DECRU®
A NetApp Company



ADMINISTRATION GUIDE

DataFort E-Series
Version 3.1.1

security

DataFort Administration Guide for E-Series DataFort Appliance

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

Part number:210-03976 A0 (011608_E311)

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 (over-current) 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 **18**
About the Decru DataFort Security Appliance 19
Encryption 19
Common Criteria Compliance 20
Hardened Architecture 20
CryptoShred Feature 20
Compartmentalization of Functions 20
Key Management 21
Lifetime Key Management Solutions 21
Configuration Database 21
Authentication Layers 22
DataFort Users 23
Security Domain 23
Installation Requirements 24
Conventions Used in this Manual 25

Chapter 2 Planning the Network Configuration **26**
Decru DataFort Capacity 27
Installation Considerations 28
Planning the Security Domain 28
DataFort Appliance Clusters 29
Failover Support in a Cluster 29
VRIDs for Cluster Members 29
Load Balancing in a Cluster 29
IPsec in a Cluster 29
Switch Connections in a Cluster 30
Virtualization 31
Virtual Server Names and IP Addresses 31
End-User Access 31
Secure Network Practices 32
Maintaining Configuration Database Backups 32
Sending Recovery Cards to Escrow 32
Planning Remote Security Logging 32
Removing the System Card 33
Preparing for Manual Security Responses 33
Placing DataFort in the Network 34
Client Co-location 34
Server Co-location 35
Workgroup Placement 35
Cluster Failover Network Topology 38
Configuring Switches for Failover 39
Planning Data Backup and Restoration 40
Snapshot Support 40

SnapMirror™ Support 40
NDMP Support 40

Chapter 3 Preparing to Install DataFort 41
Collecting Network Information 42
Preparing the Management Station 43
Management Station Security 43
Running the Installer 44
Setting Up Lifetime Key Management 45
Adding the DataFort Domain Access User 46
DataFort Windows Domain Access User 46
DataFort LDAP User 46

Chapter 4 DataFort Appliance Installation 47
Notices and Warnings 48
Power Supply Notice 48
Power Cable Notice 48
Dual Power Supply Notice 48
Lithium Battery Notice for Service Personnel 48
Perchlorate Present 48
Rack Mounting the Appliance 49
Unpacking the Appliance 49
Selecting a Location 49
Rack Mounting 49
Connecting the Appliance 51
Inserting the System Card 51
Connecting the Rear Panel Ports 52
Connecting Power 54
Assigning the Appliance IP Address 55
Setting the IP Address Using the LCD 55
Setting the IP Address Using the Serial Console 56
Powering Up and Shutting Down 57

Chapter 5 Initializing Appliances 58
About the Setup Wizard 59
Setup Wizard Functions 59
Incomplete Setup Wizard 59
About Smart Cards and Readers 59
About Remote Authorization 60
Initializing a Standalone Appliance or Cluster 61
Connect to Head of Cluster 62
Sign License Agreement 62
Recover From Database 62
Create Administrator 62
Configure Cluster and Recovery Schema 63
Network Settings 64
Add Licenses 65

Network and Certificates 65
Insert Recovery Card 65
Apply Settings 67
Apply Settings 68
Adding a Member to a Cluster 69
Connect to Head of Cluster 70
Cluster and Recovery Schema 70
Network Settings 70
Add Licenses 70
Network and Certificates 70
Insert Recovery Card 71
Apply Settings 72
Apply Settings 73

Chapter 6 Appliance Management Interfaces 74
Management Interfaces Overview 75
SecureView 75
Security Policies 76
Online Help 76
Accessing the Decru Management Console 77
Using the DMC 77
Connecting via Standard DMC 77
Connecting via Secure DMC 78
Connecting via DMC using Dual Authorization 78
Connecting to the DataFort WebUI 79
Connecting via WebUI 79
Using the DataFort WebUI 79
Connecting to the Command Line Interface 80
Using the CLI 80
Connecting via Standard CLI 80
Connecting via Secure CLI 80
Connecting via CLI using Dual Authorization 81
Connecting to CLI via DMC 82
Serial Console 83
Logging in to the Serial Console Port 83
Configuring IP Settings 83
Clearing IP Settings 83
Zeroizing the Appliance 83
Appliance Front Panel LCD 84
Touch Panel Onscreen Buttons 84
SNMP Settings 85

Chapter 7 DataFort Admin Roles and Account Administration 86
Administrator Roles 87
Account Administration 90
Adding an Administrator 90

Requiring Authorization for Login 91
Changing the Administrator Password 92
Removing an Administrator 92
Adding or Changing a Card Association 93

Chapter 8 Before Storage Administration 94
Verifying DataFort Configuration 95
Verifying System Version 95
Checking Cluster State 95
Creating Additional Administrators 95
Configuring Remote Logging 95
Determining the Defense Setting 95

Chapter 9 Storage Administration 96
Understanding DataFort Domains 97
File Servers and Domains 97
User Authentication and Domains 97
Domain Types and Subtypes 98
User Mapping and DataFort Domains 99
Userless Domains 99
Preparing to Create a NAS Cryptainer 100
Create CIFS Shares 100
Create NFS Exports 101
Creating a NAS Cryptainer 102
Open the Decru Management Console 102
Servers and Portals 102
Add a Domain 104
Add a Server 104
Add a Share 105
Add a Virtual Server 105
Virtualize a Share 106
Add a Cryptainer 106
Cryptainer Ownership 106
Creating a NAS Cryptainer From a Home Directory 107
Creating a NAS Cryptainer Using Specialty Administrators 108
Managing Secure Network Attached Storage 109
Managing Domains 109
Deleting a Domain 109
Managing Servers 110
Editing a Server 111
Managing Shares 111
Options When Adding a Cryptainer 112
Managing Cryptainers 113
Adding Virtual Servers 116
Pre-Adding Virtual Servers to a Domain 117
Managing Virtual Servers 117
Editing a Virtual Server 119
Managing Virtual Shares 119

Editing a Virtual Share 120
Restoring a Cryptainer 121

Chapter 10 iSCSI Storage Administration 122
Preparing to Create an iSCSI Cryptainer 123
Setting up Groups 123
Using iSNS 123
Preparing to Create Cryptainers Using SnapDrive 123
Creating an iSCSI Cryptainer 124
Adding an iSCSI Portal 124
Options When Adding an iSCSI Portal 125
Virtualizing the Portal 125
Options When Adding a Virtual Server 125
Adding a CIFS share for Snap Drive Support 126
Adding an Initiator 127
Encrypting a Cryptainer 127
Configuring an Initiator 127
Configuring DataFort to Support MPIO 127
Managing Secure iSCSI Storage 128
DataFort DMC Icons 128
Managing Portals 129
Managing Virtual Servers and iSCSI Routes 130
Managing Targets and LUNs 131
Managing Cryptainers 131
Managing Initiators 132
Restoring an iSCSI Cryptainer 133
Cloning an iSCSI Cryptainer 134

Chapter 11 User Administration 135
Managing Groups and Users 136
Adding Users 136
Searching for Users 136
DataFort Groups 137
Group Review 138
Adding Individual Users to Group 138
Managing Cryptainer ACL 139
Cryptainer ACL 139
ACL Capture and ACL Sync 140
Requiring Smart Card for Cryptainer Access 142
Enforcing Two-factor Authentication 142

Chapter 12 Accessing Secure Data 144
CIFS Data Access 145
About Data Access 145
CIFS Data Access Example 146
NFS Data Access 147
NFS Data Access Example 147

Migrating Data 148
Secure Existing Data Using Initial Encryption 148
Secure Existing Data by Copying 148
CIFS User Registration 149
Registering the User's Windows Password 149
Registering the User's DataFort Password 149
Changing User Passwords 150
End-User Cryptainer ACL Management 151
End-User Login to DataFort CLI 152
HTTP Data Access 153
Web Access 153
WebDAV 154
Changing Web Configuration Using the DataFort CLI 154
FTP Data Access 155
FTP Home Directory 155
TFTP Data Access 156
TFTP Commands 156
Sample TFTP Configuration 156

Chapter 13 Key Administration 157
Managing Trustees 158
Trustee Scenarios 158
Setting Up Trustees 158
Creating Trustees on a Local Network 159
Creating Trustees on a Remote Network 162
Importing and Exporting Keys 167

Chapter 14 Backup Administration 168
Saving Configurations to Lifetime Key Management 169
Best Practices for Secure Backups 169
Configuring Backups to LKM Appliance 169
Configuring Backups to LKM Software 169
Backing Up the Configuration to LKM 170
Key Purging 170
Backing Up Configurations to a Remote Location 171

Chapter 15 Managing Appliance Security 172
Managing Appliance Defense Responses 173
Defense Triggers and Responses 173
DataFort Defense Setting 174
Changing the Defense Setting 174
Clearing a Defense Alert 174
CryptoShred Button States 175
System Card CryptoShred 176
Setting Security Options 177
Selecting a Configured Security Level 177
Customizing a Security Level 178
Configuring IPsec 181

Supported Clients and Authentication Methods 181
Adding a Kerberos Rule for Windows Clients 181
Kerberos Authentication without IPsec 182
Adding a Preshared Secret Rule for Clients 182
Relevant System Properties 183
IPsec Configuration for Windows Clients 183
IPsec Configuration for Solaris Clients 183
Managing Recovery Officers and Recovery Cards 185
Replacing a Recovery Officer 185
Changing a Recovery Card Password 186
Resetting Smart Cards 187
Setting Date and Time 188
Configuring and Viewing Logs 189
Appliance Log Storage Guidelines 189
Decru Signed Syslog (DSS) 189
Configuring Log Storage 190
Windows Event Logging 191
NAS Audit Logging 191
Setting Up Syslog 192
Viewing the Log 194
Verifying Signed Log Messages 196
Zeroizing Appliances 197
Before Zeroizing 198
Zeroizing Using the DMC **198**
Zeroizing Using the CLI 199
Zeroizing Using the Serial Console 200
Emergency Serial Console Port Access 200
Setting Security Certificates 201
Setting a Self-Signed Security Certificate 201
Setting a Certificate Authority Signed Certificate 202

Chapter 16 Cluster Administration 203
Cluster Management 204
About Failing Over a Cluster 204
About Moving a Cluster 204
Cluster-Wide Management via DMC 205
Checking the Status of the Cluster 205
Resolving a Cluster Conflict 206
Checking Failover Status 206
Recovering a Cluster from Failover 206
Adding and Removing Cluster Members 207
Adding a Cluster Member 207
Removing a Cluster Member 207
Replacing a DataFort Appliance in a Cluster 208
Recovering a Cluster 209
Changing Network Properties of a Cluster Member 210

Changing Configurations in a Cluster 210
Changing the Clients NIC IP Address of a Clustered Appliance 210
Changing the File Servers NIC IP Address of a Clustered Appliance 211
Changing the IP Address of an Appliance Using NFS Local Domain 211
Changing the VRID of a Clustered DataFort Appliance 212
Changing the IPsec Secret of a Cluster 212
Changing the Hostname of a Clustered DataFort Appliance 213
Setting Cluster Properties With the CLI 214
Configuring Cluster Members for STP 214
Cluster Crypto Failover Command 214
Auto Giveback 215
Reviewing the Cluster Load Balance 215

Chapter 17 Machine Administration 216
Changing Network Settings 217
Upgrading Appliances 218
Verifying an Upgrade Package 218
Managing Licenses 219
Viewing Licenses 219
Adding Licenses 219
SNMP Settings 220
About SNMP Options 220
Setting SNMP Options 221
Additional Appliance Management Tasks 222
Adding an Appliance 222
Logging into Appliances 222
Creating Custom Appliance Groups 223
Removing an Appliance from a Custom Group 223
Removing a Custom Group 223

Chapter 18 Appliance Settings and Status 224
Viewing Settings in the DMC 225

Chapter 19 Decru Management Console Functions 226
State Displays 227
About the Appliances Tab 228
Using Tab Table Columns 228
Appliance Menu 229
Edit Menu 230
View Menu 230
Configuration Menu 231
Keys Menu 232
Topology Menu 233
Utilities Menu 233
Security Menu 234
Trustee Menu 235
Diagnostics 236

Help Menu 236

Chapter 20 CLI Administration 237

Using the CLI 238
- Connecting to the CLI 238
- CLI Help 238

Administration Commands 239
- Administrator Roles 239
- Creating a New Administrator 239
- Cluster Management 240
- System Properties and Log Management 241
- Verifying System Logs 242
- Stack Trace Settings 243
- Network Management 243
- Backup Management 243

Changing Appliance Network Port Settings 244
- Setting the Media Type 244
- Enabling Jumbo Frame Support 244

CLI Management for NFS Cryptainers 245
- NFS Administration Example 245
- Manage Domains 245
- Manage Servers 247
- Manage Shares 247
- Manage Cryptainers 248
- Group Review 251

CLI Management for Multi-Protocol Cryptainers 252
- Multi-Protocol Administration Example 252
- Set DataFort Appliance Properties 252
- Manage Domains 252
- Manage Servers 253
- Manage Shares 254
- Manage Cryptainers 255

CLI Management for CIFS Cryptainers 257
- CIFS Administration Example 257
- Manage Domains 257
- Manage Servers 258
- Manage Shares 259
- Manage Users and Groups 259
- Manage Cryptainers 260

CLI Management for iSCSI Cryptainers 261
- iSCSI Administration Example 261
- Create Cryptainer 261

Restoring a Cryptainer 262
- Restoring a CIFS Cryptainer 262
- Restoring an NFS Cryptainer or Multi-protocol Cryptainer 262

Cryptainer Aliases 263

Port Forwarding 264
IPsec Configuration and Management 265

Chapter 21 VLAN Configuration 266
Configuring the Switch Ports 267
Configuring VLAN Data Access 268
Restricting DataFort Admin Access to a Specific VLAN 270

Chapter 22 Troubleshooting 272
Restoring an Appliance 273
Front Panel LEDs 274
Power Supply LEDs 275
Network Connections and Management Interfaces 276
CIFS Cryptainers 278
NFS Cryptainers 281
iSCSI Cryptainers 283
Clusters 284
Smart Cards 285
Hardware 286

Appendix I Command Line Interface Quick Reference 287
Using the CLI 288
CLI Syntax 288
CLI Help 288
CLI Command Overview 289
Top Level Commands 289
iSCSI commands 290
KFC Commands 290
Disk commands 290
CIFS Commands 290
Cryptainer Commands 290
Forwarding Commands 291
HTTP Commands 291
FTP Commands 291
iSNS commands 291
IPsec Commands 291
NFS Commands 292
Server Commands 292
Share Commands 292
TFTP Commands 292
Virtual Interface Commands 293
Virtual IP Commands 293
VLAN Commands 293
Virus Scanning Commands 293
CLI Formatting Commands 293
Help Command 294
Quit Command 294

Active-Role Commands 294
Authorize Command 294
Domain Commands 294
Group Commands 294
Password Command 295
Role Commands 295
User Commands 295
Whoami Command 295
Trustee Commands 295
Network Commands 295
Key Management Commands 296
LKM Management Commands 296
Cluster Commands 296
Database Commands 296
System Commands 297

Appendix II Logging Functions 298
Appliance Log Event and Priority Types 299
Log message parameters 299
Log Storage Locations 301
Log Presentation 302
Temporary Logs 302
Database Logs 302
Remote Logs 303
Log Purging 305
Audit Configuration 306

Appendix III DataFort Virus Scanning 308
Considerations Before Configuration 309
Preparing the Environment 310
Configuring DataFort for Virus Scanning 311
Registering AV Scanner with DataFort 312
Notes for Virus Scanning 313
Scanning Unencrypted Files 313
Deleting a Cryptainer 313
Troubleshooting 313

Appendix IV Port IDs 315

Appendix V Specifications 317
Supported Systems 318
DataFort Appliance Specifications 319

Appendix VI Partial List of ISO Country Codes 321

Appendix VII Regulatory and Certifications 322
FCC Declaration of Conformity 323
European Union 324

Canadian ICES-003 325
VCCI Class A Statement 326
CE Statement 327
Korea MIC 328
Taiwan BSMI 329

Appendix VIII DataFort Serial Adapter 330

Appendix IX Glossary 331

Index 335

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. The DataFort appliance 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, the DataFort appliance decrypts and then forwards the data to the appropriate destination.

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

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

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

This chapter includes the following topics:

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

About the Decru DataFort Security Appliance

When installed between clients and file servers or initiators and targets, the DataFort appliance 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.

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

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

Encryption

Using the AES (Advanced Encryption Standard) algorithm, the DataFort encryption system transforms cleartext (unencrypted data) generated by network clients or initiators into ciphertext (encrypted data) intended for storage. The DataFort appliance 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.

The DataFort appliance appends 512 bytes of data to each file header, and may also append 16 additional bytes. This small addition allows the DataFort appliance 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 the DataFort appliance in a manner compliant with Common Criteria standards are available from Decru.

Hardened Architecture

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

CryptoShred Feature

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

The DataFort appliance 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

The DataFort appliance 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.

The DataFort appliance 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

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

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

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

Lifetime Key Management Solutions

Decru's Lifetime Key Management (LKM) solutions—the LKM appliance and LKM server software—store encryption keys used by multiple DataFort appliances. This consolidates all key information for the purpose of emergency data recovery. LKM retains all encryption keys, even if they are purged from the DataFort appliance or the source DataFort appliance 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 appliance. A configuration database can be saved and used to restore or clone an existing DataFort appliance.

Authentication Layers

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

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

System Card

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

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

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

Admin Cards

An Admin Card adds an additional optional authentication layer to the communication between the administrator and the appliance. Admin Cards can be used for one or more appliances (including a cluster or separate appliances). Although administrators may elect to allow logins based on username and password, there are advantages to requiring smart card authentication:

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

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

Recovery Cards

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

DataFort Users

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

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

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 appliance-verified security parameters.

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

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

User Management Interfaces

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

Security Domain

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

Installation Requirements

In order to install and configure an 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 appliance.
- User CD. The CD contains software necessary for appliance operation, such as the smart card reader driver and Decru Management Console installer.
- Serial adapter (custom RJ45 to DB9 adapter) and Category 5 cable for a serial connection.
- AC power cord or cords appropriate for the appliance model and location.
- Decru smart cards, including System, Admin and Recovery Cards.
- Smart card reader. Connects via USB to the Management Station.
- Decru product licenses. Each appliance requires appropriate licenses to use its features.
- Slide rail mounting kit including hardware and instructions (included in the appliance package)
- Network cables. Obtain the requisite number of network cables, of appropriate lengths.
- Network switch ports. Determine which Ethernet switch ports will connect the appliance to the network. Set the switch ports to auto-negotiate both speed and duplex settings. The use of any other setting can affect management performance.
- IP address, Subnet mask and Default Gateway. Each appliance requires one dedicated IP address. Know what the appropriate subnet mask and appropriate default gateway are for each dedicated IP address to be used during installation.
- Appliance name. Establish what resolvable system name will be assigned to each appliance being installed. Enter the specific IP addresses in the network's DNS to enable hostname/IP resolution prior to installation to simplify IP resolution.
- DNS information. Have the appropriate DNS information (DNS suffix, primary DNS server IP address, secondary DNS server IP address) for each IP address to be used during installation.
- NTP address (optional). Have the appropriate NTP time server information for each dedicated IP address to be used during installation.
- Recovery schema. Determine the recovery schema for the appliance. The recovery schema determines how many Recovery Cards and their associated owners must be present for sensitive data recovery operations.

Conventions Used in this Manual

The following typographic conventions are used in this manual:

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

2 Planning the Network Configuration

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

Complete installation in the enterprise positions the DataFort appliance between clients/initiators and file servers/targets, and adds a Management Station (for initial DataFort appliance 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 appliance network installation.

- Decru DataFort Capacity
- Installation Considerations
- DataFort Appliance Clusters
- Virtualization
- Secure Network Practices
- Placing DataFort in the Network
- Planning Data Backup and Restoration

DECRU DATAFORT CAPACITY

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

TABLE 1: DATAFORT CAPACITY

Item	Number	Explanation
Number of E-Series DataFort appliances in a cluster	2	A DataFort cluster supports up to 2 appliances in the NAS/iSCSI environment.
NAS Domains	8	A DataFort appliance or cluster manages up to 8 domains.
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 the DataFort appliance) 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 the DataFort appliance.
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 count that member twice.
iSCSI Groups	512	A DataFort appliance or cluster manages up to 512 iSCSI groups.
iSCSI Initiators	2048	A DataFort appliance or cluster manages up to 2048 iSCSI Initiators.
iSCSI LUNs on a Single Target	2048	One Cryptainer per LUN is supported.
iSCSI Targets	256	A DataFort appliance or cluster manages up to 256 iSCSI targets.
Servers/VLANs	32	A DataFort appliance or cluster manages up to 32 storage devices.
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 appliance or DataFort appliance 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, the DataFort appliance 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 the DataFort appliance to make these connections.

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 the DataFort appliance. Note that several Security Domains might physically reside on the same storage array, and a single Security Domain might include multiple heterogeneous storage devices.

DataFort Appliance Clusters

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

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

Failover Support in a Cluster

Decide whether to install DataFort appliances standalone or clustered. If clustered, decide which DataFort appliance in the cluster is the primary DataFort appliance 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 house encrypted data, and devise a naming plan for virtual servers (assign Virtual Server Names and IP Addresses). Clustered DataFort appliances provide failover support, allowing a functioning DataFort appliance to take over operations for a failed DataFort appliance. When a file server is added to the DataFort configuration database, it is associated with one DataFort appliance in the cluster as its primary DataFort appliance. The primary DataFort appliance handles the data for that server, but shares information about the server with a secondary DataFort appliance. Should file serving operations on the primary DataFort appliance be compromised for any reason, the secondary DataFort appliance in the cluster takes over.

VRIDs for Cluster Members

DataFort appliance 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 appliance cluster.) Be sure that Decru appliances can communicate via the VRRP protocol in the network infrastructure.

Load Balancing in a Cluster

The administrator should 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 appliance as primary. It is important to remember that if one DataFort appliance fails, the remaining DataFort appliances in the cluster serve the combined load of the cluster.

IPsec in a Cluster

Configuration changes are synchronized across a cluster. To protect communication between DataFort appliance cluster members, inter-DataFort appliance 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 appliance 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 do not interrupt data access through the cluster. The other members of the DataFort appliance cluster take over service during any switch outages.

If all cluster members are connected to a single switch, attempt to connect each DataFort appliance 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 appliance to the same switch. Connecting a clustered DataFort appliance'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.

VIRTUALIZATION

Because the DataFort appliance rests between file servers and targets and clients and initiators, some steps may need to be taken to support access to encrypted data.

VIRTUAL SERVER NAMES AND IP ADDRESSES

File servers are added to the DataFort configuration database so that the DataFort appliance can export shares on those servers as Cryptainers. Clients view file servers through the DataFort appliance, 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 the DataFort appliance in order to host Cryptainers, they are assigned virtual IP addresses and names. This allows the DataFort appliance to virtually present the stored data to network clients and initiators. Determine the IP addresses or domain names to be used in advance of setting up DataFort. The network administrator should make a list of the servers and targets to be exported through the DataFort appliance, 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 the DataFort appliance. Determine the best method for introducing the DataFort appliance to the environment before creating Cryptainers.

The administrator should create a virtual server that has the name of the real server, and then rename the real server. This allows the DataFort appliance to export the server names already in use, which means 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 have to use the new names in order to access their data.

Secure Network Practices

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

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

Maintaining Configuration Database Backups

For maximum security and recoverability, keep database backups up to date, and use Decru's Lifetime Key Management software or appliance to store encryption keys. Configure the DataFort appliance 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 appliance or DataFort appliance 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 appliance cluster, or a single set of Recovery Cards for all DataFort appliances in the company.

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

When using an escrow service, configure the DataFort appliance to use 2 out of 5 Recovery Cards for recovery procedures. Two of the Recovery Cards should be sent to the key escrow service. Whenever changes are made to the 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

The DataFort appliance provides detailed local and remote logging to help track events that occur in the Security Domain. Use the logging configuration features of the DataFort appliance 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 the DataFort appliance from resuming encryption services if it is powered off, tampered with and rebooted. This provides greater security, but can also create a service interruption in the event of a power disruption or accidental tamper event. The System Card must be retrieved from storage and reinserted in the DataFort appliance prior to resumption of service. Consider this security/reliability trade-off when determining whether to leave the System Card inserted in a running DataFort appliance.

Preparing for Manual Security Responses

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

The defense setting determines the DataFort appliance's automatic response to physical intrusion. See Defense Triggers and Responses on page 173 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 the DataFort appliance. 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, the DataFort appliance must be zeroized and then restored using the Setup Wizard, Recovery Officers, and a saved configuration database. See Restoring an Appliance.
Removing the System Card followed by shutdown and/or reboot (Removing the System Card alone does not stop DataFort operation).	Stops encryption and decryption immediately.	If the System Card is available, re-insert it and reboot the DataFort appliance.
		If the System Card was destroyed or lost, the DataFort appliance must be zeroized and then restored using the Setup Wizard, Recovery Officers, and a saved configuration database. See Restoring an Appliance.

Placing DataFort in the Network

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

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

If the DataFort appliance 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 the DataFort appliance 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.

