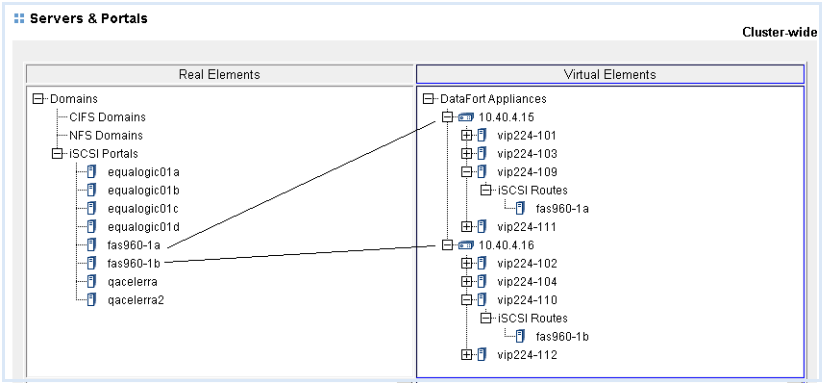
CONFIGURING AN INITIATOR

On the initiator, set up a target pointed to the Virtual Server (add the VIP as a target portal and log onto NetApp). Set up the disk. When setup is complete, the WebUI will show the Cryptainer with paths.



CONFIGURING DATAFORT TO SUPPORT MPIO

To support clustering in the iSCSI environment using Microsoft Multipath I/O (MPIO), be sure to create a VIP for each path from the initiator to the target. Virtualize the portals on a VIP at each DataFort. Each DataFort in the cluster should have an entry for the path from the initiator.



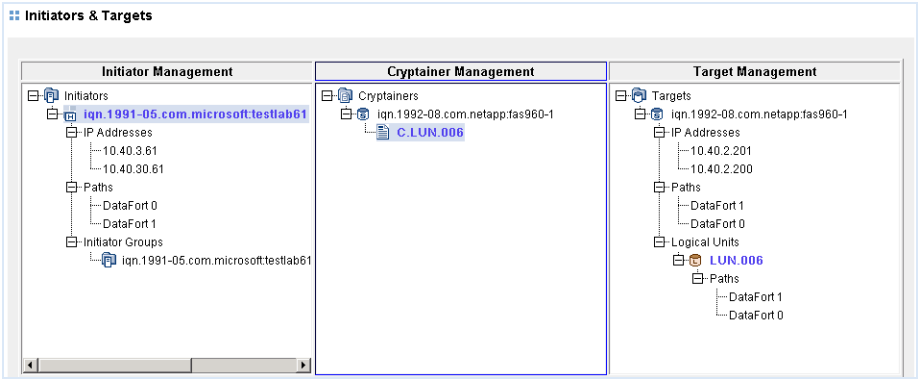
In this example, there are two Portal NICs:

- fas960-1a
- fas960-1b

They are virtualized on two VIPs:

- VIP224-109
- VIP224-110

The Client PC has two NICs. To support this, the initiator is added twice to the Initiator and Target page of the WebUI, with one IP for each NIC using the same initiator name. One Cryptainer is created, but multiple paths between the Initiator and Target are supported through multiple NICs.



MANAGING SECURE ISCSI STORAGE

Use the Servers & Portals and Initiators & Targets pages to manage secure iSCSI storage. The WebUI shows all known portals, initiators and targets, along with any Cryptainers that have been created.

Access the pages by selecting **Storage > Servers & Portals** or **Storage > Initiators & Targets** from the WebUI menu.

The Servers & Portals page can also be accessed 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.

The following sections describe options when managing iSCSI storage:

- Managing Portals
- Managing Virtual Servers and iSCSI Routes
- Managing Targets and LUNs
- Managing Cryptainers
- Managing Initiators

DATAFORT WEBUI ICONS

Icons display status information about network devices including initiators, 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.

TABLE 16: 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	
Initiator icon	Yellow !	One or more paths to initiator is offline	
Initiator 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	

TABLE 16: SAMPLE ICONS (CONTINUED)

Device	Icon State	Meaning	Example
Cryptainer icon	Yellow !	Metadata and/or rekey error, or Cryptainer is offline	
	Lock	Cryptainer is encrypted	
	No lock	Cryptainer is cleartext	

MANAGING PORTALS

Manage portals on the **Storage > Servers & Portals** page. To add a Portal, right click the iSCSI Portals entry and select Add Portal. Once the Portal is added, use the right-click per-portal menu to manage each portal. Right-click a portal in the Real Elements pane to see server management options.

TABLE 17: PORTAL MENU OPTIONS

Menu Selection	Purpose
Ping	Test DataFort access to this portal.
Server IP	Add: Add an IP address to the DataFort configuration. DataFort can use multiple server IP addresses when talking to a server, to get better performance from a server. For example, if a server has two NICs, each with a different IP address, the administrator can allocate some shares for access over one IP address, and some for access over the other.
	Resolve: If the IP address of the server has changed, use the Resolve menu option to update the information for that server in the DataFort configuration.
Virtualize On	Select the VIP that you wish to virtualize the portal on. This should be a VIP that is not being used for another portal or server.
Edit	Change portal attributes including IP address and DataFort interface. See Editing a Portal.
Delete	Delete portal.

Editing a Portal

The Edit Server page is used when an attribute of a portal changes. Make any changes and click Apply. Options when editing a portal include:

Hostname Enter or change the hostname of a server.

CIFS and NFS Domains Not needed for iSCSI.

iSCSI Access Be sure this is turned ON for an iSCSI portal.

IP address Indicate the IP address of the server. To update the server IP address after changing it at the server itself, change the IP address information here.

On Interface File Servers is the default setting. Change the default only if the Clients NIC is on a separate subnet and the real portal resides on that separate subnet.

Managing Virtual Servers and iSCSI Routes

Expand the view under a DataFort in the Virtual Elements to see the Virtual Server icon and menu. Right-click a server in the Virtual Elements pane to see virtual server management options.

Expand the view under the Virtual Server icon to view the iSCSI Routes created when a portal is virtualized on the server. It is possible to delete the route by right-clicking the icon. Do not serve iSCSI and NAS storage on the same virtual IP. See Adding Virtual Servers on page 108 for information about choosing settings when adding VIPs.

Table 18: Virtual Server Menu Options

Menu Selection	Purpose
Secure Access	Configure a secure IPsec connection to the server. See Configuring IPsec on a Virtual Server.
Certificates	Not used for iSCSI.
Move to	Move the virtual server to another DataFort IP address.
Edit	Edit Virtual Servers: change Virtual Hostname, IP address, Netmask. See Editing a Virtual Server.
Delete	Delete virtual servers that are not hosting shares which have become Cryptainers.

Editing a Virtual Server

The Edit Virtual Server page is used to modify virtual server settings. Make any changes and click Apply. Certain on-screen options do not apply to an iSCSI server, including CIFS and NFS Domain, SMB signatures and Joined CIFS Domain. When adding a virtual server, set the Floating option to OFF for iSCSI.

Note: Do not use the same virtual server for NAS and iSCSI storage.

Virtual Hostname Change the hostname of the VIP.

IP address Change the IP address of the VIP.

Netmask Change the Netmask of the VIP.

CIFS Domain Not needed for iSCSI.

NFS Domain Not needed for iSCSI.

Floating Set OFF for iSCSI. The VIP is assigned to a cluster member and it will always stay with that member. iSCSI VIPs should be of this type, because for iSCSI the redundancy is implemented using MPIO (client-driven failover).

Primary DataFort Primary DataFort serving data for VIP in cluster.

Client-side SMB Signatures Not needed for iSCSI.

Server-side SMB Signatures Not needed for iSCSI.

Joined CIFS Domain Not needed for iSCSI.

Managing Targets and LUNs

Manage targets on the **Storage > Initiators & Targets** page. Expand the target menu to view targets and LUNs. Right-click a target in the Target Management pane to see management options which include deleting the target and importing a key.

Expand the target view to see the IP address and path information for the target, as well as the LUN view and LUN menu for each storage unit on the target. Right-click a LUN to see the LUN Menu.

Table 19: LUN Menu Options

Menu Selection	Purpose
Show Cross Mapping	Shows the owner of and access to Cryptainers created on this LUN.
Create Cryptainer with	Gives the option to create a Cryptainer on the selected target. Choose whether to use an exportable key or not. Using an exportable key will allow the key to be exported to a trustee. See Importing and Exporting Keys for details.
Restore Cryptainer	Restore a deleted Cryptainer. See Restoring an iSCSI Cryptainer.
Import Key	Import a Key from a trustee to apply to this target. See Importing and Exporting Keys.
Export Key	Export a key from this target to a trustee. See Importing and Exporting Keys.
Delete	Delete the LUN from the database.

Deleting LUNs Using SnapDrive

After deleting a disk in SnapDrive, the administrator must also manually remove the LUN and its Cryptainer from DataFort. The administrator should write down the LUN (which can be obtained by looking in the SnapDrive UI) before deleting it in SnapDrive. Then manually delete the LUN and Cryptainer from the DataFort WebUI.

Managing Cryptainers

Manage Cryptainers on the **Storage > Initiators & Targets** page. Expand the Cryptainer Management tree to view individual Cryptainers. Right-click a Cryptainer in the Cryptainer Management pane to see management options.

Note: Rekeying is not supported for iSCSI Cryptainers.

Table 20: Cryptainer Menu Options

Menu Selection	Purpose
Show Cross Mapping	Right-click a Cryptainer and select Show Cross Mapping to view which initiators have access to the Cryptainer, and to see on which storage device the Cryptainer is located.
Encrypt Empty	Data within an iSCSI Cryptainer will not be encrypted until the encryption process is begun using this option. Cryptainer icons will indicate whether a Cryptainer is cleartext, waiting to be encrypted, is in the process of being encrypted, or is already encrypted. Select Encrypt Empty to assign an encryption key to an empty Cryptainer.

TABLE 20: CRYPTAINER MENU OPTIONS (CONTINUED)

Menu Selection	Purpose
Metadata	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.
Move	Select the target LUN, then right-click the Cryptainer that will be moved to that location. Moving a Cryptainer to another LUN means DataFort will encrypt/decrypt data on the new LUN using that Cryptainer key.
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	Right-click the Cryptainer collection and select Delete to remove it from the WebUI.

MANAGING INITIATORS

Manage initiators on the **Storage > Initiators & Targets** page. Expand the menu to view the IP, paths and group information for each initiator. Right-click an initiator in the Initiator Management pane to see management options.

To add a new initiator, right-click in the Initiator Management pane and select New Initiator.

TABLE 21: INITIATOR MENU OPTIONS

Menu Selection	Purpose
Show Ownership	Highlights which initiator has ownership of which LUNs and Cryptainers. By default, storage is owned by the initiator that discovers it, but ownership can be explicitly modified after LUN discovery (using the storage vendor's GUI). This menu option will display that ownership.
Permission	Show Cross Mapping: highlights which Cryptainers and targets the initiator can access. Use Grant and Revoke to change access permissions.
Add Initiator Group	Select a target from the Target management pane then select Add Initiator Group.
Delete	Right-click the initiator and select Delete to remove it from the WebUI.

Restoring an iSCSI Cryptainer

A Cryptainer that has been deleted from the configuration database can be restored. The restore procedure can be executed by a Full Administrator from any member of a DataFort cluster. The cluster must be the same one for which the Cryptainer was originally created. Note that if you are using LKM software to manage Cryptainer keys and the LKM server is on line, DataFort queries LKM for missing keys automatically.

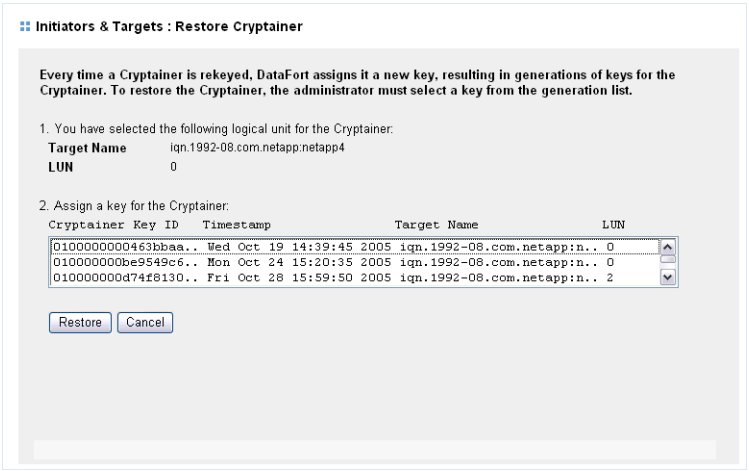
Each Cryptainer is assigned a Cryptainer ID in the DataFort configuration database. A Cryptainer that has been deleted from the DataFort configuration database can be restored using the Cryptainer ID and DataFort's restore features. Note that no more than one instance of a particular Cryptainer can exist 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. From WebUI, access the **Storage > Initiators & Targets** page.
2. Right-click the LUN where the deleted Cryptainer was originally stored. Select 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.



3. Select the Cryptainer key associated with the deleted Cryptainer.
4. Click Restore.

11 User Administration

This chapter outlines methods of managing user access to DataFort Cryptainers. The Full Administrator or a specified User Administrator can perform these functions:

- Managing Groups and Users
- Group Review
- Managing Cryptainer ACL

End users may obtain access to their secured data and manage ACL on Cryptainers they own as described in Chapter 12.

Managing Groups and Users

Users are automatically imported into DataFort as needed. Users who have access to shares that were created in preparation for becoming Cryptainers are automatically added to the DataFort configuration database. Users who are imported into the database include:

- Users who register with DataFort (see CIFS User Registration on page 142).
- Users who are added to the ACL of a Cryptainer.
- Users who are members of a group that is added to the ACL of Cryptainer.
- Users who access a Cryptainer which has the Everyone group in its ACL.

Adding Users

To add a user or group of users to the ACL for a Cryptainer, add the user or group to the ACL of the share that will become the Cryptainer (see Preparing to Create a NAS Cryptainer on page 95). Groups and users with access to a share will be the same groups that DataFort allows to access that share when it becomes a Cryptainer.

Automatic Domain Sync

DataFort automatically imports groups from the Windows domain controller, along with the users included in those groups. DataFort queries the domain controller every 30 minutes to see if any groups have been added, or if any users have been added to the groups already in the database.

- If the DataFort Group Review feature is off, DataFort automatically adds any new users that have been added to a known group. New users have the same Cryptainer access as other members of their group.
- If Group Review is on, the administrator will be required to review and accept any changes made to the Cryptainer ACL.

Disabling Automatic Domain Sync

If for some reason it is preferable to turn off DataFort's automatic sync function, use the following command. See Connecting to the DataFort Command Line Interface on page 71 for information accessing the CLI.

- Log into the DataFort CLI and set `user.domain.sync.disabled` to `true`.

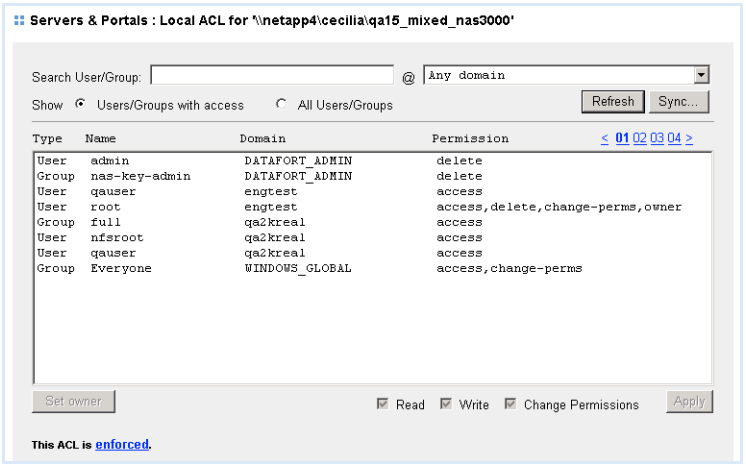
Searching for Users

It is possible to search the configuration database directly for user and domain names. Use the Exact User Name and Domain Search or a Wildcard User and Group Name Search.

Exact User Name and Domain Search

1. From the WebUI, choose **Storage > Servers & Portals**.
2. Right-click the Cryptainer and select **Access Control > ACL**.

   The ACL page appears.



3. Enter the exact user or group name into the Search field, then select the domain from the drop-down menu.
4. Click Refresh.

   The user/group will be displayed.

Wildcard User and Group Name Search

- This feature is only supported when searching in a Windows Domain.
- By default a maximum of 10 search results will be displayed, unless the **-n** option is used. To see all of the search results, set **-n** to **0**.
- A domain group search uses the domain group list command. This search uses **-g** instead of **-u**.

1. Log in to the DataFort CLI and use the **domain user list** command with the wildcard user name string. The wildcard user name string is a list of comma-separated user names. User names can contain asterisks for a wildcard query. The domain user command is:

   domain user list [-n, --num-of-users <num-of-users>] [-u, --user <user>] <domain>

Examples follow:

Example of user search where results are limited to 5 and the search term is using a wildcard "*" to search for users beginning with character "z1" and followed by any number of characters:

domain user list -n 5 -u z1* qa2003

Example of user search where results are limited to 5 using a comma-separated list:

domain user list -n 5 -u qauser,z1,z2* qa2003

Example of group search where results are limited to 5 using a comma-separated list:

domain group list -n 5 -g Dom*,Perf* qa2003

DataFort Groups

Since groups can include other groups as well as individual users, DataFort uses parent and child groups. For example, the nas-admin (Full Administrator) group is a member of the admin group in the DATAFORT_ADMIN domain. In this relationship, nas-admin is the child group and admin of the parent group. The administrator user may be a member of the nas-admin group.

There are two sets of parent groups in the DATAFORT_ADMIN domain. One set includes entries for well-known Windows security identifiers (SIDs) including the generic groups Everyone, Dialup, Network, etc. These must be defined on DataFort because they cannot be imported from any domain controller. The other set includes admin, guest, nas-user, and nas-admin. These are the groups in which DataFort users are typically included. When Windows users register with DataFort, they are added as users in the nas-user group.

If a Cryptainer is given an ACL, the group and users who are provided access by the ACL are listed on the Cryptainer ACL page of the WebUI (see Managing Cryptainer ACL on page 134).

Group Review

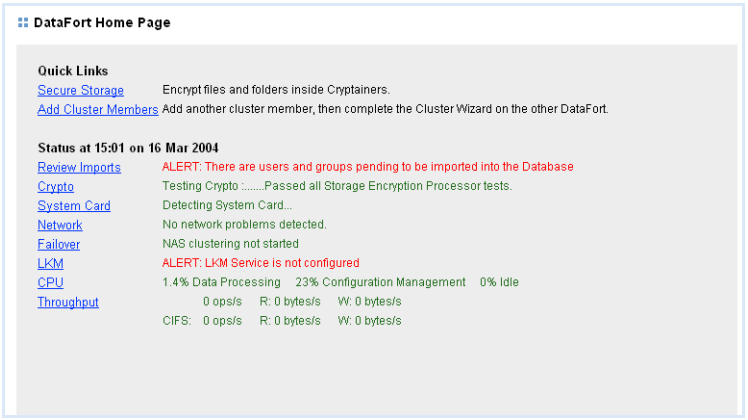
If Group Review is required by the Security Policy (see Domain Controller Security Settings on page 168), the DataFort administrator must review and accept or reject newcomers to groups in each domain. Users may be added to a Windows group, but they are not automatically given permission to access Cryptainers designated for other members of the group. When a new domain is added, the domain users will not appear until the administrator reviews and accepts the new group of users. The DataFort administrator will need to check each domain for new additions and accept or reject them on a case-by-case basis.

> **Note:** The DataFort Local ACL feature (see File Server Security Settings on page 168) protects against attacks on the file server, and the Group Review feature protects against attacks on the domain controller. It makes sense for Use Local ACL to be on when Group Review is on.

To enable new users in a group when Group Review is on:

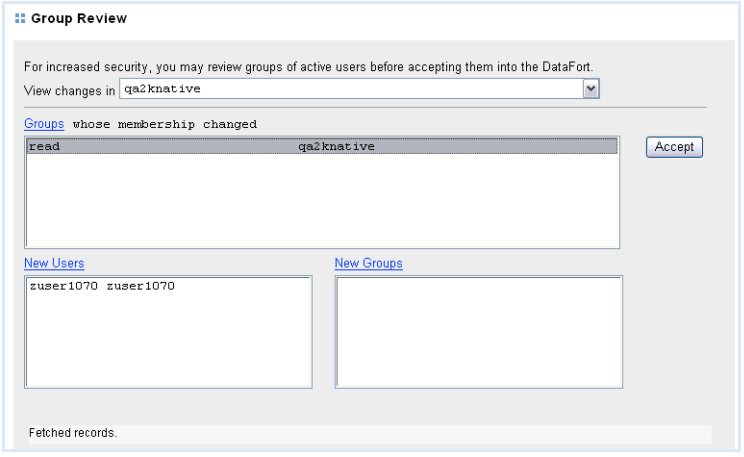
1. Access the Home page of the DataFort WebUI.

   If new users have been added to the ACL of a Cryptainer, and Group Review is on, a message will appear in the Status area of the DataFort WebUI Home page.



2. Click the Review Imports link.

   The Group Review page appears. It shows groups whose memberships have changed, and lists newly added users.



3. Click Accept to accept all the new users in the changed groups. Users cannot be accepted or rejected individually. If new users are not accepted, they will not be allowed access.

MANAGING CRYPTAINER ACL

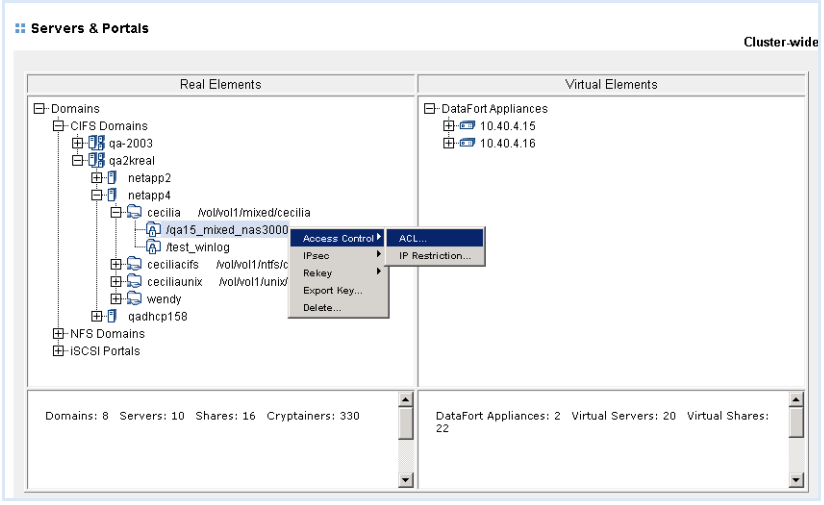
Keep the following guidelines in mind when setting access control for CIFS Cryptainers:

- The Windows administrator should set the ACL on a share at the time of its creation (before it is added to DataFort as a Cryptainer). Windows has two types of ACLs for shares: ACLs which apply everywhere in the share, and ACLs which apply to folders and files in the share. Users must have permission according to both ACLs in order to do operations in a Cryptainer.
- Note that there is a limit of 100 users per single ACL in CIFS.
- When a CIFS Cryptainer is created, the ACL is automatically synced with the ACL of the share folder on the file server at that time. Unless permissions on the share were set before the Cryptainer was created, the Cryptainer may not be accessible.
- There are two ACLs, one on the DataFort and one on the file server. They are identical when a CIFS Cryptainer is first created, because DataFort performs an auto-sync at the time the Cryptainer is created. After this time, there are many ways to make the ACLs diverge, including changing permissions on the Cryptainer itself (on the server) and using the WebUI.
- DataFort security settings affect the behavior of ACLs. If Local ACL is off, only the server's ACL is honored. If Local ACL is on, then the most restrictive permissions are used. For example, if UserA has read permission on DataFort and read/write permission on the server, the user can only read.

CRYPTAINER ACL

To view the ACL settings on a Cryptainer:

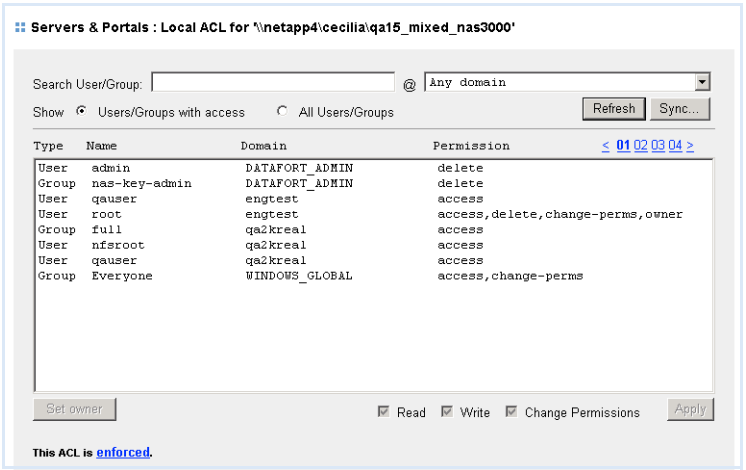
1. From the WebUI, choose **Storage > Servers & Portals**.
2. Right-click the Cryptainer and select **Access Control > ACL**.



The ACL page appears.

Users with access to the selected Cryptainer are listed.

- To modify a user's access to the Cryptainer, select the user and use the check boxes on the page. Note that if Local ACL is off, only the server's ACL is honored.
- To make a selected user the owner of the Cryptainer, click Set Owner.



3. To update the ACL of the Cryptainer (if changes have been made on the ACL of the Cryptainer on the server) click Sync.

ACL Capture and ACL Sync

The following describes two methods for setting access control on Cryptainers.

Setting the CIFS ACL Using ACL Capture

This method of setting ACL requires less action on the part of the Windows domain administrator, but requires that network users be fairly experienced using Windows.

1. From the WebUI, choose **System Config > Security > Security Policy.**
2. Click Customize.
3. Set the DataFort Security Policy so that Group Review, User Registration, Secure Password Update, and Use Local ACL are all on and click Apply to save the settings.
4. Create a share with default permissions on a server in a domain (for Windows 2000, group Everyone has full control).
5. Add the share as a Cryptainer as described in Creating a NAS Cryptainer on page 96.
6. As your planned most-privileged user, map the Cryptainer/share from a client that is a member of the same domain as the server.
7. From the client, right-click the Cryptainer/share and bring up the Properties window. Set the permissions on the share (for example, add full permissions group, mod permissions group, read-only permissions group, delete Everyone group).

8. Add full permissions for the Domain Access User for that domain so that DataFort can make changes to the ACL if necessary. (Note that this is not a security hole because DataFort specifically denies the DataFort domain access user data access.)

   Note: To exclude the administrator from those permitted to access the Cryptainer, specifically omit the Windows administrator from the Cryptainer/share ACL. With DataFort Local ACL on, the Windows administrator cannot be added to the Cryptainer ACL simply by being added to the ACL directly on the server's share.

9. Apply the permissions.

   DataFort will capture the permissions transaction between the client and the server, updating the DataFort permissions to match the permissions on the server.

   Now the permissions are set as the most-privileged user wanted them. Even the Windows domain administrator will not be able to change permissions unless the domain administrator is a member of one of the full permissions groups.

Setting the CIFS ACL Using ACL Sync

This method requires more action on the part of the Windows domain administrator, but may be desirable if setting ACL is confusing to network end users.

1. From the WebUI, choose **System Config > Security > Security Policy.**
2. Click Customize.
3. Set the DataFort Security Policy so that Group Review, User Registration, Secure Password Update and Use Local ACL are all on.
4. Click Apply to save the settings.
5. Create a share with default permissions on a server in a domain (for Windows 2000, Everyone has Full Control).
6. Add the share as a Cryptainer as described in Creating a NAS Cryptainer on page 96.
7. From the server, set the permissions on the share for the desired ACL (for example, add full permissions group, mod permissions group, read-only permissions group, and delete Everyone group).
8. Add full permissions for the Domain Access User for that domain so that DataFort can make changes to the ACL if necessary. (Note that this is not a security hole because DataFort specifically denies data access to the DataFort domain access user.)
9. At the Servers & Portals page of the WebUI, right-click the Cryptainer and select **Access Control > ACL**.

   The list of users who have access to the Cryptainer appears on the Servers & Portals: ACL page.

10. Click Sync.

    DataFort accesses the server, reads the server ACL and displays it in the Preview Sync window.

11. Click Confirm to synchronize the DataFort ACL for that Cryptainer with the permissions you just set at the server.

12 Accessing Secure Data

After a Cryptainer has been created, users with access to the original share can begin storing and accessing data in the Cryptainer, where it will be automatically encrypted. This chapter describes some of the methods by which an end user can access data secured by DataFort, as well as some other tasks the user may need to complete when accessing data secured by DataFort. See the following topics for instructions on user access to data:

- CIFS Data Access
- NFS Data Access
- Migrating Data
- CIFS User Registration
- End-User Cryptainer ACL Management
- End-User Login to DataFort CLI
- HTTP Data Access
- FTP Data Access
- TFTP Data Access

CIFS Data Access

Depending on the operative security policy, the administrator should notify end users of any new requirements for accessing their data. This information might include:

- Any new instructions for handling sensitive data.
- CIFS User Registration procedures. If User Registration is on, users must register their Windows name and password at the DataFort WebUI Login page before accessing their data.
- Changing User Passwords procedures. If the DataFort Password requirement is in effect, users will need a DataFort-specific password (separate from the Windows password) to authenticate them before they can access data.

After Cryptainers have been created:

- The administrator should notify users of names of Cryptainers they can access, and the path (through virtual servers presented by DataFort) for saving and storing sensitive data in those Cryptainers. The correct path is determined when the Cryptainer is created (see Add a Cryptainer on page 101). Subsequently, users will work with the data as though it were stored in unencrypted form. They will navigate to shares, explore the network, and access shares to which they have been granted access. Data inside the Cryptainer will appear to the qualified user as cleartext.
- Users should copy any existing directories that they want to secure into the newly created, empty Cryptainers. The data will be encrypted as it is copied into the Cryptainers. See Migrating Data. New data written directly into the Cryptainer will be encrypted automatically.