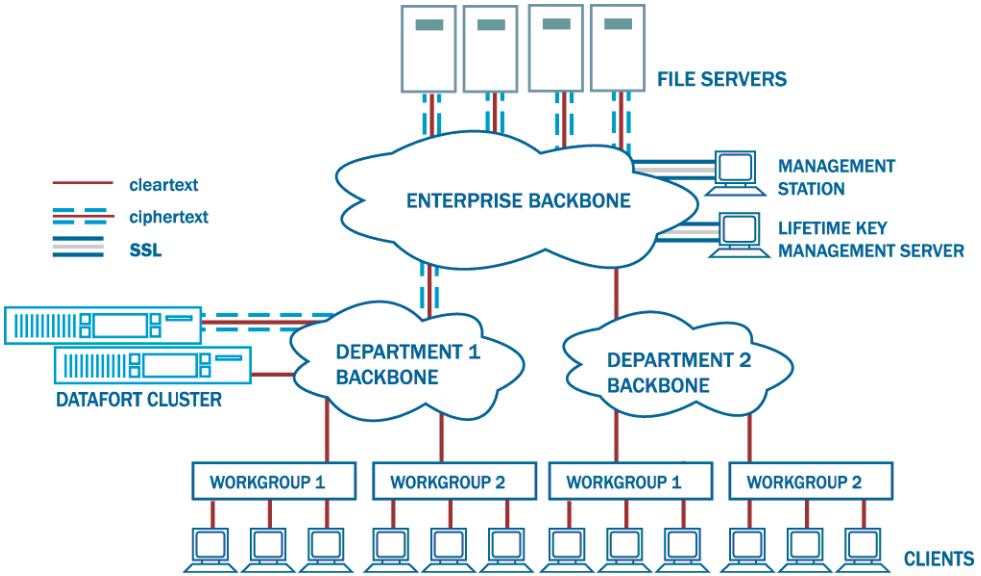


Figure 2-1: Cluster connected to a single department of the enterprise

SERVER CO-LOCATION

If the DataFort appliance cannot be placed close to the authorized clients because the clients are distributed throughout the organization, the most practical solution is to co-locate the DataFort appliance 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. Organizations choosing this deployment scenario may wish to deploy IPsec to protect data in transit between the DataFort appliance and authorized client machines. Note that IPsec for traffic between the DataFort appliance and client machines is a separately-licensed option.

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

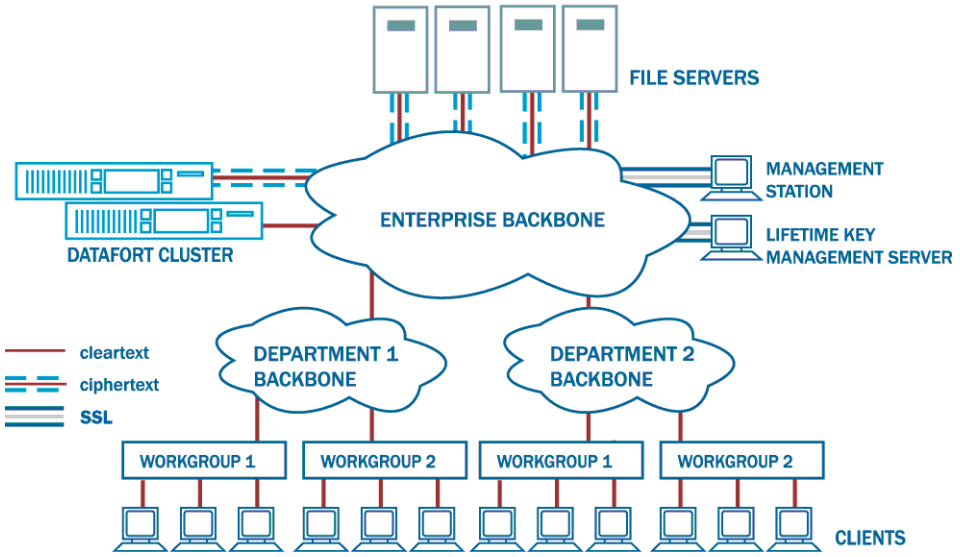


Figure 2-2: Cluster connected to the enterprise backbone

WORKGROUP PLACEMENT

In a basic installation the DataFort appliance, network clients and file servers are all connected to the same subnet. The DataFort appliance 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 appliance deployment places both the Clients NIC and File Servers NIC of the DataFort appliance or DataFort appliance cluster 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 the DataFort appliance installation is transparent to the rest of the organization.

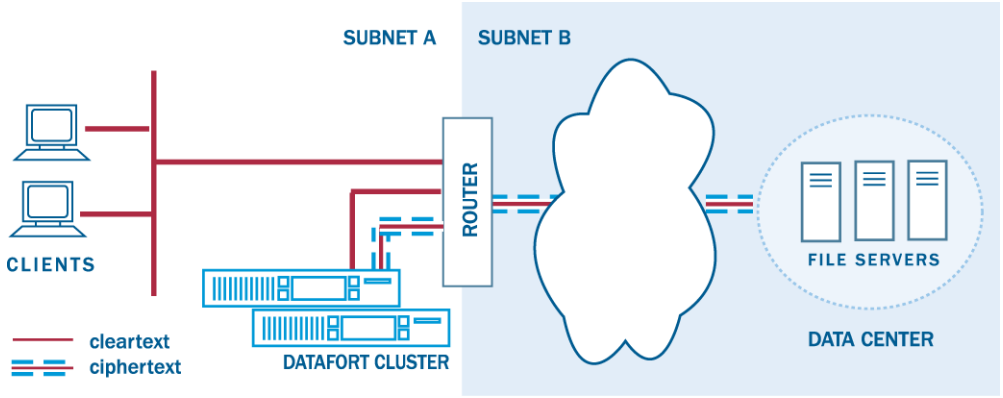


Figure 2-3: Simple deployment

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 the DataFort appliance 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 the DataFort appliance 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 the DataFort appliance. Traffic to corporate file servers does not impact the firewall device.

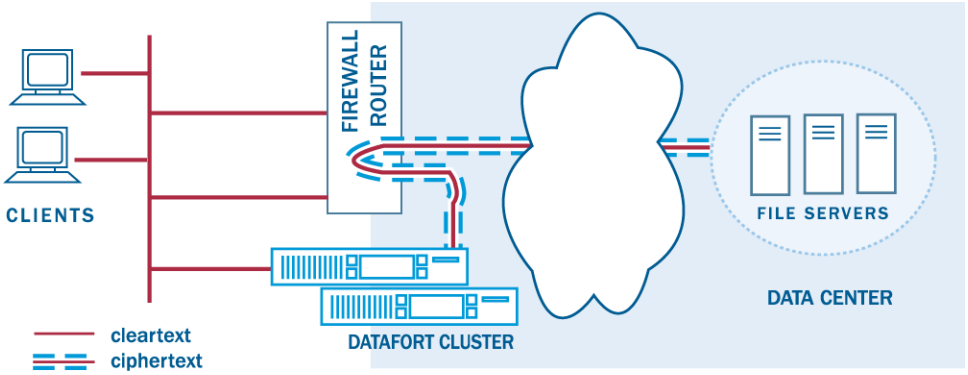


Figure 2-4: Secure enclave deployment

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 appliance 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.)

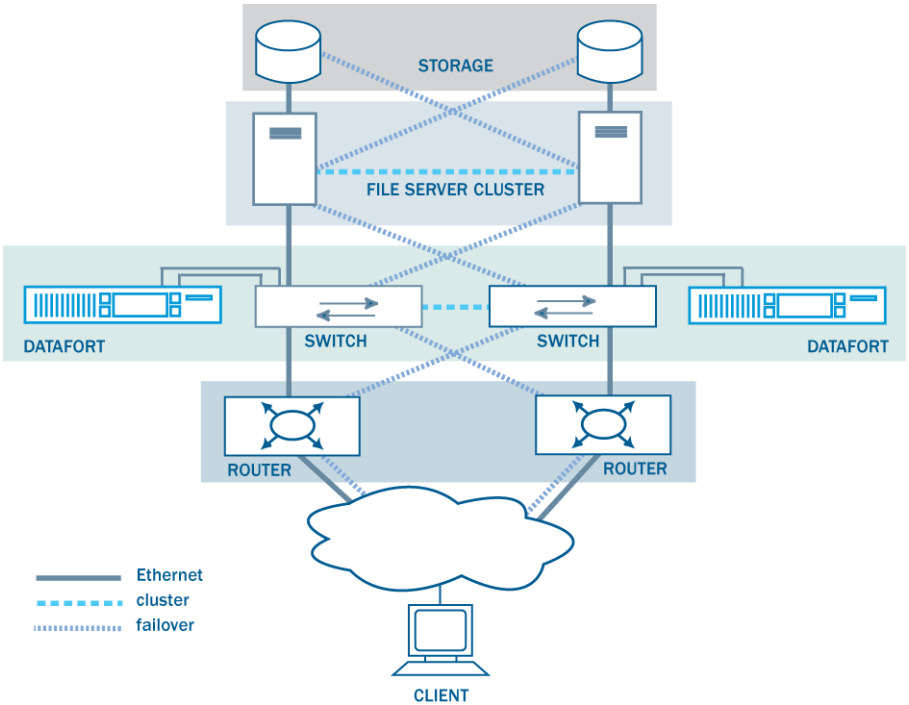


Figure 2-5: Failover paths in a DataFort cluster

Configuring Switches for Failover

Ethernet switch behavior affects how quickly a DataFort appliance 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.

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

Note: If STP holddown cannot be disabled for some reason, the DataFort appliance must be configured with an estimate of the delay. See Configuring Cluster Members for STP on page 214.

Always set the DataFort holddown to match the observed delay between link-up events and the switch actually forwarding network traffic to and from the DataFort appliance. 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

The DataFort appliance supports secure backup and restore capabilities in storage networks. In a data backup configuration, the DataFort appliance should 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 the DataFort appliance. 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 the DataFort appliance.
- Data from the servers is already encrypted, allowing for secure backups and restores.

Note: When backing up encrypted data, keep in mind that encrypted data cannot be compressed and allocate space accordingly.

As the DataFort appliance 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

The DataFort appliance 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, the DataFort appliance 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. The DataFort appliance 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

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

3 Preparing to Install DataFort

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

Key operations necessary in order to configure the DataFort appliance include:

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

Once the DataFort appliance is installed, manage the appliance using the DataFort management interfaces. See the Management Interfaces Overview on page 75 for a list of interfaces and their uses.

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

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

Collecting Network Information

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

DataFort Network Information

- Resolvable hostname for the appliance. Appliance hostnames can be up to 64 alphanumeric characters, including dashes, underscores and periods.
- DNS suffix and DNS server IP address (if DNS is used).
- DataFort Management IP address, Subnet Mask and Gateway. This is the IP address of the DataFort management interface which is presented by default on the DataFort Client Side NIC connected to the client side of the network
- 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 to support 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 (EITHER of the following):
  - LKM Server Software with fixed IP address
  - LKM Appliance

Preparing the Management Station

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

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

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

Table 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 Service Pack 1
Hardware requirements	2Ghz
	1GB RAM
	4GB free hard drive space
	An available USB port for the smart card reader from Decru
	A CD drive for installing software

Management Station Security

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

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

Running the Installer

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

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

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

Setting Up Lifetime Key Management

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

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

Lifetime Key Management Appliance

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

When using an LKM appliance, set up the appliance using the Decru Management Console as described in the *LKM Appliance Administration Guide*.

Lifetime Key Management Server Software

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

When using LKM software, install the software on a designated server as described in the *LKM Server Software Administration Guide*. Ensure the server is up and its IP address is reachable from the Ethernet network before configuring DataFort appliances. Instructions for enabling automatic updates to LKM servers are provided in Chapter 14.

Adding the DataFort Domain Access User

Before using the DataFort appliance to create Cryptainers on NAS servers, add a special user for DataFort domain access to the Windows or LDAP domains in which the DataFort appliance will be used. In a Windows domain, this user enables CIFS access, allowing the DataFort appliance 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 appliance 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.

- Set the domain access user's password without expiration date and without 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 is required when adding the domain to the DataFort configuration database.
- Create a DataFort domain access user in every domain the DataFort appliance serves.
- Give the DataFort domain access user read/write access to shares unless an owner is specified at the time of Cryptainer creation.
- If an alternate owner is not specified at the time of Cryptainer creation, the domain access user is used to access data for initial encryption or rekey of that Cryptainer data.

DataFort LDAP User

In order for the DataFort appliance 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 the DataFort appliance 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.

For the DataFort appliance to authenticate with the LDAP server via Kerberos, add this user as a principal in the 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 Appliance
- Connecting the Appliance
- Assigning the Appliance IP Address
- Powering Up and Shutting Down

Consider the Notices and Warnings when installing the appliance.

Notices and Warnings

Power Supply Notice

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



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

Power Cable Notice



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

Dual Power Supply Notice



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

Lithium Battery Notice for Service Personnel

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



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

Perchlorate Present

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

Rack Mounting the Appliance

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

- Unpacking the Appliance
- Selecting a Location
- Rack Mounting

Unpacking the Appliance

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

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

Selecting a Location

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

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



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

Rack Mounting

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



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

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

Connecting the Appliance

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

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

Inserting the System Card

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

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

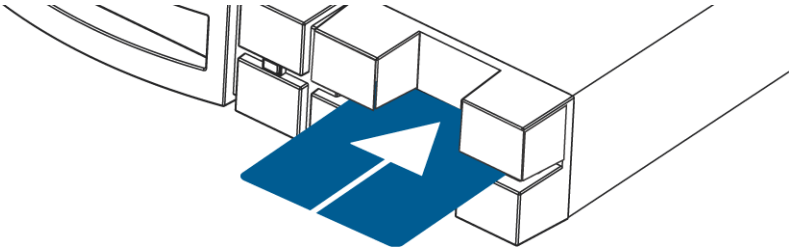


Figure 4-6: The front panel slot housing the System Card on a 1U DataFort

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

   Note: For normal operation, leave the System Card in place after boot-up. Optionally, remove the System Card for higher security. See Removing the System Card on page 33 for details.

CONNECTING THE REAR PANEL PORTS

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

- Ethernet Connection
- Serial Console Port

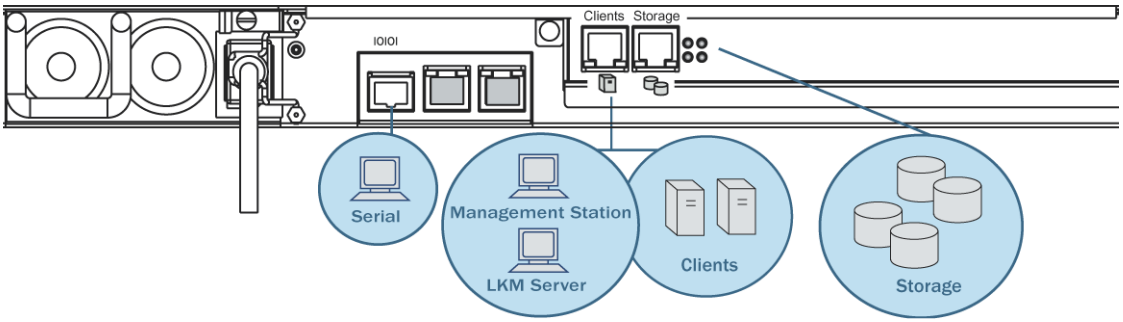


Figure 4-7: Rear panel connections 1U DataFort

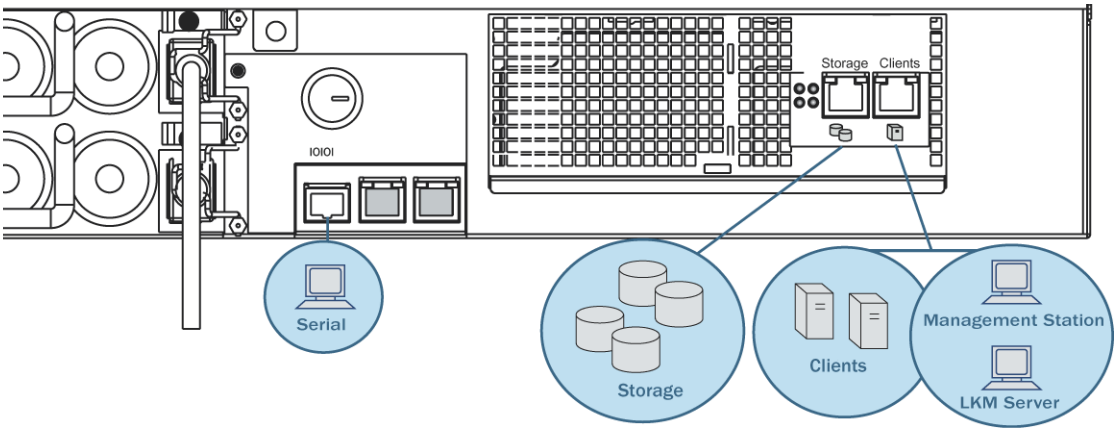


Figure 4-8: Rear panel connections 2U DataFort

Ethernet Connection

The DataFort appliance 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 appliance 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 appliance's rear panel.

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

Connecting Power

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

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

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

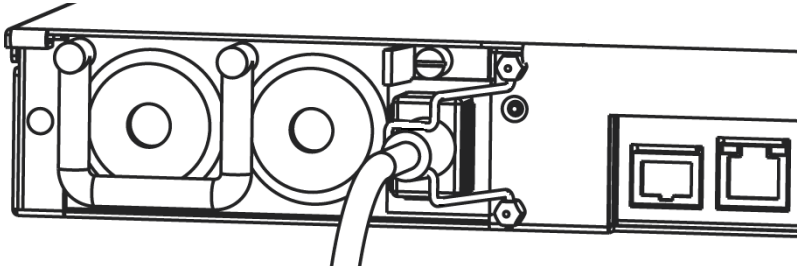


Figure 4-9: Power cord secured by the wire retaining clamp

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

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

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

   Note: Leave the appliance powered on for normal operation. See Powering Up and Shutting Down on page 57 for instructions on powering off the appliance.

Assigning the Appliance IP Address

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

2U appliance Assign the appliance IP settings using the touch-sensitive buttons on the front panel LCD as described in Setting the IP Address Using the LCD, or the serial console port, as described in Setting the IP Address Using the Serial Console.

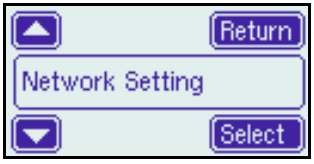
The LCD can only be used to configure IP settings for an uninitialized appliance.

1U appliance Assign the appliance IP settings using the serial console port, as described in Setting the IP Address Using the Serial Console.

Setting the IP Address Using the LCD

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

   The Network Setting option is displayed by default.



3. Touch the Select button.
4. Touch the Edit button. The screen displays a keypad of numbers, and selectable fields for the Clients NIC IP address.
5. Touch the entry field to highlight it, and then touch the keypad buttons to enter each number. Touching the decimal point button moves the focus to the next octet.



6. When finished entering the 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) connected to the Serial Console Port.
2. Set the new connection with the following properties:
   - Speed - **9600**
   - Data bits - **8**
   - Stop bits - **1**
   - Parity - **None**
   - Hardware or no flow control
3. At the shell prompt, log in using the default administrator name and password (note that these entries are space and case sensitive):
   - Login: **user**
   - Password: **MTKNMTKN**

   The main menu appears.
4. Select option **1**, and set an IP address, subnet mask and default gateway for the Clients NIC.
5. Select option **3** to save the settings and exit the terminal window.

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

Powering Up and Shutting Down

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

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

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

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

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

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

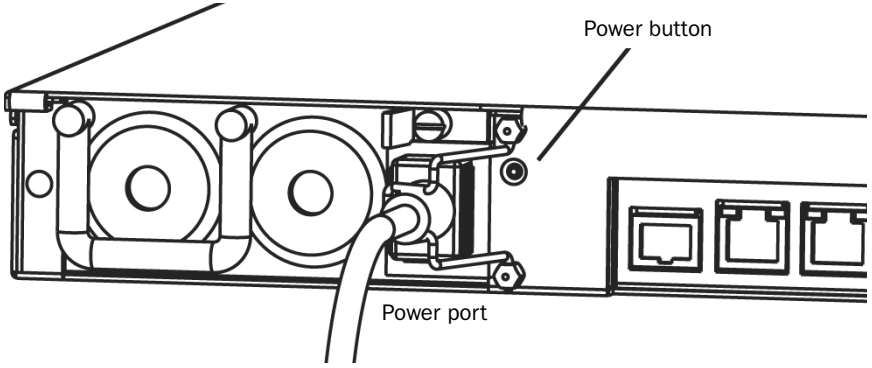


Figure 4-10: Rear panel power port and button on 1U appliance

5 INITIALIZING APPLIANCES

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

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

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

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

About the Setup Wizard

Consider the following when running the wizard:

- Initialization of a new appliance or cluster creates the first Full Administrator for that appliance or appliance cluster.
- Security settings established during this procedure require the full team of Recovery Officers. Be sure to have all smart cards and Recovery Officers available for initialization.
- To expedite setup, collect information described in Collecting Network Information on page 42 before beginning the wizard.

Setup Wizard Functions

The Setup Wizard allows an administrator to complete the procedures described in Table 4.

Table 4: Wizard Functions

Procedure	Description
Set up a new standalone appliance	The new appliance must be initialized and connected to the network. See Initializing a Standalone Appliance or Cluster on page 61.
Set up a new cluster	All cluster members must be initialized and connected to the network. See Initializing a Standalone Appliance or Cluster on page 61.
Add a new member to an existing cluster	A configured standalone appliance must already be set up. The new appliance to be added must be initialized and connected to the network. See Adding a Member to a Cluster on page 69.
Set up a new appliance with an existing saved configuration (restore a configuration)	A saved prior configuration must be accessible to the new appliance. The new appliance must be initialized and connected to the network. This procedure requires only a quorum of Recovery Officers. See Restoring an Appliance on page 273.

Incomplete Setup Wizard

If canceled before completion, the DataFort Setup Wizard retains data entered for the appliance before the cancellation. When the wizard starts again, it automatically fills in saved data and skips certain completed steps. This eliminates the need to reenter data when re-running the wizard. The retained wizard entries can be cleared if necessary. For steps to clear wizard entries, see troubleshooting Network Connections and Management Interfaces on page 276.

About Smart Cards and Readers

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

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

About Remote Authorization

Remote authorization allows an administrator to initiate and verify Recovery Card operations for some DMC operations from a remote location. See Initializing a Standalone Appliance or Cluster on page 61 and Managing Trustees on page 158.

- If the administrator initiating the remote authorization process is also a Recovery Officer, this administrator should be the last Recovery Officer to supply a card to verify that data is entered correctly and complete the approval process.
- If the administrator initiating the remote authorization process is not a Recovery Officer, the last Recovery Officer to supply a card should notify the administrator so that the administrator may verify that data is entered correctly and complete the approval process.
- When using Remote Authorization, some default passwords may be used throughout the initialization process. This creates a network security risk for the appliance being authorized remotely. To avoid this, complete the Remote Authorization process promptly, and check the configuration of the appliance to ensure that it conforms to the security policy of the organization. To do this, review the logs issued during the Remote Authorization process, or log into the appliance and verify that administrative accounts, users, and permissions are correct.

INITIALIZING A STANDALONE APPLIANCE OR CLUSTER

1. From the Windows Start Menu of the Management Station, select **Start > Programs > Decru > Decru Management Console**.
   - If no appliances have been added, the Add... pop-up screen appears automatically.
   - If appliances have been added but not the one(s) to set up, select **Appliance > Add** to open the Add... pop-up screen.
2. Enter the IP address or hostname of all appliances to be set up.

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

   To add an IP address range for multiple appliances with consecutive IP addresses: enter the first IP address of the range in the IP range start field. Press Tab to move the cursor to the IP range end field and enter the end of the IP range.
3. Click OK.
4. A security certificate warning appears. Make the appropriate selection about trusting the certificate. Options include:

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

   The added appliances appear in the DMC.
5. From the appliance tree, right-click the first appliance to configure, and select Set up.
6. From the Welcome page, click Start.

Connect to Head of Cluster

Initialize a standalone appliance or connect to the cluster head (the first DataFort appliance 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 appliance in a cluster, or will function as a standalone appliance, enter the IP address or resolvable hostname of the appliance (as configured during installation).

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

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

Sign License Agreement

Agree to the license terms to continue the wizard.

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

Recover From Database

Use this page of the wizard ONLY if this appliance replaces a previously existing appliance and a configuration database from that previous appliance is used to configure this new appliance. For information about this feature, see Restoring an Appliance on page 273.

- Click Next to skip the Recover from Database screen.

Create Administrator

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

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

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

1. Enter a username for the administrator.

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

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

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

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

CONFIGURE CLUSTER AND RECOVERY SCHEMA

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

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

- Setting the Recovery Schema
- Setting the Cluster Size

Setting the Recovery Schema

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

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

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

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

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

Setting the Cluster Size

1. Select the cluster size.

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

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

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

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

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

3. Click Next to proceed.

NETWORK SETTINGS

Enter the appropriate network settings.

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

Standalone Network Settings

For a standalone DataFort, one set of fields appears.

1. Enter a hostname for this appliance.

   The IP address, Netmask and Gateway set for the Clients NIC appear. (These were set when Assigning the Appliance IP Address on page 55.)
2. Enter an IP address and Netmask for the File Servers NIC.
3. VRID Offset: Enter the first VRID in the sequential block assigned by the network administrator (see VRIDs for Cluster Members on page 29).
4. Click Next.

Cluster Network Settings

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

1. Enter a hostname for the first appliance.

   The IP Address, Netmask and Gateway set for the Clients NIC of the first appliance appear. (These were set when Assigning the Appliance IP Address on page 55.)
2. Enter an IP Address and Netmask for the File Servers NIC of the first DataFort appliance.
3. Enter a hostname for additional cluster members.
4. Enter IP Address, Netmask and Gateway information for both the Clients NIC and the File Servers NIC of additional cluster members.
5. VRID Offset: Enter the first VRID in the sequential block assigned by the network administrator (see VRIDs for Cluster Members on page 29).
6. Click Next.
7. Agree to trust the certificate once or always.

ADD LICENSES

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

1. Enter the license key provided by Decru for each feature.
   - To enter multiple licenses enter each license and then press Enter on the Management Station keyboard to start a new line for the next license.
2. Click Next.

NETWORK AND CERTIFICATES

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

DNS

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

Certificate

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

1. Enter the country code for the appliance's location. The country code is limited to two characters in length. For the United States, enter **US**. Other codes are listed in Partial List of ISO Country Codes on page 321.
2. Enter the rest of the required information about the location of the appliance.
3. Click Next.

INSERT RECOVERY CARD

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

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

Password and Label Limitations

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

Note: Use the same Security Domain for all Recovery Cards in the set.

TABLE 5: CARD PASSWORD AND LABEL LIMITATIONS

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

Required Fields

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

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

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

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

- To set up the appliance locally, see Authorizing Setup Locally on page 66.
- To set up the appliance using Remote Authorization (RA), see Initiating Remote Authorization for Setup on page 67.

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

Authorizing Setup Locally

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

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

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

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

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

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

   Security Domain information from the first card is entered automatically. Change it to group the card differently.
5. Repeat the previous steps for all the cards specified by the recovery schema.

APPLY SETTINGS

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

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

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

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

Initiating Remote Authorization for Setup

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

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

Authorizing Setup Remotely

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

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

WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER. WAIT FOR THE NEXT BUTTON TO BECOME AVAILABLE BEFORE PROCEEDING TO THE NEXT STEP.

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

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

APPLY SETTINGS

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

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

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

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

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

ADDING A MEMBER TO A CLUSTER

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

- This requires the cluster quorum of Recovery Officers with their cards, and the shared secret of the cluster, as well as all applicable licenses for the existing and additional cluster members.

1. From the Windows Start Menu of the Management Station, select **Start > Programs > Decru > Decru Management Console**.
   - If no appliances have been added, the Add... pop-up screen appears automatically.
   - If appliances have been added but not the one(s) to set up, select **Appliance > Add** to open the Add... pop-up screen.
2. Enter the IP address or hostname of all appliances to be set up.

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

   To add an IP address range for multiple appliances with consecutive IP addresses: enter the first IP address of the range in the IP range start field. Press Tab to move the cursor to the IP range end field and enter the end of the IP range.
3. Click OK.
4. A security certificate warning appears. Make the appropriate selection about trusting the certificate. Options include:

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

   The added appliances appear in the DMC.
5. From the appliance tree, right-click an **existing** member of the cluster or a standalone appliance and select Set up.

   Note: Do not select the new appliance to be added. Select the already-configured standalone appliance or an existing member of the cluster.
6. On the Welcome page of the Wizard, click Start.

Connect to Head of Cluster

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

Cluster and Recovery Schema

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

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

Network Settings

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

1. Enter a hostname for the new appliance.
2. Enter IP Address, Netmask and Gateway information for both the Clients NIC and the File Servers NIC of the new appliance.
3. VRID Offset: Enter the first VRID in the sequential block assigned by the network administrator (see VRIDs for Cluster Members on page 29).

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

Add Licenses

1. Enter the license provided by Decru for each feature for each appliance and click Next.

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

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

Network and Certificates

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

DNS

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

Certificate

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

1. Enter a name for the appliance.

2. Enter the two-character country code for the appliance's location. For the United States, enter **US**. Other codes are listed in Partial List of ISO Country Codes on page 321.
3. Enter the rest of the required information about the appliance's location and click Next.

INSERT RECOVERY CARD

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

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

- To set up the appliance locally, see Authorizing Setup Locally on page 66.
- To set up the appliance using Remote Authorization (RA), see Initiating Remote Authorization for Setup on page 67.

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

Authorizing Setup Locally

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

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

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

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

   Note: If the card is uninitialized, the Security Domain entered for the first card in the set is applied to the entire set of Recovery Cards. If the card is initialized, the Card Label and Security Domain appear and the Recovery Officer is prompted for the password.
3. Click Next.
4. When prompted, remove the initialized card and insert a new one.
5. Repeat the previous steps for all the cards specified by the recovery schema.

APPLY SETTINGS

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

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

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

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

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

Initiating Remote Authorization for Setup

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

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

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

Authorizing Setup Remotely

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

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

   WARNING: AFTER CLICKING START, WAIT FOR THE PROGRESS BAR TO APPEAR. APPROVAL IS BEING OBTAINED FROM THE CARD. DO NOT REMOVE IT FROM THE READER. WAIT FOR THE NEXT BUTTON TO BECOME AVAILABLE BEFORE PROCEEDING TO THE NEXT STEP.

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

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

APPLY SETTINGS

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

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

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

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

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

6 APPLIANCE MANAGEMENT INTERFACES

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

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

Management Interfaces Overview

After initial setup is complete use the management interfaces to configure and manage the appliance. The available management interfaces are summarized in Table 6.

Table 6: Management Interfaces

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

SecureView

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

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

Security Policies

Security policy settings determine whether an Admin Card is required for logging in to the DMC or CLI of an appliance. By default, the appliance is set not to require an Admin Card for DMC or CLI access. To enable Secure DMC or Secure CLI (which require the presence of an Admin Card to log into the appliance), customize the security policy as described in Appliance Settings on page 179.

Note: All administrator types can log in to the DMC and the CLI. After logging in, specialized administrators are only able to perform the specialized administrative tasks authorized for their administrator type. For more about administrator types, see Chapter 7.

Online Help

Use the Decru Management Console to access online help for the appliance. Selecting an appliance in DMC and selecting the Help menu opens an online version of the administrative guide for the selected appliance. See Decru Management Console Functions on page 226 for details about the DMC Help menu.

Accessing the Decru Management Console

Use the console to manage appliances from a central location.

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

- Using the DMC
- Connecting via Standard DMC
- Connecting via Secure DMC
- Connecting via DMC using Dual Authorization

Using the DMC

- See Decru Management Console Functions on page 226 for a description of the menu options.
- If equipped with SecureView licenses, more than one appliance can be selected at once, and a menu selection applied to all selected appliances.
- Some menu options initiate operations which are described only in the *Lifetime Key Management Administration Guide*.
- As a security measure, the DMC times out after 30 minutes of inactivity. To change this behavior, log in to an appliance, then select **Edit > Preferences**, select Stay logged in, and click OK.
- Hover the cursor over key on-screen elements for more information.
- If Secure DMC access is turned on, appliances cannot be managed by accessing the DMC through Windows Terminal Services or Remote Desktop.
- It is only possible to have one DMC instance open at a time on any given Management Station. Only one management interface should be open for a given cluster at any one time.
- The screen resolution on the Management Station should be set to at least 1024 x 768 pixels.

Connecting via Standard DMC

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

1. From the Management Station, select **Start > Programs > Decru > Decru Management Console**.
2. Right-click an appliance in the appliance tree and select Log in.
3. Enter the administrator login name and password.

Connecting via Secure DMC

Secure DMC requires that an administrator present an Admin Card as well as a username and password.

A Full Administrator or Key Administrator can turn on the smart card requirement (Secure DMC) by connecting to the DMC and accessing the Management Security settings screen, as described in Appliance Settings on page 179.

1. Insert the Admin Card of a valid administrator into the Management Station smart card reader.
2. Access the DMC from the Management Station as described in Accessing the Decru Management Console on page 77.
3. Right-click an appliance and select Log in.

Connecting via DMC using Dual Authorization

By default, all administrators created using the DMC can log in to the DMC without additional authorization. By default, administrators created using the CLI require prior authentication before they can log in to the DMC or CLI. In addition, if the login privilege is revoked for a given administrator, that administrator requires the presence of an authorizing administrator in order to log in to the DMC or CLI. See Requiring Authorization for Login on page 91 for details. The authorizing administrator can be any administrator who does not require authorization.

To log in to DMC when dual authentication is required:

1. First the administrator with authorization privileges must log in. Access the DMC from the Management Station as described in Accessing the Decru Management Console on page 77.
2. Right-click an appliance and select Log in.
3. Select **Configuration > View Administrators**.
4. Right-click the Administrator to be authorized and select Authorize Login.
5. The administrator with authorization privileges should now log out.
6. The authorized administrator now has one minute to log in to the appliance.

Connecting to the DataFort WebUI

While DataFort administrators use the DMC and CLI to manage appliances, end users use a web-based user interface to authenticate for Cryptainer access or to manage ACLs for Cryptainers they own. See End-User Cryptainer ACL Management on page 151 for more information.

This section provides information for end users to connect to the DataFort WebUI. It includes the following topics:

- Connecting via WebUI
- Using the DataFort WebUI

Connecting via WebUI

End users log in to the DataFort WebUI via a web browser.

1. Open a browser window and enter **`https://<DataFort IP or Hostname>/user.htm`**.

   Note: TLS 1.0 must be enabled.

2. Acknowledge the security certificate message.
3. Agree to load the Decru management applet.

   The DataFort end user Login page appears.

   Note: If this is the first login attempt, the end user must first register with the DataFort appliance. See CIFS User Registration on page 149 for more information.

4. Enter the username and password and click Log In.

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

   The DataFort Manage Cryptainers page is displayed when an end user logs in to the DataFort WebUI.

Using the DataFort WebUI

Consider the following when using the DataFort WebUI:

- 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.
- Do not open other browser windows while running the DataFort WebUI.
- The DataFort WebUI times out after 30 minutes of inactivity.
- To log out of the WebUI, click the user name beside the Log out link at the upper right of any WebUI page.

Connecting to the Command Line Interface

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

- Using the CLI
- Connecting via Standard CLI
- Connecting via Secure CLI
- Connecting via CLI using Dual Authorization
- Connecting to CLI via DMC

Using the CLI

- See Using the CLI on page 238 for information about CLI online help.
- As a security measure, the CLI times out after 10 minutes of inactivity.

Connecting via Standard CLI

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

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

Connecting via Secure CLI

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

A Full Administrator or Key Administrator can turn on the smart card requirement (Secure CLI) by connecting to the DMC and accessing the Security Policy settings page, as described in Appliance Settings on page 179. Secure CLI requires that a session-specific password be furnished via the DMC before the administrator can log in.

1. Insert the Admin Card of a valid administrator into the Management Station smart card reader.
2. Access the DMC from the Management Station as described in Accessing the Decru Management Console on page 77.
3. Right-click an appliance and select Log in.
4. Check One Time Password.

   Note: This button is present only if

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

6. Click OK.

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

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

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

9. Open an SSH client on a workstation connected to the same network as the appliance.
10. Enter the IP address or hostname assigned to the appliance.
11. At the prompt, enter the same administrator login name.
12. When prompted for the administrator password, paste or type the Secure CLI password from step 7 into the command line. The CLI prompt is ready for commands.

Connecting via CLI using Dual Authorization

By default, all administrators created using the DMC can log in to the DMC without additional authorization. Administrators created using the CLI require prior authentication before they can log in to the DMC or CLI. In addition, if the login privilege is revoked for a given administrator, that administrator requires the presence of an authorizing administrator in order to log in to the DMC or CLI. For more details about dual authorization see Requiring Authorization for Login on page 91. The authorizing administrator can be any administrator who does not require authorization.

To log in to CLI when dual authentication is required:

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

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

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

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

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

CONNECTING TO CLI VIA DMC

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

Note: DMC CLI does not support the following features:

- Command line editing and completion
- Output paging
- Context-sensitive help

1. Select an appliance from the appliance tree and select **Appliance > Command Line**.

   The CLI tab opens. For commonly used CLI commands see CLI Administration on page 237.

2. Enter the command into the field provided.
   - Click Execute to execute the command. The command is run on all selected appliances and the output returned on the screen.
   - Click File to open a command file to run on the selected appliances. The commands are run when the file is opened. Note that the file must be an XML-formatted file.
   - To save the output of a command that has been executed, click Save and save the file in a designated location.

Serial Console

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

Use only the supplied crossover RJ45 to DB9 adapter and standard straight through Ethernet cable to connect to the serial console port on the appliance's rear panel. See Serial Console Port on page 53 for details.

Logging in to the Serial Console Port

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

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

Configuring IP Settings

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

   The main menu appears.
2. Select option **`1`** to set an IP address, subnet mask and default gateway for the 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 appliance in order to manage it from a new network. After a reboot, the original settings are restored. Use this feature when moving the appliance to a different network but zeroization is not required. When moving an appliance to a different network that does not recognize the appliance's IP address, the administrator can temporarily clear the settings so that access via DMC and CLI are possible. To change the IP settings permanently, see Changing Network Settings on page 217.

1. At the shell prompt, log in using the administrator name and password assigned to the administrator (note that these entries are space and case sensitive).

   The main menu appears.
2. Select option **`C`**.

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

Zeroizing the Appliance

Enter the zeroize command from the serial console to return the appliance to an uninitialized state. See Zeroizing Using the Serial Console on page 200 for details.

Appliance Front Panel LCD

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

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

Table 7: Read/Write Rate Display on 2U DataFort Appliances

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

Table 8: Read/Write Rate Display on 1U DataFort Appliances

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

Touch Panel Onscreen Buttons

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

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

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

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

SNMP Settings

The appliance supports both MIB II and the read-only private Decru MIB. The Decru MIB is included on the appliance CD. It provides standard MIB-II as well as Decru MIB messages. All Decru MIBs are read-only for security reasons. See SNMP Settings on page 220 for details. A separate *DataFort Appliance SNMP Alarms Guide* is available from Decru for reference.

7 DataFort Admin Roles and Account Administration

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

- Administrator Roles
- Account Administration

ADMINISTRATOR ROLES

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

The appliance also supports the creation of specialized administrators. At any time after the appliance 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 the appliance 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 Table 9 for details.

TABLE 9: ADMINISTRATOR ROLES AND PRIVILEGES

Role Name	Privileges
Full Administrator	The Full Administrator sets up each appliance for the first time by running a setup wizard as described in Initializing Appliances. The Full Administrator can complete all administrative tasks including: • Initializing Appliances • Account Administration • Storage Administration • iSCSI Storage Administration • User Administration • Key Administration • Backup Administration • Managing Appliance Security • 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 Storage Administration and iSCSI Storage Administration.
Key Administrator	A Key Administrator is responsible for applying security-related settings to appliances as described in Key Administration, as well as the ability to create or delete a Cryptainer as described in and iSCSI Storage Administration. Key Administrator tasks include: • Managing Trustees as well as importing and exporting keys • Purging keys upon backup to LKM as described in Key Purging and iSCSI Storage Administration • Setting Security Options • Configuring IPsec • Managing Recovery Officers and Recovery Cards

TABLE 9: ADMINISTRATOR ROLES AND PRIVILEGES (CONTINUED)

Role Name	Privileges
Security Administrator	A Security Administrator is responsible for applying physical security-related settings to appliances as described in Managing Appliance Security. Security Administrator tasks include: ·Managing Appliance Defense Responses ·Setting Security Options ·Configuring IPsec ·Managing Recovery Officers and Recovery Cards ·Resetting Smart Cards ·Setting Date and Time ·Configuring and Viewing Logs ·Zeroizing Appliances ·Setting Security Certificates
Backup Administrator	A Backup Administrator is responsible for managing backups of the configuration database, including those to LKM. Backup Administrator tasks described in Backup Administration include: ·Saving Configurations to Lifetime Key Management ·Backing Up Configurations to a Remote Location
Machine Administrator	A Machine Administrator is responsible for managing system properties and non-security sensitive cluster operations. This administrator can change local network settings. Machine Administrator tasks described in Machine Administration include: ·Changing Network Settings ·Upgrading Appliances ·Managing Licenses ·SNMP Settings ·The Machine Administrator can also add cluster members as described in Cluster Administration.
Read-Only Administrator	A Read-Only Administrator can view all appliance settings (see 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 the DataFort appliance. 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

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

- It is recommend to associate at least two Full Administrators with each appliance. Each administrator should have an individual Admin Card associated. See Adding or Changing a Card Association on page 93.
- Appliance administrators should be highly trusted individuals in the organization.
- Administrators should remove the Admin Card from the smart card reader when they are logged out of the DMC.

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

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

Adding an Administrator

During the Setup Wizard, a local appliance administrator account is created. Each appliance requires at least one local administrator account. Additional administrator accounts can be either added locally or mapped to an existing Active Directory domain user account. This provides the additional password benefits of Active Directory user accounts. Whenever an Active Directory administrator logs in, the appliance authenticates the user against the domain.

1. Log in to the appliance via DMC as a Full Administrator or an Accounts Administrator.
2. Select **Configuration > Add Admin**.
3. Enter the name of the new administrator.
4. Select the domain that the administrator belongs to from the drop-down list.
   - To add a local administrator account, select Local.
   - To map an existing Active Directory administrator account to an appliance administrator role, select the Active Directory domain. If the domain has not been added yet, click Add to add the domain, then enter the domain information in the Add Domain screen.
5. Enter and confirm the password. Strong passwords are an important part of the overall security of the system. Select a password consisting of at least 8 valid, randomly chosen characters.

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

6. Select the administrator role. The default selection is Read Only. See Administrator Roles on page 87 for details.

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

   - Select **Read-only** to create an administrator who can view but not modify appliance settings.
   - Select **Specialty** to create specialized administrators. Specialty administrator roles become available. Multiple roles may be selected for one administrator.
   - Select **Full Admin** to create a Full Administrator role.
7. Enter a full name for the administrator.
8. As an additional security option, require that an administrator be authenticated before being able to log in to the appliance. See Requiring Authorization for Login on page 91 for more information.
9. Click Apply.
10. Select the newly created administrator from the list.
11. To associate this administrator with an Admin Card for additional security, see Adding or Changing a Card Association on page 93.

Requiring Authorization for Login

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

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

For instructions on creating an administrator requiring prior authentication see:

- Requiring Authorization to Access the DMC
- Creating a New Administrator

Protecting Against Insider Attacks

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

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

Requiring Authorization to Access the DMC

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

   Now this administrator requires authorization to log in to the appliance. See Connecting via DMC using Dual Authorization on page 78 for authorizing DMC login, and Connecting via CLI using Dual Authorization on page 81 for authorizing CLI login.

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

Changing the Administrator Password

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

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

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

5. Enter the new password and confirm the entry.

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

6. Click Apply.

Removing an Administrator

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

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

Adding or Changing a Card Association

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

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

8 Before Storage Administration

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

These operations are performed using the DMC. For login instructions see Accessing the Decru Management Console on page 77. For a complete DMC menu options overview see Chapter 19.

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

- Verifying DataFort Configuration

Verifying DataFort Configuration

Verifying System Version

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

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

Checking Cluster State

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

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

For information about cluster states see Checking the Status of the Cluster on page 205.

Creating Additional Administrators

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

It may be desirable to create distinct administrators responsible for certain tasks, as outlined in Chapter 7.

1. From the DMC, select **Configuration > Add Admin**.
2. Create an additional administrator. If desired, associate one or both administrators with an Admin Card. See Adding an Administrator on page 90 for instructions.

Configuring Remote Logging

Configure the appliance to use remote signed logging.

1. From the DMC, select **Configuration > Log Configuration**.
2. Determine which log messages should be sent to a remote syslog server on the network. See Appliance Log Storage Guidelines on page 189 for details.

Determining the Defense Setting

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

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

1. From the DMC, select **Security > Defense**.
2. Select the appropriate defense setting. See Defense Triggers and Responses on page 173.

9 STORAGE ADMINISTRATION

This chapter includes instructions for using the Decru Management Console to manage Cryptainers, the backbone of a storage network secured by DataFort appliances. 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 the DataFort appliance. A Full Administrator as well as a Storage 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 the DataFort appliance for export as encrypted data. Steps include:

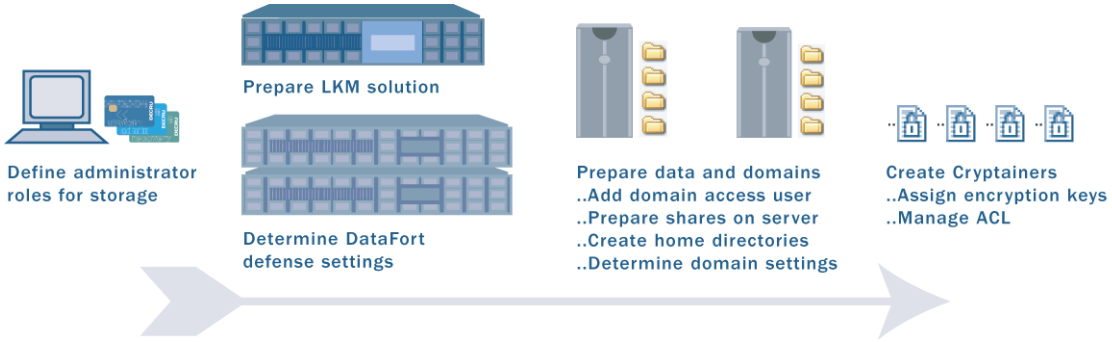


Figure 9-11: Overview of the workflow for creating NAS Cryptainers

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 Network Attached Storage
- Restoring a Cryptainer

Understanding DataFort Domains

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

The DataFort appliance 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 the DataFort appliance for communicating with the domain controller and with file servers belonging to the domain (see Adding the DataFort Domain Access User on page 46)
- The DataFort appliance also supports Userless Domains on which it does not enforce access restrictions.

File Servers and Domains

When file servers are added to the DataFort appliance 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 the DataFort appliance uses 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 still needs to accept the domain name, the access user name, and the password of the domain chosen during an authentication request by the DataFort appliance.

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 the DataFort appliance. For CIFS, a user is first verified locally by the DataFort appliance to make sure that user exists in the domain. The DataFort appliance can be configured to require that users register in order to access their data through the DataFort appliance. If user registration is required, the DataFort appliance 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 the DataFort appliance 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 uses, and therefore how the DataFort appliance learns about users and groups in the domain.

Table 10 describes the domain and subtype combinations supported by the DataFort appliance. Creating a NAS Cryptainer on page 102 includes steps required to add the domain and subtype combinations.

Table 10: 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 the DataFort appliance as a domain.	Add a Domain. Specify the NetBIOS name of the file server as the domain name. Once this domain is added, the DataFort appliance is 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. The DataFort appliance supports the LDAP server schemas inetOrgPerson and NIS. Once the domain is added, users with LDAP accounts can access CIFS file servers through the DataFort appliance.	Add a Domain. Since these users have no actual Windows accounts to use for authentication against the file server, User Mapping and Use Local ACL should be enabled. See User Mapping and DataFort Domains.
	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 the DataFort appliance 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 enabled. See User Mapping and DataFort Domains.
	Userless	Use this subtype to have the DataFort appliance 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 10: 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	Select Local for NFS/UNIX environments where there is no domain controller to query.	NFS users and groups must be added manually to the DataFort appliance. 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 the DataFort appliance 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 User Mapping feature is enabled, the DataFort appliance performs 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 46.) See File Server Related Settings on page 180 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 enable the DataFort appliance 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. A userless domain is preferable if the administrator does not want to track and manage users or access control privileges. 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 the DataFort appliance. 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. The administrator should set up the server so that it does not enforce access control if he does not want to manage users.

Preparing to Create a NAS Cryptainer

To create a Cryptainer, the DataFort administrator introduces an existing share to the DataFort appliance. This requires that the server on which the share is located be in a domain to which the DataFort appliance has access. The DataFort appliance proxies servers that are added to the configuration database, exposing a virtual server name (or IP address) to network clients. The virtual server is 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 the DataFort appliance as Cryptainers. See Create CIFS Shares and Create NFS Exports for guidelines.

Note: See Migrating Data on page 148 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 the DataFort appliance, 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 46).
- 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 the DataFort appliance for export as Cryptainers.
- The network administrator should follow standard procedures to set up shares for clients on network servers. The DataFort appliance 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 is not encrypted at the time the Cryptainer is created. See Options When Adding a Cryptainer on page 112 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 new sub-share level Cryptainers, the specified directory must not exist, but parent directories need to be present. For example, to create a new Cryptainer at \\server\share\crypt, there must not be a directory named "crypt" in \\server\share.
- Shares which will become Cryptainers should 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 the DataFort appliance.
- The DataFort appliance 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 the DataFort appliance. See Creating a NAS Cryptainer From a Home Directory on page 107.

Create NFS Exports

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

- From the operating system used to administer NFS, create exports (file locations for sharing purposes) on network servers, and set permissions.
- The server hostname should be changed and the old hostname should be used by the DataFort appliance 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 is not encrypted at the time the Cryptainer is created. See Options When Adding a Cryptainer on page 112 for choices when creating a Cryptainer.
- Unix user volumes should 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 requires 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

The DataFort appliance 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 108.

Open the Decru Management Console

1. From the Management Station, select **Start > Programs > Decru > Decru Management Console**.
2. From the appliance tree, select an appliance.
3. From the Appliance menu, select Log in.
4. From the Topology menu, select Servers and Portals.

Servers and Portals

Use the Real Elements and Virtual Elements panes of the Servers and Portals tab to manage the secure network. The Real Elements side of the tab 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 tab displays the DataFort appliance 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- or Ctrl-clicking them on screen. The maximum number of devices that can be selected at once is 255.

Real Elements Pane Menu

Right-click in the Real Elements pane to see the Real Elements pane menu.

Refresh	Refresh the Real Elements pane view.
Expand, Collapse	Expand or collapse the Real Elements tree.
List Mappings	List mappings between real and virtual elements.
Sync Users	Synchronize users.
Current Rekey Jobs	Display a list of currently running rekey jobs.
Export, Import Trustee Keys	Export to or import from a trustee. See Importing and Exporting Keys on page 167 for more information.

Virtual Elements Pane Menu

Right-click in the Virtual Elements pane to see the Virtual Elements pane menu.

Refresh	Refresh the Real Elements pane view.
Expand, Collapse	Expand or collapse the Real Elements tree.
List Mappings	List mappings between real and virtual elements.