CIFS Data Access Example

This section illustrates the encryption process and the role of the path to encrypted data, by comparing secured data access through DataFort with access directly from the server.

Viewing a Cryptainer

1. Create a Cryptainer from a share.
2. Log in to a client workstation as a user who is part of the domain that includes DataFort, and has permission to access the share that has been turned into a Cryptainer.

   For this example, consider a server named **server1** and a share named **Share1**, a virtual server **VirtualServer** (with IP address **VirtualServerIP**), and a virtual share named **secured_Share1**.
3. Select Run from the Windows Start menu and enter the network path to the virtual share through the DataFort: **\\VirtualServerIP\secured_Share1**
4. Click OK.
5. Create a file in the share, or copy an existing file into it, and add text to the file.

   The contents of the file appear in cleartext.

   WARNING: IF THE SERVER IS SET TO SHOW HIDDEN FILES, THE HIDDEN .DECRU FILE WILL BE VISIBLE. THIS FILE MUST REMAIN INSIDE THE SECURE SHARE AT ALL TIMES. DO NOT ATTEMPT TO DELETE, RENAME, OVERWRITE OR MOVE THE .DECRU FILE.

Viewing a Secure Share Directly

The following steps illustrate what an encrypted file looks like on the server. For an administrator, it's preferable to give end users only one path to their secured data: the path that goes through the DataFort. If users attempt to access files directly on the server, they will see ciphertext.

1. Select Run from the Windows Start menu and enter the IP address or domain name assigned to the server where the original share was created.

   For this example enter: **`\\server1\Share1`**

2. Click OK.

   The file created while connected through the DataFort will appear.

3. Open the file.

   The contents of the file appear in ciphertext.

> **WARNING:** NEVER ACCESS DATA DIRECTLY ON THE SERVER OR MOVE ANY DATA FROM ONE CRYPTAINER TO ANOTHER WITHOUT GOING THROUGH DATAFORT.

NFS Data Access

Only the owner of a Cryptainer can grant or revoke access to that Cryptainer. To allow the administrator to view the contents of a Cryptainer, the owner of that Cryptainer (a known user) must log in and grant the administrator access to the Cryptainer.

NFS Data Access Example

The following example illustrates the encryption process by comparing a secure share exported by DataFort with the same share mounted directly.

For the CLI commands, consider a server named **server1** and a share named **share1**, a virtual server **virtual_server1**, and a virtual share named **secure_share1**.

Granting Access to the Root User

1. The owner of the share needs to grant access to root (or whatever user has permission to mount shares) using the DataFort WebUI. See End-User Cryptainer ACL Management on page 146.

   Now that the owner of the Cryptainer has granted access to the root user, the root user can mount the Cryptainer.

Mounting the Shares

1. Log in to client1 workstation as root.
2. Mount the secure_share1 exported by the DataFort:

   ```
   mount virtual_server1:/secure_share1 /mnt/secure_share1
   ```

3. For the purpose of this illustration, also mount the share directly. Mount the server1 share named share1, from client1:

   ```
   mount server1:/share1 /mnt/server1
   ```

Viewing the Shares

View the same secure share two different ways: as exported by DataFort and as it exists on the server.

1. To view the Cryptainer exported by DataFort, log on as user1 on the client1 workstation.
2. Copy files into the **/mnt/secure_share1** directory.
3. Open a file inside the Cryptainer (under the **/mnt/secure_share1** directory).

   The file should appear as cleartext.

4. For the purpose of this illustration, view the secure share directly by opening a file from the **/mnt/server1** directory.

   The file should appear as ciphertext.

Migrating Data

After a Cryptainer has been created, users with access to the original share can begin storing data in the Cryptainer, where it will be automatically encrypted. Users can also copy existing data into a Cryptainer after it has been created. If initial encryption is on, encryption will automatically be started in the Cryptainer (see Options When Adding a Cryptainer on page 106). Existing data can be migrated into secured Cryptainers by using initial encryption or by copying.

Secure Existing Data Using Initial Encryption

To secure existing data using automatic initial encryption, create a Cryptainer by specifying the existing path on the server. Initial cleartext data is encrypted. This allows you to create a Cryptainer that is cleartext, add data to it directly on the server and then create a Cryptainer which will encrypt the contents of the share.

1. Add an empty share to DataFort as described in Creating a NAS Cryptainer on page 96.
2. Place data inside the share directly on the server.
3. Select the share and Add a Cryptainer as described in Add a Cryptainer on page 101.

Secure Existing Data by Copying

To secure data by copying it into a Cryptainer, use the following procedure to ensure that the data is encrypted properly. This example assumes there is an existing folder called Folder1 on a file server that will be converted to secure storage in a Cryptainer.

1. Rename **`Folder1`** to **`Folder1_cleartext`**.
2. Create a new folder on the file server, and name it **`Folder1`**.
3. Set the Sharing Properties of **`Folder1`** to share the folder.
4. Add **`Folder1`** to DataFort as a Cryptainer, as described in Creating a NAS Cryptainer on page 96.
5. Copy the contents of **`Folder1_cleartext`** to the newly created Cryptainer.

   Note: The data must be copied from **`Folder1_cleartext`** to **`Folder1`** through DataFort. If the data is copied locally from **`Folder1_cleartext`** to **`Folder1`**, the information will not be encrypted.
6. Delete or retain the **`Folder1_cleartext`** contents and folder, as needed.

CIFS User Registration

If User Registration is required by DataFort Security Policy, end users must register once at the WebUI Login page before they can access Cryptainers. If the DataFort Password requirement is in effect, users will also need to provide their DataFort password at the time of registration.

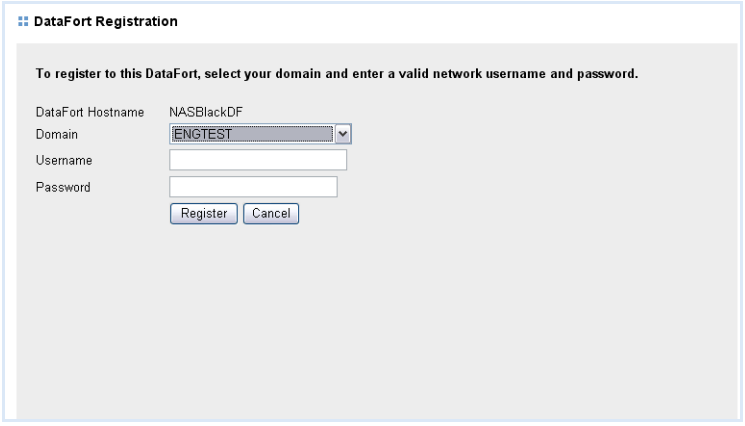
Whether the user needs to use the DataFort password or the domain password depends only on whether the DataFort password is different than the domain password. With the DataFort Password requirement turned off at the **System Config > Security > Customize** page, the user will register without seeing a place to set the DataFort password. The DataFort password will be the same as the domain password. With DataFort Password turned on, it is possible (and likely) that the user will set the DataFort password to be different from the domain password.

Whether or not User Registration is required by DataFort Security Policy, registration is required before CIFS end users can use DataFort WebUI to access Cryptainers they own.

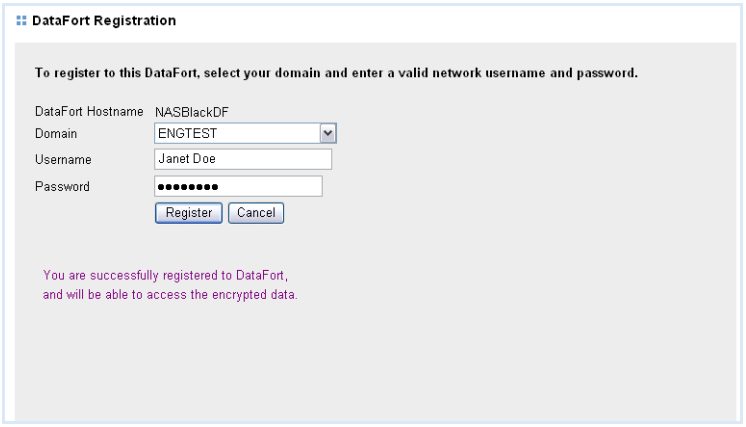
Registering the User's Windows Password

Instruct the user to complete the following steps by logging in to a standalone DataFort, or logging in to either DataFort in a cluster:

1. At a Windows computer, open Internet Explorer and enter `https://` followed by the IP address or hostname assigned to DataFort.
2. At the DataFort Login page, click the link to log in as an end user.
3. At the DataFort Login for End Users page, click the register link.
4. Select the domain that includes this user.



5. Enter the current username and password for this user.
6. Click Register.



After registering, users will be able to access the Cryptainers the network administrator has created for them. User can also modify ACL on Cryptainers they own. See End-User Cryptainer ACL Management on page 146.

If the user's Windows password changes, the user will need to update the password upon login to DataFort (see Changing User Passwords on page 144).

Registering the User's DataFort Password

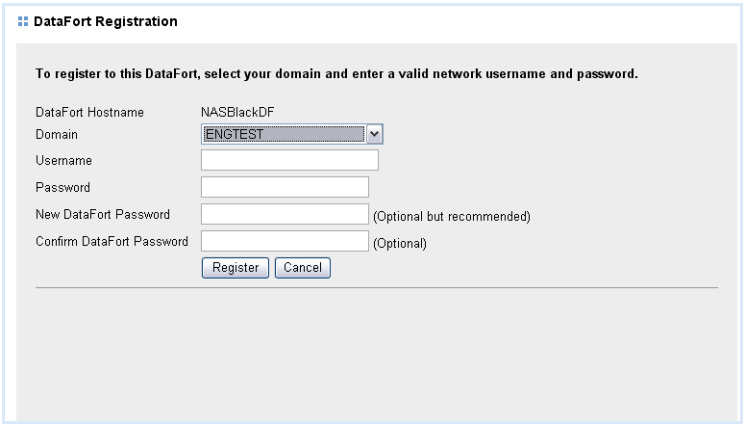
If the DataFort Password requirement is in effect, users will also need to register that password. By default the DataFort password is the same as the domain password (Windows password).

- If a user is not yet registered at the time the DataFort Password requirement is turned on, then that user will need to register both the DataFort password and the domain password at once.
- If a user has already registered at the time the DataFort Password requirement is turned on, the DataFort password is set by default to be the same as the Windows password. In this case, the user should update the DataFort password, using the Windows password as the old password and replacing it with a new DataFort password.

Instruct the user to complete the following steps for either DataFort in a cluster:

1. At a Windows computer, open Internet Explorer and enter **`https://`** followed by the IP address or hostname assigned to DataFort.
2. At the DataFort Login page, click the link to log in as an end user.
3. At the DataFort Login for End Users page, click the register link.

   The DataFort Registration page will appear.



4. Select a domain that includes this user.
5. Enter the valid current Windows username and password for this user.
6. Enter the DataFort password. If the DataFort password fields are left blank, then they will be assigned the value entered for the user's domain (Windows) password and click Register.

   After registering, users will be able to access the Cryptainers the network administrator has created for them.

   If the user's Windows password changes, the user will need to update the password upon login to DataFort (see the next section).

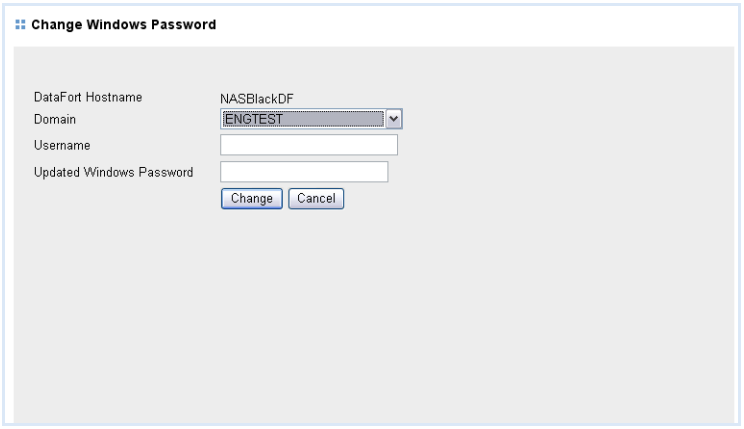
Changing User Passwords

When the user's Windows password is changed, the user must update the password registered with DataFort. If the DataFort Password requirement is in effect, users can change their DataFort password as well, via the link on the WebUI login page.

Instruct the user to complete the following steps. If DataFort is part of a cluster, the user can log in to either DataFort in the cluster.

Changing the User's Windows Password

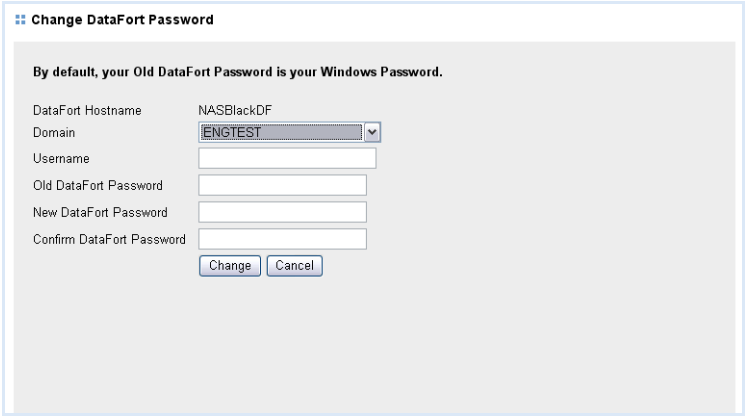
1. At a Windows computer, open Internet Explorer and enter `https://` followed by the IP address or hostname assigned to the DataFort.
2. At the DataFort Login page, click the link to log in as an end user.
3. At the DataFort Login for End Users page, click the link to update password information.
   - If the DataFort Password requirement is off, the update link will open the Change Windows Password page.
   - If the DataFort Password requirement is on, the Change button will appear on screen. Click the Change button for the Windows Password.



4. Select the domain this user is in, enter the required information and click Change.

Changing the User's DataFort Password

1. At a Windows computer, open Internet Explorer and enter **`https://`** followed by the IP address or hostname assigned to the DataFort.
2. At the DataFort Login page, click the link to log in as an end user.
3. At the DataFort Login for End Users page, click the link to update password information.
4. Click the Change button for the DataFort Password.



5. Select the domain the user is in, and enter the required information and click Change. If the user registered with DataFort before the DataFort Password requirement was turned on, the user's old DataFort password will be the same as the user's current domain (Windows) password.

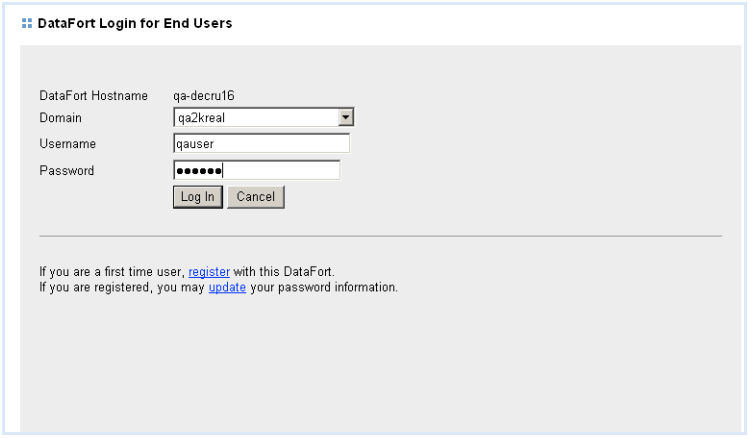
END-USER CRYPTAINER ACL MANAGEMENT

End users can log in to DataFort WebUI to view and manage the Cryptainers they own.

1. At a Windows computer, open Internet Explorer and enter **`https://`** followed by the IP address or hostname assigned to the DataFort.

   Note: CIFS users must register (see CIFS User Registration on page 142).

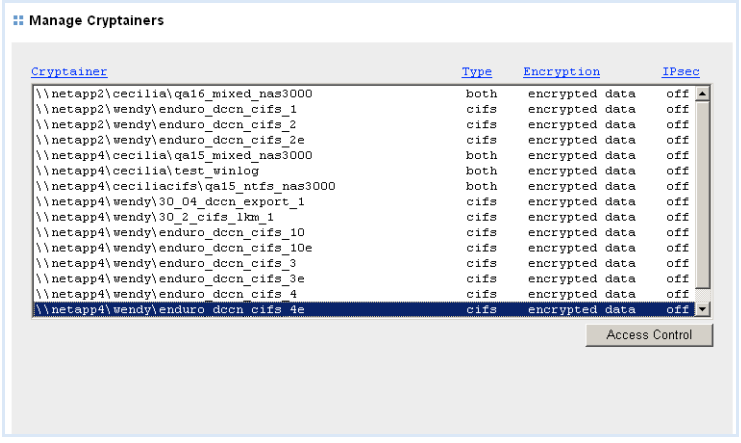
2. At the DataFort Login page, click the link to log in as an end user.



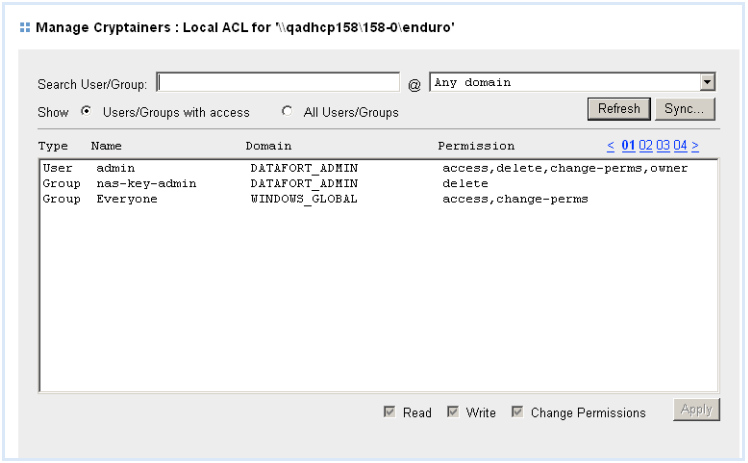
3. Enter the domain the user belongs to, the username and password, and click Log In.

   The Manage Cryptainers page is displayed, listing Cryptainers owned by the user.

4. At the Manage Cryptainers page, select a Cryptainer.



5. Click Access Control to view or change access permissions.



6. Select the user who will be granted access to the Cryptainer, and use the check boxes at the bottom of the screen to change permissions.
7. Click Apply to save the changes.

End-User Login to DataFort CLI

End users can log in to DataFort CLI from an SSH client.

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.

   Note: If the user has CIFS Cryptainers, the registration requirements are the same as for login to DataFort WebUI.
3. In the terminal window, enter the user login name and password.

After logging in, end users can list share, domain and Cryptainer settings, and can sync and manage the ACLs of Cryptainers they own.

HTTP Data Access

DataFort supports storing and accessing data via HTTP, including the WebDAV extensions. With DataFort web access you can securely access data from a web browser. WebDAV extensions, provided by the Windows operating system or a WebDAV client application, offer additional capabilities. Data stored by DataFort appears in cleartext form when accessed by authorized users through DataFort, and appears in encrypted form if accessed directly on the server.

Web access users (subject to Cryptainer user and IP access controls) can browse folder contents, upload and download files, and delete files and folders in a web browser window. WebDAV users can also create folders, and rename and copy files and folders.

HTTP makes it possible to access DataFort over a secure SSL connection, which ensures that user credentials and data are protected. In a more advanced configuration, certificates can be used as an additional means of authenticating clients.

Keep the following in mind when using HTTP data access:

- To access data via a web browser, use Internet Explorer 6.0 or Mozilla 1.4 or later.
- To access data via WebDAV, use the Map Web Folder functionality in Windows 2000, or one of the many client applications that support WebDAV, such as WebDrive or HTTP:DAV. DataFort supports web access and WebDAV from the following systems (among others): Microsoft Windows 2000 Professional/Server, Windows XP, Windows Server 2003.
- All web access and WebDAV connections are secured using SSL. DataFort supports both SSL 3.0 and TLS (Transport Layer Security): client software must have one or both of SSL 3.0 and TLS enabled. Each virtual IP address can have its own certificate for identification over SSL. DataFort also supports setting a root certificate per virtual IP address for authenticating clients. See Setting Virtual Server Certificates on page 109 for more information.
- Web access and WebDAV are automatically enabled on all virtual server IP addresses that have virtual shares configured. See Changing Web Configuration Using the DataFort CLI on page 149 to change the default.

Use the steps outlined below to use and reconfigure HTTP data access.

Web Access

1. From a browser, access the server: https://virtualserver or https://virtualserverIPaddress.
2. Enter a valid username (or domainname\username) and password.

   These will be checked against the CIFS and NFS domains associated with the virtual IP address to determine if the user is authorized. If the domain name is entered, the credentials are checked against the indicated CIFS domain and all the NFS domains associated with the virtual IP.

   Users will be able to access only data for which their credentials are valid. If the entered username and password are valid in the CIFS domain but not the NFS domain, the user will be able to access only CIFS data. If the user is a member of a different CIFS domain than the virtual IP address, the user should go to https://virtualserver/logon.html and enter the domain as well.
3. Click the link for the share this user may access.
4. To upload a file to the secured share, click Browse and locate the file to upload.

5. Click Upload. The uploaded file will appear in the share listing.
6. To view the contents of the file, click the file link in the browser window.
7. To download the file, right-click on its link and select Save Target As.
8. To delete files or folders, click the check box beside each file or folder you want to delete (you can select more than one). Then click the trash bin icon at the top of the page.
9. To log out, click the username that is at the top right corner of every listing.

WebDAV

Use these steps for WebDAV access from Windows XP. The same information must be supplied if you are running a WebDAV client.

1. Right-click My Computer and select Map Network Drive.
2. Click on the link at the bottom of the dialog to map a drive for the operating system in use.
   - Create a shortcut to a web folder or FTP site.
   - Sign up for online storage or connect to a network server.
3. Enter https://virtualserver to mount the server at the top level, or enter https://virtualserver/<share_name> to mount only the share.
4. Click Next.
5. Enter the username and password.
6. Enter a name for the mapped folder.
7. Click Next.
8. Click Finish to complete the connection.

   An entry appears in the My Network Places list corresponding to the new folder.

   After mapping the drive, data in that folder is accessed the same way as any other mapped network resource. The user may drag and drop files between the local computer and the WebDAV server, as well as create directories and delete or rename files and folders. To upload files, drag and drop them into the folder.
9. To log out, click the Log Out link.

Changing Web Configuration Using the DataFort CLI

WebDAV requires no additional configuration after setting up CIFS and/or NFS access. By default, any virtual IP address that is exporting CIFS or NFS shares will have those same shares available via HTTP. To modify WebDAV-related settings, use the DataFort CLI.

- To disable HTTP access for a given virtual IP address, you can use the CLI option **`--http-access <on|off>`** when adding the virtual IP address using the **`vip add`** and **`vip set`** commands.
- By default, Decru HTTP access listens on port 443 connections. If you wish to use a different port (for example, if port 443 is blocked by a firewall), set the property **`nas.http.port`** to the desired port.
- Note that the default life span of user credentials is one hour. After an hour, the user will be required to log in again. If you wish to change this setting, set the property **`nas.http.credentials.ttl`** to the desired life span (in minutes).

FTP Data Access

DataFort allows clients to access encrypted data using FTP (File Transfer Protocol). Clients can log in to virtual servers from an FTP client, authenticated by their username and password. FTP is controlled on a per virtual IP basis, using the DataFort CLI.

1. Log into the CLI and enable FTP for each VIP. This is the only configuration required for FTP. Enter:

   ```
   vip set --ftp-access on <vip_name>
   ```

   Note: Unlike CIFS, NFS and HTTP, the default for FTP is off. Once enabled, FTP behaves very similarly to HTTP.

2. Using any FTP client, connect to the VIP, entering your username and password. You will be authenticated against both the CIFS and NFS domains of that VIP. If the credentials are valid, you will have access to the corresponding shares.

3. Doing a directory listing after logging in will present you with a list of shares. By clicking on one share (if you are using a graphical client) or typing **`cd <share_name>`** (if you are using a text-based client), you will enter the share and have access to the data.

FTP Home Directory

The only other configuration that FTP supports is the concept of a home directory. If a home directory is set up for a client, rather than starting at the top level, the client will start in one of the shares and can access data immediately.

1. To set up a home directory, log in to CLI and enter the **`user home set`** command:

   ```
   user home set [<user>]@<domain> <real_path>
   ```

   - If the user name is specified, then the home directory is for that user only.
   - If no user name is specified, then the home directory applies to all users in the domain. Additionally, if no user name is specified, the last component of the path may be a '*' in which case the home directory for each user is obtained by appending the user's name to the path.

2. To see all configured home directories, enter:

   ```
   user home list
   ```

3. To remove a home directory entry, enter:

   ```
   user home remove [<user>]@<domain>
   ```

Note the following:

- If the share for a user's home directory is not virtualized on the VIP this user connects to, then the user will be started at the root level.
- Each principal may have only one home directory configured. Executing the **`set`** command again will just change the home directory.
- In case a home directory is specified for a specific user, and a generic rule exists for that user's domain, the specific rule takes precedence.

TFTP Data Access

DataFort allows TFTP access to encrypted data. Since TFTP is an insecure protocol, TFTP access should not be enabled for highly sensitive data. The most common use for TFTP is with diskless workstations where the boot image is stored on a central server and workstations retrieve the image using TFTP. The use of TFTP through DataFort protects the image from being taken off the server and used outside the approved setup.

TFTP Commands

TFTP is controlled on a per virtual IP basis, using the DataFort CLI. To enable TFTP, log into the CLI and execute the **vip set** command with the following options. All the TFTP options should be set at one time, using one command.

- The **tftp-mode** setting determines the type of data access permitted through TFTP. The valid mode arguments are: disabled (no TFTP access), read, write, and all (files may be both read and written). Enter:

  vip set --tftp-mode <mode>

- The **tftp-virtual-share** option determines which share/export is used to handle all TFTP file requests. For instance, if this option is set to \\virtualserver\virtualshare and that share corresponds to \\server\share, then requesting the file dir\file.txt is equivalent to requesting the file \\server\share\dir\file.txt using CIFS. Enter:

  vip set --tftp-virtual-share <path>

- The **tftp-user** is the user permitted file access. It is recommended that this be set to a user created specifically for DataFort TFTP access. That way, when looking at server logs it is easy to see which files were accessed via TFTP. The user's type must agree with the type of the share. For instance if the share specified is CIFS, then this user must be a member of a CIFS domain. In addition, if the user is a CIFS user, the user's password must be registered with the DataFort (see CIFS User Registration on page 142). Enter:

  vip set --tftp-user <user@domain>

Sample TFTP Configuration

This section describes a sample use of TFTP, which assumes the following conditions:

- One NFS domain called mydomain
- One user in mydomain named tftpuser
- One server called myserver
- One virtual server called myvirtualserver
- One share on myserver called /vol/vol0/myshare

1. Configure the storage devices as you normally would to enable NFS access.
2. Log in to the DataFort CLI and enable TFTP:

   vip set --tftp-mode all --tftp-virtual-share myvirtualserver:/vol/vol0/myshare --tftp-user tftpuser@mydomain myvirtualserver

Now users may connect to myvirtualserver via TFTP and read and write files from the myserver:/vol/vol0/myshare Cryptainer.

13 KEY ADMINISTRATION

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

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

- Managing Trustees
- Managing DataFort Defense Responses
- Setting Security Options
- Configuring IPsec
- Managing Recovery Officers and Recovery Cards

A Key Administrator can also create Cryptainers as described in Chapter 9.

Any administrator can reset smart cards:

- Smart Card Reset

Managing Trustees

A trustee is a remote DataFort with which a trust relationship has been formed, allowing exportable encryption keys to be shared. Creating trustees allows Cryptainer 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

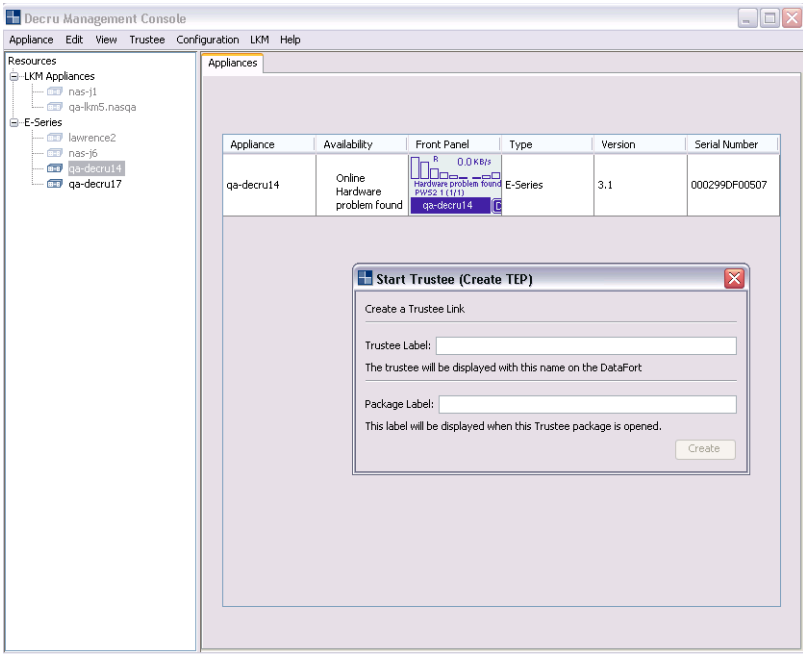
This example describes a trustee relationship between a main and a remote site. Setting up trustees requires:

- 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/for each appliance. If the Security Setup requires 2 out of 5 cards, for example, two people will have to be present to insert their cards and enter the label name and password for the card, in order to establish trustees.
- Files and information will need to be provided by the main site administrator so that the remote site administrator can import the trust package.

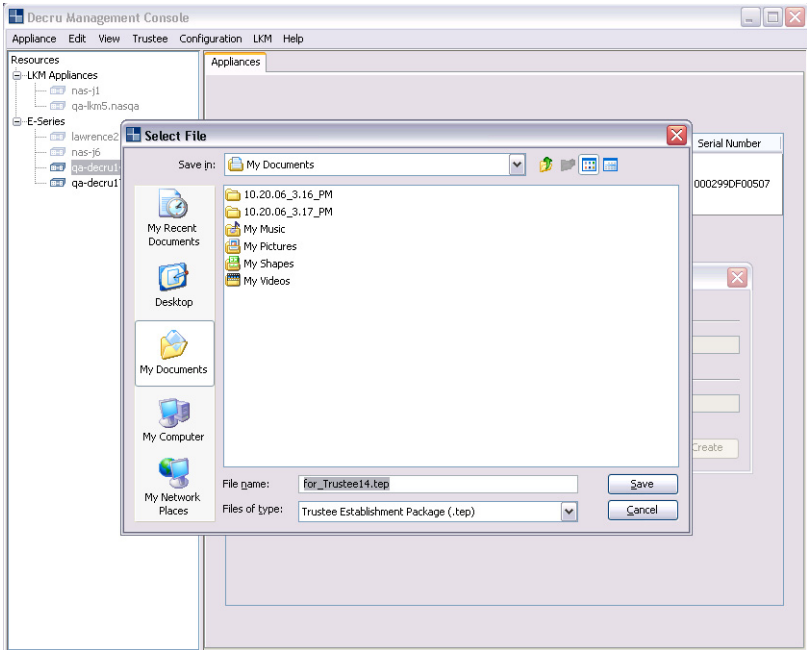
Create the Trustee Link

Trustee management requires the use of the Decru Management Console (DMC). See Decru Management Console Functions on page 219 for information about this interface.

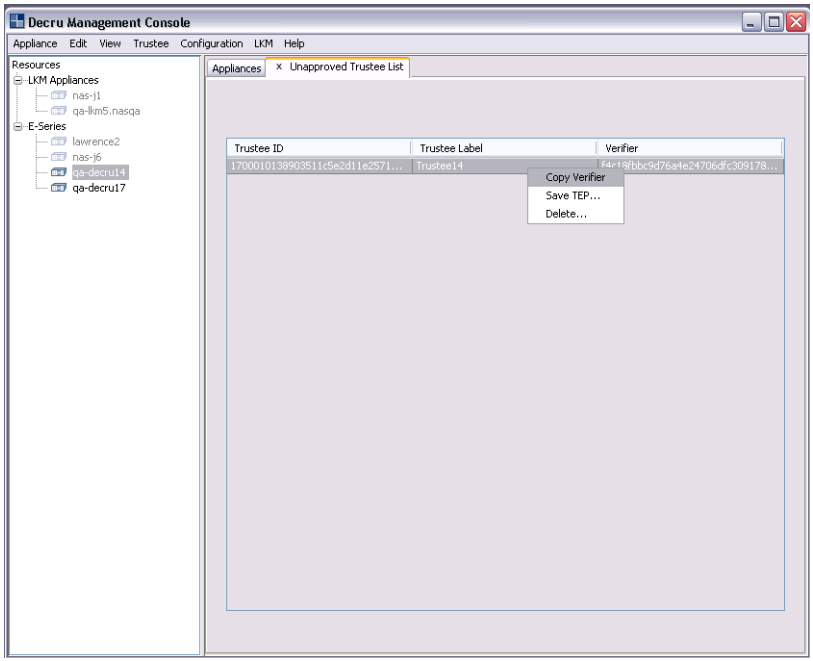
1. Choose **Start > Programs > Decru > Decru Management Console**.
2. From the Resources pane, select the first DataFort that will become a trustee.
3. From the Trustee menu, select **Start Trustee Creation**.



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



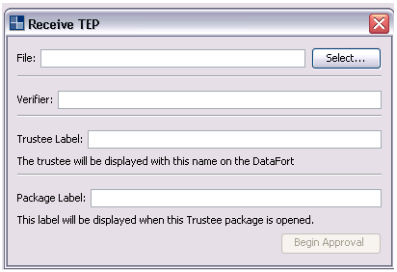
5. In the Select File window, keep the default name and choose a directory in which to save the TEP file.
6. From the Trustee menu, select Unapproved Trustee list.
7. Right-click the newly-created trustee and select Copy Verifier.



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

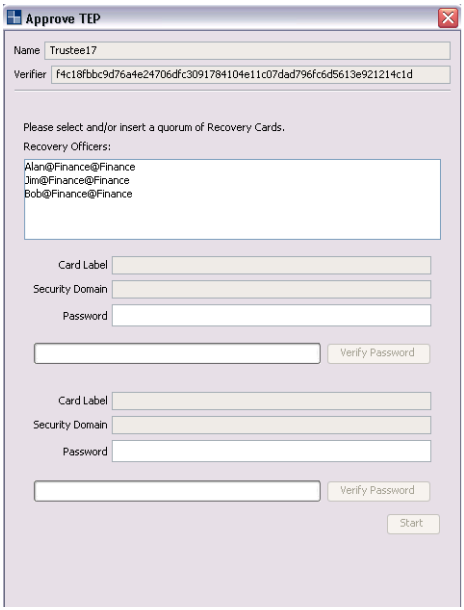
   The verifier must be communicated in a secure manner – Decru recommends communicating the information by phone or direct contact rather than email. This is the only form of authentication for key sharing and is considered sensitive material.

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



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

    The approve TEP panel appears.

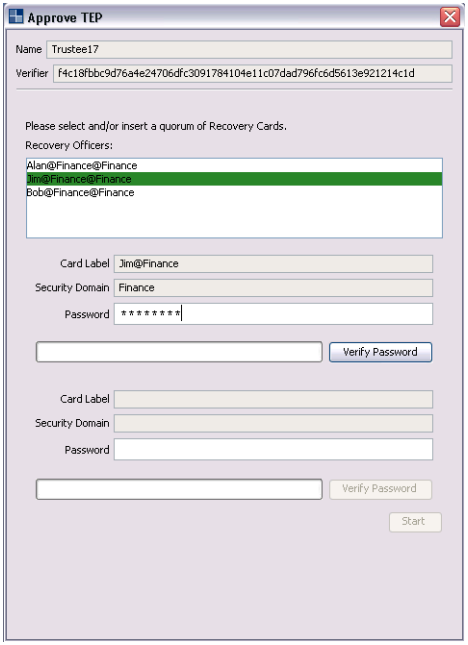


The next step requires that the smart cards be presented to DMC. The number of cards required is established by the recovery schema set for each appliance at the time it was initialized.

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

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

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



15. Click Start.

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

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

    Wait for the progress bar to appear.

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

26. Click Start.

    When finished, a Trustee created message will appear.

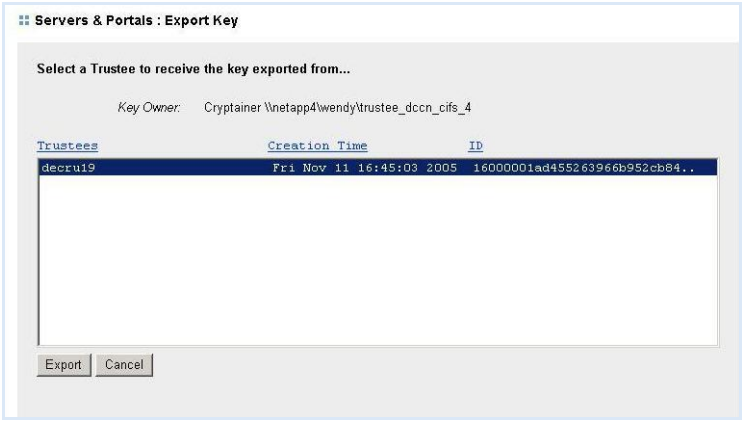
27. From the Trustee menu, select Trustee List to see the created trustee link.

IMPORTING AND EXPORTING KEYS

Once a trustee relationship is established, keys can be shared between the trustees. To share a Cryptainer key between trustees see NAS Key Import and Export and iSCSI Key Export and Import. The procedure involves logging into the WebUI of both the DataFort from which the key is being exported (the source DataFort) and the DataFort that will import the key (the target DataFort).

NAS Key Import and Export

1. At the source DataFort (from which the key will be exported) create a Cryptainer as described in Creating a NAS Cryptainer on page 96.
2. At the time of creation, set the Exportable to trustees option on the Cryptainer ON.
3. To export the Cryptainer key, right-click the Cryptainer on the **Storage > Servers & Portals** page and select Export key.
4. Select the trustee (the target DataFort) in the Export Key page.



5. Click Export.
6. You will be prompted to save the key as a .kdf file (i.e. qa-decru21_2005-11-09_1006.kdf).
7. Save this file in the desired location (from which the target DataFort will be able to retrieve it).
8. At the target DataFort, add the same server and share that was used to create the Cryptainer on the source DataFort.
9. At the **Storage > Servers & Portals** page, right-click the Real Elements pane and select Import Key.



10. Browse to the location where the .kdf file was saved and click Import.
11. At the target DataFort, right-click the share created for the purpose of importing the Cryptainer key and select Restore. See Managing Virtual Shares on page 111 for more information about restoring Cryptainers.

iSCSI Key Export and Import

1. At the source DataFort (from which the key will be exported) access the **Storage > Initiators & Targets** page.
2. Right-click a LUN in the Target Management pane and select Export Key....
3. Save the exported key file.
4. At the target DataFort access the **Storage > Servers & Portals** page, right-click in the Real Elements pane and select Import Key...
5. At the Import Trustee Keys page, browse to the saved file and click UpLoad.
6. At the target DataFort, add the Add the same server that was used to create the Cryptainer on the source DataFort, and the same initiator. See Creating an iSCSI Cryptainer on page 115 for details.
7. At the **Storage > Initiators & Target** page, right-click in the Target Management pane and select Rescan.
8. Right-click the new LUN and select Restore Cryptainer.
9. Select the Cryptainer Key ID that was imported (look for the LUN number from which the key was exported, and the latest timestamp.)



10. Select Restore.
11. Right-click the Cryptainer Management pane on the **Storage > Initiators & Targets** page and select Refresh.

    The LUN should appear, and the Cryptainer should be visible (with the lock icon indicating encryption is on) in the Cryptainer Management pane.

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 164).
- 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.

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

DATAFORT DEFENSE SETTING

Defense levels are summarized in Table 22. If in doubt, choose the Basic level.

TABLE 22: 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.		

TABLE 22: DATAFORT DEFENSE SETTINGS (CONTINUED)

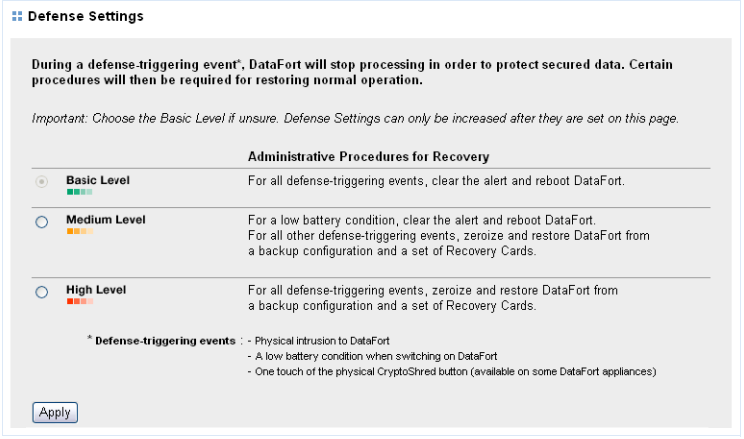
Setting	When Used	Intrusion Trigger	Response	Operation Resumes
Medium	When it is necessary to clear encryption keys in case of an intrusion but not if the battery is low.	Battery too low when system is powered on.	Encryption and decryption disabled.	After administrator determines the cause of the intrusion 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.



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.

   Note: After a defense alert, a cluster will be in a failover state. To recover normal cluster operation after DataFort reboots, log in to the WebUI of any cluster member, click the Failover link on the Home page, and click the Recover button in the Manage Failover page.

Resetting a Defense Alert via CLI

The CLI displays an alert after login.

1. Execute the **`system tamper reset`** command.

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

   Note: After a defense alert, a cluster will be in a failover state. To recover normal cluster operation after DataFort reboots, use the WebUI (as in the previous note) or use the CLI. To recover with the CLI, log in to the CLI of the cluster member that was reset, and issue the command: **`cluster comeback`**. Then, log in to the CLI of the cluster member that was not tampered with, and issue **`cluster giveback`**.

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

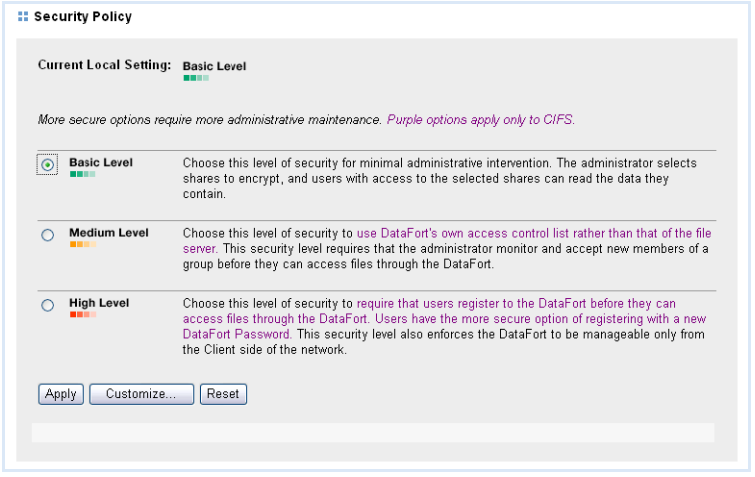
SETTING SECURITY OPTIONS

DataFort offers configurable levels of security to suit a variety of environments and to protect against certain types of security threats. The administrator uses the Security Policy page of the DataFort WebUI to set the security policy according to the needs of the network. Higher security settings require more involvement on the part of the administrator, but provide stricter access control.

CHOOSING A CONFIGURED SECURITY LEVEL

1. From the WebUI, choose **System Config > Security > Security Policy** to view or set the security policy.

   Note: Security policy settings for clusters are replicated: setting the security policy on one clustered DataFort applies the same policy to the other DataFort in the cluster automatically.



2. Review the three Preset Security Levels.
3. Select the desired security level, or leave the default level of security enabled. By default, DataFort is set with Secure Web and CLI off, and is accessible for management from the Clients or File Servers NIC.

   To see the specific settings that define a given security level, or to create a custom combination of settings, see Customizing a Security Level.
4. Click Apply.

   The Security Policy page and the Home page of the WebUI will show the selected level.

Preset Security Levels

Basic Choose this level of security for minimal administrative intervention. The administrator selects shares to encrypt, and users with access to the selected shares can read the data they contain. With Basic Security enabled, Secure WebUI is on.

Medium Choose this level of security to use the DataFort access control list rather than that of the file server. This security level requires that the administrator monitor and accept new members of a group before they can access files through DataFort. With Medium Security enabled, Secure WebUI and Secure CLI are both on.

High Choose this level of security to require that users register with DataFort before they can access Cryptainers. Users can also register with a new DataFort Password. This security level also requires that the DataFort be managed only from the client side of the network. With High Security enabled, Secure WebUI and Secure CLI are both on.

To see which features are on or off for a given preset level, see Table 23, Table 24 and Table 25.

Customizing a Security Level

Custom-configure the security setting by choosing from the available options.

1. From the WebUI, choose **System Config > Security > Security Policy**.
2. Click Customize.

   The various security setting options are listed. Settings in blue (User Registration, DataFort Password, Secure Password Update) apply only to CIFS.
3. To preview a pre-configured level, select it from the menu at the top of the screen and click Show.
4. To define your own security setting, turn any option on or off using its onscreen radio button. Security settings are divided logically into Domain Controller Related Settings, File Server Related Settings and Management Security Settings.
5. After selecting the desired options, click Apply.

   The Security Policy page and the Home page of the WebUI will show that a Customized security level has been selected.

Domain Controller Related Settings

By default DataFort controls user access to Cryptainers according to the ACL of the Cryptainer's share on the file server, and by trusting the domain controller's group membership settings. Use these settings to decrease DataFort dependence on the domain controller for access control and user authentication.

Table 23 shows whether the setting is on or off for the three preset levels, as well as the result of turning the setting on.

TABLE 23: DOMAIN CONTROLLER SECURITY SETTINGS

Setting	Basic	Medium	High	Result
Group Review	OFF	ON	ON	Requires that the administrator monitor and approve all changes made to group membership at the domain controller before they are accepted by DataFort.
User Registration	OFF	OFF	ON	Requires that end users register at the WebUI before accessing Cryptainers for the first time (as well as each time they change their domain password).
DataFort Password	OFF	OFF	ON	Requires that end users set and then present a special DataFort password (in addition to the domain password) before accessing Cryptainers for the first time. Both the user's DataFort password and domain password must be compromised before access to a Cryptainer is compromised. Changing the DataFort password always requires the old DataFort password. See CIFS User Registration for more information.
Secure Password Update	OFF	OFF	ON	Requires that an end user's old Windows password be provided before a new one can be set. With this setting off, the user is not prompted for the old password, so it would be possible for an attacker to change a user's password without knowing the original password.

File Server Related Settings

By default, DataFort trusts the access control settings on a file server, passing the permissions through to allow users access to data inside Cryptainers on the file server. Use these settings to increase the role of the DataFort in maintaining file server ACLs. DataFort always maintains a Local ACL for all Cryptainers, regardless of the Local ACL security setting.

Table 24 shows whether the setting is on or off for the three preset levels, as well as the result of turning the setting on.

TABLE 24: FILE SERVER SECURITY SETTINGS

Setting	Basic	Medium	High	Result
Use Local ACL	OFF	ON	ON	Allows DataFort to enforce its Local ACL, not accepting changes to the ACL made on the file server after the Cryptainer's initial creation. This protects against the file server administrator modifying the ACLs directly.
User Mapping	OFF	OFF	OFF	Allows only the DataFort domain access user direct access to shares on the file server. Also provides a way to manage users in environments that do not use Windows domains (such as LDAP). See User Mapping and DataFort Domains for more information. Note that when User Mapping mode is ON, the ACLs of Cryptainer shares are not synced to the DataFort when the Cryptainer is created. Additionally, ACL viewing from client Windows computers is disabled.

Management Security Settings

Use these settings to control management of the DataFort. By default, DataFort security settings are customized with Secure Web, Secure CLI and Clients NIC Management Access all OFF.

Table 25 shows whether the setting is on or off for the three preset levels, as well as the result of turning the setting on.

TABLE 25: DATAFORT MANAGEMENT SECURITY SETTINGS

Setting	Basic	Medium	High	Result
Secure Web	ON	ON	ON	Requires an Admin Card in order to access the DataFort WebUI. A smart card reader must be installed on any machine that will be used as a Management Station and a valid Admin Card must be presented in order to log in.
Secure CLI	OFF	ON	ON	Requires that the administrator log in to the WebUI with an Admin Card in order to obtain a secure password for temporary access to the CLI. If both Secure Web and Secure CLI are turned on, an Admin Card will always be required for DataFort management.
Clients NIC Management Access	OFF	OFF	ON	Requires that all administrative commands come from the Clients NIC of the DataFort. This protects against attacks from the file server side of the network (as long as DataFort is the only bridge between the file server network and the client network).

CONFIGURING IPSEC

IPsec is used for normal communication between members of a DataFort cluster, and can also be used to protect the transfer of unencrypted information between clients and DataFort.

DataFort IPsec is expressed as a set of rules, which specify which pairs of VIPs and clients must use IPsec for communication. Each IPsec rule consists of a local VIP, a specification for remote IP address(es) of one or more clients, and an authentication method using either Kerberos or shared secret. IPsec rules must be configured at both ends of the communication path.

Note: There is a limit of 512 IPsec rules; up to 2000 concurrent IPsec clients are supported per DataFort.

IPsec can also be turned on for specific Cryptainers.

- To require IPsec for an existing Cryptainer see Setting Cryptainer IPsec Restriction on page 108.
- To require IPsec as a Cryptainer is created, see Options When Adding a Cryptainer on page 106.

SUPPORTED CLIENTS AND AUTHENTICATION METHODS

Datafort supports authentication via either preshared keys or Microsoft-compatible Kerberos. IPsec on Datafort is tested to work with Windows 2000, Windows XP and Solaris clients. Please contact Decru for more information about supported platforms.

Windows clients	Either Kerberos or preshared secret can be used as the authentication method. Preshared secret is less secure in the Windows environment, so Kerberos authentication is recommended.
Solaris and Unix clients	Only Preshared secret is supported for authentication.
Combination of client platforms	Different authentication methods can be used for the same IPsec rule. Even if a shared secret is specified for an IPsec rule, as long as the VIP of the rule has joined its Windows domain, IPsec using Kerberos authentication will also work for the VIP and all clients in that domain. This may be useful in environments with various types of clients.

For instructions on setting up IPsec at clients, see:

- Adding a Kerberos Rule for Windows Clients
- Kerberos Authentication without IPsec
- Adding a Preshared Secret Rule for Clients

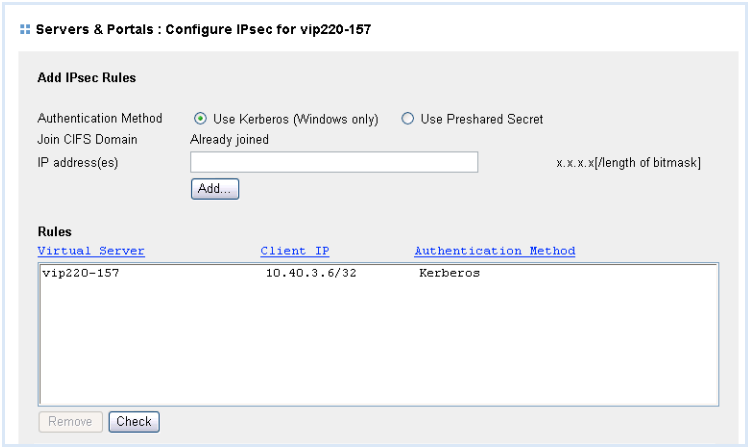
ADDING A KERBEROS RULE FOR WINDOWS CLIENTS

In the Windows environment where both the VIP and client(s) are part of the same domain, IPsec using Kerberos authentication is recommended. If you select Kerberos authentication the server must join the Kerberos domain.

1. From the Servers & Portals page, right-click a VIP and select **Secure Access > Configure IPsec**.
2. Select **Secure Access > IPsec**.
3. For Authentication Method, click Use Kerberos (Windows only).

4. If the virtual server (VIP) is not yet joined to the domain, the Join CIFS Domain line will read Not yet joined. Click the Not yet joined link.
   - In the Edit Virtual Server window, select Yes for Joined CIFS Domain. Add admin user and password. Click Apply. DataFort will contact the domain controller and add itself as a member of the domain.
   - Right-click the virtual server and select **Secure Access > IPsec**. You'll notice that the Join CIFS Domain line now reads Already joined. Proceed to step 6.
5. If the virtual server (VIP) is joined to the domain, the Join CIFS Domain line will indicate Already joined.
6. Enter the IP address of the client(s) that will connect using IPsec with Kerberos authentication.

   The client(s) can be specified as either a single IP address or an IP subnet. A single IP must be specified in the quad-dotted format, for example, 10.10.10.1. An IP subnet is specified in the same format followed by a mask length. For example, 10.10.10.0/24 covers all IP addresses that are in the 10.10.10.xxx subnet.
7. Click Add.
8. Enter the IP address of one or more additional clients that will connect using IPsec with Kerberos authentication, and click Add.
9. Click Add. The rule will appear in the Rules window.



10. To verify the IPsec rule, select the rule from the Rules window and click Check.

Kerberos Authentication without IPsec

When you add a virtual server, the domain you specify is only used internally to create a context in which to authenticate users. If you want to use Kerberos authentication without creating IPsec rules, join the virtual server (VIP) to the domain. DataFort contacts the domain controller and adds itself as a member of the domain. To join the server to the domain, right-click the virtual server in the Virtual Elements pane, and choose Edit. Click Yes beside Joined CIFS Domain, and click Apply.

Additionally, all clients and servers must be joined to the domain, and the domain controller must host the DNS. All clients, servers, and DataFort must have both forward and reverse DNS entries, as well as having the proper DNS suffixes and search paths.

Adding a Preshared Secret Rule for Clients

The preshared secret rule can be set for Windows, Unix and Solaris clients. Note that if a VIP has joined a domain and the client is configured to use Kerberos authentication, Kerberos authentication will work, even if shared secret is specified.

1. From the Servers & Portals page, right-click a VIP and select **Secure Access > Configure IPsec**.
2. Select Use Preshared Secret and enter the preshared secret set on the client. The shared secret must be 16 ASCII characters for Windows clients or 32 hex characters for Solaris clients.
3. Enter the IP address of the client that will connect using IPsec according to the rule set in the previous step.
4. Click Add.

   The rule will appear in the Rules window.



5. To verify the IPsec rule, select the rule from the Rules window and click Check.

Relevant System Properties

Recommended values for system properties that concern IPsec are shown in the table below.

Table 26: IPsec System Property Values

Property Name	Recommended Values
net.ipsec.phase1_lifetime_secs	86400
net.ipsec.phase2_lifetime_secs	28800
krb.default_realm	(not set)

TABLE 26: IPSEC SYSTEM PROPERTY VALUES (CONTINUED)

Property Name	Recommended Values
krb.default_etypes	des-cbc-crc
krb.default_etypes_des	des-cbc-crc
krb.clockskew	300

IPSEC CONFIGURATION FOR WINDOWS CLIENTS

Two management tools for configuring IPsec on Windows are the command-line IPSEC Security Policy Tool and Microsoft Management Console (MMC). To use a GUI for configuring clients, use MMC, a Microsoft system management tool for Windows 2000 and Windows XP.

Create a custom IPsec policy, first by defining a security rule, then by defining a filter list, and finally by specifying the filter action. For more detailed information on IP Security Policy for Windows consult the Microsoft website.

DataFort supports the ability to specify a rule for each client separately, or for a given subnet. For shared secret, set up a unique shared secret for each client. For Kerberos you can set up a rule for multiple clients through the subnet capability.

IPSEC CONFIGURATION FOR SOLARIS CLIENTS

The following procedure applies to DataFort beginning with version 1.6, and Solaris 9.

Verify or Install IPsec Kernel Patch

IPsec on Solaris 9 requires installation of a kernel patch to support cryptographic functionality inside the kernel. The patches may be downloaded free from sunsolve.sun.com.

- Confirm the patches are present by using the **ndd** tool. As root, issue the command:

  ```
  ndd /dev/ipsecsesp ipsecesp_status
  ```

  If the encryption packages are installed, the value of “encryption algorithms” (the second line of output) will be 3. if the patches are not installed, the value will be 1. If the patches are not already installed, install them and reboot before continuing.

Configure the IPsec Security Policy Database

Configure IPsec SPD policy entries in /etc/inet/ipsecinit.conf. The security policy database (SPD) contains policies, or rules, describing how inbound or outbound packets should be processed or filtered. Solaris 9 ships with a skeleton /etc/ipsecinit.conf file which includes some examples.

- Following the examples in the /etc/ipsecinit.conf file, configure an IPsec rule between a Solaris 9 machine with local address 10.20.20.185, and a Datafort with address 10.20.20.77 by adding the following line to /etc/ipsecinit.conf:

  ```
  { laddr 10.20.20.185 raddr 10.20.20.77 } ipsec { encr_algs 3des
    encr_auth_algs md5 }
  ```

Configure IKE rules for Solaris

The SPD describes how packets should be processed. When the Solaris kernel finds a packet which (according to the SPD) requires IPsec, but the kernel has no matching Security Association (SA), the kernel requests the IKE daemon to create a suitable SA.

Therefore, you must configure the IKE daemon to propose a suitable SA to the Datafort.

- Create an IKE config entry for SA. Solaris 9 includes an IKE daemon, /usr/lib/inet/in.iked, which is configured via the file /etc/inet/ike/config. For IPsec to a Datafort, you must configure:
  - Identity Authentication via preshared keys.
  - Oakley group 2 for the Diffie-Hellman exchange.
  - Either 3DES or (coming soon) for phase2, AES as the encryption algorithm.
  - Either sha1 or md5 as the authentication algorithm.

  Note: The Solaris 9 documentation and manual pages state that you can configure phase1 or phase2 lifetimes, either globally or per-rule. Decru recommends changing lifetimes via the **`ndd`** tool, affecting all sessions.

Configure Preshared Keys for Solaris

You must add the same preshared key used by the Datafort to the file /etc/inet/secret/ike.preshared. The Solaris format for the shared-key is a hex string, with no leading 0x.

Activate IPsec policy

A reboot is the safest way to activate the policy, however, you can re-load the kernel SPD from /etc/inet/ipsecinit.conf (see Configure the IPsec Security Policy Database) using the **`ipsecadm`** tool.

Activate IKE

A reboot is the safest way, however you can use **`ps -ef`** to find the currently-running IKE daemon, kill it, and restart a new daemon.

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.