ADD A DOMAIN

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

1. On the Servers and Portals tab, in the Domains tree, right-click CIFS and NFS Domains.
2. Select either Add CIFS Domain or Add NFS Domain, then the desired domain subtype.
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:
   - Adding a CIFS domain only imports the users and groups needed to properly enforce logins, ACLs and memberships. For other domain types (NIS,LDAP) the full domain is imported.
   - 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 97 for information. Enter the required information for the domain.
2. Enter the name and password of the DataFort domain access user into the Access User fields.
3. Click Apply.

Add an NFS Domain

1. Add a NIS, LDAP, Local or Userless domain. See Understanding DataFort Domains on page 97 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.

   The DataFort appliance 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 manually.
3. Click Apply.

ADD A SERVER

1. In the Domains tree of the Decru Management Console, right-click the domain the server should be added to. For a multi-protocol server, it is possible (but not necessary) to first select both domains by Shift- or Ctrl-clicking.
2. From the right-click menu, select Add Server.
3. Enter a hostname for the server either manually by typing it or by selecting the server name from the drop-down list. If the hostname cannot be resolved to an IP address via DNS, enter its IP address as well. Otherwise, leave the IP address field empty.
4. Select the appropriate domain from the CIFS or NFS drop-down list. For a multi-protocol server, select one from each.
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). The DataFort appliance 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. For NAS, iSCSI Access should be Off.
7. Click Apply.

If a server already exists under one domain type, it cannot be added again under the other domain type. Instead, edit the existing server and add the second domain.

To change a server from single-protocol to multi-protocol:

1. Right-click the existing server in the Real Elements pane and select Edit.
2. From the CIFS Domain and NFS Domain drop-down lists, select the appropriate domains.
3. Click Apply.

Add a Share

1. Right-click a server in the Domains tree. From the right-click menu, select:
   - CIFS or NFS: **Shares > Add Single Protocol**.
   - Multi-protocol: **Shares > Add Dual Protocol**.
2. Select the share(s) to be added:
   - CIFS or NFS: In the Add Single Protocol screen, add one or more shares by selecting them in the onscreen list of Discovered Shares. Select multiple devices by Shift- or Ctrl-clicking them on screen.
   - Multi-protocol: in the Add Dual Protocol screen, select a share from the CIFS Name drop-down list and select the equivalent name for the same share from the NFS Name drop-down list.
3. Click Apply.

   The share(s) appear in the Real Elements pane. The share name displays both CIFS and NFS names to enable easy identification of multi-protocol shares. The first share name in the entry belongs to the domain type the server/share is listed under. The second name belongs to the other domain type for easy cross-reference.

Add a Virtual Server

1. Right-click a DataFort appliance in the Virtual Elements pane.
2. Select Add Virtual Server.
3. Enter a hostname for the virtual server. If the hostname cannot be resolved to an IP address via DNS, enter its IP address as well. Otherwise, leave the IP address field empty. For more information, see Adding Virtual Servers on page 116.
4. From the CIFS and/or NFS Domain drop-down lists, select the domain to associate with the virtual server. For multi-protocol shares, select a domain from both lists.
5. From the Member IP drop-down list, select the IP address of the primary DataFort appliance.
6. Enable Floating to support failover. See Adding Virtual Servers on page 116 for more about this setting.
7. 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 to add. Shift- or Ctrl-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. Select the Cryptainer options. See Options When Adding a Cryptainer on page 112 for more information.
3. In the Path field:
   - If only one share was selected, the path field can be edited.
   - If multiple shares are selected, only share-level Cryptainers can be created.
4. In the Cryptainer Owner field:
   - Specify an owner for the Cryptainer(s) being created if needed. This owner may be an administrator, an NFS or CIFS group, or an NFS or CIFS user.
   - If the field is left blank, the administrator logged in to the DMC (or CLI) when the Cryptainer is created becomes the owner.
   - For NFS and multi-protocol Cryptainers, if an administrator is the owner, DataFort uses the root UID when creating the Cryptainer.
   - For CIFS and multi-protocol Cryptainers, if an administrator is the owner, DataFort uses the CIFS domain access user to sync ACLs and sets the domain access user as the owner in the Windows Security Descriptor.
5. Click Apply.

   The Cryptainer appears under its share in the Real Elements pane. See Managing Cryptainers on page 113 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.
- The DataFort appliance keeps track of the Cryptainer owner who can 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

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 102, use the Decru Management Console to create share-level Cryptainers in each shared home directory, all virtualized on the same VIP.
3. Log in to the DataFort 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 need to log in to the DataFort appliance 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.
- The Key Administrator can actually create the Cryptainer.

Table 11 outlines which administrators need to log into the DataFort appliance to complete each part of the process that completes Cryptainer creation.

Table 11: 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 NETWORK ATTACHED STORAGE

Use the Servers and Portals tab to manage secure NAS. NAS 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.

Add Users, View Users (NFS only)	The DataFort appliance imports user, group and membership information from domains automatically every 30 minutes. Use the Add Users menu to add a user such as the root user to the NFS domain (see Add an NFS Domain on page 104). If this is an NIS or LDAP domain, users that are added or removed are 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. Use the Users menu to list or remove users.
Validate Domain (CIFS only)	Test DataFort access to this domain.
Add Server	Add a Server found in this domain. The Add Server page for the selected type of domain appears. 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. All servers must be deleted before the domain can be removed. See Deleting a Domain on page 109.

DELETING A DOMAIN

In order to delete a domain, the servers in that domain must be deleted first. 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 113.
2. Delete all shares existing in servers in that domain. See Managing Shares on page 111.
3. Delete all servers in that domain. See Managing Servers on page 110.
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 119.
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, the administrator needs 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, set their domain to a different one. See Managing Servers on page 110 and Managing Virtual Servers on page 117.
3. Delete the domain.

Managing Servers

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

Ping	Test DataFort connectivity to this server.
Resolve Server IP	If the IP address of the server has changed, use the Resolve Server IP menu option to update the information for that server in the DataFort configuration.
Shares	Add a share for Cryptainer creation. See Add a Share for instructions.
Add Server IP	Add a server IP address to the DataFort configuration. The DataFort appliance 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.
Edit	Change server attributes including IP address, domain, iSCSI access and DataFort interface. See Editing a Server.
Delete	Delete server. All shares must be deleted before the server can be removed. See Managing Shares on page 111. When deleting a dual-protocol server from the Real Elements pane, it disappears from all domains.

EDITING A SERVER

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

Options when editing a server include:

Server 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 one from each.
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.
Interface	File servers can reside on the File Servers or Clients side of the DataFort appliance. Select the appropriate 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.

Show Cross 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 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 Restoring a Cryptainer on page 121 for instructions.
Edit	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:

Data Encryption By default, data within Cryptainers is encrypted. To leave the contents of a Cryptainer in cleartext (unencrypted) form, disable Data Encryption. This allows the DataFort appliance to manage the access control for the shares without requiring that the data in the share be encrypted. Disable Data Encryption to use the DataFort appliance only to strengthen the ACL on a share, not to encrypt its contents. Disable Data Encryption to leave data that existed before the DataFort appliance was installed in the environment as cleartext. When Data Encryption is disabled, the Cryptainer icon appears in the DMC without the lock image. To encrypt the data later, use the Rekey Cryptainer feature described in Managing Cryptainers.

Initial Encryption By default, Initial Encryption is disabled. Create empty Cryptainers with Data Encryption enabled and Initial Encryption disabled, and then copy the data to be encrypted into the Cryptainer.

If the share where the Cryptainer is created contains existing data, enabling Initial Encryption allows this data to be encrypted at the time of Cryptainer creation and added to the Cryptainer.

Ensure that none of the existing data in the share is in use or marked read-only, and that the initial encryption process is completely finished before accessing the Cryptainer to avoid halting the encryption process or having both encrypted and cleartext data in the Cryptainer.

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. Note that Cryptainers with encrypted file names cannot be rekeyed. See Rekeying Cryptainers.

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

Sync Windows ACLs Select to synchronize the Cryptainer ACL with the server when creating the Cryptainer. This ensures users have the same access as before. Enabled by default.

MANAGING CRYPTAINERS

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

ACL, ACL Sync	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. Set the owner of the Cryptainer by selecting the user and clicking Set Owner. Sync the Cryptainer ACL with the ACL on the server (only available for CIFS). See ACL Sync and ACL Preview.
Add IP Restriction	Use to restrict access to the Cryptainer from specified IP addresses. See Setting Cryptainer IP Address Restriction.
IP Restriction	Use to view or remove Cryptainer IP restrictions.
Remove All IP Restrictions	Use to remove all Cryptainer IP restrictions.
Add Alias	Use to add an Alias path to a cryptainer.
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, Pause, Resume, Cancel, or Purge a rekey job. To view current rekey jobs, right-click in the Real Elements pane and select Current Rekey 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.
Edit	Use to edit Cryptainer options and change IPsec and Secure NFS settings.
Export Trustee Keys	Export Cryptainer encryption key to a Trustee. See Importing and Exporting Keys on page 167.
Delete	Delete the Cryptainer.

Note: See Options When Adding a Cryptainer on page 112 for Cryptainer creation options.

ACL Sync and ACL Preview

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

To view Cryptainer ACLs:

1. Right-click a Cryptainer and select **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. From the drop-down list, select a domain.
3. Click Load to re-read the ACL from the server for the selected domain.

To synchronize Cryptainer ACLs:

1. Right-click a Cryptainer and select ACL Sync (CIFS Cryptainers only).
2. Click Yes to update the DataFort ACL with the ACL of the server.

   Note: A Cryptainer owner can modify the ACL of the Cryptainer. See Cryptainer ACL on page 139.

Setting Cryptainer IP Address Restriction

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

To add IP address restrictions:

1. In the Real Elements pane, right-click the Cryptainer to be restricted.
2. Select Add IP Restriction.
3. Check the desired access setting (Read, Write, or both Read and Write).
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. Click Apply.

To view, edit, or remove IP restrictions:

1. In the Real Elements pane, right-click a Cryptainer.
2. Select IP Restriction.

   The IP Restrictions screen appears, displaying a list of existing IP restrictions.

3. Right-click an IP restriction and select Edit or Remove.

   To remove all IP restrictions at once, right-click on the Cryptainer and select Remove All IP Restrictions.

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 117.
2. From the Servers & Portals tab, right-click a Cryptainer and select Edit.
3. Enable Require IPsec and click Apply.

Rekeying Cryptainers

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

Rekeying Restrictions

Rekeying a Cryptainer is essential for storage administrators. Consider the following before rekeying a Cryptainer:

- An open file cannot be encrypted. The encryption process stops if it encounters an open file, after which the encryption process must be manually restarted. In certain database applications, files are opened when the database is brought up. This means that encryption does not work until the database is brought down and all files are closed.
- Cryptainers with encrypted filenames cannot be rekeyed.
- Re-keying is a background process. Network load and NAS Array setup could limit the rekey rate.
- All file permissions within a Cryptainer should be readable and writable by the Decru access user. When the DataFort appliance encounters a file with read-only permission, it halts the re-key operation until the read only file has been modified to allow write access by the DataFort appliance. Upon changing the file permission, the re-key procedure can be resumed (manually).
- In order for the DataFort appliance to make a clean rekey run through an entire share, all files must be writable by the DataFort appliance. No users, applications, or other processes should lock any files for any reason, otherwise a manual restart of the rekey process needs to be initiated by the user. When the DataFort rekey process encounters a file locked by a user or application, the rekey halts indefinitely. Once the file is unlocked, the rekey procedure can be resumed manually. Encountering locked files in an NFS environment is not an issue. The CIFS protocol locks files when accessed, so the DataFort appliance is likely to encounter locked files. An administrator must decide which scenario is easier: Prevent users from accessing files during a rekey or manually restart the DataFort rekey operation upon encountering locked files.
- If a Cryptainer supports multi-protocol access (CIFS and NFS), the default re-key access method is NFS. This is not a user-programmable setting.
- During a Cryptainer re-key, files are locked and re-encrypted in a linear fashion. A file cannot be accessed by other applications once the DataFort appliance has locked it for rekey. Files that have not been locked by the DataFort appliance for rekey can be accessed.
- Do not invoke any file system commands to query or modify any files until the rekey has completed.
- Once a file has been encrypted with a new key, the NAS Array may kick off an Anti-Virus Scan.
- Re-keying a file modifies the date of the file.

Rekeying a Cryptainer

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

   To view the status of a rekey job, right-click in the Real Elements pane and select Current Rekey 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 appliance in the Virtual Elements pane and select Add Virtual Server to add a new virtual server.

Do not use the same virtual server for NAS and iSCSI storage. The virtual server's hostname must be resolvable to its own virtual IP address (VIP) via DNS. If not, the administrator can either add the VIP to the DNS before adding the virtual server, or enter the VIP in the IP address field.

Options when adding a server include:

Virtual Hostname	Enter the hostname of a server.
CIFS and 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 one from each.
Member IP	Select the primary DataFort appliance for this server. This DataFort appliance serves the VIP unless there is a failover to the other cluster member.
IP Address	Indicate the IP address of the server.
Floating	Enable for NAS. The VIP is assigned to a VRID, so it moves with that VRID to whichever cluster member becomes the master of that VRID during failover. Disable for iSCSI. The VIP is assigned to a cluster member and it always stays with that member. iSCSI VIPs should be of this type, because iSCSI redundancy is implemented via client-driven failover.

For a Windows client using Kerberos to communicate with the Virtual Server, it must join a CIFS domain. Either pre-add the server to the domain (See Pre-Adding Virtual Servers to a Domain on page 117) or join it to the domain later (See Editing a Virtual Server on page 119).

PRE-ADDING VIRTUAL SERVERS TO A DOMAIN

To add a Virtual Server to a CIFS domain before creating a virtual server on the DataFort appliance:

1. Open Active Directory Users and Computers.
2. In the console tree, right-click Computers and select **New > Computer**.
3. Follow the wizard to add the virtual server host.
4. In the Computers pane, right-click the new object and select Properties.
   - For Windows 2003 Server domain: Select the Delegation tab, check “Trust this computer for delegation to any service (Kerberos only)”, and click OK.
   - For Windows 2000 native domain: Click the General tab, check “Trust this computer for delegation”, and click OK.

MANAGING VIRTUAL SERVERS

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

IPsec	Configure a secure IPsec connection to the server. See Configuring IPsec on a Virtual Server.
Set VIP Certificate	Set a self-signed or Certificate Authority (CA) signed certificate for the virtual server. 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 various additional settings. 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 181.

Setting Virtual Server Certificates

The Virtual Server certificate (self- or CA-signed) authenticates the virtual IP address to clients. See Setting Security Certificates on page 201 for more information about configuring certificates.

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 appliance, User Registration must be enabled. See Setting Security Options on page 177 for more information about setting the DataFort Security Policy.
- Before configuring the DataFort appliance 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 desired SMB signature settings and click Apply.
   - If Client-side SMB Signatures are Disabled, message signing is not enabled for communication with clients.
   - If Client-side SMB Signatures are Required, only clients that support signing are allowed to connect.
   - If Server-side SMB Signatures are Disabled, message signing is not enabled for communication with servers.
   - If Server-side SMB Signatures are Required, only servers that support signing are allowed to connect.

Moving Virtual Servers in a Cluster

The administrator may encounter a situation that requires moving virtual servers in a DataFort appliance cluster, for example, to redistribute load between DataFort appliances in the cluster or other network resources.

To move two virtual IPs hosting the same Cryptainer to a different DataFort appliance in a cluster, the virtual IPs must be deleted from one cluster member and added to the second one.

1. In the DMC, log in to the DataFort appliance with the associated virtual IPs.
2. Right-click on the CIFS share and delete one of the CIFS virtual shares from the virtual IP.
3. Right-click on the first virtual IP and select Move to, selecting the second DataFort appliance as the target.
4. Right-click on the second virtual IP and select Move to, selecting the second Datafort appliance as the target.
5. Log in to the DataFort appliance that the virtual IPs were moved it.
6. Right-click on the newly moved Virtual IPs and virtualize the share on the newly moved virtual IPs.

   The VIPs should now be moved to the second DataFort.

   Note: It may be necessary to restore or re-add Cryptainers at this point.

Editing a Virtual Server

To edit a virtual server, right-click the virtual server in the Virtual Elements pane and select Edit. Options include:

Virtual Hostname	Enter the hostname of a server.
IP address/Netmask	Indicate the IP address and netmask of the server.
Member IP	Select the primary DataFort appliance for this server. This DataFort appliance serves the VIP unless there is a failover to the other cluster member.
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 one of each.
Floating	Enable for NAS. The VIP is assigned to a VRID, so it moves with that VRID to whichever cluster member becomes the master of that VRID during failover. Disable for iSCSI. The VIP is assigned to a cluster member and it always stays with that member. iSCSI VIPs should be of this type, because iSCSI redundancy is implemented via client-driven failover.
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 the DataFort appliance. See Editing Virtual Servers to Support SMB Signatures on page 118.
Joined CIFS Domain	For a Windows client using Kerberos to communicate with the VIP, it must join a CIFS domain. Check the Joined CIFS Domain option, then enter the domain user, domain password, and DN in the fields that appear.

Managing Virtual Shares

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

Show Cross 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, specify which address the DataFort appliance should use to access a virtual share. 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 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. See Editing a Virtual Share.
Delete	Delete virtual shares.

Editing a Virtual Share

Options when editing a virtual share include:

Virtual Server	Select the hostname of the server of the virtual share.
CIFS / NFS Name	Specify a name for the virtualized share.
Server IP	Specify a hostname for the server through which the virtualized share is accessed.

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 appliance cluster. The cluster must be the same one for which the Cryptainer was originally created. Note that when 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 tab of the DMC, right-click the domain where the file server with the data resides and select Add Server.
3. Right-click the server and select 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, 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 the DataFort appliance 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 tab, right-click the Cryptainer name and select ACL Sync. Click Yes when prompted.
   - If the ACL on the server has changed, update it on the server and then sync the server and the DataFort as described above.
7. There is no ACL Sync for NFS Cryptainers. Set up the ACL manually from the DMC:
   - Right-click the Cryptainer name and select ACL. Initiate a search among users and groups in one or more domains, or select Show Users/Groups without access. Click Load.
8. Right-click the user or group to add to the ACL and select Set Permissions.
9. Check the appropriate permissions and click Apply.
10. Click Apply.

10 iSCSI Storage Administration

This chapter includes instructions for using the DMC 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
- Cloning an iSCSI Cryptainer

Preparing to Create an iSCSI Cryptainer

When preparing to create iSCSI Cryptainers, follow these guidelines. Some preparations require logging in to the DataFort CLI (see Connecting to the Command Line Interface on page 80).

Setting up Groups

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

The DataFort appliance does not support the encryption of existing data in iSCSI Cryptainers. All data existing on the disk prior to the creation of the Cryptainer is rendered unreadable. The DataFort appliance only supports encryption of empty Cryptainers for iSCSI. If there is data on the storage device, it is 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 the DataFort appliance and turn iSNS off at the server. The DataFort appliance serves as the iSNS server. To enable iSNS through the DataFort appliance complete the following:

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

```
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 124.

Preparing to Create Cryptainers Using SnapDrive

SnapDrive support requires executing a specific command 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 125.

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 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 DMC 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 configuration database. The Virtual Elements side of the Servers & Portals page displays the DataFort appliances 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 DataFort appliance via the DMC.
2. Select **Storage > Servers & Portals**.
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. Select the settings for the iSCSI Portal. For a list of options see Options When Adding an iSCSI Portal on page 125.
5. Click Apply.

   Note: To support clustering in the iSCSI environment using Microsoft Multipath I/O (MPIO), repeat these steps to add the second interface of the target. See Configuring DataFort to Support MPIO on page 127.

Options When Adding an iSCSI Portal

The following options are available when adding an iSCSI Portal:

Server Hostname	Enter the server hostname or select it from the drop-down menu.
IP Address	Enter the IP address.
iSCSI Access	Enable iSCSI access.
CIFS and 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.
Interface	Servers can reside on the File Servers or Clients side of the DataFort appliance. Click the appropriate 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.

Virtualizing the Portal

1. Right-click a DataFort appliance in the Virtual Elements pane and select New Virtual Server.
2. Select the settings for the virtual server. See Options When Adding a Virtual Server on page 125.
3. Click Apply.

   Note: To support clustering in the iSCSI environment using Microsoft Multipath I/O (MPIO), repeat these steps to add a second VIP for the second interface of the target. See Configuring DataFort to Support MPIO on page 127.
4. Right-click the iSCSI Portal and select the Virtual Server it will be virtualized on.

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

Options When Adding a Virtual Server

Options when adding a server include:

Virtual Hostname	Enter the hostname of a server.
CIFS and NFS Domain	Not needed for iSCSI.
Member IP	Select the primary DataFort appliance for this server. This DataFort appliance serves the VIP unless there is a failover to the other cluster member.
IP Address	Indicate the IP address of the server.
Floating	Enable for NAS. The VIP is assigned to a VRID, so it moves with that VRID to whichever cluster member becomes the master of that VRID during failover. Disable for iSCSI. The VIP is assigned to a cluster member and it always stays with that member. iSCSI VIPs should be of this type, because iSCSI redundancy is implemented via client-driven failover.

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. See the section that applies to the iSCSI configuration:

- iSCSI File Server already exists as a CIFS Server
- iSCSI File Server does not exist as a CIFS Server

iSCSI File Server already exists as a CIFS Server

1. Right-click the existing file server under the CIFS domain and select Edit.
2. Set iSCSI Access to On and click Apply.
3. Right-click the virtual server that created for iSCSI access and select Edit.

   Note: CIFS and NFS domain information is not needed.
4. Make the CIFS domain the same domain where the file server is located and click Apply.
5. Right-click the existing file server under the CIFS domain and select **Shares > Add Single Protocol**.
6. Add a share by entering its name, or add several shares by selecting them in the onscreen list of Discovered Shares. Select multiple shares by Shift- or Ctrl-clicking them on screen.
7. Click Apply.
8. Right-click the share in 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 125.

iSCSI File Server does not exist as a CIFS Server

1. Create the CIFS domain on the DataFort appliance, and add the NetApp Filer to the CIFS domain.
2. Right-click the existing file server under the CIFS domain and select Edit.
3. Set iSCSI Access to On and click Apply.
4. Right-click the virtual server created for iSCSI access and select Edit.
5. Make the CIFS domain the same domain where the file server is located and click Apply.
6. Right-click the existing file server under the CIFS domain and select **Shares > Add Single Protocol**.
7. Add a share by entering its name, or add several shares by selecting them in the onscreen list of Discovered Shares. Select multiple shares by Shift- or Ctrl-clicking them on screen.
8. Click Apply.
9. 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 125.

Adding an Initiator

1. From the DMC, select **Topology > Initiators and Targets**.
2. Right-click in the Initiator Management Pane and select Add Initiator...
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. Follow the NetApp Snap Drive Administrative and Installation Guide to create a brand new LUN using the newly created DataFort virtual server IP as the target portal, and as the CIFS share mount point.

   After a few seconds the LUN appears, and a Cryptainer is 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 Apply.

   The status icon for the Cryptainer changes to indicate 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 DMC shows 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 appliance. Each DataFort appliance in the cluster should have an entry for the path from the initiator.

MANAGING SECURE ISCSI STORAGE

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

Access the tabs by selecting **Topology > Servers and Portals** or **Topology > Initiators and Targets** from the DMC.

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 DMC ICONS

Icons display status information about network devices including initiators, targets and Cryptainers. Images are combined to describe multiple conditions. For example, an encrypted Cryptainer that is offline shows the icon for encrypted Cryptainer along with the yellow alert icon. Use the following key to understand the icons display.

TABLE 12: 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	
Cryptainer icon	Yellow !	Metadata and/or rekey error, or Cryptainer is offline	
	Lock	Cryptainer is encrypted	
	No lock	Cryptainer is cleartext	

MANAGING PORTALS

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

Ping	Test DataFort access to this portal.
Resolve Server IP	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.
Add Server IP	Add an IP address to the DataFort configuration. The DataFort appliance 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.
Add Route (Virtualize)	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

Options when editing a portal include:

Server Hostname Enter or change the hostname of a server.

CIFS and NFS Domains Not needed for iSCSI.

iSCSI Access Enable iSCSI Access 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.

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 appliance in the Virtual Elements pane 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 116 for information about settings when adding VIPs.

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

IPsec	Configure a secure IPsec connection to the server. See Configuring IPsec on a Virtual Server.
Set VIP Certificate	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

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 and NFS Domain	Not needed for iSCSI.
Floating	Disable 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/Server-side SMB Signatures	Not needed for iSCSI.
Joined CIFS Domain	Not needed for iSCSI.

Managing Targets and LUNs

Manage targets and LUNs from the Initiators and Targets tab. Expand the Targets tree to view targets and LUNs. Right-click a target in the Target Management pane to see management options.

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 LUN management options.

Add Cryptainer	Create a Cryptainer on the selected target. Select whether to use an exportable key or not. Using an exportable key allows the key to be exported to a trustee. See Importing and Exporting Keys on page 167 for details.
Restore Cryptainer	Restore a deleted Cryptainer. See Restoring an iSCSI Cryptainer on page 133.
Clone Cryptainer	Create a new Cryptainer with the key of an existing Cryptainer.See Cloning an iSCSI Cryptainer on page 134.
Export Trustee Keys	Export a key from this target to a trustee. See Importing and Exporting Keys on page 167.
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 DMC.

Managing Cryptainers

Manage Cryptainers from the Initiators and Targets tab. Expand the Cryptainer Management tree to view individual Cryptainers. Right-click a Cryptainer in the Cryptainer Management pane to see Cryptainer management options.

Note: Rekeying is not supported for iSCSI Cryptainers.

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.
Move Selected	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.

Edit	Enter a custom name for the Cryptainer in the Cryptainer Name field. 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 appliance as well as with an LKM server if one is configured. Forcing metadata on allows the DataFort appliance to write this metadata to a block of the LUN when a Cryptainer is created, regardless of what is already on the disk.
Delete	Delete the Cryptainer.

Managing Initiators

Manage initiators from the Initiators and Targets tab. Expand the Initiators tree to view the IP, paths and group information for each initiator. Right-click an initiator in the Initiator Management pane to see Initiator management options.

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

Show Ownership	Display which initiator discovered and owns which LUNs and Cryptainers.
Add Initiator Group (from selected Target)	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 DMC.

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 appliance cluster. The cluster must be the same one for which the Cryptainer was originally created. Note that if LKM software is used to manage Cryptainer keys and the LKM server is on line, the DataFort appliance 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 the DataFort appliance's restore features. Note that no more than one instance of a particular Cryptainer can exist simultaneously (it is not possible to restore the same Cryptainer to multiple places at once).

A Cryptainer restore requires the following:

- The original encrypted data and the port and LUN information of the original Cryptainer location.
- The Cryptainer ID.
- A DataFort appliance that remembers the original Cryptainer. The DataFort appliance 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 the appliance recovers the Cryptainer information from LKM). Any DataFort appliance using the configuration database that contains information about the original Cryptainer works.

1. From the DMC, select **Topology > Initiators and Targets**.
2. Right-click the LUN where the deleted Cryptainer was originally stored and select Restore Cryptainer.

   The Restore Cryptainer screen appears. It displays information about the selected device 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 Apply.

Cloning an iSCSI Cryptainer

Cloning an existing iSCSI Cryptainer assigns that Cryptainer's encryption key to a new Cryptainer.

1. From the DMC, select **Topology > Initiators & Targets**.

   Note: In order to clone a Cryptainer onto a LUN, the LUN must not have any Cryptainer associated with it. Double-click the target LUN and verify that there is no Cryptainer ID in the Properties pane below the Target Management column.

2. Remove any Cryptainer on the LUN where the Cryptainer clone will reside.
3. Select the Cryptainer to be cloned.
4. Right-click the LUN where the Cryptainer clone will reside and select Clone Cryptainer.

   The Clone Cryptainer screen appears. It displays information about the Cryptainer to be restored.

5. Click Apply.

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
- Requiring Smart Card for Cryptainer Access

End users may obtain access to their secured data and manage ACL on Cryptainers they own as described in Accessing Secure Data on page 144.

MANAGING GROUPS AND USERS

Users are automatically imported into the DataFort appliance 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 the DataFort appliance (see CIFS User Registration on page 149).
- 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 100). Groups and users with access to a share will be the same groups that the DataFort appliance allows to access that share when it becomes a Cryptainer.

Automatic Domain Sync

The DataFort appliance automatically imports groups from the Windows domain controller, along with the users included in those groups. The DataFort appliance 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 disabled, the DataFort appliance 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 enabled, the administrator is required to review and accept any changes made to the Cryptainer ACL.

Disabling Automatic Domain Sync

To disable the DataFort appliance's automatic sync function, log in to the DataFort CLI and run the following command:

```
system property set user.domain.sync.disabled true.
```

See Connecting to the Command Line Interface on page 80 for information accessing the CLI.

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 DMC, select **Topology > Servers and Portals**.
2. Right-click the Cryptainer and select ACL.
3. Select the domain from the drop-down menu and enter the exact user or group name into the User/Group search field.
4. Click Load.

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 is 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, the DataFort appliance 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 the DataFort appliance 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 the DataFort appliance, 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 screen of the DMC (see Managing Cryptainer ACL on page 139).

GROUP REVIEW

If Group Review is required by the Security Policy (see Domain Controller Related Settings on page 179), 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 do not appear until the administrator reviews and accepts the new group of users. The DataFort administrator must 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 Related Settings on page 180) protects against attacks on the file server, and the Group Review feature protects against attacks on the domain controller. Use Local ACL should be enabled when Group Review is enabled.

The following steps need to be reviewed based on the outcome of bug 35290

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

1. Log in to the DataFort appliance via DMC.

   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 DMC Appliance tab.

2. Select **Security > Group Review**.

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

3. Right-click each user to accept or reject. If new users are not accepted, they are not allowed access.

ADDING INDIVIDUAL USERS TO GROUP

When several users or groups are added to a group and Group Review is on, the DataFort Administrator can only add or cancel all users added to the specific group.

To allow only individual users to be added, use the DataFort CLI.

1. Check which users were added by logging in to the DataFort CLI and running the following command:

   ```
   user group list --uflags comers
   ```

2. To confirm all users, run the following command:

   ```
   user comers confirm
   ```

3. To confirm only one user (user1), run the following command:

   ```
   user comers confirm --name user1
   ```

4. To cancel a user added along with the group (user2) run the following command:

   ```
   user comers cancel --name user2
   ```

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 the DataFort appliance 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.
- When a new CIFS Cryptainer is created, the permissions are imported from the file system ACLs and not the share level ACLs.
- 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 appliance and one on the file server. They are identical when a CIFS Cryptainer is first created, because the DataFort appliance 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 DMC.
- 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 the DataFort appliance and read/write permission on the server, the user can only read.
- After a Cryptainer is created, a group can be set as the owner of that Cryptainer. All members of that group can modify the ACL of that Cryptainer. Note that a group cannot be assigned as an owner at the time the Cryptainer is created since groups are not registered users. Once the Cryptainer is created, add the group as an owner.

CRYPTAINER ACL

To view the ACL settings on a Cryptainer:

1. From the DMC, select **Topology > Servers and Portals**.
2. Right-click the Cryptainer and select ACL.

The ACL screen appears. Users with access to the selected Cryptainer are listed.

- To modify a user's access to the Cryptainer, right-click the user and select Set Permissions. Check the appropriate Permissions check boxes and click Apply. Note that if Local ACL is off, only the server's ACL is honored.
- To make a user the owner of the Cryptainer, right-click the user and select Set Owner.

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 DMC, select **Security > Management Security.**
2. Set the DataFort Security Policy so that Group Review, User Registration, Secure Password Update, and Use Local ACL are all enabled and click Apply to save the settings.
3. Create a share with default permissions on a server in a domain (for Windows 2000, group Everyone has full control).
4. Add the share as a Cryptainer as described in Creating a NAS Cryptainer on page 102.
5. As the planned most-privileged user, access the Cryptainer/share from a client that is a member of the same domain as the server.
6. 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).
7. Add full permissions for the Domain Access User for that domain so that the DataFort appliance can make changes to the ACL if necessary. Note that this is not a security hole because the DataFort appliance 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 enabled, the Windows administrator cannot be added to the Cryptainer ACL simply by being added to the ACL directly on the server's share.
8. Apply the permissions.

   The DataFort appliance captures the permissions transaction between the client and the server, updating the DataFort appliance 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 is not 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 DMC, select **Security > Management Security.**
2. Set the DataFort Security Policy so that Group Review, User Registration, Secure Password Update and Use Local ACL are all enabled and click Apply to save the settings.
3. Create a share with default permissions on a server in a domain (for Windows 2000, Everyone has Full Control).
4. Add the share as a Cryptainer as described in Creating a NAS Cryptainer on page 102.
5. 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).

6. Add full permissions for the Domain Access User for that domain so that the DataFort appliance can make changes to the ACL if necessary. Note that this is not a security hole because the DataFort appliance specifically denies data access to the DataFort domain access user.)
7. From the DMC, select **Topology > Servers and Portals**.
8. Right-click the Cryptainer and select ACL.
9. Review the ACL for the Cryptainer. Click Close when done.
10. Right-click the Cryptainer and select ACL Sync.
11. Click Yes to synchronize the DataFort ACL for that Cryptainer with the permissions just set at the server.

Requiring Smart Card for Cryptainer Access

Some Windows domain environments employ two-factor authentication using smart cards. When users access data through the DataFort appliance in such an environment, it is possible to also enforce two-factor authentication using smart cards for Cryptainer access. In this case, the DataFort appliance requires the user to present a smart card in addition to user credentials in order to access a Cryptainer.

Enforcing Two-factor Authentication

Keep the following in mind when enabling this feature:

- Kerberos authentication must be used to enable this feature.
- Changing the property value does not affect users who are already logged in. It only affects connections made after the property is set.
- The smart card is detected at user login. If the user logs in with the smart card and then removes it, the smart card is still considered present as long as the user remains logged in.

Table 13 outlines the effect of setting the property value.

Table 13: End User Smart Card Requirement Values

Property value	DataFort enforces domain policy requiring smart card	DataFort enforces that smart card is present	Comments
0	No	No	The DataFort appliance does not enforce anything (same as default).
1	No	Yes, if domain policy requires smart card	The DataFort appliance enforces the domain policy. If the domain policy requires a smart card for the user, the DataFort appliance requires it as well; if the domain policy does not require it, the DataFort appliance does not either.
2	No	Yes	The DataFort appliance enforces that the smart card is present, regardless of the domain policy.
3	Yes	Yes	The DataFort appliance enforces two things: that the domain policy requires a smart card, and that the smart card is present.
4	Yes	No	The DataFort appliance enforces the domain policy requiring a smart card, but not whether the card is present.
(anything else)	(N/A)	(N/A)	The DataFort appliance denies access.

1. Log in to the DataFort CLI and execute the command:

   `system property set sys.security.cifs.requiresmartcard <value>`

2. Notify all end users of the smart card policy.

   CAUTION:THIS IS A GLOBAL PROPERTY, AND CANNOT BE SET PER DOMAIN. SETTING THE PROPERTY REQUIRES ALL USERS TO ADHERE TO THE SMART CARD REQUIREMENT.

12 Accessing Secure Data

After a Cryptainer is created, users with access to the original share can begin storing and accessing data in the Cryptainer, where it is automatically encrypted. This chapter describes some methods by which an end user can access data secured by the DataFort appliance, as well as some other tasks the user may need to complete when accessing data secured by the DataFort appliance. 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

Configure the data access security policy via the Management Security screen of the DataFort DMC. See Setting Security Options on page 177 for details. Depending on the security policy, the administrator notifies end users of any new requirements for accessing their data. This information might include:

- Any new instructions for handling sensitive data.
- Whether smart cards are required for Cryptainer access. See Requiring Smart Card for Cryptainer Access on page 142.
- 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 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 notifies users of names of Cryptainers they can access, and the path (through virtual servers presented by the DataFort appliance) 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 106). Subsequently, users work with the data as though it were stored in unencrypted form. They navigate to shares, explore the network, and access shares to which they have been granted access. Data inside the Cryptainer appears 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 is encrypted as it is copied into the Cryptainers. See Migrating Data. New data written directly into the Cryptainer is encrypted automatically.

About Data Access

- A file written through the file server directly, bypassing the DataFort appliance, can not be accessed through the DataFort appliance. To access the file through the DataFort appliance, copy the file through the DataFort appliance into the Cryptainer storage vault.
- The.decru file is a hidden system file containing metadata for a Cryptainer. It is created at the time the Cryptainer is created. Deletion of the.decru file does not impact data access but prevents the DataFort appliance from recovering the Cryptainer if it is inadvertently deleted. A .decru file is created in cleartext Cryptainers as well as encrypted ones. To encrypt the contents of a cleartext Cryptainer, delete the .decru file and create a new Cryptainer.

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 the DataFort appliance 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 the DataFort appliance 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 appliance: **\\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 IS 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 is preferable to give end users only one path to their secured data: the path that goes through the DataFort appliance. If users attempt to access files directly on the server, they 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 appliance appears.
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 THE DATAFORT APPLIANCE.

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 the DataFort appliance 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 DMC. See End-User Cryptainer ACL Management on page 151.

   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 appliance:

   ```
   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 the DataFort appliance and as it exists on the server.

1. To view the Cryptainer exported by the DataFort appliance, 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 appears 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 appears as ciphertext.

Migrating Data

After a Cryptainer is created, users with access to the original share can begin storing data in the Cryptainer, where it is automatically encrypted. Users can also copy existing data into a Cryptainer after it has been created. If initial encryption is on, encryption starts automatically in the Cryptainer. See Options When Adding a Cryptainer on page 112. 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 creating a Cryptainer that is cleartext, add data to it directly on the server and then create a Cryptainer which encrypts the contents of the share.

1. Add an empty share to the DataFort appliance as described in Creating a NAS Cryptainer on page 102.
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 106.

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 the DataFort appliance as a Cryptainer, as described in Creating a NAS Cryptainer on page 102.
5. Copy the contents of **`Folder1_cleartext`** to the newly created Cryptainer.

   Note: The data must be copied from **`Folder1_cleartext`** to **`Folder1`** through the DataFort appliance. 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 the DataFort security policy, end users must register once at the WebUI Login page before they can access Cryptainers. See Connecting to the DataFort WebUI on page 79 for more information about end user access to the DataFort WebUI.

If the DataFort Password requirement is in effect, users must also provide their DataFort password at the time of registration. See Setting Security Options on page 177 for more about setting these requirements.

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 disabled, the user registers without seeing a place to set the DataFort password. The DataFort password is the same as the domain password. With DataFort Password enabled, the user should set the DataFort password to be different from the domain password.

Whether or not User Registration is required by the 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 appliance, or logging in to either DataFort appliance in a cluster:

1. Open a browser window and enter:

   ```
   https://hostname/register.htm
   ```

2. Select the domain that includes this user.
3. Enter the current username and password for this user.

   Note: If DataFort passwords are enabled, fields appear to register that password as well. See Registering the User's DataFort Password for details.

4. Click Register.

   After registering, users are 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 151.

   If the user's Windows password changes, the user needs to update the password upon login to the DataFort appliance (see Changing User Passwords on page 150).

Registering the User's DataFort Password

If desired, configure the DataFort appliance to require its own password in addition to the domain password when a user accesses Cryptainers for the first time. If the DataFort Password requirement is in effect, users also need to register that password. By default the DataFort password is the same as the domain password (Windows password).

Note: DataFort passwords must be enabled for this feature to work. See Domain Controller Related Settings on page 179.

- If a user is not yet registered at the time the DataFort Password requirement is enabled, then that user needs 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 enabled, 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 the DataFort appliance:

1. Open a browser window and enter:

   `https://hostname/register.htm`

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

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

   If the user's Windows password changes, the user needs to update the password upon login to the DataFort appliance. See Changing User Passwords.

CHANGING USER PASSWORDS

When the user's Windows password is changed, the user must update the password registered with the DataFort appliance. 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 for the DataFort appliance:

Changing the User's Windows Password

1. Open a browser window and enter:

   `https://hostname/password.htm`

   - If DataFort passwords are enabled, click the Change button for the Windows password.
   - If DataFort passwords are not enabled, continue to the next step.

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

Changing the User's DataFort Password

Note: DataFort passwords must be enabled for this feature to work. See Domain Controller Related Settings on page 179.

1. Open a browser window and enter:

   `https://hostname/password.htm`

2. Click the Change button for the DataFort Password.
3. Select the domain the user is in, and enter the required information and click Change. If the user registered with the DataFort appliance 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 the DataFort WebUI to view and manage the Cryptainers they own. See Connecting to the DataFort WebUI on page 79.

1. Open a browser window and enter:

   ```
   https://hostname/user.htm
   ```

   Note: CIFS users must register. See CIFS User Registration on page 149.

2. Select the domain the user belongs to, enter the username and password, and click Log In.

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

3. At the Manage Cryptainers page, select a Cryptainer.
4. Click Access Control to view or change access permissions.
5. 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.
6. 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 appliance.
2. Enter the IP address or hostname assigned to the DataFort appliance.

   Note: If the user has CIFS Cryptainers, the registration requirements are the same as for login to the 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

The DataFort appliance supports storing and accessing data via HTTP, including the WebDAV extensions. With DataFort web access users can securely access data from a web browser. WebDAV extensions, provided by the Windows operating system or a WebDAV client application, offer additional capabilities. Stored data secured by the DataFort appliance appears in cleartext form when accessed by authorized users through the DataFort appliance, 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 the DataFort appliance 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. The DataFort appliance 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. The DataFort appliance supports both SSL 3.0 and TLS (Transport Layer Security); client software must have one or both of them enabled. Each virtual IP address can have its own certificate for identification over SSL. The DataFort appliance also supports setting a root certificate per virtual IP address for authenticating clients. See Setting Virtual Server Certificates on page 117 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 154 to change the default.

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

Web Access

1. Open a browser window and enter:

   `https://virtualserver` or **`https://virtualserverIPaddress`**.

2. Enter a valid username (or domainname\username) and password.

   These are 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 can 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 can 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 appears 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 to delete (multiple item selection is possible). 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 when 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 makes 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, 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. To use a different port (for example, if port 443 is blocked by a firewall), set the system 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 must log in again. To change this setting, set the system property **`nas.http.credentials.ttl`** to the desired life span (in minutes).

FTP Data Access

The DataFort appliance 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.

Enable FTP for each VIP by modifying a system property:

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

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

  Note: Unlike CIFS, NFS and HTTP, by default FTP is disabled. Once enabled, FTP behaves very similarly to HTTP.

1. Using any FTP client, connect to the VIP, entering the username and password. The user is authenticated against both the CIFS and NFS domains of that VIP. If the credentials are valid, the user has access to the corresponding shares.
2. Requesting a directory listing after logging in presents a list of shares. By clicking on one share (if using a graphical client) or typing `cd <share_name>` (if using a text-based client), the user enters the share and has 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 starts in one of the shares and can access data immediately.

1. To set up a home directory, log in to the CLI and run the following 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 is started at the root level.
- Each principal may have only one home directory configured. Running the `set` command again only changes 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

The DataFort appliance 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 the DataFort appliance 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 run 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). Run the following CLI command:

  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. Run the following CLI command:

  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 DataFort (see CIFS User Registration on page 149). Run the following CLI command:

  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 by running the following command:

   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

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

Archiving encryption keys to LKM appliances allows the DataFort appliance to back up keys as a safety precaution as well as purge unused keys from its key databases. For details about archiving keys to LKM appliances see the *LKM Appliance Administration Guide*.

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

- Managing Trustees
- Importing and Exporting Keys

MANAGING TRUSTEES

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

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

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

TRUSTEE SCENARIOS

The establishment of trustees enables several enterprise scenarios:

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

SETTING UP TRUSTEES

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

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

This section contains the following topics:

- Creating Trustees on a Local Network
- Creating Trustees on a Remote Network

Creating Trustees on a Local Network

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

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

This section contains the following topics:

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

Create Trustee Link

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

   Note: By default the Trustee Label shows the hostname or IP address of the other appliance though this can be changed.
3. On the Trustee Setup screen, notice that both appliances appear and click Create Link.
4. Select a method to authorize trustees:
   - To authorize trustees locally, see Authorizing Trustees Locally (Approve TEP/TAP) on page 159.
   - To authorize trustees using Remote Authorization, see Initiating Remote Authorization to Approve TEP on page 160.

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

Authorizing Trustees Locally (Approve TEP/TAP)

1. On the Approve TEP (Trustee Establishment Package) screen, select from the following:
   - For multiple card readers, insert the quorum of cards into the readers, enter the passwords and click Start.
   - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the password and click Start.

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

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

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

2. On the Approve TAP (Trustee Acceptance Package) screen, select from the following:
   - For multiple card readers, insert a quorum of cards into the readers, enter the passwords and click Start.
   - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the password and click Start.

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

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

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

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

Initiating Remote Authorization to Approve TEP

1. On the Approve TEP (Trustee Establishment Package) screen, select a quorum of cards from the Recovery Officers list to use throughout the authorization process and click Enable Remote Authorization.

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

2. When the Remote Authorization enabled message appears, close the Approve TEP screen. Notify the Recovery Officer who will approve the TEP that it is safe to continue the TEP approval process and introduce Recovery Cards remotely. See Authorizing TEP Approval Remotely on page 160.

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

Authorizing TEP Approval Remotely

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

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

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

4. When the progress bar is complete, close the Approve TEP screen and notify the Recovery Officer(s) who will approve the TEP that it is safe to continue the TEP approval process.

   Note: Do not close the Approve TEP screen if you are the last officer to Approve the TEP as the last officer to supply a card automatically initiates the TAP approval process. See Initiating Remote Authorization to Approve TAP on page 161.

Initiating Remote Authorization to Approve TAP

1. In the Decru Management Console, in the appliance tree, select both appliances.
2. From the Trustee menu, click Create Trustee Link.
3. On the Approve TAP (Trustee Acceptance Package) screen, select a quorum of cards from the Recovery Officers list and click Enable Remote Authorization.
4. When the Remote Authorization enabled message appears, close the Approve TAP screen and notify the Recovery Officer(s) who will approve the TAP that it is safe to continue. See Authorizing TAP Approval Remotely on page 161.

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

Authorizing TAP Approval Remotely

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

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

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

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

Creating Trustees on a Remote Network

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

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

This section contains the following topics:

- Start Trustee Creation (Create TEP)
- Receive TEP
- Receive TAP
- Delete Unapproved TAP Trustee

Start Trustee Creation (Create TEP)

1. In the Decru Management Console, in the appliance tree, select the first appliance.
2. From the Trustee menu, select Start Trustee Creation.
3. On the Start Trustee (Create TEP) screen, enter the following and click Create.
   - A Trustee Label or hostname for the appliance.
   - A Package Label or hostname for the package.
4. On the Select File screen, verify the TEP file name and select a file location, then click Save.
5. From the Trustee menu, select View Unapproved Trustees.
6. On the View Unapproved Trustees tab, right-click the correct Trustee Label and select Copy Verifier.
7. Paste the verifier into a text file and save it.
8. Send the verifier file and the TEP file separately to the second appliance. See Receive TEP.

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

Receive TEP

To receive the TEP (Trustee Establishment Package), the second appliance needs the TEP file and verifier received from the first appliance. See Start Trustee Creation (Create TEP) on page 162.

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

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

4. Click Begin Approval.
5. Select a method to authorize trustees:
   - To authorize trustees locally, see Authorizing TEP Approval Locally on page 163.
   - To authorize trustees using Remote Authorization, see Initiating Remote Authorization to Approve TEP on page 164.

Authorizing TEP Approval Locally

1. On the Approve TEP (Trustee Establishment Package) screen, select from the following:
   - For multiple card readers, insert the quorum of cards into the readers, enter the passwords and click Start.
   - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the password and click Start.

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

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

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

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

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

Initiating Remote Authorization to Approve TEP

1. On the Approve TEP (Trustee Establishment Package) screen, select a quorum of cards from the Recovery Officers list to use throughout the authorization process and click Enable Remote Authorization.

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

2. When the Remote Authorization enabled message appears, close the Approve TEP screen and notify the Recovery Officer who will approve the TEP that it is safe to continue the TEP approval process and introduce Recovery Cards remotely. See Authorizing TEP Approval Remotely on page 164.

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

Authorizing TEP Approval Remotely

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

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

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

6. When the progress bar is complete, close the Approve TEP screen and notify the Recovery Officer(s) who will approve the TEP that it is safe to continue the TEP approval process.
7. On the Select File screen, select a TAP file name and location and click Save.
8. While on the View Unapproved Trustees tab, select **View > Refresh** to update the trustee verifier.
9. Right-click the trustee and select Copy Verifier.
10. Paste the verifier into a text file and save it.
11. Send the verifier file and the TAP file separately to the first appliance. See Receive TAP on page 165.

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

Receive TAP

To receive the TAP (Trustee Acceptance Package), the first appliance needs the TAP file and verifier received from the second appliance. See Receive TEP on page 162.

1. In the Decru Management Console, in the appliance tree, select the first appliance.
2. From the Trustee menu, select Receive TAP.
3. On the Receive TAP screen, browse to the TAP file and copy the verifier into the provided field.
4. Click Begin Approval.
5. Select a method to authorize trustees:
   - To authorize trustees locally, see Authorizing TAP Approval Locally on page 165.
   - To authorize trustees using Remote Authorization, see Initiating Remote Authorization to Approve TAP on page 165.

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

Authorizing TAP Approval Locally

1. On the Approve TAP screen, select from the following:
   - For multiple card readers, insert the quorum of cards into the readers, enter the passwords and click Start.
   - For a single card reader, select a quorum of cards from the Recovery Officers list, enter the password and click Start.

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

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

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

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

   Note: When the administrator of the first appliance approves the TAP, it is recommended they notify the administrator of the second appliance so that they can delete the unapproved TAP trustee. See Delete Unapproved TAP Trustee on page 166.

Initiating Remote Authorization to Approve TAP

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

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

2. When the Remote Authorization enabled message appears, close the Approve TAP screen and notify the Recovery Officer(s) who will approve the TAP that it is safe to continue. See Authorizing TAP Approval Remotely on page 166.

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

Authorizing TAP Approval Remotely

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

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

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

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

   Note: When the first appliance approves the TAP, it is recommended they notify the second appliance so that they can Delete Unapproved TAP Trustee.

Delete Unapproved TAP Trustee

The first appliance should approve the TAP before the second appliance deletes the unapproved TAP trustee. This retains a backup TAP trustee file until the process is complete. See Receive TAP on page 165.

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

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

Importing and Exporting Keys

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

Exporting a Key

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

Importing a Key

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

14 BACKUP ADMINISTRATION

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

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

- Saving Configurations to Lifetime Key Management
- Backing Up Configurations to a Remote Location

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

Note: Do not use the LKM Settings page of the DMC to configure backups to an LKM appliance. Refer to the *LKM Appliance Administration Guide* for instructions.

Saving Configurations to Lifetime Key Management

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

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

Best Practices for Secure Backups

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

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

Configuring Backups to LKM Appliance

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

Configuring Backups to LKM Software

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

The DataFort appliance 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. The DataFort appliance supports automated configuration backups to four LKM servers.

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

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

Backing Up the Configuration to LKM

Use this procedure to perform a manual backup to LKM.