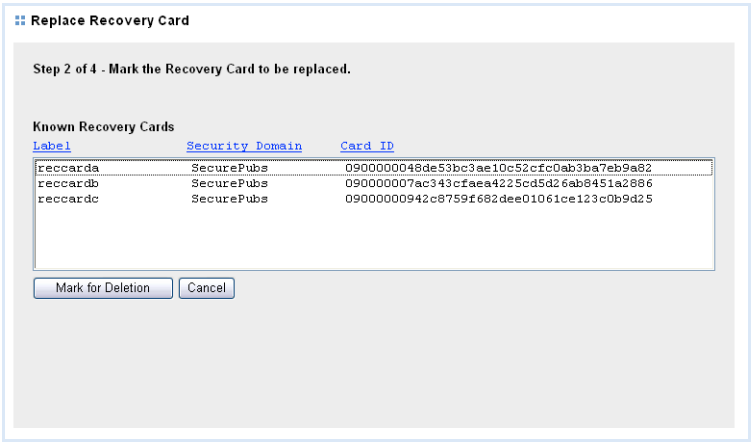
REPLACING A RECOVERY CARD

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



   The current set of cards is displayed.

2. Click Begin.



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

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

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

CHANGING A RECOVERY CARD PASSWORD

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

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



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

SMART CARD RESET

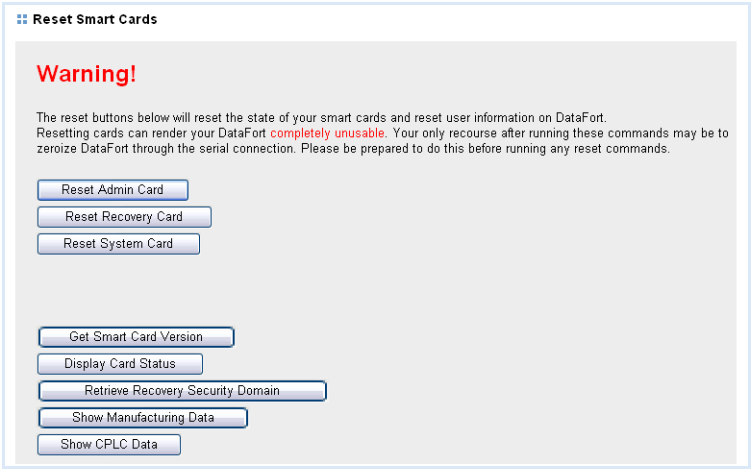
It is possible to completely reset a smart card using a special DataFort Reset Smart Cards page. This page also allows the administrator to check smart card versions and status.

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

1. Enter the following path into the browser window:

   `https://<nameofDataFort>/resetcards.htm`

   The Reset Smart Card page will appear.



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

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

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

14 BACKUP ADMINISTRATION

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

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

- Saving Configurations to Lifetime Key Management Software
- Downloading Configurations to a Remote Location

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

Note: Do not use the LKM Settings page of the WebUI to configure backups to an LKM appliance. Refer to the *LKM Appliance Administration Guide* for instructions.

Saving Configurations to Lifetime Key Management Software

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 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 address of a working LKM server, configuration changes will be backed up automatically every hour. The configuration can also be backed up to LKM manually.

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

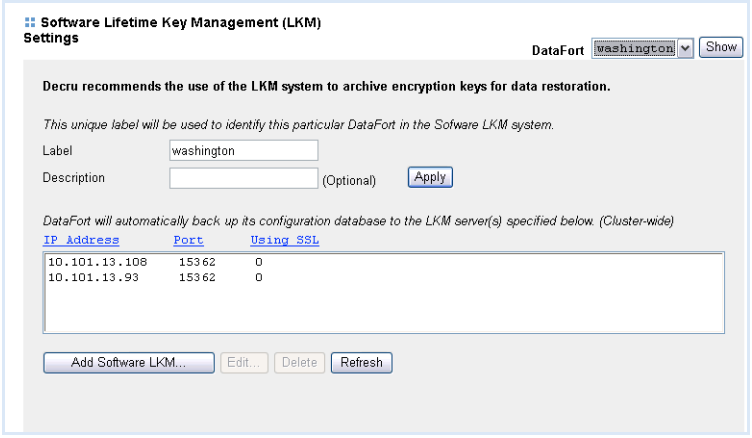
Configuring Backups to LKM Software

Use this procedure to set up regular automatic backups to LKM software. DataFort supports up to four servers for the LKM system. Backups will be sent to all LKM servers at the same time. Enter the IP addresses for each LKM server as described below.

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

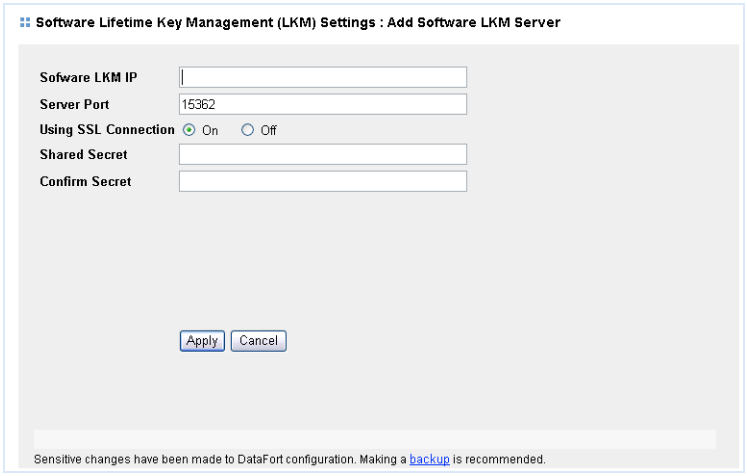
DataFort supports automated configuration backups to four LKM servers.

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



3. Click Add.

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



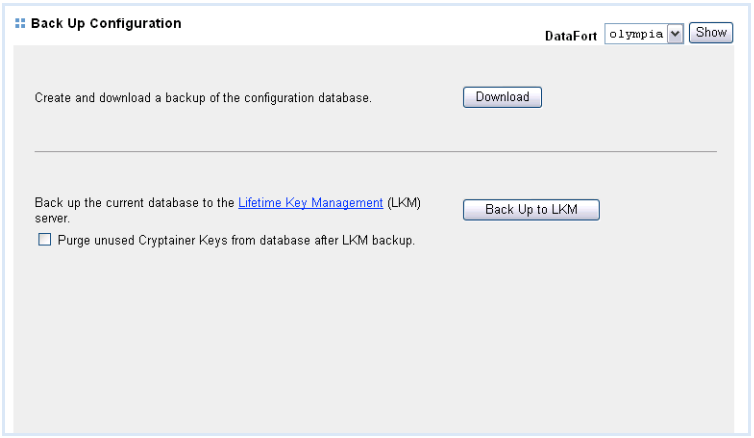
4. Enter the IP address of the LKM software server.
5. Leave the Server Port at its default setting. If the default port is not available on the LKM server, see the LKM documentation for instructions for changing the setting.

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

Backing Up the Configuration to LKM

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

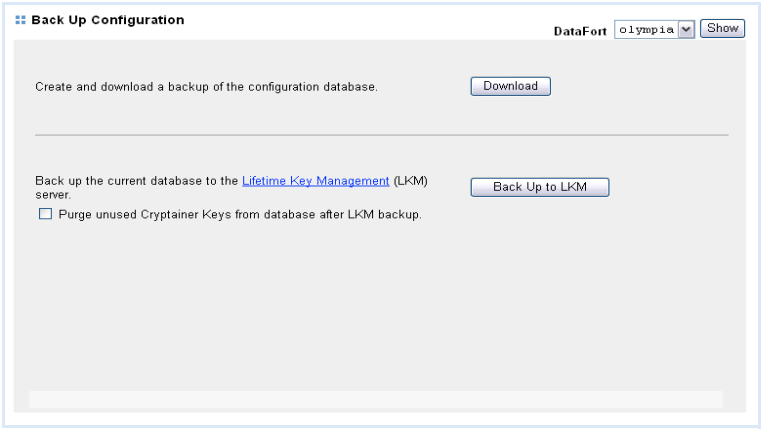
Keys are automatically backed up to LKM when LKM is in use. When backing up to LKM manually, you have the option to purge keys by checking the Purge unused Cryptainer keys... box on the Back Up Configuration page of the WebUI. This removes unused keys from the DataFort database, and stores them only in LKM.

Only keys that are no longer current (meaning they are not assigned to Cryptainers) are allowed to be purged. 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.

DOWNLOADING CONFIGURATIONS TO A REMOTE LOCATION

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

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



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

15 PHYSICAL SECURITY ADMINISTRATION

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

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

Setting Date and Time

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

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

Configuring and Viewing Logs

DataFort logs events in these categories:

- Security
- Operations
- Performance
- NAS Audit Trail

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 186 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**.
2. The default settings are in effect until they are changed. If you want log information to be stored remotely, indicate the storage location according to the instructions below.
3. Select the desired settings and then click Apply. Clicking Reset restores the default settings.

Setting and Enabling a Remote Storage Address

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

   Clicking Reset restores the default settings.

Recommended Configuration

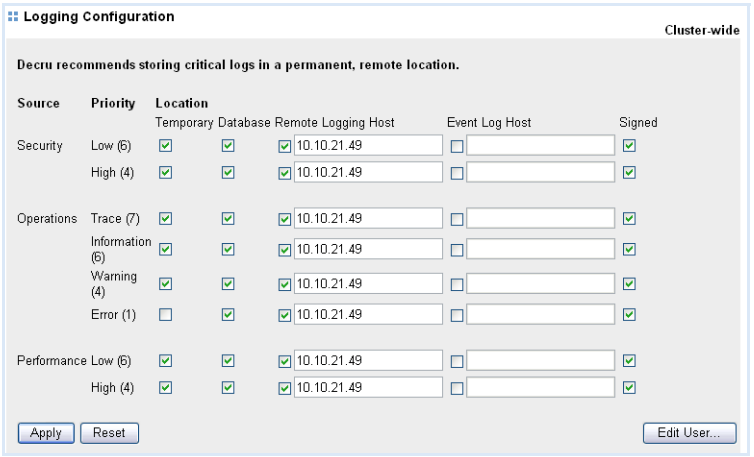
A recommended logging configuration will set DataFort to send secure DSS logs to multiple locations. For high security installations, configure DataFort logging as follows:

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

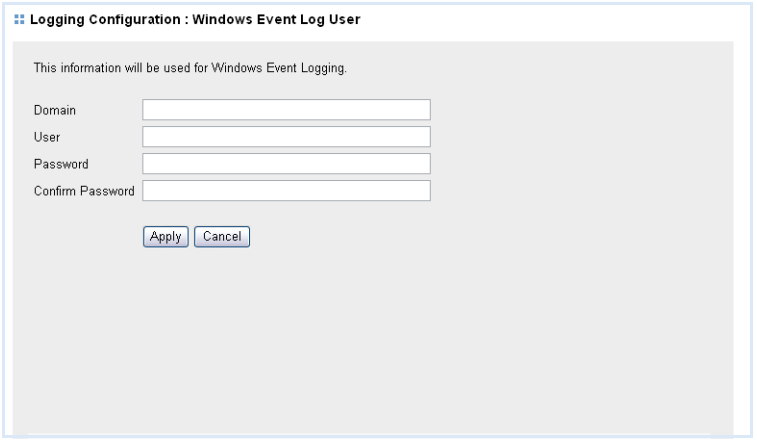
WINDOWS EVENT LOGGING

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

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



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

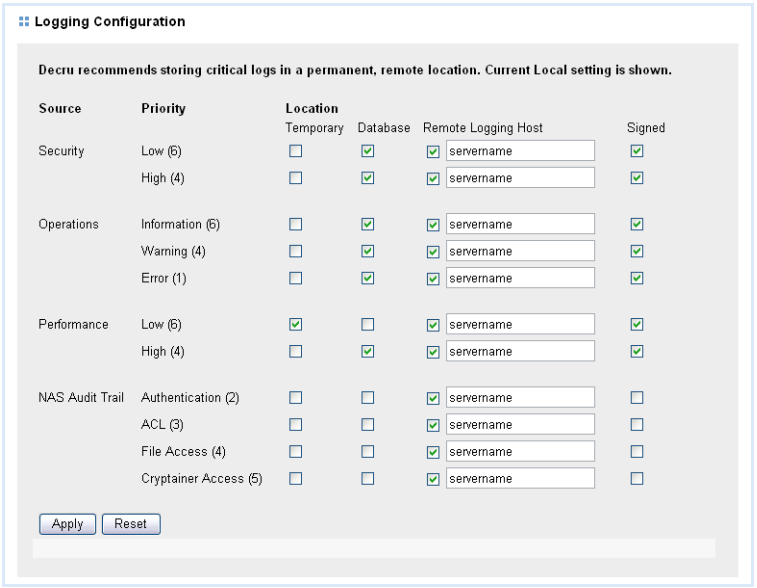


3. Enter information about the user who will log into the Windows host to generate the events including the domain to which that user belongs, and the name and password of the user. This user must have permission to log events to that host.
4. Click Apply.
5. Choose **System Config > General > Configure Log.**
6. In the Event Log Host column, check each box that should be logged to the Windows host and enter the IP address of the Windows host in these boxes.

   Note: It is a good practice to enter the same IP address for all event log host fields. Enter different IP addresses only if the user login is the same for all entered IP addresses.

7. Click Apply.

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



SETTING UP SYSLOG

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

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

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

```
local0.* /var/log/DataFort1
# local0 is for Security messages
local1.* /var/log/DataFort1
# local1 is for Operations messages
local2.* /var/log/DataFort1
# local2 is for Performance messages
local3.* /var/log/DataFort1
# local3 is for NAS audit messages
```

3. Signal syslogd to start receiving messages from DataFort.

Syslogd Mapping

Table 27 shows the Descriptive Name, System Property Name, Syslog Facility and Level mapping for DataFort logs.

TABLE 27: 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
nas audit authentication	sys.proc.syslogd.conf.nas_auth	local3.crit
nas audit acl	sys.proc.syslogd.conf.nas_acl	local3.err
nas audit file access	sys.proc.syslogd.conf.nas_file_access	local3.warning
nas audit Cryptainer access	sys.proc.syslogd.conf.nas_cry_access	local3.notice

Temporary Files Mapping

Table 28 describes the mapping for temporary logs.

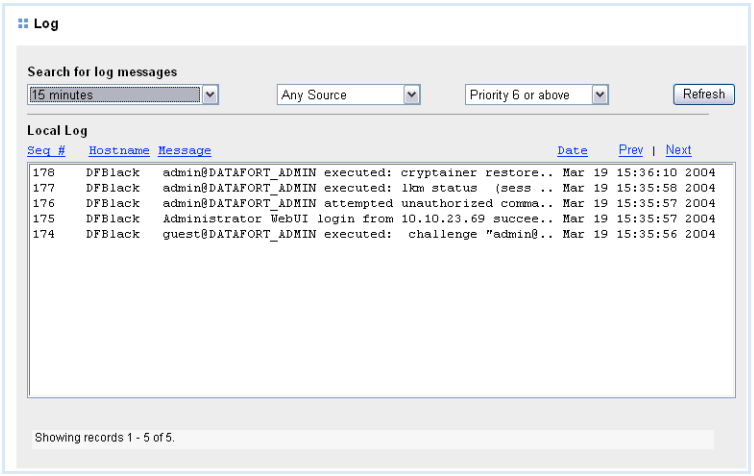
TABLE 28: TEMPORARY LOG MAPPING

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

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.

See Auditing Log Messages for information about using the log to spot unauthorized attempts to access data, and to verify that these attempts have been prevented by DataFort.

- To filter the view by time, select a display period from the drop-down menu at the left. You may display events from the last minute, 5 minutes, 15 minutes, 1 hour, 1 day, 1 week or Any Time Frame.
- To select a single type of event to view, select Security, Operations, Performance or NAS Audit Trail 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.

Auditing Log Messages

NAS auditing messages in the log show types of operations on the network, including failed and successful attempts by users to access data. Review the logs regularly to check for unusual activity. Table 29 provides samples of auditing messages that may appear in the log.

TABLE 29: AUDITING LOG MESSAGES

Activity	Sample Log Message
CIFS AUDITING	
Connection with server established	Established CIFS session with server SERVER.
Connection with server not established	Unable to establish CIFS session with server SERVER.
Local authentication of user succeeded	CIFS User DOMAIN\USER from IP 10.10.0.1 has been locally authenticated by the DataFort.
Local authentication of user failed	CIFS User DOMAIN\USER from IP 10.10.0.1 could not be locally authenticated by the DataFort.
User unknown to DataFort	A connection from CIFS User DOMAIN\USER from IP 10.10.0.1 has been rejected by the DataFort because the user is unknown.
User not registered	A connection from CIFS User DOMAIN\USER (from IP 10.10.0.1) has been rejected by the DataFort because the user has not yet registered.
File opened	User DOMAIN\USER from IP 10.10.0.1 has opened the file FILE in Cryptainer CRYPT
File open denied	User DOMAIN\USER from IP 10.10.0.1 was not allowed to open the file FILE in Cryptainer CRYPT
File created	User DOMAIN\USER from IP 10.10.0.1 has created the file FILE in Cryptainer CRYPT
File create denied	User DOMAIN\USER from IP 10.10.0.1 was not allowed to create the file FILE in Cryptainer CRYPT
File deleted	User DOMAIN\USER from IP 10.10.0.1 has deleted the file FILE in Cryptainer CRYPT
File deletion denied	User DOMAIN\USER from IP 10.10.0.1 was not allowed to delete the file FILE in Cryptainer CRYPT
File renamed	User DOMAIN\USER from IP 10.10.0.1 has renamed the file FILE to FILE2 in Cryptainer CRYPT.
File rename denied	User DOMAIN\USER from IP 10.10.0.1 was not allowed to rename the file FILE to FILE2 in Cryptainer CRYPT
Directory creation	User DOMAIN\USER from IP 10.10.0.1 has created the directory DIR in Cryptainer CRYPT.
Directory creation denied	User DOMAIN\USER from IP 10.10.0.1 was not allowed to create the directory DIR in Cryptainer CRYPT
Directory deleted	User DOMAIN\USER from IP 10.10.0.1 has deleted the directory DIR in Cryptainer CRYPT

TABLE 29: AUDITING LOG MESSAGES (CONTINUED)

Activity	Sample Log Message
Directory deletion denied	User DOMAIN\USER from IP 10.10.0.1 was not allowed to delete the directory DIR in Cryptainer CRYPT
NFS AUDITING	
Mount request granted	Mount access granted (uid=0, client=165.13.20.2, share=165.10.1.5:/homes/bob).
Mount request denied	Mount access denied (uid=0, client=165.13.20.56, share=165.10.1.5:/homes/bob).
Unmount request granted	Unmount access granted (uid=0, client=165.13.20.2, share=165.10.1.5:/homes/bob).
Unmount request denied	Unmount access denied (uid=0, client=165.13.20.56, share=165.10.1.5:/homes/bob).
File created	User UNIX\bob from IP 165.13.20.2 has created the file “myfile” in Cryptainer virt-server:/homes/bob.
File removed	User UNIX\bob from IP 165.13.20.2 has deleted the file “myfile” in Cryptainer virt-server:/homes/bob.

VERIFYING SIGNED LOG MESSAGES

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

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

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

If logs appear to be missing, compare the logs saved to separate remote locations (logs can be sent to up to four locations, as indicated in Recommended Configuration on page 186) 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 234.

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 LKM, LKM can provide a recent copy of the configuration database for recovery after zeroization.

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

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

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.

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

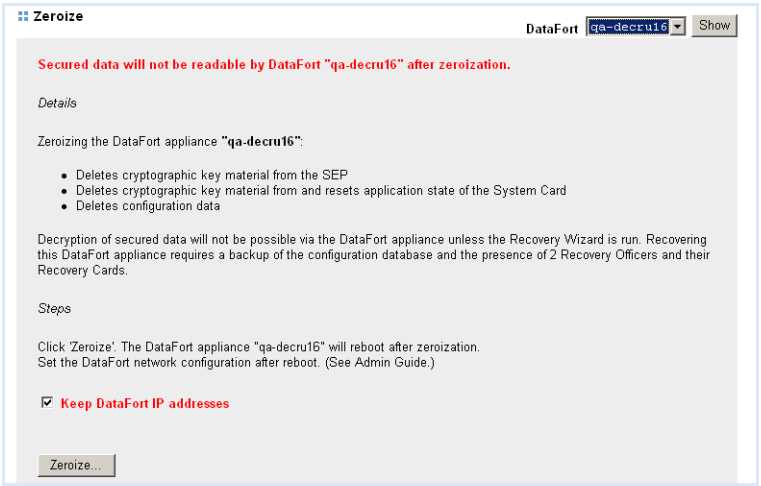
Zeroizing After Setup

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 185.

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 addresses box checked.



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

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

   DataFort will reboot.
5. 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 44.
6. 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 44.
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 74).
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 44.
6. After the DataFort has been assigned IP settings, complete the configuration by running the Setup Wizard.

Emergency Serial Console Port Access

If all Admin Cards and passwords for a DataFort are lost, it 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.

16 CLUSTER ADMINISTRATION

A cluster is created using the Setup Wizard. See Chapter 5 for instructions on completing the wizard. Note that standalone DataFort appliances cannot be joined together to form a cluster.

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

Cluster management tasks include:

- Cluster Management
- Setting Cluster Properties With the CLI

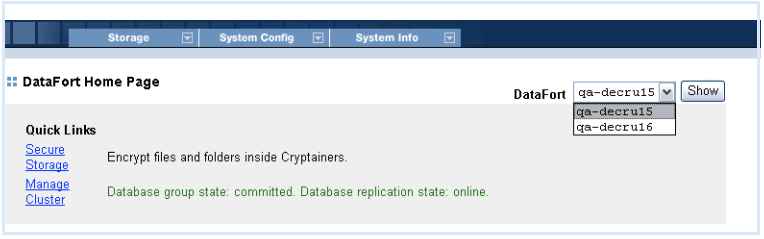
CLUSTER MANAGEMENT

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.

If one DataFort in the cluster goes offline, the remaining appliance will automatically take over operations. All cluster members keep the same configuration database.

CLUSTER-WIDE MANAGEMENT VIA WEBUI

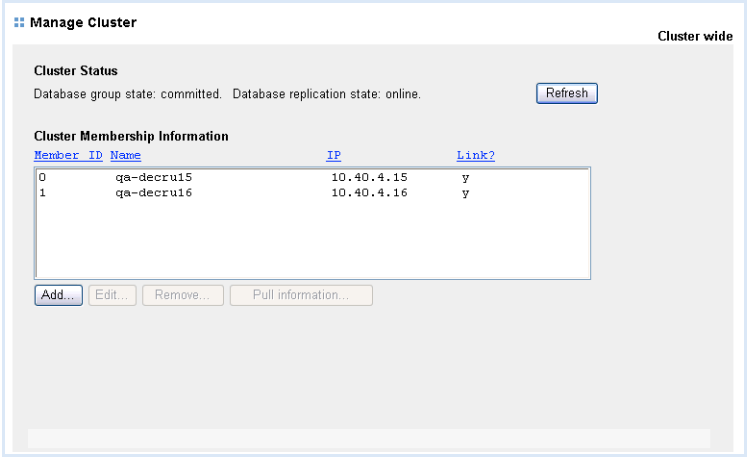
Most WebUI operations are cluster-wide and when completed on any member will apply to the entire cluster. The text **Cluster-wide** appears in the upper right corner of relevant WebUI pages to indicate this. Other settings are specific to individual DataFort appliances, but can still be set from any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



CHECKING THE 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, Changing the Clients NIC IP Address of a Clustered DataFort, Replacing a DataFort in a Cluster and Recovering a Cluster for details on using the WebUI to manage the cluster.



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

If the cluster is not in a committed/online state, some action may be required in order to resolve the cluster condition. Check Table 30 for a description of cluster states.

TABLE 30: 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

To create a cluster from the outset, follow instructions in Chapter 5 which describe how to initialize a standalone DataFort and then add a cluster member by running the Setup Wizard on another DataFort.

A DataFort can be removed from the cluster at any time. See Removing a Cluster Member. 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.

CHECKING FAILOVER STATUS

The cluster is in a normal state with respect to serving data when all VRIDs are serving their primary DataFort. The cluster is failed over when some or all VRIDs are serving a secondary DataFort instead.

A failed over cluster is indicated by:

- A red warning on the WebUI Home page, next to the Failover link.
- Entries in red in the Manage Failover screen. Click the Failover link on the Home page to see this screen.

Failover can be triggered intentionally in preparation for some operations on cluster members. Failover is also a normal response to some ordinary events, such as a reboot, a newly formed cluster, or a chassis intrusion. If the system property auto giveback is off (see Auto Giveback on page 205), you can easily recover the normal cluster state manually.

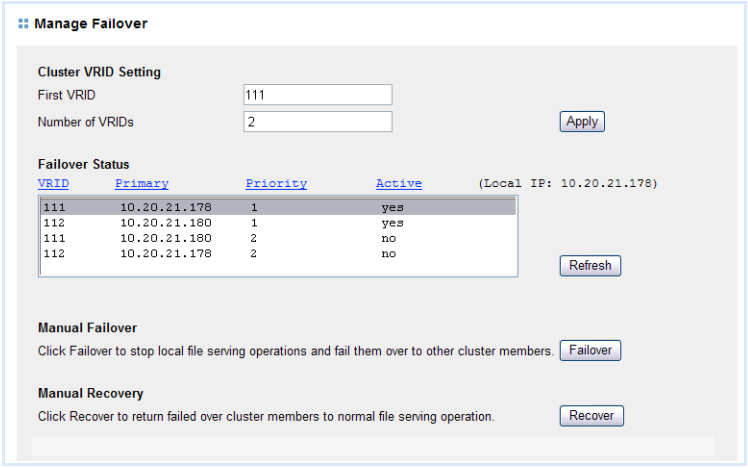
Recovering a Cluster from Failover

To recover from a failed-over cluster state:

1. Log in to the WebUI of a cluster member.
2. Click the Failover link on the Home page.

   You will see entries in red indicating VRIDs that are not served by their primary DataFort. The primary DataFort has been failed over.
3. In the Manage Failover screen, click Recover.
4. Verify the recovered cluster.

   When recovery is complete, the VRIDs will be served by their primary DataFort appliances (each VRID will have a different DataFort IP as primary) and there will be no entries in red in the Failover Status window. The Failover status line on the Home page will read “NAS clustering is running,” instead of showing a red alert.



Adding a Cluster Member

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

- A DataFort must be uninitialized when added to a cluster. Initialized standalone DataFort appliances cannot be joined to form a cluster. To zeroize an initialized DataFort so it can be added as a new cluster member, see Zeroizing the Decru DataFort on page 193.
- 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.
- 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.

Changing Configurations in a Cluster

Functioning DataFort appliances in a cluster share configuration information, including Cryptainers, servers, clients and security settings. Changing some settings requires suspending file serving operations while the change is being made. Use the manual failover feature to suspend file serving when making changes such as Changing the Clients NIC IP Address of a Clustered DataFort and Changing the VRID of a Clustered DataFort.

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.

1. Log in to the WebUI of the cluster member that will be removed from the cluster. (If the DataFort is offline or down, skip to step 5.)
2. Click the Failover link on the Home page.
3. In the Manage Failover page, click Failover. This will send all operations to the other cluster members.
4. Log out of the failed-over DataFort.
5. Power the failed-over DataFort down and remove it from the network, disconnecting the cables.
6. Log in to a remaining DataFort in the cluster, and click the Manage Cluster link on the Home page.
7. Select the offline DataFort in the Cluster Membership Information window.
8. Click Remove.

About Failing Over a Cluster

To halt the file serving operations on one or all DataFort members in a cluster (without breaking the cluster) use the Manage Failover page of the WebUI. If you wish to suspend operations on the entire cluster, fail all of the members over. Instructions to fail cluster members over are included in the instructions for each of the operations that require this action.

About Moving a Cluster

Moving a DataFort cluster to a different subnet can involve changing one or both of the IP settings, or changing the VRIDs of one or all DataFort appliances. File serving operations must be suspended while these changes are made.

Because a DataFort's Clients NIC is also its management IP, changing the IP setting of the Clients NIC is a non-trivial operation. Changing the network to which cluster members are connected on the client side involves halting all operations on the cluster members, changing the Clients NIC IP address, connecting the DataFort cluster members to the new network, changing all exported IP addresses, and restoring normal operation. If the File Servers NIC needs to be changed as well, this must be completed as a separate procedure after the Clients NIC is successfully changed.

Changing the Clients NIC IP Address of a Clustered DataFort

Note: If you are also changing the IP setting of the File Servers NIC, follow instructions for Changing the File Servers NIC IP Address of a Clustered DataFort after completing this procedure. You cannot change the File Servers NIC until the cluster is re-established using the new Clients NIC IP address.

1. Log in to the WebUI of the DataFort whose IP address you want to change. Click the Failover link on the Home page (or choose **System Config > Cluster > Manage Failover**).
2. Click Failover.
3. Choose **System Config > Network > IP settings**.
4. Change the Clients IP address.
5. Log out of the WebUI of this DataFort.
6. Log in to the WebUI of another cluster member. Click the Manage Cluster link on the Home page.
7. Select the DataFort with the changed IP information.
8. Click Edit.
9. At the prompt, enter the new IP information. Click OK.
10. Log back in to the WebUI of the cluster member with the newly changed IP. Click the Manage Cluster link on the Home page.
11. Wait until the status is committed/online.
12. Click the Failover link on the Home page (or choose **System Config > Cluster > Manage Failover**). Click Recover.

Changing the File Servers NIC IP Address of a Clustered DataFort

If you are also changing the IP address of the Clients NIC, do so before changing it for the File Servers NIC (see the previous procedure).

1. Log in to the WebUI of the DataFort whose IP address you want to change.
2. Choose **System Config > Network > IP Settings**.
3. Change the File Servers IP address.
4. Click Apply.

Changing the VRID of a Clustered DataFort

The following assumes a cluster of DataFort A and DataFort B. While you are changing a VRID in a cluster all file serving operations must be suspended.

1. Log in to the WebUI of DataFort A and click the Failover link on the Home page.
2. Click Failover.

   The Failover button only fails over the DataFort you are logged in to.
3. Log out of DataFort A.
4. Log in to the WebUI of DataFort B and click the Failover link on the Home page.
5. Click Failover.
6. Enter the initial VRID, and the number of VRIDs the cluster will use. If you are not sure about the number of VRIDs, use the number of DataFort appliances in the cluster (or just leave the number unchanged).
7. Click Apply.
8. In the Manage Failover screen, click Recover.

Changing the IPsec Secret of a Cluster

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

1. Log in to the WebUI of one cluster member.
2. Clicking the Manage Cluster link on the Home page (or choose **System Config > Cluster > Manage Cluster**).
3. Click Edit.
4. Enter and confirm the new IPsec secret.
5. Click Set.

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 44 and connect the new DataFort to the network.
11. Run the Setup Wizard for the new DataFort.

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 193).

- 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 202. 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:

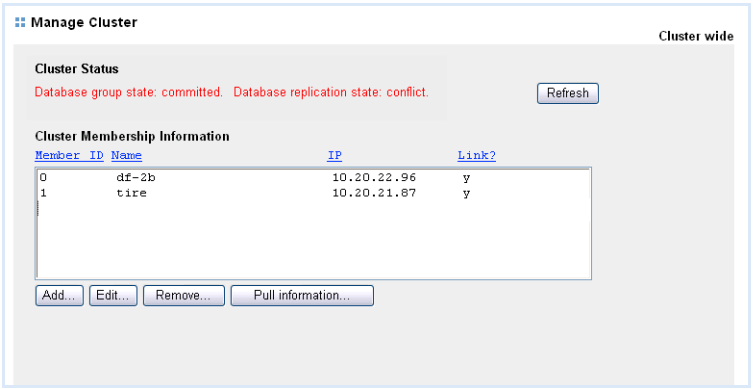
- A saved configuration database from the previous configuration.
- A valid cluster license from Decru for each DataFort unit.
- The minimum set of Recovery Officers and Recovery Cards required by the recovery schema selected when the original standalone DataFort was set up.

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 44.
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.



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."

Setting Cluster Properties With the CLI

You can use the DataFort CLI to set certain properties that affect the behavior of the cluster or monitor the cluster. See the following topics for useful commands:

- Configuring Cluster Members for STP
- Cluster Crypto Failover Command
- Auto Giveback
- Reviewing the Cluster Load Balance

Configuring Cluster Members for STP

Ethernet switches usually implement spanning-tree protocol (STP) which causes the switch to impose a holddown period when a link is detected on a previously disconnected Ethernet port. DataFort does not implement spanning-tree, therefore the best practice is to disable the STP holddown period altogether on switches connected to the DataFort network.

If STP holddown cannot be disabled for some reason, the DataFort must be configured with an estimate of the delay (in seconds) from the physical-layer link-up event until the switch will forward traffic in both directions.

By default, the DataFort is set to delay 15 seconds. If this delay is sufficient for the switch to which DataFort is connected, leave it unchanged. To view the delay setting, use the following CLI command:

```
system property get net.inet.ip.stp_holddown
```

This will return the current delay setting of `15`.

Note that since each cluster member should be connected to a different switch, each DataFort in the cluster may require a different delay setting. To increase the delay to 30 seconds, use the following CLI command:

```
system property set net.inet.ip.stp_holddown 30
```

You will see a verification of the command:

```
NOTICE: Property 'net.inet.ip.stp_holddown' was modified.
```

CLUSTER CRYPTO FAILOVER COMMAND

A DataFort cluster member will automatically stop serving clients if an intrusion is detected or a fatal failure is detected in the SEP. To disable this setting, use the following CLI command:

```
system property set nas.cluster.crypto_failover false
```

In this case, automatic failover will not be performed upon detecting either of these conditions, and since cryptographic operations will be disabled, clients will be refused service until the administrator resets the intrusion status or triggers failover from the CLI (by using **`cluster failover`**) or the WebUI (using the Failover button accessed by choosing **System Config > Cluster > Manage Failover**).

AUTO GIVEBACK

By default, when a DataFort in a cluster is powered up after being powered down (for example if it is power-cycled during normal operation), it will not start serving its primary VRID automatically. Instead, the secondary DataFort for that VRID will go on serving it until it receives an explicit **`cluster giveback`** command. This behavior is recommended for production environments.

To change this setting, use the following CLI command:

```
system property set nas.cluster.auto_giveback true
```

If all DataFort appliances in a cluster have the property **`nas.cluster.auto_giveback`** set to **`true`**, the cluster redistributes the load when the offline DataFort comes back online. This setting may cause more interruptions in service in some situations, and therefore is not the default and is not recommended for high-availability configurations.

REVIEWING THE CLUSTER LOAD BALANCE

The **`system load list`** command produces a list of the average NFS, CIFS, and iSCSI traffic on DataFort VIPs. To view the system load table, use the following CLI command:

```
system load list
```

View the resulting table to see the traffic load per VIP. If the traffic reported is too much or too little on a certain VIP, you may want to make modifications including:

- Splitting traffic up between VIPs or additional DataFort appliances.
- Purchasing more DataFort appliances.

17 MACHINE ADMINISTRATION

Machine administration includes tasks that allow network properties to be set and DataFort upgrades to be executed.

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

Note: A specified Machine Administrator can also add a new member to a cluster, as described in Cluster Administration on page 196.

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

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

Only a Full Administrator can manage SNMP:

- SNMP Settings

Note: DataFort appliance Date and Time can only be set by a Full or Security Administrator. See Setting Date and Time on page 185.

Network Settings

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

> **Note:** These instructions are for standalone DataFort appliances. For instructions on changing clustered DataFort network settings, see Changing the Clients NIC IP Address of a Clustered DataFort on page 200.

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 Clients IP address, you will lose connection to the WebUI and will need to log back in to the new IP address.

Some other reconfiguration may be necessary if the File Servers NIC changes, and the file servers are not reachable from the new subnet. The file servers or appropriate routers will need to be reconfigured. In addition, if the IP addresses of the file servers change, then the (real) IP addresses of those file servers stored on the DataFort will need to be updated. See Managing Servers on page 105.

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.

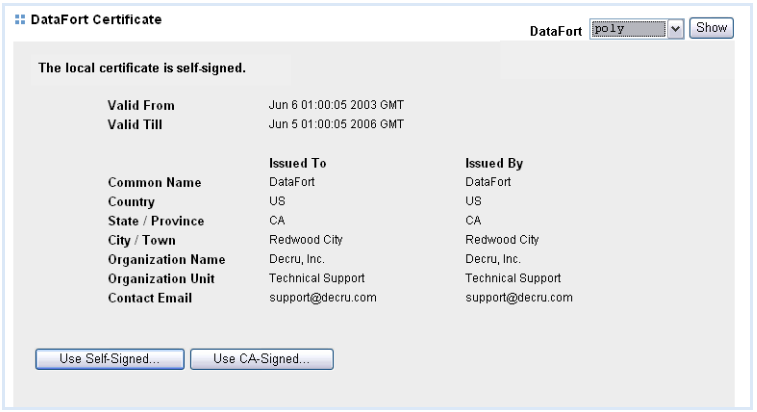
SETTING SECURITY CERTIFICATES

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 211. Keep the following in mind:

- A certificate must be generated independently for each DataFort in a cluster.
- Create the certificate and then use it until its expiration date.
- Only a Full Administrator can set the security certificate

SETTING A LOCAL SECURITY CERTIFICATE

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



2. Click Use Self-Signed.



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

3. Enter the information for the locally signed certificate. This information will appear when certificate details are viewed.

   Note: Country codes are established by the International Organization for Standardization (ISO). For a partial list of country codes, see Partial List of ISO Country Codes on page 289.

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

   The certificate warning appears.

8. Click View Certificate.

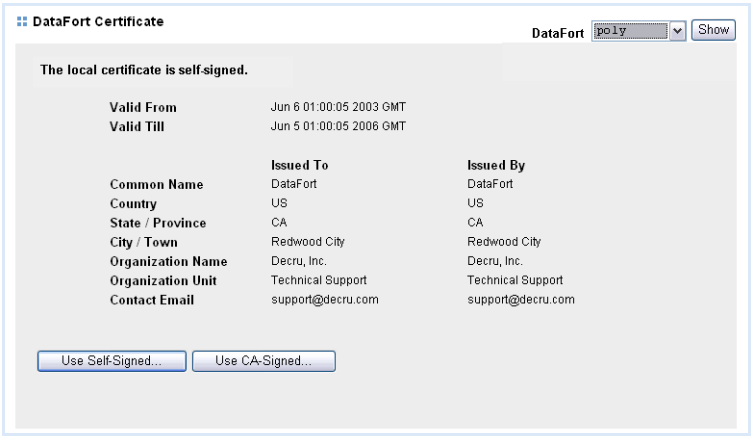


9. Click Install Certificate.
10. Complete the Install Certificate Wizard.

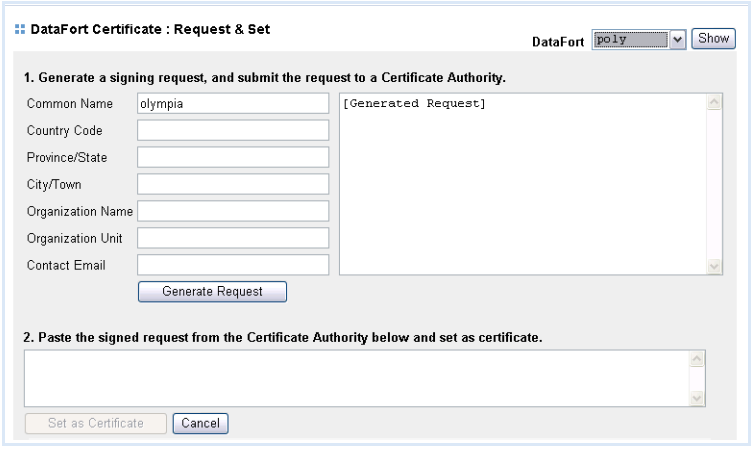
    The certificate has been installed. When you connect to the WebUI, no security certificate warning should appear; instead you will see a valid certificate message.

SETTING A CERTIFICATE AUTHORITY SIGNED CERTIFICATE

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



2. Click Use CA-Signed.



3. Enter the required information into the fields provided and click Generate Request. This generates a PEM-encoded request which can be submitted to a known certificate authority such as VeriSign or a local certificate authority.

   Note: Country codes are established by the International Organization for Standardization (ISO). For a partial list of country codes, see Partial List of ISO Country Codes on page 289.

4. When you receive the signed request from the CA, paste it into the box provided. Cut and paste the entire contents of the certificate file, including the BEGIN and END lines.

5. Click Set as Certificate.
6. Log out of the WebUI.
7. Open an HTTPS connection to the DataFort.

   The certificate warning appears.
8. Click View Certificate.



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

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

MANAGING LICENSES

DataFort features (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.

SNMP Settings

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

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

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

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

Enabling SNMP

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

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

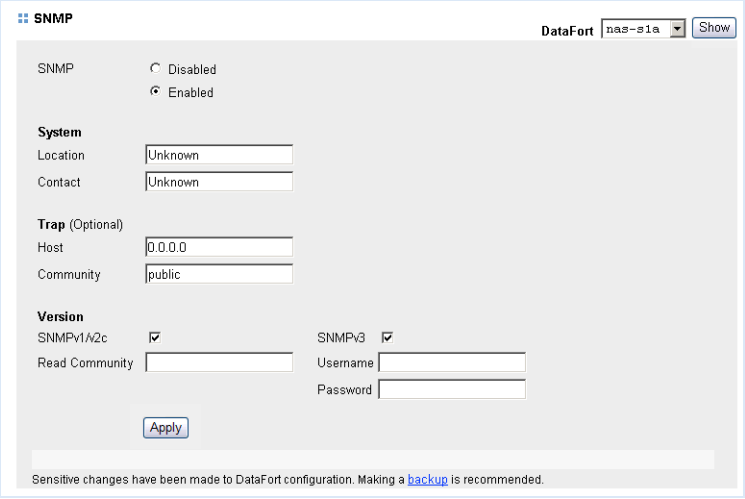
SNMP Configuration

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

System location	sysLocation.0 under MIB-II. A description of the physical location where the device is installed or operating.
System contact	sysContact.0 under MIB-II. The contact information for the person or organization responsible for managing the device.
SNMP parameters	Read Community: community string used to read SNMP MIB. Trap Host: hostname (or IP address) which SNMP traps are sent to. Trap Community: community string used to send SNMP traps.

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

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



System

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

Trap

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

Version

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

18 DataFort Appliance Settings and Status

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

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

Viewing Settings in the WebUI

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

- View DataFort Logs
- View DataFort Throughput and CPU Usage
- View 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 or NAS Audit Trail 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 186.

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 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.

19 DECRU MANAGEMENT CONSOLE FUNCTIONS

The Decru Management Console (DMC) is the only interface for running the Setup Wizard for a DataFort appliance. It also provides an alternate interface for some DataFort management functions generally performed from the DataFort WebUI. If Lifetime Key Management appliances are in use, the DMC can be used to manage both LKM and DataFort appliances from a central location.

Note: The DMC is the sole management interface for the Lifetime Key Management (LKM) Appliance. For full documentation of the DMC, see the *LKM Appliance Administration Guide*.

The console menus provide tools for the following:

- Appliance Management
- License and Administration Management
- Logging Configuration

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

APPLIANCE MANAGEMENT

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

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

   Once an appliance is added to the Decru Management Console, icons show appliance status. Table 31 shows possible state displays.

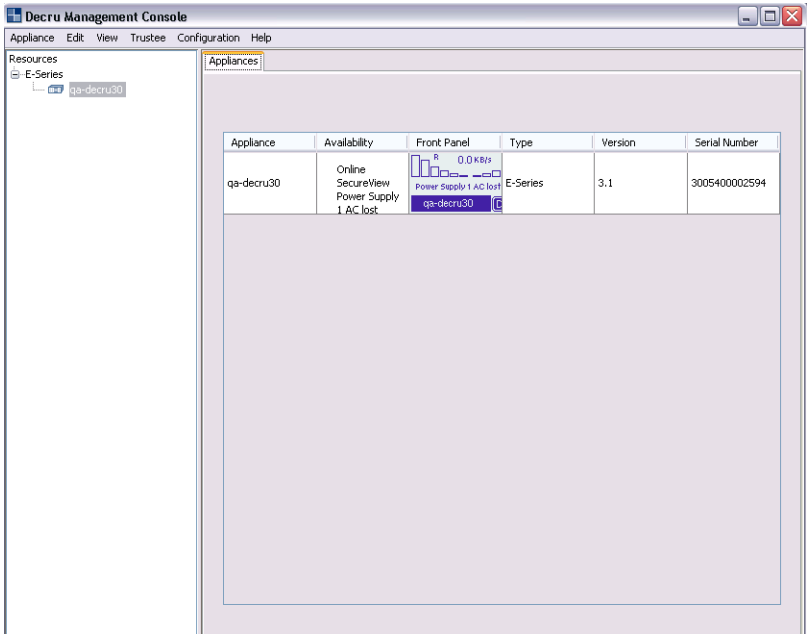


TABLE 31: APPLIANCE STATUS INDICATORS

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

Adding an Appliance

Use the Appliance menu to add an LKM or DataFort appliance so it can be managed by the console.

1. Choose **Start > Programs > Decru > Decru Management Console**.
2. Choose **Appliance > Add**.

   The Add... pop-up screen appears.
3. Enter the IP address or hostname of the appliance.

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

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

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

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

Logging into Appliances

Log into an appliance after it has been added.

1. Select an appliance in the Resources pane and choose **Appliance > Login**.
2. Enter the administrator name and associated password at the Login page and click OK.

   If the correct credentials were entered and the appliance is correctly configured, the status of the appliance will change to online. See Appliance Status Indicators on page 220 for information about status icons.

Removing an Appliance

Remove an appliance from the Management Console.

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

Running the Setup Wizard

Use the wizard to configure LKM and DataFort appliances.

1. Select an appliance in the Resources list and choose **Appliance > Setup**.
2. Run the wizard for the appliance. See Initializing DataFort Appliances on page 47 for detailed instructions.

Verifying an Upgrade Package

Verify an upgrade package before running it on the appliance.

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

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

Upgrading an Appliance

Upgrade the appliance version with an upgrade package from Decru.

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

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

Backing Up an Appliance

Back up the configuration database of the selected appliance.

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

Creating Trustees

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

Use the DMC to set up trustees. See Managing Trustees on page 153 for instructions.

Viewing Details

Shows the system version information for the appliance.

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

Accessing DataFort WebUI

Opens the WebUI for the DataFort appliance.

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

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

Accessing Command Line Interface

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

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

   The CLI will open. See CLI Administration on page 229 for commonly-used commands.
2. Enter the command into the field provided.
   - Click Execute to execute the command. The command will be run on all selected appliances and the output returned on the screen.
   - Click File to open a command file to run on the selected appliances. The commands will be run when the file is opened. Note that the file must be an XML formatted file.
   - To save the output of a command that has been executed, click Save and save the file in a designated location.

Collecting Tech Support Info

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

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

Rebooting Appliances

Reboots selected appliance.

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

Zeroizing Appliances

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

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

Exiting the Console

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

License and Administration Management

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

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

Managing Licenses

To view the licenses on selected appliances:

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

  All known licenses for the selected appliances appear.

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

Adding a License

To add licenses to selected appliances:

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

2. Enter the license into the provided field and click Apply.

   All known licenses for the selected appliances appear.

MANAGING ADMINISTRATORS

To view the administrators with permission to manage selected appliances:

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

   All known administrators for the selected appliance appear.

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

Adding an Admin Card to an Administrator

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

Removing an Admin Card from an Administrator

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

Deleting an Administrator

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

ADDING AN ADMINISTRATOR

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

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

   The Add Administrator page appears.

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

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

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

Specialty administrators can be used to separate tasks for increased security. The roles have separately defined permissions, ensuring that administrators only have permission to execute certain designated commands. If desired, compound administrators possessing the characteristics of more than one speciality administrator can also be created. See Administrator Roles on page 78 for more information about administrator roles.

LOGGING CONFIGURATION

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

- Security
- Operations
- Performance

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

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

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

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

   The Logging Configuration page will appear.

2. Select the desired settings and then click Apply.

DECRU MANAGEMENT CONSOLE MENUS

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

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

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

APPLIANCE MENU

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

Add	Add an appliance to the Management Console. See Adding an Appliance on page 221.
Remove	Remove an appliance from the Management Console.
Log in	Log in to an appliance as an administrator. See Logging into Appliances on page 221.
Log out	Log out of an appliance as an administrator.
Set up	Set up an LKM or DataFort appliance by running the Setup Wizard. See Initializing a Standalone DataFort or DataFort Cluster on page 49.
Verify	Verify the validity of an upgrade package before upgrading. See Verifying an Upgrade Package on page 221.
Upgrade	Upgrade an appliance. Upgrades should be done only after consulting Decru support. See Upgrading an Appliance on page 222.
Back up	Back the configuration database up as a file to a specified location. See Backing Up an Appliance on page 222.
Details	Shows the system version for the selected appliance. See Viewing Details on page 222.
WebUI	Opens the WebUI of the selected appliance (DataFort only). See Accessing DataFort WebUI on page 222.
Command Line	Opens the CLI. Whatever command is run will be executed on all selected appliances. See Accessing Command Line Interface on page 222.

Collect Tech Support Info	Creates a file containing information useful to technical support when troubleshooting for the selected appliance. The file is by default placed in the tech support folder of the Decru Management Console directory. See Collecting Tech Support Info on page 223.
Reboot	Reboot the selected appliance. See Rebooting Appliances on page 223.
Zeroize	Zeroize the selected appliance. See Zeroizing Appliances on page 223.
Smart Card Utilities	Resets a smart card and displays card information.
Exit	Exit the Management Console. See Exiting the Console on page 223.

Edit Menu

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

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

View Menu

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

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

Trustee Menu

A trustee relationship between two appliances allows encryption keys to be shared between those appliances even if they have no Recovery Cards in common, and are not on the same network. Trustees send messages to establish a relationship before key sharing. The first message is the Trustee Establishment Package (TEP). The second message is the Trustee Acceptance Package (TAP).

Start Trustee Creation	Starts the process of creating a trustee for selected appliance. See Creating Trustees on page 222.
Receive TEP	Allows selected appliance to receive a Trustee Establishment Package. See Creating Trustees on page 222.

Receive TAP	Allows selected appliance to receive a Trustee Acceptance Package. See Creating Trustees on page 222.
Unapproved Trustee List	Displays list of trustees not yet approved (waiting to accept a TAP). See Creating Trustees on page 222.
Trustee List	Displays list of trustees. See Creating Trustees on page 222.

CONFIGURATION MENU

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

License	View licenses. See Managing Licenses on page 223.
Add License	Add licenses. See Adding a License on page 223.
Administrators	View and manage administrators. See Managing Administrators on page 224.
Add Admin	Add an administrator. See Adding an Administrator on page 224.
Log Configuration	See Logging Configuration on page 225
Replace Recovery Officer	The Configuration Menu offers the Replace Recovery Officer menu. This allows you to replace a Recovery Card in the set, thereby replacing the associated Recovery Officer as well. See Removing an Administrator on page 87 for instructions on using the DataFort WebUI to manage administrators. To replace a recovery card using DMC, refer to the *LKM Appliance Administration Guide.*

HELP MENU

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

20 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.

- See Using the CLI for an overview using the CLI.

Frequently used procedures are described in this chapter, including:

- Administration Commands
- CLI Management for NFS Cryptainers
- CLI Management for Multi-Protocol Cryptainers
- CLI Management for CIFS Cryptainers
- CLI Management for iSCSI Cryptainers
- Restoring a Cryptainer
- Special 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 268 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 example, file servers with shares must be added to the configuration database before Cryptainers can be created. 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 71). 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

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:

nas-readonly-admin	Read Only Administrator
nas-machine-admin	Machine Administrator
nas-backup-admin	Backup Administrator
nas-storage-admin	Storage Administrator
nas-key-admin	Key Administrator
nas-physical-security-admin	Security Administrator
nas-datafort-account-admin	Admin Account Administrator
nas-admin	Full Administrator
nas-user-admin	User Administration

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 cluster, as well as a list of member DataFort appliances, their IPs and member IDs. Shows current status of the cluster as well as the IP addressees of each cluster member.
cluster config	Cluster configuration commands.
cluster enable	Enables clustering. This command breaks any pre-existing cluster connectivity and forces a re-negotiation of the cluster.
cluster rexec	Allows commands to be issued remotely to all other DataFort appliances in the cluster as identified by IP address or name.
cluster rsh	Connects directly to another member of the cluster as identified by IP address or name. The **ctl-d** command breaks out of this into the previous shell.
cluster disable	Allows the temporary removal of a cluster member without having to run a wizard in order to reintroduce the cluster member. This is useful if a DataFort appliance needs to be moved or isolated for servicing. There is no indication in the WebUI that the member has been disabled. To disable a member, log into another member of the cluster and execute the **cluster disable <member-ip or name>** command, identifying the DataFort to be removed by name or IP address. To allow the member back into the cluster, execute the **cluster enable <member-ip or name>** command from another cluster member.
cluster giveback	To cause the DataFort on which the command is executed to stop hosting VRIDs for which it is not primary:
cluster failover	To cause the DataFort on which the command is executed to stop hosting all VRIDs, and stop advertising that it can host VRIDs:
cluster comeback	Issuing **cluster comeback** after a **cluster failover** causes the DataFort on which the command is executed to start advertising that it can host VRIDs. It doesn't automatically start hosting VRIDs which some other DataFort in the cluster is hosting unless the auto giveback property is set to true: **system property set nas.cluster.auto_giveback true.** For more information, see Auto Giveback on page 205.
cluster config vrid list	To display which DataFort appliances are primary, secondary, and hosting which VRIDs

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 <msg>
   ```

2. Single quotes, double quotes, and backslashes in the message must be preceded with a backslash and the entire message must be surrounded by double quotes. For example, to verify the following log message, execute the **system log verify** command that follows the log message:

   ```
   2004-02-10 16:21:22 Local1.Info 10.20.21.163 Feb 10 16:21:22
   boxmanager: Executed: share virtual add --ip "his" \\\\his\\chi
   "nas-hiro1" (sess id: 228933632)  [AAAAAEMAAAAFAAAAgnUpQA== 3NKQl8/
   5r3x6n+Rw]
   ```

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

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

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

This returns:

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

Execute the verification procedure again to check sequence validity:

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

This returns:

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

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

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

Stack Trace Settings

DataFort has the capability to dump a trace of the platform execution stack in the event of a kernel panic. This stack trace information is useful for debugging, but may expose DataFort state information. Decru does not believe that this information poses a security risk or leaks any user or critical data, as no function arguments are leaked in the trace. However, the administrator should determine whether or not stack trace dumps should be enabled. To change the stack trace setting, log into the CLI and execute the appropriate **system property** command:

Stack trace is on by default. To disable stack trace:

```
system property set sys.stacktrace.enabled 0
```

To enable stack trace:

```
system property set sys.stacktrace.enabled 1
```

To retrieve a stack trace:

```
system util stacklog
```

Network Management

The following network commands are useful in managing the network:

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

Backup Management

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

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

CLI Management for NFS Cryptainers

Prepare to create Cryptainers:

- From the operating system you are using to administer NFS, create exports on network servers, and set permissions. See Create NFS Exports on page 96
- Use the Security Settings page of the DataFort WebUI to modify the management settings and group review settings of DataFort. See Setting Security Options on page 166.

The following sections provide examples of creating, configuring and managing Cryptainers in the NFS environment.

NFS Administration Example

The next sections describe a sample installation which assumes the following conditions:

- One NIS domain called nfsdomain
- One LDAP domain called myldap
- One server called server1 with one empty share /share1 which is exported as a Cryptainer called secure_share1
- One user with username user1 with Unix id, GID 100,100 (with password: defaultpass)
- One user with username user2 with Unix id, GID 200,200 (with password: defaultpass)
- One user with username user4 with Unix id, GID 502,502 (with password: user4s_password)

Manage Domains

Add domains that include the servers that will host Cryptainers. The basic domain commands allow domains to be added and deleted. This section includes commands to add NIS and LDAP domains.

Note: These are sample commands. For a list of domain-related commands and command syntax, type `domain ?` into the CLI.

Add an NIS Domain

- Add an NIS domain that includes servers where exports that will become Cryptainers are located:

```
domain add [-u user -p password] nfsdomain nfs nis
```

The username and password are optional for NFS NIS domains. When you enter the access user name and password, DataFort will create the root user account automatically.

DataFort requires the root user to mount exports and create Cryptainers on file servers. Other users are imported from the NIS automatically as Cryptainers are created for them.

Add a Local Domain

Local NFS domains are similar to a local passwd file on a Unix host. The administrator can add users to a local NFS domain, and use that domain for permission-checking on NFS requests.

1. Add a local NFS domain:

```
domain add localnfsdomain nfs local
```

2. Add users to this domain:

```
user add --domain localnfsdomain --id 502,502 --password
user4_password nas-user user4
```

Once an NFS request is forwarded to a server, its relation to DataFort NFS domains (local or NIS) disappears. The request will be authenticated with the server's passwd file or NIS domain using the request's UID and GIDs. It is a good practice to keep the server's set of users synchronized with that on DataFort, either by using the same NIS domain as a source of user information, or by manually synchronizing the local NFS domain on DataFort with the list of users defined on the server.

Note: DataFort supports multiple NIS and local domains which can have overlapping UID/GID ranges. To avoid confusion, it is preferable that a virtual IP address in a specific NFS domain hosts shares only from back-end servers that have the same set of users in their domain.

Add an LDAP Domain

Adding an LDAP domain is the same as adding an NIS domain, except that the DataFort domain access user name and password must to be specified when the domain is added.

- Add an LDAP domain, specifying the DataFort domain access user (see Adding the DataFort Domain Access User on page 36):

```
domain add -u user -p userpassword --server ldapserver.company.com
myldap nfs ldap
```

Verify Domains and Users

1. Verify that the domain was added to the database:

```
domain list
```

2. Verify that the users were added to the database:

```
user list
```

Remove a Domain

- Remove a domain:

```
domain remove mydomain
```

DIsable Automatic Domain Controller Discovery

By default DataFort will auto-discover domain controllers in added domains. It is possible to disable auto-discovery to prevent DataFort from using unspecified domain controllers to connect to a domain. Using the feature in domains that span many sites can limit network traffic to nearby sites and reduce network congestion.

To prevent auto-discovery of domain controllers, issue the following command:

```
system property user.domain.sync.no_autodiscover 1
```

To revert to the default and allow auto-discovery:

```
system property user.domain.sync.no_autodiscover 0
```

MANAGE SERVERS

Add servers where shares that will become Cryptainers are located. Basic server commands allow servers to be added and deleted.

Note: The following are examples of command usage. For a list of server-related commands, type `server ?` into the CLI.

Add a Server and Verify

1. Add a server to the DataFort configuration database. Indicate either the name or IP address of the server:

   ```
   server add --nfs-domain nfsdomain server1
   ```

2. Verify that the server was added to the database:

   ```
   server list
   ```

Change Server Settings

- Change settings, such as name, domain(s), IP address. For a list of settings and options for this command, type `server set?` in the CLI.