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

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

Key Purging

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

Only keys that are no longer current (meaning they are not assigned to 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 returns a table of entries and a percent full number. Should the database be more than 75% full, consider purging keys. Use the `keyman purgekeys` command to specify which keys are purged at backup. Use the `keyman purgekeys start -a` command to define the age of the keys to be purged in days.

Backing Up Configurations to a Remote Location

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

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

15 MANAGING APPLIANCE SECURITY

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

- Managing Appliance Defense Responses
- Setting Security Options
- Configuring IPsec
- Managing Recovery Officers and Recovery Cards
- Resetting Smart Cards
- Setting Date and Time
- Configuring and Viewing Logs
- Zeroizing Appliances
- Setting Security Certificates

MANAGING APPLIANCE DEFENSE RESPONSES

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

DEFENSE TRIGGERS AND RESPONSES

A defense response can be triggered by the following:

Chassis Intrusion	If the appliance chassis is opened, this causes an automatic defense response. If chassis intrusion has been detected, there should be physical evidence (such as scratches, a broken lock or a stolen chassis key).
Loss of Power	If the appliance is left without power for a long time (more than 3 weeks) a defense response can be triggered. The appliance battery powers the intrusion-detection circuit even when the appliance is switched off. When this battery becomes low (because the appliance has been powered off for an extended period), it becomes possible for an intrusion to occur without detection or notification. For this reason, a low battery triggers an intrusion alert.
CryptoShred Button	If the appliance is equipped with a CryptoShred button, pressing the button activates the defense response.

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

- The first response level disables the SEP and makes the DataFort appliance unusable for cryptographic operations. It is still possible to access management interfaces and view logs, but encrypted data is inaccessible. To resume normal operation and data access perform an administrative reset (see Clearing a Defense Alert on page 174).
- The second response level protects the data by automatically clearing all encryption keys in the DataFort. Recovery from this response requires zeroization and data recovery. When encryption keys are cleared (Medium and High levels) all encrypted data becomes immediately unusable. Zeroization is required before DataFort configuration can be restored.

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

DataFort Defense Setting

Defense levels are summarized in Table 14. If in doubt, select the Basic level.

Table 14: DataFort Defense Settings

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

Changing the Defense Setting

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

Clearing a Defense Alert

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

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

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

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

Resetting a Defense Alert via DMC

1. Select **Security > Clear Intrusion**.
2. Select the appliance(s) to clear alerts on.
3. Click Apply.

   The appliance reboots, clearing the alert.
4. Close the connection to the appliance.

Resetting a Defense Alert via CLI

The CLI displays an alert after login.

1. Execute the `system tamper reset` command.
2. Execute the `system reboot` command.

   Reboot the appliance as instructed to clear the alert.
3. Close the connection to the appliance.

CryptoShred Button States

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

Normal State	In this state, the CryptoShred button is not depressed and the DataFort appliance operates normally. If the button is pressed once, the DataFort appliance defense response is triggered in accordance with the DataFort Defense Settings. Recovery procedures can be completed by an administrator.
Activated State	Once the CryptoShred button has been pressed, the DataFort appliance remains in the defense response state until the button is pressed again to release it. As long as the button is depressed, recovery procedures are prevented.

System Card CryptoShred

Data processing (encryption and decryption) can be halted manually on DataFort appliances that do not have the CryptoShred button by removing the System Card and turning off the appliance. If the DataFort appliance 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 the DataFort appliance 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 the DataFort appliance by pressing the switch on the rear panel.

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

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

   Restore Operation if System Card was Destroyed: To return the DataFort appliance to normal operations, the DataFort appliance has to be zeroized and reconfigured with the wizard and Recovery Officers. See Zeroizing Appliances on page 197. A new System Card has to be initialized. The DataFort appliance can be restored to the last configuration that was downloaded or backed up.

Setting Security Options

The DataFort appliance offers configurable levels of security to suit a variety of environments and to protect against certain types of security threats. The administrator uses the Management Security screen of the DMC 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.

Selecting a Configured Security Level

1. In the DMC, select **Security > Management Security** to view or set the security policy.

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

2. Select each one of the Preset Security Levels on page 178 from the drop-down list and review its settings.

3. Select the desired security level, or leave the default level of security enabled. By default, Secure DMC and CLI are disabled, and the DataFort appliance management interface is accessible from the Clients or File Servers NIC.

   To create a custom combination of settings, see Customizing a Security Level on page 178.

4. Click Apply.

Preset Security Levels

Select from the following preconfigured security levels:

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

To see which features are on or off for a given preset level, see Table 16, Table 17 and Table 15.

Customizing a Security Level

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

1. In the DMC, select **Security > Management Security**.
2. To preview a pre-configured level, select it from the drop-down list at the top of the screen.
3. To define custom security settings, turn any option on or off using its onscreen radio button. Security settings are divided logically into Appliance Settings, Domain Controller Related Settings, and File Server Related Settings.
4. After selecting the desired options, click Apply.

Appliance Settings

Use these settings to control management of the DataFort appliance. By default, DataFort security settings are customized with Secure DMC, Secure CLI and Clients NIC Management Access all OFF.

Table 15 shows whether the setting is on or off for the three preset levels, as well as the result of turning the setting on.

TABLE 15: DATAFORT MANAGEMENT SECURITY SETTINGS

Setting	Basic	Medium	High	Result
Secure DMC	ON	ON	ON	Requires an Admin Card in order to access the DataFort DMC. 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 DMC with an Admin Card in order to obtain a secure password for temporary access to the CLI. If both Secure DMC 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 appliance. This protects against attacks from the file server side of the network (as long as the DataFort appliance is the only bridge between the file server network and the client network).

Domain Controller Related Settings

By default the DataFort appliance 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 the DataFort appliance's dependence on the domain controller for access control and user authentication.

Table 16 shows whether the setting is on or off for the three preset levels, as well as the result of turning the setting on.

TABLE 16: 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 the DataFort appliance.
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).

TABLE 16: DOMAIN CONTROLLER SECURITY SETTINGS

Setting	Basic	Medium	High	Result
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, the DataFort appliance 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 appliance in maintaining file server ACLs. The DataFort appliance always maintains a Local ACL for all Cryptainers, regardless of the Local ACL security setting.

Table 17 shows whether the setting is on or off for the three preset levels, as well as the result of turning the setting on.

TABLE 17: FILE SERVER SECURITY SETTINGS

Setting	Basic	Medium	High	Result
Use Local ACL	OFF	ON	ON	Allows the DataFort appliance 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 appliance when the Cryptainer is created. Additionally, ACL viewing from client Windows computers is disabled.

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 the DataFort appliance.

Note: IPsec between clients and DataFort appliances requires the purchase of an accelerator card for DataFort appliances from Decru. Adding an accelerator card to the client is also recommended for optimal performance.

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 115.
- To require IPsec as a Cryptainer is created, see Options When Adding a Cryptainer on page 112.

SUPPORTED CLIENTS AND AUTHENTICATION METHODS

The DataFort appliance supports authentication via either preshared keys or Microsoft-compatible Kerberos. IPsec on the DataFort appliance 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 also works 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. When selecting Kerberos authentication the server must join the Kerberos domain.

1. From the Servers and Portals tab, right-click a virtual server and select IPsec.

2. Click Add Kerberos (Windows only).
3. If the virtual server (VIP) is not yet joined to the domain, the Add Kerberos button is greyed out. Click Join to first join the virtual server to a CIFS Domain.
   - In the Join a domain screen, enter an admin user and password. Click Apply. The DataFort appliance contacts the domain controller and adds itself as a member of the domain.
   - Once the virtual server is added to the domain, the CIFS Domain field indicates Joined and the Add Kerberos button is available. Click Add Kerberos and proceed to step 4.
4. 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.
5. Click Apply. The rule appears in the IPsec rule list.
6. To verify an IPsec rule, select a rule from the list and click Check Status.

Kerberos Authentication without IPsec

When adding a virtual server, the specified domain is only used internally to create a context in which to authenticate users. To use Kerberos authentication without creating IPsec rules, join the virtual server (VIP) to the domain. The DataFort appliance contacts the domain controller and adds itself as a member of the domain. To join the server to the domain:

1. Right-click the virtual server in the Virtual Elements pane, and select Edit.
2. Check Joined CIFS Domain, and enter a username and password of an administrator known to the domain
3. 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 appliances 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 works, even if shared secret is specified.

1. From the Servers and Portals tab, right-click a virtual server and select IPsec.
2. Click Add Shared Secret
3. 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.
4. Enter the IP address of the client(s) that will connect using IPsec according to the rule set in the previous step.
5. Click Apply.
6. To verify an IPsec rule, select a rule from the list and click Check Status.

Relevant System Properties

Recommended values for system properties that concern IPsec are shown in the table below.

Table 18: 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)
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.

The DataFort appliance 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 set up a rule for multiple clients through the subnet capability.

IPsec Configuration for Solaris Clients

The following procedure applies to DataFort appliances 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) is 3. if the patches are not installed, the value is 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 appliance 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, the administrator must configure the IKE daemon to propose a suitable SA to the DataFort appliance.

- 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 the DataFort appliance, 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 suggest to configure phase1 or phase2 lifetimes, either globally or per-rule. The administrator should change lifetimes via the **`ndd`** tool, affecting all sessions.

Configure Preshared Keys for Solaris

The administrator must add the same preshared key used by the DataFort appliance 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. Alternatively, 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. Alternatively, 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 DataFort operation but they are essential for key and data recovery operations. Recovery Cards are initialized in sets, and each Recovery Card is associated with one Recovery Officer. If a Recovery Officer leaves the company or loses a Recovery Card, a quorum of Recovery Officers with their cards must assemble to initialize a replacement card and re-form the set. Changes made to a Recovery Card are replicated across the cluster.

Lost Recovery Card Best Practice

If a Recovery Card is lost or stolen, it must be replaced. In addition, it is best practice is to replace and destroy the remaining cards in the quorum to eliminate a possible security breach if another Recovery Card is lost or stolen.

When a Recovery Card is lost, replace all of the cards from the original set one by one, then reset the old cards using the smart card reset function. Be sure not to reset the old cards until the original set has been replaced on every DataFort cluster and appliance that uses them. For more information see Replacing a Recovery Officer and Resetting Smart Cards on page 187.

Replacing a Recovery Officer

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

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

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

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

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

     Repeat until all cards are processed.

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

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

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

Changing a Recovery Card Password

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

1. In the DMC, select **Security > Change Recovery Card Password**.
2. Insert the card for which the password will be changed into the Management Station smart card reader. Strong passwords are an important part of the overall security of the system. New passwords should be 8 or more characters, and include letters, digits and punctuation marks.
3. Enter the existing password.
4. Enter the new password twice.
5. Click Apply.

Resetting Smart Cards

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

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

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

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

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

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

Setting Date and Time

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

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

Configuring and Viewing Logs

The appliance logs events in these categories:

- Security
- Operations
- Performance
- NAS Audit Trail

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

- Temporary (RAM inside the appliance)
- Database (Appliance configuration database)
- Remote Logging Host (remote syslog server)
- Windows Event Log. See Windows Event Logging on page 191.

Note: It is recommended that logs be stored in more than one location. For an example of a secure logging configuration see Recommended Configuration on page 191.

For more information about logging, see Logging Functions on page 298.

Appliance Log Storage Guidelines

Keep in mind the following when configuring appliance logging:

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

Decru Signed Syslog (DSS)

Log signatures can be enabled if remote logging is being used. Signed logs offer a way to authenticate log messages and verify that the log is complete. The logs are sortable for missing messages and can be verified using CLI commands. The feature is applicable only to remote syslog servers.

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

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

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

CONFIGURING LOG STORAGE

To configure the storage location for log information:

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

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

2. Select the desired settings and then click Apply. Alternatively:
   - Click Factory Default to reset the log configuration to the original Decru default settings.
   - Click Current to reset any unsaved changes to the log configuration to the last saved configuration.

Setting and Enabling a Remote Storage Address

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

Adding Time Zone Information to Syslog Timestamp

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

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

Express time in UTC

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

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

   ```
   system property set sys.syslogd.utc_timezone 1
   ```

2. Restart the system log daemon by running the following command:

   ```
   system log restart
   ```

Include Time Zone

To add time zone information in the appliance syslog timestamp:

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

   ```
   system property set sys.syslogd.print_timezone 1
   ```

2. Restart the system log daemon by running the following command:

   ```
   system log restart
   ```

Recommended Configuration

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

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

Windows Event Logging

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

1. Select **Configuration > Log Configuration**.
2. Enter the following information about the user who will log into the Windows host to generate the events: The domain the user belongs to, the user name, and the password. This user must have permission to log events to that host.
3. In the Event Log Host column, enter the IP address of the Windows host in the box for each item to be logged.

   Note: It is a good practice to enter the same IP address for all event log host fields. Enter different IP addresses only if the user login is the same for all entered IP addresses.
4. Click Apply.

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

NAS Audit Logging

If a CIFS or NFS client is getting access denied error messages trying to connect to a Cryptainer through the DataFort appliance, enable NAS Audit Logging. In conjunction with a Technical Support Info collection, NAS Auditing may help determine why the access failure is occurring.

To enable NAS Audit logging

1. Log in to an appliance via the DMC.
1. With an appliance selected in the Resources pane, select **Configuration > Log Configuration**.
2. Select Operations trace for database, and everything under NAS Audit Trail for temporary.
3. Click Apply.
4. Retry access to the Cryptainer.
5. Log in to the DataFort CLI and view the output of the access failure from the DataFort appliance:

```
system util cat /var/log/audit
```

To enable Verbose NAS Audit logging

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

```
system property set sys.proc.syslogd.conf.nas_auth enable
system property set sys.proc.syslogd.conf.nas_acl enable
system property set sys.proc.syslogd.conf.nas_file_access enable
system property set sys.proc.syslogd.conf.nas_cry_access enable
```

2. To retrieve the NAS Audit log after reproducing the issue, run the following command:

```
system util cat /var/log/audit
```

Setting Up Syslog

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

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

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

```
local0.* /var/log/Appliance1
```

   # local0 is for Security messages

```
local1.* /var/log/Appliance1
```

   # local1 is for Operations messages

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

   # local2 is for Performance messages

```
local3.* /var/log/Appliance1
```

   # local3 is for NAS audit messages

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

Syslog Mapping

Table 19 shows the Descriptive Name, System Property Name, Syslog Facility and Level mapping for appliance logs.

TABLE 19: 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 20 describes the mapping for temporary logs.

TABLE 20: TEMPORARY LOG MAPPING

Name	Temp File
security	/var/log/security
operations	/var/log/operation
performance	/var/log/performance
nas audit	/var/log/audit

VIEWING THE LOG

To view the appliance log:

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

To add and remove columns:

1. Right-click on a column title.

   The Column Editor screen appears.

2. Select to add and remove columns.
3. Click OK.

   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 the DataFort appliance.

   - Sort log entries by a particular column by clicking on its column title. Click the column title again to toggle sorting in ascending or descending order.
   - Select a log entry to view its full message details, displayed at the bottom of the pane.
   - Click Refresh to view new logs after making a change to the settings.

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 21 provides samples of auditing messages that may appear in the log.

TABLE 21: 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 DataFort.
Local authentication of user failed	CIFS User DOMAIN\USER from IP 10.10.0.1 could not be locally authenticated by DataFort.
User unknown to DataFort	A connection from CIFS User DOMAIN\USER from IP 10.10.0.1 has been rejected by 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 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

TABLE 21: AUDITING LOG MESSAGES (CONTINUED)

Activity	Sample Log Message
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
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 engtest\dcrusr from IP 10.50.2.184 has created the file "foo (file FH3[33 fb 6a 00 27 bb 51 02 20 00 00 00 0... fb 6a 00 27 bb 51 00])" in Cryptainer netapp5:/vol/nas/mixed/ishvar1/cleartext_audit.
File changed	User engtest\dcrusr from IP 10.50.2.184 has written to "(FSID=1493677097 FID=5222973 FH3[33 fb 6a 00 27 bb 51 02 ... fb 6a 00 27 bb 51 00])" in Cryptainer netapp5:/vol/nas/mixed/ishvar1/cleartext_audit.

TABLE 21: AUDITING LOG MESSAGES (CONTINUED)

Activity	Sample Log Message
File accessed	User engtest\dcrusr from IP 10.50.2.184 has read from "(FSID=1493677097 FID=5222973 FH3[33 fb 6a 00 27 bb 51 02 2... fb 6a 00 27 bb 51 00])" in Cryptainer netapp5:/vol/nas/mixed/ishvar1/cleartext_audit.
File permissions changed	User engtest\dcrusr from IP 10.50.2.184 has set the Unix permissions of "(FSID=1493677097 FID=5222973 FH3[33 fb 6... 0776, UID n/c, GID n/c" in Cryptainer netapp5:/vol/nas/mixed/ishvar1/cleartext_audit.
File removed	User engtest\dcrusr from IP 10.50.2.184 has deleted the file "foo" in Cryptainer netapp5:/vol/nas/mixed/ishvar1/cleartext_audit.
File access denied	User engtest\spec from IP 10.40.101.215 was denied access by the server to the file or directory "(FSID=7138672 FID=18832759 FH3[40 00 00 00 62 37 0b 00 20 00 00 00 01 1f 5d 77 64 4f 26 13 70 ed 6c 00 40 00 00 00 62 37 0b 00]) requested 2d granted 20" in Cryptainer ndev-980a-1:/vol/nas_dev/encrypted.

VERIFYING SIGNED LOG MESSAGES

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

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

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

If logs appear to be missing, compare the logs saved to separate remote locations (logs can be sent to up to four locations, as indicated in Recommended Configuration on page 191) to verify that breaks in the log are replicated. Remote logs can also be compared to the internal appliance log.

The administrator can use the CLI to verify the correctness of the log using the **`system log verify`** command. See Verifying System Logs on page 242.

ZEROIZING APPLIANCES

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

- Zeroizing Using the DMC
- Zeroizing Using the CLI
- Zeroizing Using the Serial Console
- Emergency Serial Console Port Access

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

TABLE 22: KEY RECOVERY AND ZEROIZATION

Key Type	Example	Recovered by Setup Wizard
Keys that protect user data	• Cryptainer keys • Parent keys which encrypt Cryptainer keys	Recovered using the wizard, in order to ensure data can be decrypted by the recovered DataFort appliance.
Keys that authenticate one DataFort appliance to another, or a DataFort appliance to an end user	• SSL keys • SSH keys • IPsec keys	Not recovered, in order to prevent one DataFort appliance from falsely appearing to be a different DataFort appliance.
Secrets belonging to DataFort appliance users	• User passwords	Recovered using the wizard, in order to allow the same users to access a recovered DataFort appliance without recreating passwords.

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

Before Zeroizing

In order to protect against data loss, either decrypt encrypted data before zeroization and re-encrypt it with another DataFort appliance, 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 appliance is zeroized, it can only be recovered using a backup copy of the configuration database. If the DataFort appliance was in a cluster, the other cluster members will have retained all of the configuration information about the network.

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

Zeroizing Using the DMC

It may be necessary to back up the configuration database before zeroization is permitted.

From the DMC, select **Utilities > Back up** and save the configuration to a secure location.

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

1. Be sure the System Card is inserted in the appliance.
2. In the Decru Management Console, from the appliance tree, select one or more appliance(s).

   Shift- or Ctrl-click to select multiple appliances.
3. From the Appliance menu, select Zeroize.
4. On the Zeroize screen, select whether to keep the appliance's IP Address.
5. Enter the confirmation code listed on the screen (ZeroizeYes) and click Apply.
6. Wait a few minutes while the operation completes and the appliance reboots.
7. If IP settings were not preserved by checking Keep IP address, assign the appliance IP settings as described in Assigning the Appliance IP Address on page 55.
8. Complete the configuration by running the Setup Wizard.

ZEROIZING USING THE CLI

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

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

1. Verify the System Card is inserted in the appliance.
2. Log in to the CLI with a valid administrator username and password.
3. Execute the **`system zeroize`** command. To preserve the existing IP address, use the **`system zeroize [-k, --keep_ip]`** command. A prompt appears to enter a confirmation code.
4. Enter the command again, followed by the code.

   `system zeroize [confirmation-value]`

5. Wait a few minutes while the operation completes and the appliance reboots.
6. If they were not preserved, reassign the appliance IP settings as described in Assigning the Appliance IP Address on page 55.
7. Complete the configuration by running the Setup Wizard.

Zeroizing Using the Serial Console

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

1. Verify the System Card is inserted in the appliance.
2. Connect the appliance serial console port (see Serial Console Port on page 53).
3. Log in to the serial console with a valid administrator username and password.
4. To zeroize the appliance, enter option **z**.
5. Enter a confirmation code when prompted.
6. Wait a few minutes while the operation completes and the appliance reboots.
7. Assign the appliance IP settings. See Assigning the Appliance IP Address on page 55.
8. After the appliance has been assigned IP settings, complete the configuration by running the Setup Wizard.

Emergency Serial Console Port Access

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

1. Connect a Management Station or other PC to the appliance serial console port (see Serial Console Port on page 53).
2. Connect a smart card reader to the PC connected to the serial port.
3. Insert one of the Recovery Cards for the appliance into the smart card reader.
4. Make a note of the Recovery Card label (e.g. RecoveryCard1).
5. Remove the Recovery Card from the card reader.
6. Remove the System Card from the appliance front panel slot.
7. Insert the Recovery Card into the appliance front panel slot.
8. On the PC, launch a terminal client to connect to the appliance.
9. At the login prompt, enter the Recovery Card label as the username and enter the Recovery Card password.

   If authentication succeeds, the console menu is displayed.
10. Enter option **z** to zeroize the appliance.
11. Assign the appliance IP settings. See Assigning the Appliance IP Address on page 55.
12. After the appliance has been assigned IP settings, complete the configuration by running the Setup Wizard. See Initializing a Standalone Appliance or Cluster on page 61.
13. If a current backup of the appliance configuration database is available, the configuration can be restored using the Recover from Database function of the wizard.

Setting Security Certificates

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

After the certificate is set and installed, no further security warnings appear when logging in to the appliance unless a change has been made to the IP address or hostname of the appliance, or cryptographic operations have been disabled. It may be desirable to install a certificate signed by a certificate authority as described in Setting a Certificate Authority Signed Certificate on page 202. Keep the following in mind:

- A certificate must be generated independently for each appliance in a cluster.
- Create the certificate and then use it until its expiration date.
- Only a Full Administrator can set the security certificate.
- SSL private keys are cleared by zeroization, and may not be backed up or transferred to other appliances. If signed certificates have been purchased, they have to be replaced for zeroized appliances. See Zeroizing Appliances on page 197 for more about zeroization.

Setting a Self-Signed Security Certificate

1. Log in to the appliance via the DMC.
2. Select **Security > Certificates**.

   The appliance hostname appears in the Common Name field. The Common Name must be the hostname or IP address of this appliance. If a hostname is used, it must be resolvable by DNS.
3. Enter the information for the self-signed certificate. This information appears when certificate details are viewed.

   Note: Country codes are established by the International Organization for Standardization (ISO). For a partial list of country codes, see Partial List of ISO Country Codes on page 321.
4. Click Apply.

   After a moment, the certificate prompt appears.

   If it does not appear automatically, verify the appliance in question is still selected in the appliance pane, then select the Appliances tab.
5. Review the certificate and accept it.

Setting a Certificate Authority Signed Certificate

Generating the Certificate Request

1. Log in to the appliance via the DMC.
2. Select **Security > Certificates**.
3. Click Generate CA Request.
4. This generates a PEM-encoded request which can be submitted to a known certificate authority such as VeriSign or a local certificate authority.

   Note: Country codes are established by the International Organization for Standardization (ISO). For a partial list of country codes, see Partial List of ISO Country Codes on page 321.

Setting the CA-signed Certificate

1. Log in to the appliance via the DMC.
2. Select **Security > Certificates**.
3. Click Set CA Certificate.
4. Paste the certificate received from the certificate authority into the box provided. Cut and paste the entire contents of the certificate file, including the BEGIN and END lines.
5. Click OK.
6. Click Apply.

   After a moment, the certificate prompt appears.

   If it does not appear automatically, verify the appliance in question is still selected in the appliance pane, then select the Appliances tab.
7. Review the certificate and accept it.

16 CLUSTER ADMINISTRATION

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

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

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

Cluster administration tasks include:

- Cluster Management
- Cluster-Wide Management via DMC
- Adding and Removing Cluster Members
- Recovering a Cluster
- Changing Network Properties of a Cluster Member
- 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, disabled or removed to restore full cluster operation.

About Failing Over a Cluster

To halt the file serving operations on one or all members in a DataFort appliance cluster (without breaking the cluster) use the View Cluster Failover tab of the DMC. 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 appliance 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 appliance's Clients NIC also presents the 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 appliance 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.

If one DataFort appliance in the cluster goes offline, the remaining appliance automatically take over operations. All cluster members keep the same configuration database.

Cluster-Wide Management via DMC

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

Checking the Status of the Cluster

To check the status of a cluster, log in to one of the cluster members via the DMC and select **Appliance > View Cluster Members**.

Cluster status is defined by the Group State and Replication State of the configuration database shared by the cluster members. All cluster members are listed in the table in the View Cluster Members tab.

If the cluster is not in a committed/online state, some action may be required in order to resolve the cluster condition. Check Table 23 for a description of cluster states.

Table 23: 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 appliance also shows this as its cluster state.	n/a
recover	**committed/recover** Cluster members are synchronizing configuration information. When the process is complete the state will change to committed/online.	**aborted/recover** Cluster members are not communicating. Check network connections and cluster configuration. If one member of the cluster has failed, replace it with a new DataFort appliance.
conflict	**committed/conflict** There is a conflict between configuration databases that cannot be automatically resolved.	n/a

Resolving a Cluster Conflict

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

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

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

Checking Failover Status

The cluster is in a normal state with respect to serving data when all VRIDs are serving their primary DataFort appliance. The cluster is failed over when some or all VRIDs are serving a secondary DataFort appliance instead.