  ```
  server set --ip 10.20.22.138 server1
  ```

Remove a Server

- To remove a server from the configuration database, indicate the server name or IP address:

  ```
  server remove server1
  ```

Manage Virtual Servers

1. Add a virtual server (VIP):

   ```
   vip add [--nfs-domain mynfsdomain] myvirtualserver
   ```

2. Remove a virtual server (VIP):

   ```
   vip remove myvirtualserver
   ```

3. List virtual servers:

   ```
   vip list
   ```

4. Change the properties of a virtual server (VIP):

   ```
   vip set myvirtualserver
   ```

   To see the properties you can change, type `vip set ?` in the CLI.

MANAGE SHARES

Add shares located on the servers that have been added. These shares will become Cryptainers. Basic share commands add and delete shares, and assign some access control settings at the share level.

Note: The following are examples of command usage. For a list of share-related commands, type `share ?` into the CLI.

Add a Share and Verify

1. Add shares that exist on a server which is in the DataFort configuration database. Indicate the server where the share is located and the real name of the share:

   ```
   share add server1:/share1
   ```

2. Verify that the share was added to the database:

   ```
   share list
   ```

Remove a Share

- To remove a share, indicate the real name of the share:

  ```
  share remove server1:/share1
  ```

Place Restrictions on Share Access

- To indicate exactly which clients can have mount access to a given share, associate the share with the IP addresses of the permitted clients:

  ```
  share grant mount server1:/share1 10.10.20.168
  ```

Remove Restrictions on Share Access

- To remove limitations on the IP addresses of clients that have access to a given share:

  ```
  share revoke mount server1:/share1 10.10.20.168
  ```

Virtualize a Share

1. Virtualize a share:

   ```
   share virtual add --nfs-virtual-name newnfsname server1:export1
   virtualserver
   ```

2. Change the virtualize settings for a share:

   ```
   share virtual set --nfs-virtual-name newnfsname
   virtualserver1:virtualexport1
   ```

3. Stop virtualizing a share:

   ```
   share virtual remove virtualserver1:virtualexport1
   ```

MANAGE CRYPTAINERS

Basic Cryptainer commands add and delete Cryptainers, and assign access control settings. All Cryptainer commands now specify the real path, not the virtual path.

Note: The following are examples of command usage. For a list of Cryptainer-related commands, type `cryptainer ?` into the CLI.

Create a Cryptainer at the share level, specifying ownership of the share at the time of creation.

- If the Cryptainer is a directory inside a share which has already been mounted, no other access control settings need to be applied.
- If the Cryptainer is a whole share, the owner may need to grant root access in order to allow the Cryptainer to be mounted as a share. See Manage Cryptainer ACL on page 240.

The administrator who is logged in can create a Cryptainer for a user, but cannot grant access to a Cryptainer unless the administrator owns that Cryptainer. If the administrator does not specify a user at the time of Cryptainer creation, the administrator is the default owner of that Cryptainer.

Type **`cryptainer add ?`** for a list of options you can specify when the Cryptainer is created.A few examples are provided below.

Create a Cryptainer

1. Create a Cryptainer for a known share, omitting the owner field to specify that the administrator logged in to the CLI is the owner of the Cryptainer:

   ```
   cryptainer add server1:share1
   ```

2. Alternatively, specify another owner:

   ```
   cryptainer add --owner user1@nfsdomain server1:share1
   ```

   This will create the Cryptainer and add the owner (user1) to the configuration database.

3. Verify that the Cryptainer was added to the DataFort configuration database:

   ```
   cryptainer list
   ```

Create a Cleartext Cryptainer

It is possible to leave the contents of a Cryptainer in cleartext (unencrypted) form. This will allow you to manage the access control for the share using the DataFort, but will not require that the data in the share be encrypted. This might be useful if the following scenarios apply in your environment:

- You want to use DataFort only to strengthen the ACL on a share, not to encrypt its contents.
- You do not want to encrypt data that existed before DataFort was installed in the environment.

  Note: Cleartext Cryptainers are only supported with NFS v3. Clients using NFS v2 will get a permission denied error when attempting to access a cleartext Cryptainer.

- To create a Cryptainer with unencrypted content:

  ```
  cryptainer add --dataenc off server1:share1
  ```

Manage Cryptainer ACL

Access control for a Cryptainer is set by its owner. In environments where clients and servers are configured to require that root mount shares to make them accessible to users, root access to a Cryptainer must be granted by the owner of that Cryptainer.

If the entire share is a Cryptainer, the root user must be granted access to the Cryptainer in order to mount the Cryptainer. However, if the Cryptainer is actually a directory inside a share (which can already be mounted by root), the user can access the Cryptainer without granting access to root.

Note: If DataFort is configured for Secure CLI (see Management Security Settings on page 169) users will not be able to access the CLI to grant access to Cryptainers they own.

1. In this example, the owner of the Cryptainer (user1) allows the root user to mount the Cryptainer, by granting access to the root user. The root user does not need full access to the share, so granting read permission is sufficient.

   For this, the command is:

```
cryptainer grant read server1:share1 user1@nfsdomain
```

User1 now owns a Cryptainer and has granted root access to the Cryptainer so it can be mounted. User1 can also use this access control command to grant other nas-users access.

2. The owner of the Cryptainer grants user2 access to the Cryptainer:

```
cryptainer grant access server1:share1 user2@nfsdomain
```

3. View access control settings on Cryptainers:

```
cryptainer acl list
```

4. Revoke access to a Cryptainer:

```
cryptainer revoke access server1:share1 user2@nfsdomain
```

5. Grant group access to a Cryptainer:

```
cryptainer grant access server1:share1 group@nfsdomain
```

6. Revoke group access to a Cryptainer:

```
cryptainer revoke access server1:share1 group@nfsdomain
```

Set the DCS Requirement on a Cryptainer

- You can use `cryptainer set` to specify options on an existing Cryptainer, such as an IPsec or DCS requirement. To set the DCS requirement on an NFS share:

```
cryptainer set --dcs on server2:share1
```

Note that this requirement can also be set by the end user who owns the Cryptainer.

Submounting Shares

Submounting mounts an NFS export inside the advertised export. You can submount outside a Cryptainer, at the Cryptainer level, or within a Cryptainer. The only restriction is that you may not submount inside a Cryptainer using filename encryption. The client will see “permission denied” or “access denied” if it tries to perform such a mount operation.

1. Be sure the `plaintext` property is set to off:

```
system property set sys.security.nfs.plaintext off
```

2. Create a Cryptainer:

```
cryptainer add --owner user1@nfsdomain server1:share1
```

3. Create a Cryptainer within the existing Cryptainer, using the submount path:

```
cryptainer add --owner user1@nfsdomain -a on server1:share1/
subdir1/subshare1
```

Root user can mount directly to the submounted share. Permissions are inherited from the main Cryptainer.

Remove a Cryptainer

- To remove a Cryptainer from the configuration database:

```
cryptainer remove server1:share1
```

GROUP REVIEW

Group Review enables the DataFort administrator to review and approve group, user, or group membership additions. To enable or disable Group Review, go to the Security Settings page of the WebUI and make the desired change. See Domain Controller Related Settings on page 167 for instructions.

When Group Review is on, the administrator can review changes using the following CLI commands:

- To view users that have been added to groups since Group Review was turned on, but have not yet been confirmed:

  ```
  user group list --uflags comers
  ```

- To view groups that have been added to other groups (nested groups) since Group Review was turned on, but have not yet been confirmed:

  ```
  group group list --flags comers
  ```

- To confirm additions to groups in the configuration database, including users and nested groups:

  ```
  user comers confirm
  ```

- To view users in the database who currently have access to Cryptainers:

  ```
  user group list --uflags normal
  ```

- To view all users in the database:

  ```
  user list
  ```

CLI Management for Multi-Protocol Cryptainers

You can use the DataFort CLI to create Cryptainers for a combination CIFS and NFS environment. Note that multi-protocol Cryptainers must be created at the share level.

Note: In the DataFort CLI, shares, servers and Cryptainers used for CIFS and NFS are referred to as “both” type shares, servers and Cryptainers.

Multi-Protocol Administration Example

The next four sections describe a sample installation which assumes the following conditions:

- One NFS domain called nfsdomain
- One CIFS domain called cifsdomain
- One both type server called server2
- One CIFS share on server2 called share2 with a virtual name share2_secure
- One NFS share on server2 called share1 with a virtual name share1_secure
- Two multi-protocol (both) shares on server2 called cifsshare1 and nfsshare1 with virtual names cifsshare1_secure and nfsshare1_secure

Set DataFort Properties

1. Set the nofilecaching property on DataFort for CIFS and NFS to true:

```
system property set nfs.nofilecaching true
system property set cifs.nofilecaching true
```

Manage Domains

Add a Domain

Add the domain that will include the Cryptainers as a CIFS and as an NFS domain. Enter at least one CIFS and one NFS domain of any allowed subtype (local, NIS and LDAP).Note that the name must be unique (you cannot have the same named domain in NFS and CIFS).

1. Add a domain for CIFS, including the CIFS access user name and password, the domain name, type and subtype:

```
domain add -u DCRUSR -p dcr-usr1 cifsdomain cifs windows
```

2. Add a domain for NFS, including the domain name, type and subtype. The username and password are optional for NFS NIS domains. When you enter the access user name and password, DataFort will create the root user account automatically.

```
domain add nfsdomain nfs nis
```

Or:

```
domain add [-u user -p password] nfs nis
```

Add Root User to a Domain

DataFort requires the root user to mount exports and create Cryptainers on file servers. Other users are imported from the NIS automatically as Cryptainers are created for them. Since the root user is not part of the domain, it must be added to the DataFort manually:

- Add an account for the root user in the domain:

```
user add --id 0,0 --domain nfsdomain.company.com nas-user root
password
```

Verify Domains

- Verify that the domain was added to the database:

```
domain list
```

Remove a Domain

- Remove a domain:

```
domain remove nfsdomain
```

  Or:

```
domain remove cifsdomain
```

MANAGE SERVERS

Add a Server and Verify

1. Add servers that will contain Cryptainers to the domains. Identify the domain names and the real server name:

```
server add --cifs-domain cifsdomain --nfs-domain nfsdomain server2
```

2. Verify that the server was added to the database:

```
server list
```

Change Server Settings

- To change the type of a server, just provide the missing domain. For example, if you added a server as a CIFS server, but now want to access NFS shares on it also, enter

```
server set --nfs-domain mynewnfsdomain myserver
```

Remove a Server

- To remove a both type server from the configuration database, indicate the real server name:

```
server remove server2
```

Manage Virtual Servers

1. Add a virtual server (VIP):

```
vip add [--cifs-domain mycifsdomain] [--nfs-domain mynfsdomain]
myvirtualserver
```

2. Remove a virtual server (VIP):

```
vip remove myvirtualserver
```

3. List virtual servers:

```
vip list
```

4. Change the properties of a virtual server (VIP):

```
vip set myvirtualserver
```

To see the properties you can change, type `vip set ?` in the CLI.

MANAGE SHARES

Add a Share and Verify

1. Add a share as a both type share, including the real server name and the real share name for each share type:

```
share both add server2 cifsshare1 nfsshare1
```

2. Verify that the share was added:

```
share list
```

This returns a table which indicates the name and type of each share:

```
|Type    |Real Name                  |Virtual Name
|------  |-------------------------  |--------------------------------
-
|nfs     |server2:/share1            |share1_secure
|cifs    |\\server2\share2           |\\virtual_server2\share2_secure
|both    |\\server2\\cifsshare1      |\\virtual_server2\cifsshare1_secure
         |server2:/nfsshare1         |virtual_server2:/nfsshare1_secure
```

The both type shares show as two lines in the list of shares, the second line with an empty type field.

Remove a Share

1. To remove a both type share from the database, indicate the real name of the server and share. Use the CIFS or NFS format of the `share remove` command:

```
share remove server2:nfsshare1
```

Or:

```
share remove \\server2\cifsshare1
```

Change Share Settings

- To change the type of a share, just provide the appropriate new name. For example, to change a CIFS share to be a multi-protocol share, enter:

```
share set -n export_path\\server1\share1
```

Virtualize a Share

1. To virtualize a both share, use either the CIFS or NFS form of **share virtual add**.

   ```
   share virtual add --nfs-virtual-name newnfsname server1:export1
   virtualserver
   ```

   Or:

   ```
   share virtual add --cifs-virtual-name newcifsname \\server1\share1
   virtualserver
   ```

2. To change virtualization settings, use either the CIFS or NFS form of **share virtual set**.

   ```
   share virtual set --nfs-virtual-name newnfsname
   virtualserver1:virtualexport1
   ```

   Or:

   ```
   share virtual set --cifs-virtual-name newcifsname
   \\virtualserver1\virtualshare1
   ```

3. To stop virtualizing a both share, use either the CIFS or NFS form of **share virtual remove**:

   ```
   share virtual remove virtualserver1:virtualexport1
   ```

   Or:

   ```
   share virtual remove \\virtualserver1\virtualshare1
   ```

MANAGE CRYPTAINERS

Create a Cryptainer at the share level. It is now optional to specify the owner of the Cryptainer. By default (if the owner is not specified), the administrator who adds the Cryptainer is its owner.

If the NFS root user is not the owner of the Cryptainer, the share owner may need to grant root access in order to allow the Cryptainer to be mounted. See Manage Cryptainer ACL on page 240 for information about other owners granting access to a Cryptainer.

By default, read, write, change and delete permissions on the Cryptainer are granted to the person who creates the Cryptainer. If the type of the Cryptainer is CIFS or both, and the User Mapping security setting (see File Server Related Settings on page 168) is off, the ACL will be synchronized automatically from the root Cryptainer folder on the server. The creator or owner of the new Cryptainer must have full permissions on the location on the server where the Cryptainer is being created.

Create a Cryptainer

1. Add a Cryptainer to the server that was added as a both type server, using the both type share. Omit the owner field to specify that the administrator who is logged in to the CLI is the default owner of the Cryptainer. Use the CIFS or NFS format of the **cryptainer add** command:

   ```
   cryptainer add \\server2\cifsshare1
   ```

   Or:

   ```
   cryptainer add server2:nfsshare1
   ```

2. Alternatively, specify another owner:

   ```
   cryptainer add --owner root@cifsdomain
   \\server2\cifsshare1
   ```

Or:

```
cryptainer add --owner root@nfsdomain
server2:nfsshare1
```

3. Verify that the Cryptainer was added to the DataFort configuration database:

```
cryptainer list
```

This returns a table which indicates the name and type of each Cryptainer:

```
|nfs          |virtual_server2:/share3                    |Created
|cifs         |\\virtual_server2\share4\                  |Created
|both         |\\virtual_server2\cifsshare1_secure
              |virtual_server2:/nfsshare1_secure          |Created
```

The both type shares show as two lines in the list of shares, the second line with an empty type field.

Remove a Cryptainer

1. To remove a both type Cryptainer from the configuration database use either the NFS or CIFS format of the `cryptainer remove` command:

```
cryptainer remove server2:nfsshare1
```

Or:

```
cryptainer remove \\server2\cifsshare1
```

CLI Management for CIFS Cryptainers

Most DataFort CIFS management is done using the DataFort WebUI. However, for a large network it may be desirable to perform some management tasks using the CLI, such as creating large numbers of Cryptainers. An example might be creating home Cryptainer directories for 1000 users.

- From the operating system you are using to administer CIFS, add a special user for DataFort domain access to the Windows or LDAP domains in which DataFort will be used. See Adding the DataFort Domain Access User on page 36. Use the Security Settings page of the DataFort WebUI to modify the management settings and group review settings of DataFort. See Setting Security Options on page 166.
- On network file servers, create the CIFS shares that will later become Cryptainers for clients.

CIFS Administration Example

This section describes a sample installation which assumes the following conditions:

- One CIFS Windows domain called cifsdomain, one LDAP domain called cifsldapdomain, and one NIS domain called cifsnisdomain
- One server called server3
- One CIFS share on server3 called cifsshare3 with virtual name cifsshare3_secure
- The domain access user DCRUSR with password dcr-usr1

Use the following commands to script the process of adding a large number of Cryptainers to the configuration database.

Manage Domains

Add CIFS domains which include the servers that will host Cryptainers.

Add a Domain and Verify

1. Add a domain for CIFS of any subtype (Windows, LDAP, NIS), including the CIFS access user name and password, the domain name, type and subtype:

```
domain add -u DCRUSR -p dcr-usr1 cifsdomain cifs windows
domain add -u DCRUSR -p dcr-usr1 cifsldapdomain cifs ldap
domain add -u DCRUSR -p dcr-usr1 cifsnisdomain cifs nis
```

2. Verify that the domain was added to the database:

```
domain list
```

Remove a Domain

- Remove a domain from the database:

```
domain remove mycifsdomain
```

MANAGE SERVERS

Add a Server and Verify

1. Add servers to the domains; these will host the Cryptainers. Identify the domain names and the real server name or IP address:

   ```
   server add --cifs-domain cifsdomain server3
   ```

2. Verify that the server was added to the database:

   ```
   server list
   ```

Change Server Settings

To change server settings, use the **`server set`** command.

For example, use **`server set`** to change the IP address of a CIFS server in the configuration database. This command does not change the IP address on the server. It changes the configuration database so that DataFort will be able to access the server at its new address.

1. Change the IP address on the server (server3) and update the DNS Server.
2. Use the **`server set`** command to change the server's IP address in the configuration database:

   ```
   server set --ip 10.20.22.148 server3
   ```

Remove a Server

- To remove a server from the database, indicate the real server name:

  ```
  server remove server3
  ```

Manage Virtual Servers

1. Add a virtual server (VIP):

   ```
   vip add [--cifs-domain mycifsdomain] myvirtualserver
   ```

2. Remove a virtual server (VIP):

   ```
   vip remove myvirtualserver
   ```

3. List virtual servers:

   ```
   vip list
   ```

4. Change the properties of a virtual server (VIP):

   ```
   vip set myvirtualserver
   ```

   To see the properties you can change, type **`vip set ?`** in the CLI.

MANAGE SHARES

Add a Share and Verify

1. Use the **`share add`** command to add shares located on the servers that were added above. These shares will become Cryptainers. Indicate the server on which the share is located, and the name of the share:

   ```
   share add \\server3\cifsshare3
   ```

2. Verify that the share was added to the database:

```
share list
```

Remove a Share

- To remove a share from the database:

```
share remove \\server3\cifsshare3
```

Virtualize a Share

1. To virtualize a share:

```
share virtual add --cifs-virtual-name cifsshare3_secure
\\server3\cifsshare2
```

2. Use `share virtual set` to change virtualization settings, such as the VIP to virtualize on, the server IP to access share via, or the virtualized share name (as in this example):

```
share virtual set --cifs-virtual-name newcifsshare3_secure
\\server3\cifsshare3
```

3. To stop virtualizing a share:

```
share virtual remove --cifs-virtual-name cifsshare3_secure
\\server3\cifsshare3
```

Manage Users and Groups

View CIFS Groups

Use the `user group list` command to view CIFS user and group relationships:

- Use the `domain` parameter of the `user group list` command to view the group memberships in a specific domain. Note that the domain argument is case-insensitive:

```
user group list --domain cifsdomain
```

- Use the `group` parameter of the `user group` command to view to all the users in a group. Note that the group argument is case-sensitive.

```
user group list --group group1
```

- Use the `name` parameter of the `user group list` command to view all of the group relationships for a user. Note that the name argument is case-sensitive.

```
user group list --name user1
```

Manage Cryptainers

Add Cryptainers

You can use CLI commands to script the process of adding a large number of Cryptainers to the configuration database.

- Add Cryptainers to the DataFort configuration database using the `cryptainer add` command. If no owner is specified at time of creation, the user issuing the command will have ownership.

```
cryptainer add \\server3\cifsshare3
```

Note: Cryptainer ACL must be set using Windows mapping functionality at the share itself. The Cryptainer will have the same ACL settings as the share.

Set the DCS Requirement on a Cryptainer

- You can use `cryptainer set` to specify options on an existing Cryptainer, such as an IPsec or DCS requirement. To set the DCS requirement on a CIFS share:

```
cryptainer set --dcs on \\server1\cifsshare1
```

- Note that this requirement can also be set by the end user who owns the Cryptainer.

CLI Management for iSCSI Cryptainers

Most DataFort iSCSI management is done using the DataFort WebUI. However, for a large network it may be desirable to perform some management tasks using the CLI.

iSCSI Administration Example

The next sections describe a sample installation which assumes the following conditions:

- One server called netapp1, with an iSCSI name of “iqn.1992-08.com.netapp:netapp1
- One client with IP Address of 10.40.3.84 and iSCSI name of “iqn.1991-05.com.microsoft:testlab84.qa2kreal.nas.qa.decru.com”

Create Cryptainer

Add the target on which Cryptainers will exist, then associate it with a virtual IP address. Then add the initiator.

1. Add server:

```
server add --iscsi-access on netapp1
```

2. Add a virtual server. The floating option must be turned off.

```
vip add -f off vip227-99
```

3. Add the virtual server route to the target:

```
server route add netapp1 vip227-99
```

4. Add the iSCSI target:

```
iscsi target add 10.50.2.12 iqn.1992-08.com.netapp:netapp1
```

5. Verify the iSCSI target path:

```
iscsi target path list
```

6. Add the initiator:

```
iscsi initiator add 10.40.3.84 iqn.1991-
05.com.microsoft:testlab84.qa2kreal.nas.qa.decru.com
```

7. Execute a disk rescan to add LUNs and Cryptainers:

```
disk rescan
```

8. Verify LUNs and Cryptainers have been added:

```
iscsi lu list
```

9. Turn on encryption for the Cryptainer:

```
iscsi cryptainer rekey request --empty 0x0000000000002639
iscsi cryptainer rekey notify
```

10) Verify encryption on the Cryptainer:

```
iscsi cryptainer list
```

10. Verify encryption on the Cryptainer:

```
iscsi cryptainer list
```

11. Execute the **kfc list** command to verify setup :

```
kfc list
```

RESTORING A CRYPTAINER

The **cryptainer restore** command is used to obtain access to data stored in a Cryptainer that has been deleted from the DataFort configuration. The requirements for a Cryptainer restore include:

- The original encrypted data including the .decru file.
- A DataFort that remembers the original Cryptainer. DataFort stores information about Cryptainers in its configuration database permanently, even if the Cryptainers are deleted.

Restoring a CIFS Cryptainer

1. Copy the original encrypted data to a folder on a server (for this example, server3). Note that it is not necessary that it be the server of the original Cryptainer.
2. Make the folder a CIFS share on the server (for this example, cifsshare4).
3. Add the server to the DataFort (if necessary):

```
server add --cifs-domain cifsdomain server3
```

4. Add the share using the **share add** command:

```
share add \\server3\cifsshare4
```

5. Virtualize the share:

```
share virtual add --cifs-virtual-name cifsshare4_secure
\\server3\cifsshare4
```

6. Restore the Cryptainer using the **cryptainer restore** command:

```
cryptainer restore \\virtual_server3\cifsshare4_secure
```

7. Synchronize the ACL on the Cryptainer with the ACL on the server:

```
cryptainer acl sync \\virtual_server3\cifsshare4_secure
```

Restoring an NFS Cryptainer or Multi-protocol Cryptainer

The procedure for restoring a multi-protocol Cryptainer is the same as for CIFS. Restoring an NFS Cryptainer differs mainly in the formatting of the paths. After an NFS Cryptainer is restored, you must reset the ACL on the Cryptainer manually.

SPECIAL COMMANDS

CRYPTAINER ALIASES

The CLI can be used to create Cryptainer aliases, so that files replicated with a mirroring backup process can be encrypted in both the primary and mirror volume using the same Cryptainer key. If Cryptainer aliases are used, you can read and write to the primary volume, and read the backup.

You can set up a Cryptainer on a primary volume mirrored by SnapMirror. SnapMirror is a NetApp technology which provides read-only, asynchronous mirrors of volumes (or qtrees) on NetApp filers. Volumes are replicated from a source filer to a destination, which may be a different volume on the same filer or a volume on a different filer.

With DataFort placed in front of the mirroring components, use these steps to implement SnapMirror Cryptainers:

1. If the Cryptainer does not already exist on the primary volume, create one.
2. Set the nofilecaching property on DataFort for CIFS and NFS to true:

   ```
   system property set nfs.nofilecaching true
   system property set cifs.nofilecaching true
   ```

3. Wait until the .decru file from the primary volume is replicated by SnapMirror to the mirrored volume.
4. Restore the Cryptainer at the mirror location using the **`cryptainer restore`** command. Restoring the Cryptainer adds the path to the mirror volume to the DataFort configuration database.

There are some restrictions on Cryptainer aliases. Since there is only one ACL for the entire Cryptainer, including all of its aliases, the ACL may be synced only against the primary path. Another restriction is that only the primary path is rekeyed.

Note: When backups are done directly to the server, file metadata caching should either be turned off, or the file caches should be cleared after every data modification.

PORT FORWARDING

DataFort supports port forwarding for use in configurations where the server subnet and client subnet have no connection other than through DataFort. In this configuration, it would normally be impossible to administer any servers from the client network.

WARNING: ALL THE TRAFFIC GENERATED WHILE FORWARDING, INCLUDING SERVER-SIDE TRAFFIC, WILL BE PLAINTEXT.

By enabling port forwarding, the administrator can have DataFort forward all connections on a given TCP port (i.e. 23 for telnet or 80 for HTTP) from the client side to the server side. This allows users on client workstation to manage servers.

To forward all connections on the given TCP port from the specified client-side VIP to the given server, binding to the given server-side VIP, use the **`forwarding add`** command:

```
forwarding add <client-vip> <server> <port>
```

To clear all entries from the forwarding configuration, use:

```
forwarding clear
```

To list all entries in the configuration:

```
forwarding list
```

To restart the port forwarder:

```
forwarding restart
```

IPsec Configuration and Management

The following commands configure IPsec rules on DataFort. Similar rules must be set on each client that uses IPsec to communicate with DataFort. See Configuring IPsec on page 170 for more detailed information. In general, use preshared secret for NFS Cryptainers with Solaris clients, and use Kerberos authentication for CIFS Cryptainers with Windows clients. Note that an IPsec license from Decru is required on the DataFort from which you issue IPsec commands.

1. To add an IPsec rule that uses a preshared secret for authentication:

   ```
   ipsec add -s 0123456789012345 virtualserver 10.10.20.168
   ```

   For Solaris clients, the secret must be a 32-byte hexadecimal string preceded by 0x (for example, `0x01234567890123456789012345678901)`; for Windows clients it must be 16 bytes long.

2. To add an IPsec rule that uses Kerberos authentication (after the virtual server "virtualserver" has joined its CIFS domain with the `vip join` command):

   ```
   vip join -u administrator -p password virtualserver
   ipsec add -k virtualserver 10.10.20.168
   ```

3. To show a list of IPsec rules:

   ```
   ipsec list
   ```

4. To remove an IPsec rule:

   ```
   ipsec remove virtualserver 10.10.20.168
   ```

WebUI Display

One of the system properties controls the display in the Servers & Portals pane of the WebUI. To speed up the display of large numbers of entries, set the number of items initially displayed as follows.

- To set the initial limit of shares under a server to some number nnn:

  ```
  system property set web.tree.limit.shares nnn
  ```

- To set the initial limit of virtual shares under a virtual server:

  ```
  system property set web.tree.limit.virtualshares nnn
  ```

- To set the initial limit of Cryptainers under a share:

  ```
  system property set web.tree.limit.cryptainers nnn
  ```

  The default limit is 300. If the list exceeds the preset limit, the list is truncated. Extra nodes are replaced by the overflow placeholder "All..."

VLAN TAGGING

The VLAN Tagging feature allows DataFort to work on multiple distinct VLANs. This feature is based on the ability to virtualize both client-side and server-side network ports with respect to each corresponding distinct VLAN.

To add a VLAN to the DataFort, use the **vlan** CLI command:

```
vlan add <vlan-id> <netmask>
```

To specify a specific VLAN on a VIP, use the –vlan option:

```
vip set --vlan <vlan-id> <vip-name>
```

Following is an example of VLAN Tagging usage. This example assumes the following environment:

- Two VLANs with IDs 3 and 5. Clients are on VLAN 3, file servers are on VLAN 5.
- DataFort client side port attached to a tagged switch port configured to present VLAN 3 and the 'default' VLAN (0 on some switches).
- DataFort server side port attached to a tagged switch port configured to present VLAN 5.
- Client in VLAN 3: client1
- Server in VLAN 5: server1

1. Ensure that client1 in VLAN 3 cannot ping server1 in VLAN 5 and vice versa.
2. Add the VLANS to DataFort:

```
vlan add 3 255.255.0.0
vlan add 5 255.255.0.0
```

3. Add the client side VIP clientvip1 (note the vlan option):

```
vip add --cifs-domain domain.com --vlan 3 clientvip1
```

4. Set the vlan on the server side VIP:

```
vip set --vlan 5 servervip1
```

5. Add the server and share and virtualize the share on cvip1.
6. Create a Cryptainer vlan-cryptainer1.

To verify the VLAN settings are correct the following steps may be helpful:

- Verify client1 can access data on vlan-cryptainer.
- Verify client1 cannot ping server1 and vice versa.
- If file access seems to not be working through DataFort, use the DataFort **net util ping** command to ensure connectivity and review the VLAN IDs are correct and are assigned to the correct VIPs. Most often connectivity issues arise as a result of VLAN ID numbering confusion.
- If you lose connectivity to the DataFort management interface, you probably misconfigured the switch. Ensure the client side port on DataFort is configured to receive all VLANs (on some switches this is designated as VLAN ID 0).

21 TROUBLESHOOTING

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

- Restoring a DataFort
- Front Panel LEDs
- Power Supply LEDs
- Network Connections and Management Interfaces
- CIFS Cryptainers
- NFS Cryptainers
- iSCSI Cryptainers
- Clusters
- Smart Cards
- Hardware Issues

Restoring a DataFort

If a standalone DataFort is lost, a saved configuration database from that DataFort can be used to configure a replacement DataFort. The recovered DataFort will then be able to retrieve data that was encrypted using the previous DataFort. The Setup Wizard assigns a new DataFort the configuration from a pre-existing DataFort. The replacement DataFort will retain all parameters stored in the configuration database of the original DataFort, including network, Cryptainer, access control and encryption key information.

If a cluster member is lost, it should not be restored using the wizard. It should be deleted from the cluster and replaced as described in Replacing a DataFort in a Cluster on page 202. Use the wizard to restore the head of a cluster only if all members have been lost.

The procedure is conducted by a Full Administrator. The recovery procedure requires:

- A new or reset System Card.
- A new or zeroized DataFort.
- The minimum set of Recovery Officers and Recovery Cards as determined by the recovery schema of the cluster.
- A saved database from the DataFort that is to be restored.

1. Connect the new or zeroized DataFort to the network and assign it the IP settings of the old DataFort. See Assigning the DataFort IP Address on page 44.
2. Start the wizard. See Initializing DataFort Appliances on page 47.
3. At the Recover from Database page, browse to the saved configuration database.

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

Front Panel LEDs

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

Table 32: 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 33: Front Panel LEDs - 1U

Color	Behavior	Indication
Green	Solid	DataFort on network, no errors, no traffic
Green	Blinking	DataFort on network, no errors, with traffic
Red	Solid	Network error, no traffic
Red	Blinking	Error found, with traffic

Power Supply LEDs

The power supply module on the 2U model DataFort provides a single external bicolor LED to indicate the status of the power supply. When AC is applied to the power supply unit and standby voltages are available, the LED will blink green. The LED will be solid green to indicate that all the power outputs are available. It will be solid amber to indicate that the power supply has failed, there is a shutdown due to over-current, over-temperature, or if the unit is indicating a predictive failure.

Table 34: Power Supply LEDs

Power Supply Condition	Power Supply LED
No AC power to all power supply units	Off
No AC power to this power supply unit only	Amber
AC present / Only standby outputs on	Blink green
Power supply DC outputs ON and OK	Green
Power supply failure (includes over voltage, over temperature)	Amber
VRM failure (voltage regulator module - cage related)	Blink green
240VA limit (cage related)	Blink green
Current limit	Amber

Network Connections and Management Interfaces

Table 35 contains troubleshooting tips for the network and management connections to DataFort.

Table 35: Network Connections and Management Interfaces

Problem	Possible Cause and Solution
No Ethernet network connection	• Both NIC ports must be connected. Check port and cable connections.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**.
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.

TABLE 35: NETWORK CONNECTIONS AND MANAGEMENT INTERFACES (CONTINUED)

Problem	Possible Cause and Solution
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	• By default, to access the DataFort WebUI you must have access to the Clients NIC from the Management Station. (Note that you can configure DataFort to be manageable from either NIC.) Make sure DataFort and the Management Station are on the same subnet. • If Secure Web is turned on, a valid administrator name and Admin Card are needed when logging in. • TLS 1.0 must be explicitly enabled in Internet Explorer. SeePreparing the Management Station. • 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.
Lost login and/or password information for sole administrator	• Log in using a Recovery Card and zeroize the appliance. See Emergency Serial Console Port Access.
Need to turn off WebUI smart card requirement (Secure Web) via CLI	• If you are unable to access the WebUI in order to turn off the smart card requirement, you can do so via CLI: • Log in to the CLI and enter: **`system property get sys.security.web.usesmartcard`** to check the setting. A setting of **`1`** requires the Admin Card in order to log in to the WebUI; **`0`** disables the requirement. If necessary, enter: **`system property set sys.security.web.usesmartcard 0`** to disable the smart card requirement. A Security or Full Administrator can set this property.
CLI sessions take a long time to establish	• This can occur if the DNS servers are unavailable. Log in through WebUI and change the DNS servers, or wait for the SSH to connect and then change the DNS servers from the CLI.

CIFS Cryptainers

Table 36 contains troubleshooting tips for CIFS Cryptainers.

Table 36: CIFS Cryptainers

Problem	Possible Cause and Solution
Users are not imported (user registration fails, or user not found when trying to grant access)	• Make sure the DataFort domain access user is in the domain. • Note that users are only imported into the DataFort's configuration database under the following circumstances: - The user registers his or her password. - The user is part of an ACL for a Cryptainer or is in a group which is part of a Cryptainer ACL. - The user connects to DataFort (i.e. by mapping a drive). - The user is explicitly granted some permissions to an ACL.
	• If there is a time mismatch between the domain controller and DataFort, there will be an error and users may not appear. Check the time settings. • Configure an NTP server for DataFort, or reset the time on DataFort using the WebUI.
	• DataFort syncs with domain user information. Make sure that the domain name is correct and the correct domain controller is specified for the domain.
	• Right-click the domain in the Servers & Portals page of the WebUI and select Test Access to test access to the domain.
	• If Group Review is on, users will not appear until the administrator reviews and accepts the users.
Cannot add a CIFS server	• Server must be up. Right-click the server in the Servers & Portals page of the WebUI and select Ping to test access to the server. • CIFS service must be started on the server. Try getting a listing of shares from the client to make sure that the CIFS service is started. • Server name must be resolvable by DNS. If the server name is not resolvable by DNS, use the IP address instead.
Cannot add Cryptainers to a CIFS server	• If a server comes online after the DataFort powers up, DataFort may not be able to add Cryptainers to it. Power servers up before DataFort. • If the DataFort domain access user is not configured properly, DataFort will be unable to communicate with the server.
Unable to create CIFS Cryptainer (or sync ACL, or restore Cryptainer)	• CIFS service must be started on the server. Try getting a listing of shares from the client to make sure that the CIFS service is started. • The share selected to become a Cryptainer might already contain a .decru file from a previous Cryptainer or from another DataFort. Never use the same share for more than one Cryptainer. • Right-click the server in the Servers & Portals page of the WebUI and select Ping to test access to the server. • Check the share permissions (not just the folder permissions) on the share you are trying to make into a Cryptainer. • Be sure the server is set up for sharing.

TABLE 36: CIFS CRYPTAINERS (CONTINUED)

Problem	Possible Cause and Solution
Cryptainer won't restore	• Verify that the permissions on the share and contents of the share (including the .decru file) allow write access to the DataFort domain access user.
User can't access CIFS Cryptainers	• If the Use Local ACL setting is on, the ACL on DataFort will be enforced and there will be no unauthorized Cryptainer access through DataFort. • Map the share as the user attempting to access the Cryptainer to see if that user has access to the share directly on the server.
	• Check if User Registration was turned off recently. Users who were connected to a share immediately before User Registration was turned off may not be able to access or connect to a share immediately afterwards. • Try disconnecting the share and reconnecting to it. • Try logging out from your client machine and then logging back in. If that doesn't work, reboot the client machine.
	• Make sure you're not trying to map as the DataFort domain access user. The DataFort domain access user never has access to Cryptainers. • The domain of the user who is trying to map must be known to DataFort. • If the DataFort just rebooted, it will take a while for the user and group membership listings to be generated. Wait up to 30 minutes and try again.
	• Check if the user remained connected to DataFort while the user was removed from DataFort's configuration (and perhaps added back). In this case, the user may lose access to some Cryptainers through this connection. The user should disconnect from DataFort, and then re-connect.
Creating a Cryptainer causes an error that the server does not support TCP	• UDP is used to create, restore, and remove Cryptainers on the server. If UDP is disabled on the server (generally unlikely), DataFort cannot perform these operations. DataFort only supports TCP over UDP.
Can't create Cryptainer from FAT/FAT32 volume	• FAT/FAT32 volumes are not supported by DataFort. Right-click on the icon for the hard drive on which the share resides and select Properties. If the File System is FAT32, it cannot become a Cryptainer.
Local ACL missing some users/groups after syncing or setting ACL	• Users who are not in the configuration database cannot be added to a Cryptainer ACL. A log message is generated every time such an attempt is made. • Check Group Review settings.
Can't access Cryptainer or share	• The file server may not be up, or may not be sharing correctly. Check the file server to see if it is running correctly and sharing the expected volumes/disks. • The DataFort may have detected an intrusion which stops all encryption/decryption. This can be checked from either the WebUI Home page or CLI. Reset intrusion and investigate why DataFort detected intrusion.
Samba servers don't work in a cluster	• When adding a Samba server to a DataFort cluster, the NetBIOS field is required.

NFS Cryptainers

Table 37 contains troubleshooting tips for NFS Cryptainers.

Table 37: NFS Cryptainers

Problem	Possible Cause and Solution
Unix group memberships are not imported	• If Group Review is on, newly imported groups must be confirmed before memberships can be imported.
Cannot create NFS Cryptainer	• DataFort does not create parent directories. • Check permissions on server and directories. • Make sure the server is set up for export.
	• A valid Unix ID must be set for the user creating the Cryptainer.
	• Most NFS servers have a feature called rootsquash which is turned on by default. If the administrator is trying to create a Cryptainer with the root as owner, it will fail if the NFS server has rootsquash turned on. Turn rootsquash off on the server in order to create a Cryptainer with root as its owner. • When you create a new Cryptainer, make sure that the Cryptainer directory does not exist (except for cleartext Cryptainers).
Error: Cryptainer creation failed due to time out	• This time-out error occurs when a server is added to the server side interface when it should be on the client side interface. • Remove and add the server again using the client side option.
Cannot add a server/share/Cryptainer	• Try mounting the server and share directly from an NFS client machine. If you cannot mount it directly, DataFort can't either. • Check permissions on the server. • Right-click the server in the Servers & Portals page of the WebUI and choose Ping to test access to the server. • If you can mount the server, check the IP-based export permissions on the server. The DataFort File Servers IP should be allowed read and write access. If it is, after you have mounted the share, try following the Cryptainer path for the failed Cryptainer creation operation. Using the Cryptainer owner as your login, try creating a directory under the Cryptainer path. If you cannot do this, then DataFort cannot create the Cryptainer directory. Find the cause of this directly on the server and try again from DataFort. • When you create a new Cryptainer, make sure that the Cryptainer directory does not exist (except for cleartext Cryptainers).
User has no access to Cryptainer	• Check that the user has been added to the configuration database. If Group Review is on, the user may be awaiting confirmation. To view all users that have access to Cryptainers, execute the `user group list --uflags normal` command.
User cannot mount a share from DataFort	• Make sure a user with UID 0 exists in DataFort. Typically, client machines use UID 0 when they mount a share, and DataFort will only allow this operation if the user is known to DataFort.

TABLE 37: NFS CRYPTAINERS (CONTINUED)

Problem	Possible Cause and Solution
Creating/writing/ reading a file fails	• Check whether the file is located inside a Cryptainer. If it is not, DataFort will not allow any read or write access to it, as a safety measure. To work around this restriction the Security Administrator or Full Administrator can temporarily set the property **`sys.security.nfs.plaintext`** to the value **`1`**. This is not recommended in installations where maximum security is required.
Some operation (chown, chmod, etc.) fails on a file	• Depending on the way clients and servers are configured, there can be peculiarities in the way permissions are handled. Always try a scenario similar to the failed one from the client directly to the server. If it doesn't work directly, there is a problem with the configuration that is unrelated to DataFort. If the operation works directly, then look at ACLs on DataFort and make sure the user that is attempting the operation has the necessary permissions. To view the ACL on a Cryptainer, right-click it in the Servers & Portals page of the WebUI and select Access Control > ACL.
Clients cannot access new cleartext Cryptainer	• Make sure no clients are mounting the share where the cleartext Cryptainer is being created. • Only NFS v3 clients should access that share. Access to files in the cleartext Cryptainer will be denied to all NFS clients if an NFS v2 client attempts to use the share. The Storage Administrator or Full Administrator can disable NFS v2 access to DataFort by using the following commands from the CLI: • **`system property set nfs.version.nfs.2.udp 0`** • **`system property set nfs.version.nfs.2.tcp 0`** • If the cleartext Cryptainer was created over existing data, clients may see “Permission Denied” errors. Clients must either unmount and remount the share they are using, or the clients need to be rebooted. Clients will not see these errors if they did not have access to the share before Cryptainer creation.

iSCSI Cryptainers

Table 38 contains troubleshooting tips for iSCSI Cryptainers.

Table 38: iSCSI Cryptainers

Problem	Possible Cause and Solution
No targets displayed in WebUI after adding an initiator	• Check in the target management windows, right-click and select Rescan. • Verify that the initiator name is correct. • Verify that the initiator IP address is correct. • If using a QLogic cards, verify that the initiator IP address is that of the QLogic card.
Encrypting icon is displayed on Cryptainer after selecting Encrypt > Empty	• Refresh the Cryptainer a few times. • Select Encrypt > Empty again.

CLUSTERS

Table 39 contains troubleshooting tips for DataFort clusters.

TABLE 39: CLUSTERS

Problem	Possible Cause and Solution
Giveback does not work properly	• Check System Config > Cluster > Manage Failover page of the WebUI. If the clustered DataFort appliances seem to be working, but one of them is serving all VRIDs, try clicking Recover. If this does not work, make sure the File Servers NIC cable is plugged in. If it is unplugged, the DataFort will not serve any VRIDs. • Access the System Config > Cluster > Manage Failover page of the WebUI of the DataFort that is not servicing servers and click Recover.
Cluster will not form	• The DataFort cluster license may have expired. Obtain a valid license for each DataFort in the cluster.
Client connection dropped	• More than one cluster member could be serving the same file server. This could be the result of a misconfigured spanning-tree holddown. See Configuring Cluster Members for STP.
Can't change server-side IP of clustered DataFort	• If the cluster state is not committed/online and the administrator tries to change the server side IP, there will be an error message. (It is possible to change the client side IP even if the cluster is not committed/online.)
One cluster member is offline	• If the DataFort is permanently offline, it should be replaced. Follow the instructions in Replacing a DataFort in a Cluster. • If the DataFort is expected to come back online, and there is no urgent need to make configuration changes, keep the cluster intact and wait for the DataFort to come back online.
Cluster is in committed/ conflict state	• Determine which cluster member has the accurate configuration, and manually resolve the conflict or contact Decru for assistance.

SMART CARDS

Table 40 contains troubleshooting tips for working with smart cards.

TABLE 40: 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: `system property set sys.security.web.usesmartcard 0` to disable the smart card requirement for the WebUI. Then log in to the WebUI and associate a replacement Admin Card with an existing or new administrator. A Security Administrator or Full Administrator can change the system property. A Full Administrator is required to create or change associations with an Admin Card. • If both CLI and WebUI login are smart card enabled and all Admin Cards are lost, you will have to zeroize DataFort using the serial console.
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.

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.

> **WARNING:** THERE ARE NO SERVICEABLE PARTS INSIDE THE DATAFORT. DO NOT OPEN THE CHASSIS.

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 example, file servers with shares must be added to the configuration database before Cryptainers can be created. 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 71. 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.

iscsi...	iSCSI kernel commands...	iSCSI commands
kfc...	SAN kernel commands...	KFC Commands
disk...	SAN disk commands...	Disk commands
cifs...	CIFS subsystem commands...	CIFS Commands
cryptainer...	Cryptainer commands...	Cryptainer Commands
forwarding...	Port forwarding subsystem commands...	Forwarding Commands
http...	HTTP subsystem commands...	HTTP Commands
ftp...	FTP subsystem commands...	FTP Commands
isns...	iSNS commands...	iSNS commands
ipsec...	IPsec commands...	IPsec Commands
nfs...	NFS subsystem commands...	NFS Commands
server...	Server commands...	Server Commands
share...	Share commands...	Share Commands
tftp...	TFTP subsystem commands...	TFTP Commands
vif...	Virtual interface commands...	Virtual Interface Commands
vip...	Virtual IP address or hostname commands...	Virtual IP Commands
vlan...	Virtual LAN commands...	VLAN Commands
vscan...	Virus scanning commands...	Virus Scanning Commands
cli...	Command line administration commands...	CLI Formatting Commands
help +	Command line usage help	Help Command
quit	Quit the current client session	Quit Command
active-role...	Active role commands...	Active-Role Commands
authorize +	Authorize admin login	Authorize Command
domain...	User/group domain commands...	Domain Commands
group...	Group commands...	Group Commands
password +	Change user password	Password Command
role...	Role commands...	Role Commands
user...	User commands...	User Commands
who	Display who is logged in	
whoami	Display effective user ID	Whoami Command
trustee...	Trustees management commands...	Trustee Commands
net...	Network commands...	System Commands
keyman...	Key management commands...	Key Management Commands
lkm...	LKM management commands...	LKM Management Commands
cluster...	Cluster commands...	Cluster Commands
db...	Database administration commands...	Database Commands
system...	System commands...	System Commands

iSCSI COMMANDS

Type **iscsi ?** to view iSCSI commands.

cryptainer...	iSCSI Cryptainer commands...
dump	Dump iSCSI Kernel State
igroup...	iSCSI Initiator group commands...
initiator...	iSCSI Initiator commands...
lu...	iSCSI Logical Unit commands...
target...	iSCSI Target device commands...
cryptainer...	iSCSI Cryptainer commands...
dump	Dump iSCSI Kernel State

KFC COMMANDS

Type **kfc ?** to view SAN kernel commands used when managing iSCSI storage.

config	Configure FC kernel
list	Display SAN kernel statistics
querystats	Query the Fibre Channel driver for its properties
request...	SAN kernel Request commands...
reset	Reset SAN kernel DB
sync	Query the fabric to update the status of all devices
util...	SAN kernel utility commands...
vp...	SAN kernel virtual port commands...
wwn...	Fibre Channel primary port node/port WWN utils...

DISK COMMANDS

Type **disk ?** to view disk commands used when managing iSCSI storage.

rescan	Force DataFort to rescan the network for disks

CIFS COMMANDS

Type **cifs ?** to view CIFS commands.

state...	CIFS runtime state commands...
stats	Display the CIFS subsystem performance statistics
sync	Sync database state to the CIFS subsystem

CRYPTAINER COMMANDS

Type **cryptainer ?** to view Cryptainer management commands.

acl...	Cryptainer ACL commands...
add +	Add Cryptainers to known shares
alias...	Cryptainer alias commands...

grant +	Grant permission on Cryptainer to a user or group
ip...	Cryptainer commands for setting IP address based ACLs...
key +	Show encrypted Cryptainer key
list +	List all Cryptainers
owner...	Cryptainer owner commands...
rekey...	Cryptainer rekey commands...
remove +	Remove a Cryptainer
restore +	Restore a Cryptainer
revoke +	Revoke permission on Cryptainer from a user or group
rvall +	Revoke all permissions from a Cryptainer
set +	Change Cryptainer settings
status +	Check Cryptainer status

FORWARDING COMMANDS

Type **forwarding ?** to view port forwarding commands.

add +	Add a entry to the forwarding configuration
clear	Clear the entries in the forwarding configuration
list +	List forwarding configurations
restart	Restart the port forwarder

HTTP COMMANDS

Type **http ?** to view HTTP commands.

state...	HTTP runtime state commands...
sync	Sync database state to the HTTP subsystem

FTP COMMANDS

Type **ftp ?** to view FTP commands.

state...	FTP runtime state commands...
sync	Sync database state to the FTP subsystem

iSNS COMMANDS

Type **isns ?** to view iSNS commands

restart	Restart iSNS process
server...	iSNS server commands...
stop	Stop iSNS process

IPSEC COMMANDS

Type **ipsec ?** to view IPsec commands.

add +	Add an IPsec rule
list +	Show a list of IPsec rules

remove +	Remove an IPsec rule
restart +	Restart IPsec
rmall +	Remove all IPsec rules for a given virtual host
set +	Set the properties for an IPSec rule
status +	Display the status of the IPsec module

NFS Commands

Type **nfs ?** to view NFS commands.

howto	How to use NFS
sync	Sync database state to the NFS subsystem
portmap...	Portmap daemon commands...
state...	NFS runtime state commands...
stats	Display the NFS subsystem performance statistics

Server Commands

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

add +	Add a server that will host Cryptainers
discover +	Query a Windows DC for member servers
ip...	Commands for manipulating server IPs...
list +	List known servers
ping +	Ping a server
remove +	Remove a server from the database
set +	Change server settings

Share Commands

Type **share ?** to view share commands.

acl...	Share ACL commands...
add +	Add a share
both...	Commands specific for multi-protocol shares...
discover +	Query a server for its shares
grant +	Grant permission on share to an NFS client IP
list +	Show a list of known shares
remove +	Remove a known share
revoke +	Revoke permission on share from an NFS client IP
set +	Change share settings
virtual...	Commands for virtualizing shares...

TFTP Commands

Type **tftp ?** to view TFTP commands.

state...	TFTP runtime state commands...
sync	Sync database state to the TFTP subsystem

Virtual Interface Commands

Type `vif ?` to view virtual interface commands.

`add +`	Add a virtual interface
`list +`	List virtual interfaces
`remove +`	Remove a virtual interface

Virtual IP Commands

Type `vip ?` to view virtual IP commands.

`add +`	Add a virtual IP address or hostname
`certificate...`	VIP certificate commands...
`dump`	Dump interface configuration state
`join +`	Join a VIP to either a Windows domain or a Kerberos realm
`list +`	List virtual IP addresses or hostnames
`remove +`	Remove a virtual IP address or hostname
`serverside...`	File Servers NIC IP address commands...
`set +`	Change settings for a virtual IP address or hostname
`status +`	Show diagnostic status (Kerberos, etc) for a VIP
`sync +`	Sync various configurations from DB
`unjoin +`	Unjoin a VIP from its domain/realm

VLAN Commands

Type `vlan ?` to view VLAN commands.

`add +`	Add a VLAN ID
`list +`	List VLAN IDs
`remove +`	Remove a VLAN ID

Virus Scanning Commands

Type `vscan ?` to view virus scanning commands.

`route...`	Virus scanning route commands...
`share...`	Virus scanning share commands...

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

DOMAIN COMMANDS

Type `domain ?` to view domain controller commands.

`add +`	Add a domain
`controller...`	CIFS domain controller commands...
`group...`	Domain group commands...
`hash...`	Commands for synchronizing password hashes...
`list +`	List domains
`migrate +`	Move all users and groups in a domain to another domain
`remove +`	Remove a domain
`set +`	Set domain settings
`user...`	Domain user commands...
`validate +`	Validate domain access

GROUP COMMANDS

Type `group ?` to view user group commands.

`add +`	Add a group
`domain...`	Domain commands for synchronizing Windows groups...
`groups...`	Nested group membership commands...
`list +`	List groups
`remove +`	Remove a group
`review +`	Check whether group review is needed

Password Command

Type `password` to change an admin password.

`password +`	Change password

Role Commands

Type `role` to view role commands.

`list +`	List roles
`path...`	Role path commands...

User Commands

Type `user` to view user commands.

`add +`	Add a user account
`cifs...`	User CIFS commands...
`comers...`	User new comers commands...
`domain...`	Domain commands for synchronizing users...
`group...`	Group membership (non-nested) commands...
`home...`	User home directory commands...
`list +`	List all users in database
`remove +`	Remove a user from the database
`role...`	User role commands...
`set +`	Set user settings

Whoami Command

Type `whoami` to see the current user ID.

`whoami`	Display effective user ID

Trustee Commands

Type `trustee ?` to view trustee commands.

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

Network Commands

Type `net ?` to view network management commands.

`apply +`	Apply network changes
`connection...`	Network connection administration commands...
`interface...`	Network interface commands...
`status +`	Display network status
`util...`	Network utilities...

Key Management Commands

Type **keyman** to view key management commands.

cryptainerkeys +	Query Cryptainer Keys
lkmkeys +	LKM key management commands...
masterkeys +	Query Master Keys
purgekeys	Purge unused Cryptainer and Master Keys

LKM Management Commands

Type **lkm** to view Lifetime Key Management commands.

status	Check the status of the connection to the configured LKM System

Cluster Commands

Type **cluster ?** to view the cluster commands.

comeback	Notify cluster members of intention to return to operation
config...	Cluster configuration commands...
enable	Enable clustering
failover	Relinquish normal operation and failover to a cluster member
giveback	Give back operation to a cluster member DataFort
heartbeat...	Cluster heartbeat commands...
rexec +	Execute a CLI command on member DataFort(s)
rsh +	Access the CLI of specified 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
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 DATAFORT VIRUS SCANNING

Network Attached Storage (NAS) arrays—such as NetApp FAS/NearStore and EMC Celerra—have integrated antivirus functionality that allows on-the-fly scanning of files as they are read, created, and modified. Special accommodation must be made to detect viruses in files that are encrypted in storage.

When a DataFort appliance is used to encrypt the data stored on a NetApp or EMC NAS array that will be scanned for viruses, the Antivirus scanners (AV scanners) must have access to the data in unencrypted form in order to correctly scan the file contents and detect viruses.

This appendix describes how to integrate DataFort into an existing antivirus architecture using NetApp® VScan or EMC Celerra Anti Virus Agent (CAVA). Some of the information in this document applies to both virus scanning software applications. Where the procedure is different, follow the appropriate steps for your antivirus system. See:

- Considerations Before Configuration
- Steps Before You Begin
- Configuring DataFort for Virus Scanning
- Notes for Virus Scanning

Considerations Before Configuration

The following lists some considerations when implementing DataFort support of virus scanning.

- Ensure that DataFort Cryptainer Filename Encryption is turned off for Cryptainers that will be scanned for viruses. Virus scanning through DataFort is not supported when using Cryptainers with encrypted filenames.
- Ensure that you have the proper administrative rights on the DataFort appliance, NAS Array, AV Scanner, and windows domain controller to accomplish the proper installation.
- New Virtual Server(s) will need to be created on DataFort, pending the addition of each AV Scanner. This will require additional IP Addresses on your network.
- Ensure that the proper security scheme is in place to administer the possible addition of AV Scanners on your network.
- Consult your NAS array and antivirus software documentation regarding the number of AV Scanners needed in you environment paired with the added resource congestion which may be added to your infrastructure due to these additions.
- If using EMC CAVA software paired with Trend Micro ServerProtect for EMC NAS, please consult the EMC CAVA documentation for alternate EMC CAVA installation procedures.

Steps Before You Begin

Be sure to have the Virus Scanning software documentation available before beginning this process. Consult CAVA and NetApp documentation for direction when completing the steps outlined below.

Complete these steps before you configure DataFort to support virus scanning:

1. Prepare the NAS array (see the documentation for the appropriate type of array):
   - EMC Celerra: Make sure that the CIFS Server is set up properly for CAVA to work with a domain.
   - NetApp: Set up the NetApp NAS array for CIFS.
2. Create a share, or multiple shares, on the NAS array.
3. Export CIFS share(s) as DataFort Cryptainers.
4. If a specified account is used in order to scan files on the array, this user must be granted access to the Cryptainers. This user should be granted whatever permissions will be needed to support the scanning configuration (such as read, write, execute).

   Note: If Local ACL is being enforced on DataFort, the user that the AV scanner accesses files with must be explicitly added to the DataFort ACL.
5. Create one or more AV scanners (servers) on which the Virus Scanning application will run. For CAVA this will require the installation of the CAVA software on the AV scanner in addition to the AV software itself.

CONFIGURING DATAFORT FOR VIRUS SCANNING

The command examples in this procedure assume:

- A NAS array with hostname (for NetApp) netapp1 in the domain domain1.domain.com or (for CAVA) cifs_server in the domain domain1.domain.com
- Two shares on the NAS Array (share1 & share2) have been exported as Cryptainers (cryptainer1 and cryptainer2) on a DataFort with hostname DataFort1.
- Two AV scanners with hostnames vscan1 and vscan2.

To configure virus scanning on files to be encrypted by DataFort complete these steps. This procedure only needs to be completed on one DataFort in a cluster.

1. Log in to the DataFort CLI.
2. Add the AV scanner(s) to DataFort as a server (in the same domain as the server and DataFort VIP) with the command. If you set up multiple AV Servers, you can add more using the same command. For example:

```
server add --cifs-domain domain1.domain.com vscan1
server add --cifs-domain domain1.domain.com vscan2
```

3. Add the IP addresses that will be use to route virus scanning traffic to DataFort. Assume:
   - df-cvscan1 is on the same network as the DataFort client interface.
   - df-svscan1 is on the same network as the DataFort server interface.

For every AV scanner and filer that need to communicate with each other there must be a unique client side VIP and a unique server side VIP to facilitate that connection.

Two IP addresses will be added for each AV scanner that will be used with DataFort. If you set up multiple AV Servers, you can add more using the same command. For example:

```
vip add -i clients --cifs-domain domain1.domain.com df-cvscan1
vip add -i file-servers --cifs-domain domain1.domain.com df-svscan1
vip add -i clients --cifs-domain domain1.domain.com df-cvscan2
vip add -i file-servers --cifs-domain domain1.domain.com df-svscan2
```

4. Set up routes from the server issuing the virus scan request to the AV scanner. If you set up multiple AV Servers, you can add more using the same command. For example:

   For EMC CAVA servers, enter:

```
vscan route add cifs_server vscan1 df-cvscan1 df-svscan1 emc
vscan route add cifs_server vscan2 df-cvscan1 df-svscan2 emc
```

   For NetApp VScan servers enter:

```
vscan route add netapp1 vscan1 df-cvscan1 df-svscan1 netapp
vscan route add netapp2 vscan2 df-cvscan1 df-svscan2 netapp
```

5. Add the share to be scanned as represented by the NAS array to DataFort:

```
vscan share add \\cifs_server\exported_share /fs_vol1/cifs/share1
```

For CAVA, this share can be found from `EMC Celerra Manager->DataMover->CIFS->Path`.

For NetApp, this share representation can be found by typing `cifs shares` on the NetApp NAS array console.

Registering AV Scanner with DataFort

Use the CAVA or NetApp documentation to find the appropriate command line interface commands.

EMC CAVA

To register the AV scanner with DataFort:

1. Log in to EMC Celerra Manager by a SSH session.
2. Edit the viruschecker.conf file by adding the df-svscan1 IP address. In CAVA CLI, enter:

   ```
   vi /nas/tmp/viruschecker.conf
   ```

3. Add the IP address of df-svscan1 to the viruschecker.conf file.
4. Save the updated viruschecker.conf file.
5. In CAVA CLI, enter:

   ```
   server_file DataMover -put viruschecker.conf viruschecker.conf
   server_viruschk DataMover -update
   ```

6. In CAVA CLI, enter:

   ```
   server_viruschk DataMover
   ```

7. Verify that the DataFort VIP is set up properly and that its status is ONLINE. Take the appropriate action as outlined in Table 1.

Table 1: CAVA Message and Action

CAVA CLI message	Action
`ERROR_AUTH`	Verify that the CAVA domain user is added to the Administrator group of the AV scanner. See the CAVA documentation for instructions.
`ONLINE`	Begin using the system normally. If DataFort does not detect a virus file, reboot the AV Scanner.

NetApp VScan

To register the AV scanner with DataFort:

1. Start the Virus Scanning software (for example: Symantec, MacAfee, TrendMicro).
2. Open the Configuration page.
3. Set the RPC client to be the client-side VIP added (for example df-scscan1 and df-cvscan2).

   Note: The virus scanning service must be running as an account that has access to the Cryptainer according to the DataFort ACLs.

NOTES FOR VIRUS SCANNING

Scanning Unencrypted Files

After configuring AV scanners as described above, all virus scanning will be done through DataFort. There are two options for scanning files that are written directly to the NAS array (with data not encrypted by DataFort):

- For each share that will be accessed directly, create a cleartext Cryptainer on the DataFort and add the corresponding share using the **`vscan share add`** command as for encrypted Cryptainers.
- Partition the encrypted/unencrypted data between two or more vfilers (arrays).

Deleting a Cryptainer

If you delete a Cryptainer that had an associated **`vscan`** share and then later add the Cryptainer back, you must manually delete the **`vscan`** share and add it back.

Troubleshooting

You may see errors on the NetApp console in the following form:

> Mon Aug 30 08:31:06 PDT [rpc_0:warning]: CIFS: Virus scanner <ip of virus scanner> completed a scan on modified file <path to file> for client <ip of client> as user <user> but returned the following status: [0x5] and status message: Internal server error

Such errors could be caused by:

- Scanning cleartext files direct to the NAS array (bypassing DataFort) without adding a cleartext Cryptainer for the associated shares
- Scanning unencrypted files that are mistakenly placed inside of encrypted Cryptainers
- Scanning cleartext files inside of shares when no Cryptainer exists
- A Cryptainer without a matching **`vscan`** Cryptainer alias

For example, to find out if every Cryptainer has a matching **`vscan`** Cryptainer alias, type:

```
cryptainer list
```

For NetApp VScan DataFort **`cryptainer list`** output should look similar to this:

```
------------------------------------------------------------------------
Type | Name                                              |Options    |
|----|---------------------------------------------------|-----------|
|cifs|\\netapp1\cryptainer1                                |e-------a- |
|cifs|\\netapp1\VSCAN_ADMIN$\cryptainer1                   @|e-------a-|
|cifs|\\netapp1\cryptainer2                                |e-------a- |
|cifs|\\netapp1\VSCAN_ADMIN$\cryptainer2                   @|e-------a-|
------------------------------------------------------------------------
listed: 4 object(s)
```

For EMC CAVA DataFort **`cryptainer list`** output should look similar to this:

```
------------------------------------------------------------------------
Type | Name                                                |Options    |
|----|-----------------------------------------------------|-----------|
|cifs|\\cifs_server\cryptainer1                              |e-------a- |
|cifs|\\cifs_server\CHECK$\cryptainer1                       @|e-------a-|
|cifs|\\cifs_server\cryptainer2                              |e-------a- |
|cifs|\\cifs_server\CHECK$\cryptainer2                       @|e-------a-|
------------------------------------------------------------------------
listed: 4 object(s)
```

APPENDIX III 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
CIFS Protocol	Clients	Windows 2000 Windows Server 2003 Windows XP Windows 98 Windows NT 4.0 SP 6
	File Servers	BlueArc EMC IP4700 EMC Clarion NetApp filers running Data OnTap Samba Windows 2000/Windows Server 2003 Windows NT 4.0 SP 6 Windows XP
NFS Protocol	Clients	Support v2 and v3 NFS UDP and TCP protocols
	File Servers	Support v2 and v3 NFS UDP and TCP protocols

SPECIFICATIONS

- DataFort E510 Specifications
- DataFort E515/E515A Specifications

TABLE 2: DATAFORT E510 SPECIFICATIONS

Item	Detail	Specification
Hardware	Rack mountable	Standard 19" EIA rack (2U height)
	Weight	34.6 lbs (15.7 kg)
	Size	43.2 cm (17.00") W x 8.8 cm (3.46") H x 53.2 cm (20.95") D
	Security	Chassis: Optional pick-resistant Medeco lock, intrusion detection
	Network Ports	Two Gigabit Ethernet (IEEE 802.3ab compliant) ports for network connectivity and management 10/100/1000Base-T, autonegotiation required
	Serial Port	RJ45 serial console port
	Power Supply	2 Universal: 100-240V/6A, 50/60 Hz, Hot swappable
	LED	Power status, network activity
	LCD	Liquid Crystal display with touch-panel capability
	Smart Card	1 internal smart card reader
Environment	Temperature	Operating Temperature: 5°C to 40°C (41°F-104°F) Storage Temperature: -10°C to 60°C (14°F-140°F)
	Humidity	Operating Humidity: 85% RH at 35°C
Regulatory Compliance	EMC	Canada ICES-003 Class B United States FCC Class B Japan VCCI Class B Korea RRL Class B European Community CE (EN55022 Class B, EN55024, EN61000-3-2 Class A, & EN61000-3-3) Australia/New Zealand AS/NZS 3548 Class B International CISPR 22 Class B
	Safety	Canada CSA 60950 United States UL 60950 Japan IEC60950 A4 European Community EN60950, TUV International IEC 60950

TABLE 3: DATAFORT E515/E515A SPECIFICATIONS

Item	Detail	Specification
Hardware	Rack mountable	Standard 19" EIA rack (1U height)
	Weight	E515: 10.4 kg (22.9 lbs) E515A: 11.3 kg (25.0 lbs)
	Size	43.2 cm (17") W x 4.4 cm (1.73") H x 53.2 cm (20.95") D
	Security	E515 and E515A chassis: Optional pick-resistant Medeco lock, optional CryptoShred button E515 chassis: intrusion detection
	Network Ports	Two Gigabit Ethernet (IEEE 802.3ab compliant) ports for network connectivity and management 10/100/1000Base-T, autonegotiation required
	Serial Port	RJ45 serial console port
	Power Supply	E515: 100-240 VAC/3A, 47-63 Hz E515A: 90-250 VAC, 3.5A, 47-440 Hz
	LED	Front LED: Power/Fault
	LCD	Character display, 20 characters by 2 lines
	Smart Card	1 internal smart card reader
Environment	Temperature	Operating Temperature: 5°C to 40°C (41°F-104°F) Storage Temperature: -10°C to 60°C (14°F-140°F)
	Humidity	Operating Humidity: 85% RH at 35°C
Regulatory Compliance E515	EMC	Canada ICES-003 Class B United States 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

Appendix IV Partial List of ISO Country Codes

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

Table 1: ISO Country Codes

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

APPENDIX V GLOSSARY

ACL — Access Control List. A list of users with permission to access a resource on a network. DataFort maintains ACLs for Cryptainers: each Cryptainer is matched to a user or group of users with permission to access data in that Cryptainer.

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.

chassis — The physical encasement of a device. DataFort is designed to resist and detect any attempt to open the chassis.

CIFS — Common Internet File System. A protocol used by computers to access files and directories over a network. CIFS is a public version of the SMB (Simple Message Block) protocol, developed by Microsoft, therefore CIFS-compliant devices are able to access Windows files over a network.

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.

client	A device which initiates requests as part of a client/server model. In this model, one entity (the client) requests a resource from a second entity (the server). An example of this model can be found when a workstation makes a request for data from a storage device: the workstation is the client, and the storage device is the server.
cluster	A cluster is a set of interconnected devices. If one fails, the other can continue providing the service. By clustering DataFort devices, total system redundancy is increased, decreasing the probability of any downtime.
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. Data within a Cryptainer can be encrypted by DataFort with a Cryptainer Key, using AES.
cryptography	The science of rearranging data by applying algorithms mathematically to combine cleartext and an encryption key. The resulting ciphertext appears to be random, but contains all of the original information.
DataFort CLI	The command line interface used to manage the DataFort device. The CLI allows remote users to log in to DataFort and administer it by entering text commands over SSH.
DataFort WebUI	A graphical user interface used to manage the DataFort device via a web browser using SSL. Commands are entered by selecting from drop-down menus and filling out web forms.
failover	The ability to withstand the failure of one or several system components by transferring access to data from a failed path to a healthy one.
IKE	Internet Key Exchange. IKE is a key management protocol standard that is used in conjunction with the IPsec standard.
IPsec	Internet Protocol Security. A standard for secure network communication. Communication between clustered DataFort devices occurs over IPsec; IPsec communication is a licensed option between DataFort and clients.
key	In cryptography, a key is a value applied to cleartext (using an algorithm) in order to generate ciphertext, or applied to ciphertext to generate cleartext. Each cipher requires a key in order to encrypt or decrypt data.
LDAP	Lightweight Directory Access Protocol. A network protocol for accessing a hierarchical directory of information on a directory server. The directory server contains information such as usernames, passwords and email addresses.

Lifetime Key Management (LKM)	Decru's proprietary solution for encryption key management. LKM software and the LKM appliance both store key information.
Management Station	A Windows PC equipped with a smart card reader, from which a DataFort administrator can manage the DataFort via the DataFort WebUI.
Master Key	The Master Key is generated by DataFort at initialization time, and is unique to each DataFort. It is ultimately required in order to decrypt other keys in the configuration database.
MIB	Management Information Base. A set of network objects that can be managed using the Simple Network Management Protocol (SNMP).
NAS	Network Attached Storage. Hard disk storage connected to a LAN (Local Area Network) and assigned an IP address, not attached directly to a computer.
NFS	Network File System. A network protocol typically used with Unix systems which allows users running an NFS client to store and access files on remote computers running the NFS server as if they were local.
NTP	Network Time Protocol, used to synchronize computer clocks on the Internet.
quorum	The minimum number of Recovery Officers required to complete sensitive DataFort management procedures.
RAID	Redundant Array of Inexpensive Disks. In a RAID, storage access is virtualized so that a group of disks is exposed to the network as a single virtual disk volume.
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.
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.
UDP	User Datagram Protocol. User Datagram Protocol is a communications protocol for messages between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP). Services that can be run on both TCP and on UDP (such as NFS) are often deployed with UDP when speed is a concern and deployed with TCP when on a lossy network.

Appendix VI Regulatory and Certifications

- FCC B Declaration of Conformity
- European Union
- Canadian ICES-003
- VCCI Class A Statement
- CE Statement

FCC B Declaration of Conformity

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

In order to maintain compliance with FCC regulations, shielded cables must be used with this equipment. Operation with non-approved equipment or unshielded cables is likely to result in interference to radio and TV reception. The user is cautioned that changes and modifications made to the equipment without the approval of manufacturer could void the user's authority to operate this equipment.

European Union

This equipment is intended to operate under the following environmental conditions with respect to EMC:

1. A separate defined location under user's control.
2. Earthing and bonding shall meet the requirements of ETS 300 253 or CCITT K27.
3. Where applicable, AC power distribution shall be one of the following types: TN-S and TN-C [as defined in IEC 364-3] In addition, if equipment is operated in a domestic environment, interference may occur.

Canadian ICES-003

This Class A digital apparatus meets all requirements of the Canadian ICES-003 Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutee les exigences du Regiements sur le material brouilleur du Canada.

VCCI Class A Statement

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－ A

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take corrective actions. VCCI-A

CE Statement

The standards compliance label on the appliance contains the CE mark which indicates that this system conforms to the provisions of all European Council Directives, laws, and standards.

The appliance is in conformity with the provisions of the following EC Directives, including all amendments, and national legislation implementing these directives:

- 89/336/EEC
- 93/68/EEC
- 73/23/EEC

The following harmonized standards have been applied

- EN55022: 1998 Plus A1: 2000 & A2: 2003
- EN61000-3-2: 2001
- EN61000-3-3: 1995 Plus A1: 2001
- EN55024: 1998 Plus A1: 2000 & A2: 2003
- EN60950-1: 2001+A11: 2004

INDEX

A

Access Control List (ACL) 132, 290
  ACL Capture 135
  ACL Preview 107
  ACL Sync 107
  CIFS 95
  Cryptainer ACL management 134
  end user Cryptainer ACL management 146
  NFS 240
  Use Local ACL 168
Adding and Removing Cluster Members 198
Admin Card 18, 290
  associate with administrator 83
administrator 18, 290
  add 81
  associate card 83
  associate with Admin Card 83
  change password 85
  change the card association 87
  delete profile 87
  dual authorization, login 70
  login to CLI 71
  login to WebUI 68
  new 89
  number recommended 81
  require login authorization 84
  roles outlined 78
  Security Administrator 113, 152, 179, 184
  specialty administrator, create 82
administrator roles 78
administrator roles, CLI 231
AES 16, 290
alert, clearing 164
ARP table 235
associate Admin Card with administrator 83
auditing DataFort logs 191
authentication 18, 290
authorization for login 84
authorizing administrator 84
auto giveback 198, 205
automatic domain sync 130
automatic domain sync disabled 130

B

backup
  DataFort configuration 26, 179
backup, data
  planning 32
battery iv, 39

C

Category 5 cable 19, 42, 43, 74
certificates
  Management Station to DataFort 208
change password
  administrator 85
change password, Recovery Card 177
changing the user's password 143
chassis 16, 290
  intrusion 162
  lock 16
CIFS 15, 290
  administration example 248
  CIFS message signing 110
  data access example 138
  DataFort domain access user 36
  domain types 93
  groups 250
  Security Policy settings 167
  SMB signatures 110
  supported clients and file servers 286
  User Registration 142
ciphertext 16, 290
ciphertext and cleartext 24, 138, 290
clear all DataFort settings 193
clear an intrusion (defense alert) 164
clear smart cards 178
cleartext 16, 290
CLI 71
  command help 230, 269
  commands and admin roles 231
  connect from SSH client 71
  general information 230, 269
  help 275
  login 71, 147
  permissions 229

Quick Reference 268
quit 275
system commands 233, 278
time-out 269
top level commands 270
turn off Secure Web 260
WebUI access 72
CLI documentation 230, 269
CLI login with dual authentication 72
Clients NIC
changing IP address in cluster 200
Clients NIC Management Access 169
connecting to client subnet 42
interface for unencrypted data 42
cluster 291
auto (crypto) failover 205
auto giveback property 205, 232
change configurations 200
change IP address of member 200
change network 200
change to standalone 200
check failover status 198
commands, CLI 277
configure for STP 204
failover 24, 31, 200
forming, after initial setup 198
heartbeat 25, 277
intrusion detection 205
IPsec tunnel 25
load balancing 25
management 196
management using CLI 232
manual failover 200
recover from failover 199
recovery guidelines 202
remove member 200
replace an offline member 202
requirements 199
resolving conflict 203
restore previous configuration 202
set properties with CLI 204
state 198
state after wizard 89
troubleshooting 266
VRID 201
cluster conflict 203
cluster disable command 232
cluster size 196
cluster-wide operations 197
Common Internet File System (CIFS) 15
configuration database 17, 291
applied to new DataFort 257
backup to LKM 89, 180
backup using WebUI 183
changes synchronized in cluster 25
contents 179
event log capacity 185
purging unused keys after backup 182
size 182
used for recovery 257
Cross Mapping, iSCSI Cryptainers 126
Cryptainer 291
Access Control menu 107
access, inherited from group 130
access, NFS, with CLI 240
ACL 107, 132, 134
add, with WebUI 101
aliases 253
before creating 88
cleartext 106, 240
create (add), with WebUI 106
create CIFS, with CLI 250
create multi-protocol, with CLI 246
create NFS, with CLI 240
Data Encryption 106
defined 17
Delete 107
Filename Encryption 106
icon with no lock 106
Initial Encryption 107
IP address restriction 107, 108
IPsec, require for client 107, 108
key 107
manage CIFS, with CLI 248
manage multi-protocol, with CLI 243, 246
manage NFS, with CLI 236, 239
manage, using WebUI 107
mount, NFS 140
multi-protocol 96
NFS with root access, CLI 240
NFS, view ACL with CLI 241
options when creating 106
owner 102
owner (NFS), CLI 240
Rekey 107, 108
Require IPsec 106

Restore command, WebUI 106, 126
restoring 252
share level or sub-share level 95, 96
troubleshooting CIFS 261
troubleshooting NFS 263, 265
Cryptainer encryption key 17
Cryptainer ID 128
Crypto Failover 205
cryptographic test 217
CryptoShred 17, 165
CryptoShred button 17, 162, 165
states 165

D

data
encryption 17
migration 141
DataFort
administrators 217
assigning IP settings 44
back panel connections 41, 74
capacity 22
CLI, connecting to 71
connecting ports to network 42
DataFort Password 142, 168
DATAFORT_ADMIN domain 132
Defense Setting 162
deployment 29
diagram, back panel 41
Domain Access User 36
domains 92
emergency shutdown 165
groups 132
LDAP User 37
licenses 57, 213
Login page 68
management interfaces 66
recovery 257
Recovery Officers 217
restoring a previous configuration 257
specifications 287
troubleshooting 256
upgrading 207
users 18, 130
WebUI, connecting to 68
where installed 16
zeroizing 193
DataFort CD-ROM 19
DataFort CLI 71, 291
login 71
DataFort CLI Reference Guide 229, 268
DataFort Throughput 217
DataFort WebUI 68, 291
login 68
DCS
administrator roles 231
requirement on Cryptainer 241, 251
decru file 138
Decru licenses 57, 213
Decru Management Console 219
menus 219
Decru MIB 76, 214
Decru Signed Syslogd (DSS) 186
default security setting 169
defense
alert, clearing 164
response 162
triggers 162
Defense Setting
changing after setup 162
summary 162
defense setting 27, 162
deleted Cryptainer
purge unused keys 182
restore 112, 128
deleting targets 126
disable automatic domain sync 130
disabling a cluster member 232
DMC 219
documentation 19
domain 92
add CIFS, with CLI 248
add multi-protocol, with CLI 243
add NFS, with CLI 236
add, with WebUI 97
join VIP to CIFS domain 171
manage CIFS, with CLI 248
manage multi-protocol, with CLI 244
manage NFS, with CLI 237
name 97
select for user registration 142, 144
types and subtypes 92, 93
userless 94
domain controller
and DataFort 130
dual authentication login, CLI 72

dual authentication login, WebUI 70
dual authorization 70, 72, 84

E

emergency shutdown 165
emergency zeroization via serial console 195
Enabling SNMP 214
enabling TLS 35
encrypted file, viewing 139, 140
encryption 16
end user
  access to Cryptainers 24
  DataFort password 145
  login to CLI 147
  login to WebUI 146
  manage Cryptainer ACL 146
  notification 138
  Windows password 142, 143, 144
escrow service 26
event logs 185
export, NFS 96, 236

F

failover 24, 290, 291
  Ethernet switch configuration 31
  recovering a cluster 199
  status 198
fan modules, replacing 267
feature licenses 57
Fibre Channel 15
File Servers NIC
  changing IP address in cluster 201
  connecting to file servers subnet 42
  interface for encrypted data 42
file servers subnet 42
filename encryption 106
Floating 101, 117, 125
front panel
  display 75
  LCD used to assign IP address 44
  LED 258
  System Card slot 41
Front Panel Dual LEDs - 2U 258
Front Panel LEDs - 1U 258
FTP 150
  commands, CLI 272
  home directory 150
full database 182

G

Group Review 132, 168
  accept changes 133
groups, imported from domain controller 130

H

hardware maintenance 267
hidden .decru file 138
hidden shares, naming 95
Home page
  link to NAS Topology 96, 115
  new user alert 132
  returning to 68
HTTP 148, 272

I

IKE 291
initial encryption of Cryptainer 107
installation
  in rack 40
  planning 24
  precautions iv, 40
  requirements 19
International Organization for Standardization (ISO) 211, 289
Internet Explorer 286
  for accessing WebUI 68
  user access to DataFort 142, 145, 146
intrusion detection 162, 164
  in cluster 205
IP address 19
  additional for server 105, 124
  DataFort, assigning 44
  DataFort, current 217
  IP restriction 107, 108
  of CIFS server, in configuration database 249
  preserve during zeroization 193
IP settings
  assigning from LCD 44
  assigning from serial console 74
  changing, with WebUI 207
  DataFort, assigning from serial console 45
IPsec 25, 291
  add rules to DataFort, with CLI 172, 254
  configure Solaris clients 173
  configure VIP, with WebUI 109, 125
  configure Windows clients 173
  Kerberos rule for Windows clients (CLI) 170

require for clients 106, 107
support 170
iSCSI node name 17
ISO 289
IT power systems iii, 39

J

join CIFS domain 171

K

Kerberos authentication 254
client to DataFort requires joining domain 170
configure DataFort, with CLI 170, 254
used without IPsec 171
with LDAP server 37
key 291
encryption key 17, 107
escrow 26
Key Purging 180
key, chassis 162

L

LCD 75, 218
assigning DataFort IP settings 44
bar graph 75
buttons 76
touch panel interface 66
web page 218
LDAP 291
supported server schemas 93
User for DataFort 37
with CIFS or NFS domains 93
LED 258
LEDs
power supply 258
licenses 19, 213
IPsec 254
managing 213
Lifetime Key Management (LKM) 17, 292
limited administrator 84
Limits
Number of DataFort appliances in a cluster 22
Lithium battery iv, 39
LKM 26, 180
secondary server support 36
server saves latest configuration backup 26
server, requirements 36
server, specifying settings in WebUI 89, 180
LKM appliance setup 36, 89
LKM servers
number supported 180
LKM software setup 36
LKM using SSL 181
load balancing 25
with IP addresses 109
Local domain 94
login
CLI 71
CLI, dual authorization 72
CLI, end-user 147
requiring authorization 84
WebUI 68, 70
WebUI, dual authorization 70
WebUI, end-user 146
Login page 68
logs, DataFort 185
auditing 191
configuring storage location 186
Decru Signed Syslogd (DSS) 186
filtering 190, 217
guidelines 185
syslog mapping table 189
temporary file mapping 189
viewing, with WebUI 189

M

Management Console 66
Management Console installation 35
Management Station 18, 292
for WebUI 96, 115
Management Console installer 35
requirements 286
Management Station requirements 34
Management Station security 35
Master Key 17, 292
metadata 186
MIB 76, 214, 292
mounting DataFort in rack 40
mounting shares, NFS 140
MPIO 116, 118, 125
multi-appliance management 219
multi-protocol Cryptainer 96
ACL Sync after restore 112
add, with WebUI 101
create and manage, with CLI 243
owner 102

multi-protocol server
  add, with WebUI 97, 98
multi-protocol share
  add, with WebUI 99
  virtualize, with WebUI 101

N

NAS 15, 292
  network diagram 16, 24, 30
NAS Topology view 96, 97, 115
nas-admin 132
nas-user 132
NDMP (Network Data Management Protocol) 32
network
  connection to DataFort ports 41
  diagram, NAS 16, 24, 30
  information needed for setup 34
  manage, with CLI 235
  planning backup and restore 32
  settings, changing 207
Network Attached Storage (NAS) 15
network commands, CLI 235
Network File System (NFS) 15
Network switch ports 19
NFS 15, 273, 292
  administration example 236
  Cryptainer ACL 240
  data access example 140
  domain types 93
  groups 240
  preparing the network 96, 236
  supported clients and file servers 286
NIS 93
node name 17
NTP time server 19

O

online help 67, 228
owner, of Cryptainer 102

P

Parent Key 17
password
  administrator, changing 85
  end-user DataFort password 142, 168
  one-time, CLI 71
  Recovery Card, changing 177
port
  Clients 42
  File servers 42
  forwarding 253
power
  precautions iii, 39
power button 46
power cord 19
power down DataFort 46
power supply
  LEDs 258
  notice iii, 39
  replaceable 267
  specifications 288
powering down 46
powering up 46
primary filer 32
protect against insider attacks 84
purging keys 182

Q

quorum 19, 26, 175, 176, 178, 292

R

rack installation 40
rack mounting kit 19
Real NAS Elements 96, 115
real server
  add and manage CIFS, with CLI 249
  add and manage multi-protocol, with CLI 244
  add and manage NFS, with CLI 238
  add, with WebUI 98
  manage, with WebUI 105
Recovery Cards 18, 175, 292
  change password 177
  replacement procedure 175
Recovery Officers 18, 292
  required for forming cluster 203
  required for replacing DataFort 202, 257
  required for replacing Recovery Card 153, 175
  required for Setup 48
rekey jobs, status 108
Remote Desktop 68, 260
remote filer 32
replacing a Recovery Card 175
replacing an offline cluster member 202
requiring login authorization 84
reset DataFort 193
reset smart cards 178

restore a previous DataFort configuration 257
Restore Cryptainer 106, 126
restore, planning 32
Reviewing the Cluster Load Balance 205
RJ45 to DB9 adapter 19, 43, 74

S

SAN 15
secret share 292
Secure CLI 67, 169
  login 71
  turn on and off via WebUI 169
Secure CLI default setting 166
Secure Password Update 168
secure shell (SSH) support 66
Secure Sockets Layer (SSL) 66
Secure Web 67, 68, 169
  turn on and off via CLI 260
  turn on and off via WebUI 169
Secure Web default setting 166, 169
SecureView 67
Security Administrator 113, 152, 179, 184
Security Certificate 208
  Certificate Authority Signed, installing 211
  self-signed, installing 208
Security Domain 19, 292
  planning 22
Security Policy 166, 167
  customize 167
  planning 26
  pre-configured levels 166, 167
security, implementing and maintaining 22
Sensors 218
SEP 16, 205, 217, 293
serial console 74
  assigning DataFort IP settings 45
  clearing IP Settings 74
  connecting serial port 43, 74
  emergency access 195
  interface 66
  menu options 74
  zeroizing DataFort 75
serial number 218
server
  add CIFS, with CLI 249
  add multi-protocol, with CLI 244
  add NFS, with CLI 238
  add, with WebUI 98
  manage CIFS, with CLI 249
  manage multi-protocol, with CLI 244
  manage NFS, with CLI 238
  manage, with WebUI 105
  multi-protocol 97, 98
servicing DataFort 267
share
  add CIFS, with CLI 249
  add multi-protocol, with CLI 245
  add NFS, with CLI 239
  add, with WebUI 99
  CIFS 95
  icons 101
  manage CIFS, with CLI 250
  manage multi-protocol, with CLI 245
  manage NFS, with CLI 239
  manage, with WebUI 106
  multi-protocol 99
  view CIFS shares 138
  view NFS shares 140
  virtualize CIFS, with CLI 250
  virtualize multi-protocol, with CLI 246
  virtualize NFS, with CLI 239
  virtualize, with WebUI 101
shutting down 46
size of the configuration database 182
smart card reader 18, 19
  installing 35
  port connection 35
Smart Card Reset 178, 185
smart cards 19, 293
  checking versions and status 178
  reset procedure 178
  summary 18
  troubleshooting 267
SMB signatures 110
SnapDrive 114, 126
SnapMirror 32
snapshot 32
SNMP 66, 214, 293
  MIBs 214
  setting with WebUI 214
  turning on and off 214
  version 215
software CD-ROM 19
spanning-tree protocol 31, 204
specialized administrators 78
specifications 285

SSH 66, 293
  CLI access 71, 72, 230
SSL 148, 181, 293
stack trace 235
Standard CLI 71
standard rack mount 40
status and settings 216
Storage Area Network (SAN) 15
Storage Encryption Processor (SEP) 16
STP 31, 204
supported platforms 286
switch connections in a cluster 25
syslog, syslogd (syslog daemon) 185, 188
System Card 18, 293
  inserting 41
  removing, in emergency 165
System Config menu (WebUI)
  General, Upgrade 207
  Network, IP Settings 207
  Network, SNMP Agent 214
  Recovery, Backup 183
  Recovery, Replace Recovery Card 175
  Security, Security Policy 166, 167
  Security, Zeroize 193
  System Users 217
  System Users, Administrators 89
  view settings 217
System Info menu (WebUI)
  Status 218
  Status, Log 189, 217
system properties, CLI 233
System Requirements 286
system users 217

T

TAP 153, 227
tape compression 207
Tape Settings 207
tape settings 207
TEP 153, 227
Termial Services 260
Terminal Services 68
TFTP 151, 273
time and date
  setting from WebUI 185
time servers 185
time-out
  CLI 71
  serial session 74
  WebUI 68
trap 215
troubleshooting 256
  CIFS Cryptainers 261
  clusters 266
  network connections 259
  NFS Cryptainers 263, 265
  smart cards 267
Trustee Acceptance Package 153, 227
Trustee Establishment Package 153, 227
Trustees 153

U

UDP 293
upgrading DataFort 207
USB 19
Use Local ACL 168
user management of Cryptainer ACL 146
User Mapping 94, 168
user notification 138
User Registration 142, 168
  instructions for user 142, 145
user updating password information 144
userless domain 94
users and groups
  CIFS, manage with CLI 250
  manage access 130, 134
  NFS, manage with CLI 239, 240

V

Verifying System Logs 234
Virtual NAS Elements 96, 115
virtual server (VIP)
  add NFS, with CLI 238
  configure IPsec 109, 125
  manage CIFS, with CLI 249
  manage multi-protocol, with CLI 244
  manage NFS, with CLI 238
  manage, with WebUI 109, 125
  planning 24
  set certificate 109, 125
virtualize
  CIFS share, with CLI 250
  multi-protocol share, with CLI 246
  NFS share, with CLI 239
  share, with WebUI 101
VLAN commands, CLI 274

VLAN Tagging 255
VRID 25
  changing 201
VRRP (Virtual Router Redundancy Protocol) 25

W

Web Access 148
WebCLI 72
WebDAV 148, 149
WebUI
  accessing 68
  keyboard shortcuts 69
  login 68, 146
  login with Secure Web 68
  required display setting 68
  time-out 68
  user registration 142
WebUI access to cluster members 197
WebUI login with dual authentication 70
Windows
  domain access user for DataFort 36
Windows event logging 186
Windows Event Viewer 186

Z

zeroization without admin card 195
zeroizing DataFort 193
  using serial console 195
  using WebUI or CLI 193