A failed over cluster is indicated by entries in red in the View Cluster Failover tab. Select **Configuration > View Cluster Failover** to see this tab.

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 215), the admin can recover the normal cluster state manually.

Recovering a Cluster from Failover

To recover from a failed-over cluster state:

1. Log in to a cluster member via the DMC.
2. Select **Configuration > View Cluster Failover**.

   Entries in red indicate VRIDs that are not served by their primary DataFort appliance. The primary DataFort appliance has been failed over.
3. In the View Cluster Failover tab, click Manual Recover.
4. Verify the recovered cluster.

   When recovery is complete, the VRIDs are served by their primary DataFort appliances (each VRID has a different DataFort IP as primary) and there are no entries in red in the View Cluster Failover tab.

Adding and Removing Cluster Members

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

A DataFort appliance can also be removed from the cluster at any time. See Removing a Cluster Member. Keep in mind that in most cases once a DataFort appliance is removed from the cluster, it must be zeroized and reintroduced to the cluster using the Setup Wizard.

Adding a Cluster Member

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

- A DataFort appliance must be uninitialized when added to a cluster. Initialized standalone DataFort appliances cannot be joined to form a cluster. To zeroize an initialized DataFort appliance so it can be added as a new cluster member, see Zeroizing Appliances on page 197.
- Cluster members are added by running the Setup Wizard for the existing DataFort appliance, not the appliance to be added. For detailed instructions on adding a member to a cluster, see Adding a Member to a Cluster on page 69.
- 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 or Machine Administrator can run the wizard and add a cluster member.

Removing a Cluster Member

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

1. Log in to the cluster member that will be removed from the cluster. (If the DataFort appliance is offline or down, skip to step 5.)
2. Select **Configuration > View Cluster Failover**.
3. On the View Cluster Failover tab, click Manual Failover. This sends all operations to the other cluster members.
4. Log out of the failed-over DataFort appliance.
5. Power the failed-over DataFort appliance down and remove it from the network, disconnecting the cables.
6. Log in to a remaining DataFort appliance in the cluster
7. Select **Appliance > View Cluster Members**.
8. Right-click the offline DataFort appliance and select Delete.

Replacing a DataFort Appliance in a Cluster

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

- A new or zeroized DataFort appliance.
- A DataFort appliance remaining from the original cluster.
- The minimum set of Recovery Officers and Recovery Cards as determined by the recovery schema of the cluster.

1. Power down the offline DataFort appliance and remove it from the network, disconnecting the cables.
2. Log in to an online member of the cluster.
3. Select **Appliance > View Cluster Members**.
4. Right-click the offline DataFort appliance and select Delete.
5. Log out of the online DataFort appliance.
6. Replace the removed DataFort appliance with the new, uninitialized DataFort appliance.
7. Assign an IP address to that DataFort appliance and connect it to the network.
8. Run the Setup Wizard from an online member of the cluster, adding the new DataFort appliance.

Recovering a Cluster

Follow the cluster recovery procedures to return an entire cluster to a previous configuration or to replace all members of a cluster. This procedure is used to replace missing or damaged clustered DataFort appliances. The replacement DataFort appliances must be zeroized. See Zeroizing Appliances on page 197.

- If one cluster member is lost, it should not be restored using the wizard. It should be deleted from the cluster and replaced as described in Adding a Cluster Member on page 207. Use the wizard to restore the first member of a cluster only if all members have been lost.
- If no cluster members are online, run the wizard on one DataFort appliance, using a saved configuration database from a lost cluster member, then add the second cluster member.

This procedure requires:

- A saved configuration database from the previous configuration.
- The minimum set of Recovery Officers and Recovery Cards required by the recovery schema selected when the original standalone DataFort was set up.

1. Connect the first (new or zeroized) DataFort appliance to the network and assign it the IP settings of one of the cluster members to be replaced.
2. Connect the other (new or zeroized) DataFort appliance to the network, and assign it IP settings.
3. Complete the setup wizard on the first DataFort appliance, using the saved configuration database from the old cluster. Add the second DataFort appliance during the wizard.

Changing Network Properties of a Cluster Member

The network settings can be changed for a cluster member.

- Changing Configurations in a Cluster
- Changing the Clients NIC IP Address of a Clustered Appliance
- Changing the File Servers NIC IP Address of a Clustered Appliance
- Changing the IP Address of an Appliance Using NFS Local Domain
- Changing the VRID of a Clustered DataFort Appliance
- Changing the IPsec Secret of a Cluster
- Changing the Hostname of a Clustered DataFort Appliance

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 Appliance and Changing the VRID of a Clustered DataFort Appliance.

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

Changing the Clients NIC IP Address of a Clustered Appliance

> **Note:** To change the IP setting of the File Servers NIC as well, follow instructions for Changing the File Servers NIC IP Address of a Clustered Appliance after completing this procedure. The admin cannot change the File Servers NIC until the cluster is re-established using the new Clients NIC IP address.

1. Log in to the DataFort appliance with the IP address to be changed.
2. Select **Configuration > View Cluster Failover**.
3. Click Manual Failover.
4. Select **Configuration > Network**.
5. Change the Clients IP address.
6. Log out of the DataFort appliance.
7. Log in to another cluster member.
8. Select **Appliance > View Cluster Members**.
9. Right-click the DataFort appliance with the changed IP information and select Edit.
10. Enter the new IP information and click Apply.
11. Log back in to the cluster member with the newly changed IP.
12. Select **Appliance > View Cluster Members**.

13. Wait until the status is committed/online.
14. Select **Configuration > View Cluster Failover**.
15. Click Manual Recover.

Changing the File Servers NIC IP Address of a Clustered Appliance

To also change 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 DataFort appliance with the IP address to be changed.
2. Select **Configuration > Network**.
3. Change the File Servers IP address.
4. Click Apply.

Changing the IP Address of an Appliance Using NFS Local Domain

If a DataFort appliance is set up at one location to encrypt data for a local NFS domain and needs to be moved to another location with a different IP address, the IP needs to change but encrypted data must remain accessible after the move.

1. Log in via the DMC to the DataFort appliance that will be moved.
2. Select **Topology > Servers and Portals**.
3. Unvirtualize all shares on any VIPs that will no longer be accessible after the IP change by right-clicking each share under the VIP and selecting Delete.
4. Right-click every VIP that the NFS Domain is using, select Edit, and change the NFS domain to the DataFort_Admin domain.

   Note: Delete any VIPs that will not be kept.
5. Log in to the DataFort CLI and run the following command to enable vif multinet:

   ```
   system property set nas.vif.multinet 1
   ```
6. Back in the DMC, select **Configuration > Network**.
7. Change all IP or hostname information that needs to be changed and click Apply.
8. Once the changes are complete, log in to the DataFort appliance at the new IP address. Be sure to have serial console access in case the new IP address is not accessible.

   If the DataFort appliance is in a cluster, it may be necessary to change the IP for the cluster after changing the IP information.
9. Log in to both clustered DataFort appliances.
10. Select **Appliance > View Cluster Members**.
11. Verify that the new IP appears on the cluster page. To change it, right-click the appropriate DataFort appliance and select Edit.
12. Create the new VIP that will be used for all NFS clients.
13. Virtualize the NFS shares (exports) on this VIP.
14. Test access to the original files through the new VIP.
15. Log in to the DataFort CLI and run the following command to change the vif property back to 0:

    ```
    system property set nas.vif.multinet 0
    ```

Changing the VRID of a Clustered DataFort Appliance

The following assumes a cluster of DataFort A and DataFort B. While changing a VRID in a cluster all file serving operations must be suspended.

1. Log in to DataFort A via the DMC.
2. Select **Configuration > View Cluster Failover**.
3. Click Manual Failover.

   The Manual Failover button only fails over the DataFort appliance currently selected in the Resources pane.
4. Log out of DataFort A.
5. Log in to DataFort B via the DMC.
6. Select **Configuration > View Cluster Failover**.
7. Click Manual Failover.
8. Click VRID Settings.
9. Enter the initial VRID, and the number of VRIDs the cluster will use. If unsure about the number of VRIDs, use the number of DataFort appliances in the cluster (or just leave the number unchanged).
10. Click Apply.
11. In the View Cluster Failover tab, click Manual Recover.

Changing the IPsec Secret of a Cluster

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

Changing the IPsec Secret Using the DMC

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

   Note: If the appliances do not have a SecureView license installed, or the administrator logins for each cluster member are different, repeat these steps for each cluster member individually. In this case, due to the temporary shared secret discrepancy, cluster status remains aborted/recover until the change to the cluster has been completed.
3. Select **Configuration > Set Cluster IPsec Shared Secret**.
4. Enter the new IPsec shared secret twice and click Apply.
5. Once the process is complete and all cluster members are updated, select **Appliance > View Cluster Members** to verify that cluster status has returned to committed/online.

Changing the IPsec Secret Using the CLI

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

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

Changing the Hostname of a Clustered DataFort Appliance

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

Note: A configured DataFort appliance cannot be moved from one cluster to another. To move an initialized DataFort appliance to another cluster, it must be zeroized and added. See Adding a Cluster Member on page 207.

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

```
system property set net.hostname newhostname
clu config set-local --name newhostname
system property set sys.datafort.label newhostname
system reboot
```

Setting Cluster Properties With the CLI

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. The DataFort appliance does not implement spanning-tree, therefore the best practice is to disable the STP holddown period altogether on switches connected to the DataFort appliance network.

If STP holddown cannot be disabled for some reason, the DataFort appliance 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 appliance is set to delay 15 seconds. If this delay is sufficient for the switch to which the DataFort appliance is connected, leave it unchanged. To view the delay setting, log in to the DataFort CLI and run the following command:

```
system property get net.inet.ip.stp_holddown
```

This returns the current delay setting of `15`.

Note that since each cluster member should be connected to a different switch, each DataFort appliance 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
```

The appliance returns the following confirmation:

```
NOTICE: Property 'net.inet.ip.stp_holddown' was modified.
```

Cluster Crypto Failover Command

A DataFort cluster member automatically stops serving clients if an intrusion is detected or a fatal failure is detected in the SEP. To disable this setting, log in to the DataFort CLI and run the following command:

```
system property set nas.cluster.crypto_failover false
```

In this case, automatic failover is not performed upon detecting either of these conditions, and since cryptographic operations are disabled, clients are refused service until the administrator resets the intrusion status or triggers failover from the CLI (by using `cluster failover`) or the DMC (using the Manual Failover button accessed by selecting **Configuration > View Cluster Failover**).

AUTO GIVEBACK

By default, when a DataFort appliance in a cluster is powered up after being powered down (for example if it is power-cycled during normal operation), it does not start serving its primary VRID automatically. Instead, the secondary DataFort appliance for that VRID goes on serving it until it receives an explicit **`cluster giveback`** command. This behavior is recommended for production environments.

To change this setting, log in to the DataFort CLI and run the following 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 appliance 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, log in to the DataFort CLI and run the following 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, make modifications including:

- Splitting traffic up between VIPs or additional DataFort appliances.
- Adding more DataFort appliances.

17 MACHINE ADMINISTRATION

Machine administration includes various appliance management tasks.

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

> **Note:** A specified Machine Administrator can also add a new member to a cluster, as described in Cluster Administration on page 203.

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

- Changing Network Settings
- Upgrading Appliances
- Managing Licenses

Only a Full Administrator can manage SNMP:

- SNMP Settings

> **Note:** Appliance Date and Time can only be set by a Full or Security Administrator. See Setting Date and Time on page 188.

Additional appliance management tasks include:

- Adding an Appliance
- Logging into Appliances
- Creating Custom Appliance Groups
- Removing an Appliance from a Custom Group
- Removing a Custom Group

CHANGING NETWORK SETTINGS

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

Note: These instructions are for standalone DataFort appliances. For instructions on changing clustered DataFort appliance network settings, see Changing Network Properties of a Cluster Member on page 210.

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

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

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 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 appliance needs to be updated. See Managing Servers on page 110.

Upgrading Appliances

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

> **Note:** While the appliance is being upgraded, there is a small window of time during which the appliance's intrusion detection is disabled. Upgrades should only be performed when the administrator can maintain physical security of the appliance.

All upgrades require the administrator to power cycle the appliance by selecting **Appliance > Reboot** in the DMC. Note that the System Card must be inserted in the appliance before power is cycled.

Verifying an Upgrade Package

1. Select **Utilities > Verify**.
2. Browse to the Upgrade file and click Apply.

   After the package is verified, a hash is displayed in a screen.
3. Verify the displayed hash with the known valid hash.

Managing Licenses

Appliance features require a software license issued by Decru before they can be enabled. A Security Administrator or Full Administrator is required when adding or removing a license.

Viewing Licenses

1. Log in to the appliance via DMC.
2. Select **Configuration > View Licenses**.
3. Review currently installed licenses and verify they are valid.

   A license becomes invalid when it expires. The license may be linked to the appliance serial number, in which case the license must be updated if an appliance is configured using a database from an appliance with a different serial number.

   To remove an expired license, select it and click Delete.

Adding Licenses

If necessary, obtain a new license from Decru and add it by following these steps:

1. Log in to the appliance via DMC.
2. Select **Configuration > Add License**.
3. Enter the license into the License ID field.
4. Click Apply.

SNMP Settings

This section contains the following topics:

- About SNMP Options
- Setting SNMP Options

About SNMP Options

Decru appliances supports both MIB II and the read-only private Decru MIB. The Decru MIB is included on the appliance CD. It provides standard MIB-II as well as Decru MIB messages. All Decru MIBs are read-only for security reasons. Only a Full Administrator can configure SNMP settings. A separate *Appliance SNMP Alarms Guide* is available from Decru for reference.

Decru appliances support SNMP v1, v2c, v3 queries but send only v1 traps. The various types of traps, which are sent via the RMON mechanism, are described in the *Appliance SNMP Alarms Guide*.

Decru uses Net-SNMP agent with the following protocols:

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

  Note: Decru appliances do not support sending SNMPv3 traps.

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

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

Setting SNMP Options

1. Log in to the appliance via DMC.
2. Select **Configuration > SNMP Agent**.
3. On the SNMP Agent screen, enable or disable SNMP for the appliance.
4. Enter the following:

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

5. Click Apply.

Additional Appliance Management Tasks

Adding an Appliance

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

1. Select **Start > Programs > Decru > Decru Management Console**.
2. Select **Appliance > Add**.

   The Add... pop-up screen appears.
3. Enter the IP address or hostname of the appliance.

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

   To add an IP address range for multiple appliances with consecutive IP addresses: enter the first IP address of the range in the IP range start field. Press Tab to move the cursor to the IP range end field and enter the end of the IP range.
4. Click OK.
5. A security certificate warning appears. Make the appropriate selection about trusting the certificate.

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

   Once added, the appliance appears in the console listed under Resources. Appliances appear offline until the administrator logs in via the DMC.

Logging into Appliances

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

1. Select an appliance from the appliance tree and select **Appliance > Log in**.
2. Enter the administrator name and associated password at the Login page and click OK.

   If the correct credentials were entered and the appliance is correctly configured, the status of the appliance changes to online. See State Displays on page 227 for information about status icons.

Creating Custom Appliance Groups

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

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

   Note: When adding a DataFort appliance to the DMC on another Management Station, the appliance retains its existing custom group membership. If these custom groups do not yet exist on the other DMC, they are automatically created.

Removing an Appliance from a Custom Group

1. In the Decru Management Console, from the appliance tree, select one or more appliance(s).
   - Shift- or Ctrl-click to select multiple appliances.
2. Select **View > Remove from Custom Group**.
3. When prompted, click Yes to remove the appliance from the custom group.

Removing a Custom Group

1. In the Decru Management Console, from the appliance tree, select an appliance group or nested group.
2. Select **View > Remove Custom Group(s)**.
3. When prompted, click Yes to remove the custom group.

18 Appliance Settings and Status

The Decru appliance provides information on status and settings in the DMC, LCD, SNMP and CLI interfaces:

- See Viewing Settings in the DMC for an overview of status and settings visible in the DMC.
- The Appliance 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 DMC

The DMC can be used to view current settings, including:

- View Appliance Logs
- View Appliance Date and Time Settings
- View Appliance Crypto Status
- View Appliance Information
- View Appliance Sensors
- View Appliance LCD

View Appliance Logs

Select **Diagnostics > View System Log**.

- Sort log entries by a particular column by clicking on its column title.
- Click the column title repeatedly to toggle sorting in ascending or descending order.
- Right-click a column title to customize column layout.
- Select a log entry to view its full message details displayed at the bottom of the pane.
- Click Refresh to view new logs after making a change to the settings.

To configure logs see Configuring Log Storage on page 190.

View Appliance Date and Time Settings

Select **Configuration > Date/Time**. The date and time settings of the appliance are displayed.

View Appliance Crypto Status

Select **Diagnostics > Run Crypto Tests**. The appliance continually monitors the state of its cryptographic system, halting file serving operations if a failure occurs. Select this option to run the test manually and display the results.

View Appliance Information

Select **Diagnostics > View System Information**. The system version for the appliance and the serial number are displayed.

View Appliance Sensors

Select **Diagnostics > Check Appliance Sensors**. This shows 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 appliance hardware.

View Appliance LCD

Select the Appliances tab to display the LCD graph and messages for each selected appliance.

19 DECRU MANAGEMENT CONSOLE FUNCTIONS

The Decru Management Console (DMC) is an application that is installed on the Management Station and serves as the graphical management interface for Decru appliances.

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

- State Displays
- About the Appliances Tab
- Appliance Menu
- Edit Menu
- View Menu
- Configuration Menu
- Keys Menu
- Topology Menu
- Utilities Menu
- Security Menu
- Trustee Menu
- Diagnostics
- Help Menu

State Displays

The condition of each appliance is indicated in the DMC with an icon in the appliance tree of the DMC screen. Table 24 shows possible state displays for appliances in the Management Console.

Table 24: Appliance Status Indicators

Icon	Icon Appearance	Appliance State
	Blue	The two online states are reflected in the appearance of the appliance font: Online (black) and Linked (black bold).
	Blue with yellow alert	Online with error. See About the Appliances Tab on page 228. for status details.
	Gray with exclamation	Logged off. Administrator name and/or password is incorrect, or log in is timed out (this occurs after 30 minutes if inactive).
	Yellow with open icon	Not initialized. IP address is set, but setup wizard not completed.
	Red	Offline.
	Gray	Not logged in.

About the Appliances Tab

The Appliances tab contains the following default columns:

- Appliance—Displays the appliance by name.
- Availability—Displays the appliance state.
- Front Panel LCD—Displays the contents of the LCD on the front of the appliance. Includes the appliance name, status or error messages, Number of Keys, and CPU Load.
- Type—Displays the appliance type.
- Version—Displays the appliance operating system version.
- Serial Number—Displays the appliance serial number.

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

Using Tab Table Columns

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

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

APPLIANCE MENU

Log in	Log in to an appliance as an administrator. See Logging into Appliances on page 222.
Log out	Log out of an appliance.
Add	Add an appliance. See Adding an Appliance on page 222.
Add Cluster Members	Add a cluster member to DMC. See Adding a Member to a Cluster on page 69.
Add Linked Appliances	Add appliances linked to an LKM appliance to DMC. See the *Lifetime Key Management Administration Guide*.
Remove	Remove an appliance from the DMC appliance tree. Several appliances may be removed at once if SecureView is enabled. Shift- or Ctrl-click to select multiple appliances.
Link	Select a link policy to archive or share keys between two appliances, one of which must be an LKM. See the *Lifetime Key Management Administration Guide*.
Link LKM Software	Back up DataFort appliance configuration and key database to an LKM server for emergency data recovery. See Saving Configurations to Lifetime Key Management on page 169.
View Link Report	View details about appliance links, including key sharing group, in the Linked Appliances table. See the *Lifetime Key Management Administration Guide*.
View Cluster Members	View a list of members in the cluster and their current state. See Checking the Status of the Cluster on page 205.
Set up	Set up an appliance by using the Setup Wizard. See Initializing a Standalone Appliance or Cluster on page 61.
Reboot	Reboot one or more selected appliances.
Zeroize	Zeroize one or more selected appliances. See Zeroizing Appliances on page 197.
Exit	Exit the Management Console.

Edit Menu

Cut	Cut a text entry.
Copy	Copy a text entry.
Paste	Paste a text entry.
Find	Search for text in the active pane of the DMC. The search is not case sensitive.
Find Again	Find next result in the same search.
Preferences	Select to stay logged in to prevent the DMC session with the selected appliance(s) from expiring. Select to refresh the selected appliance(s) at a regular customizable interval.

View Menu

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

All	List all appliances in the Resource pane.
Type (default)	Display appliances sorted by type, including KM-Series, FC-Series, E-Series, and S-Series appliances.
Subnet	Display appliances sorted by subnet.
Custom Groups	Display appliances organized into custom appliance groups.
Add Custom Groups	Add a custom appliance group to monitor appliances based on organizational hierarchies. See Creating Custom Appliance Groups on page 223.
Remove Custom Group(s)	Remove a custom appliance group. See Removing a Custom Group on page 223.
Remove from Custom Group	Remove an appliance from a custom appliance group. See Removing an Appliance from a Custom Group on page 223.
Refresh	Refresh the appliance information displayed in the active view.

CONFIGURATION MENU

View Administrators	View and manage administrators. See DataFort Admin Roles and Account Administration on page 86.
Add Admin	Add an administrator. See Adding an Administrator on page 90.
View Licenses	View licenses. See Viewing Licenses on page 219.
Add License	Add licenses. See Adding Licenses on page 219.
View OpenKey Clients	View OpenKey clients linked to an LKM. See the *Lifetime Key Management Administration Guide*.
View OpenKey License Usage	View OpenKey license usage. See the *Lifetime Key Management Administration Guide*.
Network	Update the hostname of the appliance, the IP address, and the netmask and gateway settings of an appliance. See Changing Network Settings on page 217.
SNMP Agent	Configure SNMP agent options. See SNMP Settings on page 220.
Date/Time	Update the date, time and time zone settings of an appliance. See Setting Date and Time on page 188.
Log Configuration	Configure appliance event logging and log storage. See Configuring and Viewing Logs on page 189.
Set Cluster IPsec Shared Secret	Change the IPsec shared secret of a cluster. See Changing the IPsec Secret of a Cluster on page 212.
View Cluster Failover	View and manage cluster failover status and settings. See Checking Failover Status on page 206.

KEYS MENU

View Parent Keys	View all parent keys stored on an appliance. See Key Management on page 21.
View Parent Keys from LKM	View all parent keys stored on an LKM appliance. See the *Lifetime Key Management Administration Guide*.
View Data Encryption Keys	Locate specific Data Encryption keys stored in LKM. See the *Lifetime Key Management Administration Guide*.
Translate Keys	Translate Cryptainer keys that have been decrypted from one DataFort appliance's parent key and encrypted with another DataFort's parent key, so that both appliances can access the Cryptainer. See the *Lifetime Key Management Administration Guide*.
Change Key Sharing Group for Appliance	Change a policy based key sharing group for DataFort appliances that are Trustees of an LKM appliance. See the *Lifetime Key Management Administration Guide*.
Change Key Sharing Group for Keys	Change a key sharing group for any individual key. See the *Lifetime Key Management Administration Guide*.
Move Unshared Keys into Key Sharing Group	Move unshared keys into a key sharing group. See the *Lifetime Key Management Administration Guide*.
Make Key Archive	Create a archive of parent keys for an LKM client. See the *Lifetime Key Management Administration Guide*.
Make Cryptainer Key Archive	Create an archive of parent keys for a Cryptainer. See the *Lifetime Key Management Administration Guide*.
Export Keys	Export key files to a local hard drive. The files can then be deleted from the LKM appliance, or imported back into an LKM appliance (the original or another one). Only key information is shared. See the *Lifetime Key Management Administration Guide*.
Import Keys	Import key files that have been exported from another LKM appliance. See the *Lifetime Key Management Administration Guide*.
Key Recovery	Recovers key files in the rare event the LKM appliance and its peers are down. See the *Lifetime Key Management Administration Guide*.
Purge Unused Keys	Remove unused keys from the DataFort database. See Key Purging on page 170.

Topology Menu

Servers and Portals	Manage NAS storage and Cryptainers. See Servers and Portals on page 102.
Initiators and Targets	Manage iSCSI storage and Cryptainers. See iSCSI Storage Administration on page 122

Utilities Menu

Command Line	Opens the DMC Command Line Interface (CLI) for all selected appliances. See Connecting to CLI via DMC on page 82.
Back up	Back up the configuration database of an appliance. See Saving Configurations to Lifetime Key Management on page 169.
Back up appliances to LKM	Back up configuration databases of all appliances linked to an LKM appliance to that LKM appliance. See the *Lifetime Key Management Administration Guide*.
Back up appliances from LKM	Back up the most recent configuration database of all appliances backed up to an LKM appliance to a secondary location. See the *Lifetime Key Management Administration Guide*.
Verify	Verify the validity of an upgrade package before upgrading. See Verifying an Upgrade Package on page 218.
Upgrade/Downgrade	Upgrade or downgrade an appliance. Perform upgrades and downgrades only after consulting Decru support. See Upgrading Appliances on page 218.

SECURITY MENU

View Recovery Cards	View Recovery Cards for individual appliances or groups of appliances. Use to compare card usage when sharing cards between appliances and when redefining how a card is shared, or to locate and replace a Recovery Officer.
View Recovery Cards from LKM	View all Recovery Cards associated with appliances connected to an LKM appliance. Use to locate a card if an appliance is down.
Replace Recovery Officer	Replace Recovery Officers. See Replacing a Recovery Officer on page 185.
Change Recovery Card Password	Recovery Card passwords can be changed for additional security. See Changing a Recovery Card Password on page 186.
Smart Card Utilities	Reset a smart card and display card information. See Resetting Smart Cards on page 187.
Management Security	Configure appliance, domain controller, and file server related security options. See Setting Security Options on page 177.
Defense	Specify the automatic appliance response to evidence of threat or intrusion. See Managing Appliance Defense Responses on page 173.
Certificates	Configure appliance security certificates. See Setting Security Certificates on page 201.
Clear Intrusion	Reset the tamper alert and reboot the system if an intrusion alert appears. See Clearing a Defense Alert on page 174.

TRUSTEE MENU

Create Trustee Link	Create a Trustee link between two appliances. This allows the appliances to share key information. Both appliances must be selected. See Managing Trustees on page 158.
Start Trustee Creation	Create a Trustee relationship. See Setting Up Trustees on page 158.
Receive TEP	Allow selected appliance(s) to receive a Trustee Establishment Package. See Authorizing TAP Approval Locally on page 165.
Receive TAP	Allow selected appliance(s) to receive a Trustee Acceptance Package. See Authorizing TAP Approval Locally on page 165.
View Unapproved Trustees	Display list of trustees not yet approved (waiting to accept a TAP). See Delete Unapproved TAP Trustee on page 166.
View Trustees	Display list of trustees.
Export Trustee Keys, Import Trustee Keys	Once a trustee relationship is established it is possible to transfer keys between the two clusters using the import and export key options. See Importing and Exporting Keys on page 167.

DIAGNOSTICS

View System Information	View system version information for the selected appliance.
View System Log	View the appliance log file. See Configuring and Viewing Logs on page 189.
Run Crypto Self Test	Run a self-test on the appliance's Storage Encryption Processor to check the state of its cryptographic system.
View Storage Details	View information about SAN or SCSI storage devices.
Check Appliance Sensor	View the status of the hardware including Temperature Sensors, Fan Sensors, Voltage Sensors and Power Supply Sensors. This information can be used by Decru Technical Support to diagnose problems with the appliance hardware.
Collect Tech Support Info	Create a file containing information useful to Decru Technical Support for troubleshooting appliances.

HELP MENU

Help Contents	Open a PDF file of the Administration Guide for the selected appliance type.
About	Show information about this version of the Decru Management Console.

20 CLI ADMINISTRATION

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

- The CLI cannot be used to replace smart cards, manage keys, or recover data.
- A Full Administrator logged in to the CLI can execute all CLI commands; specialty administrators are restricted to executing commands associated with their role.
- A list of top-level commands can be found in the Command Line Interface Quick Reference on page 287 of this guide. Refer to the separate *DataFort CLI Reference Guide* for a complete list of commands and parameters.

Procedures described in this chapter include:

- Using the CLI
- 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
- Cryptainer Aliases
- Port Forwarding
- IPsec Configuration and Management
- Changing Appliance Network Port Settings

USING THE CLI

Some CLI commands must be run in a specific order for desired results. The command line provides 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 Command Line Interface on page 80. By default, Secure CLI is disabled. See Setting Security Options on page 177. Open only one DMC or CLI session per appliance or appliance cluster at one time.

CLI HELP

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

Administration Commands

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

- Administrator Roles
- Creating a New Administrator
- Cluster Management
- System Properties and Log Management
- Stack Trace Settings
- Network Management

Administrator Roles

Use the CLI to find out which administrators can run 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 desired specialty administrator and enter:

   ```
   cli doc -n
   ```

   The list of commands executable by the type of administrator who is currently logged in appears.

2. Enter the name of the current administrator into the **system property get** command to see the current values of system properties, preceded by permissions for the named administrator role. RW indicates that the administrator logged in has read and write permission, R- indicates read-only permission. A lower-case w indicates a property that can only be changed via DMC.

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

Creating a New Administrator

New administrators can be created by a Full Administrator using CLI commands. When an administrator is created using the DMC, the new administrator is granted the authorizer role and replicated across the cluster by default. By default, any administrator created using the CLI requires prior authentication of another administrator before logging in to the DMC or CLI.

To create an administrator using the DataFort CLI:

1. Log in to the CLI as a Full Administrator.
2. To create an administrator for a single DataFort appliance, add a user, indicating the type from the list of Administrator Roles in the **<group>** field:

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

3. To create an administrator that is replicated to cluster partners add a user with the **`--replicate`** flag, indicating the type from list of Administrator Roles in the **`<group>`** field:

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

4. To add the authorizer role to the newly created administrator so that dual authentication is not required when logging in:

   ```
   user role grant authorizer@DATAFORT_ADMIN username@DATAFORT_ADMIN
   ```

CLUSTER MANAGEMENT

The following commands are useful when managing clusters.

`cluster status`	Shows the status of a DataFort appliance 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`	Configures the cluster.
`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. Pressing **`Ctrl-d`** on the keyboard 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 DMC 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 appliance to be removed by name or IP address. To allow the member back into the cluster, execute the **`cluster enable <member-ip or name>`** command from another cluster member.

System Properties and Log Management

Use the CLI to view system logs, search for messages, and to aid in Verifying System Logs.

`system property get`

View the current values of system properties, and see permissions for the administrator currently logged in.

To view the current values of system properties in a detailed view that shows permissions for the administrator logged in, and lists all the administrator roles that are permitted to change (set) those properties, use:

```
system property get -d
```

Output is of the form: `security-admin RW global sys.security.web.usesmartcard: 0`

This output means that Security Administrators and up are able to modify the property, in this case Secure DMC. Only a Full Administrator is above a Security Administrator. RW indicates that the administrator logged in has read and write permission, R- indicates read-only permission. A lower-case w indicates that the property can be changed from the DMC only. The output (after the colon) shows the current value of the property. In this case 0 indicates that Secure DMC is off.

`system selftest`

Performs a series of tests on the appliance and configured servers.

`system utility lcdmessages`

Displays text of any warnings currently on the appliance LCD.

`system version`

Displays current system version, including Platform Serial Number, Platform Firmware Version, Platform Firmware Build ID, database version, HBA firmware information, SEP information and System Card information.

`system reboot`

Reboots the appliance. Adding the `-p` flag to `system reboot` power-cycles the box. This is necessary after upgrades.

`system log list`

Lists system logs in the database. Various filtering options are available, for example:

Search for messages of priority 1 and type SEC:

```
system log list -p 1 -t SEC
```

Search for messages starting from 2002/1/17 1pm to 2pm (the interval `i` is in seconds):

```
system log list -b '2002-01-17 13:00:00' -i 3600
```

To search for messages of the last 24 hours:

```
system log list -b now -i -86400
```

To search for the last 10 messages:

```
system log list -o -10
```

VERIFYING SYSTEM LOGS

1. To verify a signed log message, use:

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

   The **<mesg>** parameter is a log message to be verified in the form **"mesg-text [meta-data signature]"**

2. Single quotes, double quotes, and backslashes in the message must be preceded with a backslash. The entire message must be surrounded by double quotes. For example, to verify the following log message, run 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]"
   ```

Another example of this command is:

```
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: The Signed Log Authentication script is provided on the appliance user CD.

Stack Trace Settings

The appliance can dump a trace of the platform execution stack in the event of a kernel panic. This stack trace information is useful for debugging, but may expose appliance state information. This information does not pose a security risk or leaks any user or critical data, as no function arguments are leaked in the trace. The administrator should determine whether or not stack trace dumps should be enabled. To change the stack trace setting, log into the CLI and run the appropriate 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 clear 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 LKM or another designated site. Enter `db export ?` to see the options, and see the *LKM Appliance Administration Guide* for more information. Using the interactive backup mode (`db export -u`) requires that a user name and password be entered.

Changing Appliance Network Port Settings

By default, the media type is set to auto negotiate on all appliance Ethernet network interfaces. Valid settings are defined in Table 25.

Table 25: Valid Media Type Values

Interface	Valid Values
net.[interface].media	1000baseTX
	100baseTX
	auto (default setting)
net.[interface].mediaopt	half-duplex
	full-duplex

Note: 1000baseTX half-duplex is not a valid configuration. The appliance automatically changes it to full-duplex in this case.

Use the DataFort CLI to modify network port settings. Valid interface types are:

`client`	Client-side network interface of DataFort appliance
`server`	Server-side network interface of DataFort appliance

Note: The following changes should only be performed during a scheduled maintenance window as they could temporarily affect cluster stability.

Setting the Media Type

To change the media type of the DataFort client and server network interfaces:

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

```
system property set net.client.media [value]
system property set net.client.mediaopt [value]
system property set net.server.media [value]
system property set net.server.mediaopt [value]
```

2. Apply the settings by running the following command:

```
net apply
```

Enabling Jumbo Frame Support

The DataFort appliance uses the default Ethernet MTU size of 1500 bytes. If the environment supports jumbo frames the MTU size can be increased to a maximum of 8998 bytes.

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

```
system property set net.client.mtu <value>
system property set net.server.mtu <value>
```

2. Apply the settings by running the following command:

```
net apply
```

CLI Management for NFS Cryptainers

Prepare to create Cryptainers:

- From the operating system used to administer NFS, create exports on network servers, and set permissions. See Create NFS Exports on page 101
- Use the Management Security screen of the DMC to modify the management settings and group review settings of the DataFort appliance. See Setting Security Options on page 177.

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, run the CLI command **`domain ?`**.

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 entering the access user name and password, the DataFort appliance creates the root user account automatically.

The DataFort appliance 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 is authenticated with the server's passwd file or NIS domain using the request's UID and GIDs. Keep the server's set of users synchronized with that on the DataFort appliance, either by using the same NIS domain as a source of user information, or by manually synchronizing the local NFS domain on the DataFort appliance with the list of users set on the server.

Note: DataFort supports multiple NIS and local domains which can have overlapping UID/GID ranges. To avoid confusion, a virtual IP address in a specific NFS domain should host 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 46):

```
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 the DataFort appliance auto-discovers 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 by running the following CLI command:

```
system property user.domain.sync.no_autodiscover 1
```

Using the feature in domains that span many sites can limit network traffic to nearby sites and reduce network congestion. 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, run the CLI command `server ?`.

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, run the CLI command `server set ?`.

  ```
  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 that can be changed, run the CLI command `vip set ?`.

MANAGE SHARES

Add shares located on the servers that have been added. These shares 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, run the CLI command `share ?`.

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, run the CLI command `cryptainer ?`.

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 249.

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.

Run the CLI command **`cryptainer add ?`** for a list of options to specify when creating the Cryptainer. 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 creates 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 allows managing the access control for the share using the DataFort appliance, but does not require that the data in the share be encrypted. This can be useful if the following scenarios apply in the environment:

- The administrator only wants to strengthen the ACL on a share, not encrypt its contents.
- The administrator does not want to encrypt data that existed before the DataFort appliance 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 the DataFort appliance is configured for Secure CLI (see Appliance Settings on page 179) users cannot 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.

   ```
   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

- 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 run the following CLI command:

```
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. Submount outside a Cryptainer, at the Cryptainer level, or within a Cryptainer. It is not possible to submount inside a Cryptainer using filename encryption. The client sees “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 Management Security screen of the DMC and make the desired change. See Domain Controller Related Settings on page 179 for instructions.

When Group Review is enabled, the administrator can review changes using the following CLI commands:

- To view users that have been added to groups since Group Review was enabled, 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 enabled, 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
  ```

If SNMP is configured and Group Review is enabled, the appliance also sends an SNMP trap that a new user is imported into the user list via their group membership.

CLI Management for Multi-Protocol Cryptainers

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 Appliance Properties

1. Set the nofilecaching property on the DataFort appliance 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 (It is not allowed to 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 entering the access user name and password, the DataFort appliance creates 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

The DataFort appliance 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 appliance 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, provide the missing domain. For example, if a server was added as a CIFS server, but now should allow access to NFS shares on it also:

```
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 that can be changed, run the CLI command `vip set ?`.

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, provide the appropriate new name. For example, to change a CIFS share to be a multi-protocol share:

```
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 249 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 is disabled, the ACL is 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 appliance CIFS management is done using the DMC. 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 used to administer CIFS, add a special user for DataFort domain access to the Windows or LDAP domains in which the DataFort appliance will be used. See Adding the DataFort Domain Access User on page 46. Use the Management Security screen page of the DMC to modify the management settings and group review settings of the DataFort appliance. See Setting Security Options on page 177.
- 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 the DataFort appliance is 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 that can be changed, run the CLI command **`vip set ?`**.

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

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 has ownership.

  ```
  cryptainer add \\server3\cifsshare3
  ```

  Note: Cryptainer ACL must be set using Windows mapping functionality at the share itself. The Cryptainer has the same ACL settings as the share.

Set the DCS Requirement on a Cryptainer

- 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 appliance iSCSI management is done using the DMC. 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
```

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 appliance that remembers the original Cryptainer. The DataFort appliance 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 appliance (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, the administrator must reset the ACL on the Cryptainer manually.

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, it is possible to read from and write to the primary volume, and read the backup.

It is possible to 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 a DataFort appliance 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 the DataFort appliance 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 disabled, or the file caches should be cleared after every data modification.

PORT FORWARDING

The DataFort appliance supports port forwarding for use in configurations where the server subnet and client subnet have no connection other than through the DataFort appliance. 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, IS PLAINTEXT.

By enabling port forwarding, the administrator can have the DataFort appliance 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 the DataFort appliance. Similar rules must be set on each client that uses IPsec to communicate with the DataFort appliance. See Configuring IPsec on page 181 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 appliance from which IPsec commands are issued.

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
   ```

21 VLAN CONFIGURATION

Many network environments use virtual LAN (VLAN) functionality for improved network management. The following section describes introducing a DataFort appliance into a VLAN network environment and configuring it to communicate with clients and storage.

This guide describes a common VLAN network environment, but every VLAN network environment is different. The administrator should use these steps as a basis for understanding VLAN configuration and adjust the process accordingly for the environment.

Keep the following terms in mind when setting up a DataFort appliance for use with VLANs

VIP	Virtual IP address, used to virtualize file servers.
Client-side VIP	IP address of the virtual server presenting a Cryptainer on the DataFort Clients NIC.
Server-side VIP	IP address of the DataFort File Servers NIC used to talk to server.
Server IP	IP address of the file server storing the data.
Client IP	IP address of the client accessing the data.

Procedures described in this chapter include:

- Configuring the Switch Ports
- Configuring VLAN Data Access
- Restricting DataFort Admin Access to a Specific VLAN

CONFIGURING THE SWITCH PORTS

As described in Connecting the Rear Panel Ports on page 52, the DataFort E-Series appliance has two physical network interface cards (NICs) located on the rear panel. The Clients NIC is for traffic from clients to the appliance. This is referred to by the appliance operating system as bge0. The File Servers NIC is for traffic from the appliance to storage. This is referred to by the appliance operating system as bge1.

VLAN traffic is identified by labels inserted into network packets. This VLAN tagging functionality allows the DataFort appliance to distinguish and process VLAN traffic once it knows what VLANs are present in the network environment.

Configure the VLAN environment as follows:

- Configure the switch port connected to the Clients NIC to see VLAN traffic for all client VLANs that require access to storage through the DataFort appliance.
- Configure the switch port connected to the File Servers NIC to see VLAN traffic for all storage servers that will be accessed through the DataFort appliance.
- Configure the switch(es) to forward untagged packets. This is important for clustered DataFort appliances. They emit heartbeats in form of VRRP broadcasts in order to monitor other cluster member's health. These heartbeats do not have VLAN tags. If untagged packets are not forwarded, the cluster does not function properly.

CONFIGURING VLAN DATA ACCESS

1. Log in to the DataFort CLI.
2. Check that VLAN is enabled by running the following command:

   ```
   system property get nas.vlan.enabled
   ```

   Verify the system property is set to 1 to enable VLAN functionality. If not, run the following command:

   ```
   system property set nas.vlan.enabled 1
   ```

3. Add all client and server VLANs by running the following command for each VLAN:

   ```
   vlan add <vlan-id> <netmask>
   ```

4. When finished, verify all VLANs were added correctly:

   ```
   vlan list
   ```

   The command returns a list of current VLANs.

   ```
   ------------------------------------------------------------------
   |VLAN ID|Default Netmask|Virtual Interfaces (Clients/File Servers)|
   |-------|---------------|-----------------------------------------|
   |100    |255.255.248.0  |vlan0 / vlan1                            |
   |200    |255.255.248.0  |vlan2 / vlan3                            |
   ------------------------------------------------------------------
   ```

   To see all virtual interfaces:

   ```
   vif list
   ```

   The command returns a list of current interfaces, including VLAN interfaces.

   ```
   ------------------------------------------------------------------
   |Interface Name |Parent Interface Name |Default Netmask|Type      |
   |---------------|----------------------|---------------|----------|
   |bge0           |                      |255.255.0.0    |physical  |
   |bge1           |                      |255.255.0.0    |physical  |
   |vlan0          |bge0                  |255.255.0.0    |VLAN 100  |
   |vlan1          |bge1                  |255.255.0.0    |VLAN 100  |
   |vlan2          |bge0                  |255.255.0.0    |VLAN 200  |
   |vlan3          |bge1                  |255.255.0.0    |VLAN 200  |
   ------------------------------------------------------------------
   ```

5. Add the domain the file server is associated with to the DataFort appliance:

   ```
   domain add -u <username> -p <password> --server <server>
   <domain_name> <type> <subtype>
   ```

   Example: `domain add -u dcrusr -p password --server Server_1 Domain_1 CIFS Windows`

6. Add a unique client-side VIP for each client VLAN:

   vip add --cifs-domain <cifs-domain> --vlan <vlan> --ip <ip> <hostname>

   Example: **vip add --cifs-domain Domain_1 --vlan 200 --ip 10.10.10.10 virtualserver1**

   This creates a virtual server presenting the encrypted storage on the client side.

   Note: Keep in mind that depending on the environment, client and server may be in the same VLAN, different VLANs, or one in a VLAN and the other not.

7. Add a unique server-side VIP for each VLAN containing one or more file servers:

   vip serverside set --vlan <vlan-id> <new_vip> <netmask>

   Example: **vip serverside set --vlan 200 10.200.1.30 255.255.0.0**

   This creates a virtual IP on the DataFort File Servers NIC and enables communication with all file servers on that VLAN.

   - If there are multiple file servers on the same VLAN, one VIP for that VLAN is sufficient.
   - If there are multiple file servers on multiple VLANs, add a new VIP for each VLAN.

8. Add a file server to the DataFort appliance:

   server add --cifs-domain <cifs-domain> --vlan <vlan-id> --ip <server_ip><server_name>

   Example: **server add --cifs-domain Domain_1 --vlan 200 --ip 10.200.1.3 fileserver_1**

   Note: Use the –vlan option when adding a server in a VLAN. Otherwise virtualization will fail.

9. Add a share from an added file server:

   share add \\fileserver_1\share1

10. Virtualize the share on the previously-created virtual server to present it on the client side:

    share virtual add \\fileserver_1\share1 virtualserver1

11. Add a Cryptainer to the share:

    cryptainer add \\fileserver_1\share1\cryptainer1

12. Verify that the client can access the Cryptainer through the virtual server.

    For further information about Cryptainer management refer to Storage Administration on page 96.

RESTRICTING DATAFORT ADMIN ACCESS TO A SPECIFIC VLAN

This optional setting restricts access to the DataFort administrative interface to a specific VLAN.

> **CAUTION:** IF THIS PROCEDURE IS DONE INCORRECTLY, ACCESS TO THE DATAFORT ADMINISTRATIVE INTERFACE CAN BE LOST, REQUIRING ZEROIZATION OF THE APPLIANCE. DURING CONFIGURATION THE ADMINISTRATOR SHOULD BE ABLE TO ACCESS BOTH CLIENT AND FILE SERVER NICS OF THE APPLIANCE.

1. Log in to the DataFort CLI.
2. Check that VLAN is enabled by running the following command:

   ```
   system property get nas.vlan.enabled
   ```

   Verify the system property is set to 1 to enable VLAN functionality. If not, run the following command:

   ```
   system property set nas.vlan.enabled 1
   ```

3. View all current network interfaces:

   ```
   vif list
   ```

   The command returns a list of current interfaces.

   ```
   ------------------------------------------------------------
   |Interface Name|Parent Interface Name|Default Netmask|Type    |
   |--------------|---------------------|---------------|--------|
   |bge0          |                     |255.255.0.0    |physical|
   |bge1          |                     |255.255.0.0    |physical|
   ------------------------------------------------------------
   ```

4. View the physical interface that currently presents the administrative interface:

   ```
   system property get net.admin.interface
   ```

5. Add the VLAN:

   ```
   vlan add <vlan-id> <netmask>
   ```

6. View all current network interfaces:

   ```
   vif list
   ```

   The command returns a list of current interfaces, including VLAN interfaces.

   Adding the VLAN creates two new virtual interfaces, one on each physical interface for the new VLAN.

   Note the actual VLAN ID listed in the Type column as opposed to the DataFort internal virtual interface name in the first column.

```
-------------------------------------------------------------
|Interface Name|Parent Interface Name|Default Netmask|Type    |
|--------------|---------------------|---------------|--------|
|bge0          |                     |255.255.0.0    |physical|
|bge1          |                     |255.255.0.0    |physical|
|vlan0         |bge0                 |255.255.0.0    |VLAN 100|
|vlan1         |bge1                 |255.255.0.0    |VLAN 100|
-------------------------------------------------------------
```

7. Change the interface that the administrative interface is presented on from bge0 to vlan0 (the virtual interface on the Clients NIC that communicates over VLAN 100):

   ```
   system property set net.admin.interface vlan0
   ```

   Note: Be sure to use the DataFort internal virtual interface name, not the VLAN ID.

8. Apply the change by running the following command:

   ```
   net apply
   ```

   The DataFort Clients NIC (the administrative interface) can now be accessed from VLAN 100.

22 TROUBLESHOOTING

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

- Restoring an Appliance
- Front Panel LEDs
- Power Supply LEDs
- Network Connections and Management Interfaces
- CIFS Cryptainers
- NFS Cryptainers
- iSCSI CryptainersClusters
- Smart Cards
- Hardware

Restoring an Appliance

If a standalone appliance is lost, a saved configuration database from that appliance can be used to configure a replacement appliance. The recovered appliance is then able to retrieve data that was encrypted using the previous appliance. The Setup Wizard assigns a new appliance the configuration from a pre-existing appliance. The replacement appliance retains all parameters stored in the configuration database of the original appliance, including network, Cryptainer, access control and encryption key information.

If a cluster member is lost, it should not be restored using the wizard. It should be deleted from the cluster and replaced as described in Adding a Cluster Member on page 207. Use the wizard to restore the head of a cluster only if all members have been lost.

The procedure is conducted by a Full Administrator. The recovery procedure requires:

- A new or reset System Card.
- A new or zeroized appliance.
- The minimum set of Recovery Officers and Recovery Cards as determined by the recovery schema of the cluster.
- A saved database from the appliance that is to be restored.

1. Connect the new or zeroized appliance to the network and assign it the IP settings of the old appliance. See Assigning the Appliance IP Address on page 55.
2. From the DMC appliance tree, right-click the appliance to restore and select Set up to start the wizard. See Initializing Appliances on page 58.
3. Click Start, then click Next.
4. Accept the certificate.
5. If prompted, accept the license agreement.
6. At the Recover from Database page, browse to the saved configuration database. This file, with the extension .XDF, was created previously when backing up the appliance configuration in the DMC by selecting **Utilities > Back up**. See Backing Up Configurations to a Remote Location on page 171.
7. Create a new administrator account (optional), then click Next.
8. Select the cluster size and recovery schema, then click Next.
9. Edit the network settings (optional), then click Next.
10. Edit the license information (optional), then click Next.
11. Enter DNS and certificate information (optional), then click Next.
12. Insert Recovery Cards from the original appliance configuration as prompted, then click Next. The appliance needs the minimum number of Recovery Cards required for recovery procedures as set in the original configuration.
13. Click Next to apply the settings.
14. Click Finish when the wizard is finished.

For more detailed information about wizard steps, see Initializing Appliances on page 58.

Front Panel LEDs

Depending on the type of chassis, the appliance front panel features one or two bicolored LEDs that signal the status of the appliance, as summarized in the tables below.

Table 26: Front Panel Dual LEDs - 2U

LED Name	Position	Color	Behavior	Indication
Status LED	Top	Green	Solid	Appliance on network, no errors
		Red	Solid	Error Alarm: appliance not functional. Check LCD for messages.
Network LED	Bottom	Green	Solid	Network link
		Red	Solid	Network error

Table 27: Front Panel LEDs - 1U

Color	Behavior	Indication
Green	Solid	Appliance on network, no errors, no traffic
Green	Blinking	Appliance on network, no errors, with traffic
Red	Solid	Network error, no traffic
Red	Blinking	Error found, with traffic

Power Supply LEDs

The power supply module on the 2U model appliance provides a single external bicolor LED to indicate the status of the power supply. When AC is applied to the power supply unit and standby voltages are available, the LED blinks green. The LED is solid green to indicate that all the power outputs are available. It is solid amber to indicate that the power supply has failed, there is a shutdown due to over-current, over-temperature, or the unit is likely to fail.

Table 28: Power Supply LEDs

Power Supply Condition	Power Supply LED
No AC power to all power supply units	Off
No AC power to this power supply unit only	Amber
AC present / only standby outputs ON	Blink green
Power supply DC outputs ON and OK	Green
Power supply failure (includes voltage and/or temperature exceeded)	Amber
VRM (voltage regulator module) failure, cage related	Blink green
240VA limit (cage related)	Blink green
Current limit	Amber

Network Connections and Management Interfaces

Table 29 contains troubleshooting tips for the network and management connections to the appliance.

Table 29: 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 appliance. Check the LCD on the front panel for messages. • The appliance must have an IP address assigned. See Assigning the Appliance IP Address.
Power not on	• On 2U appliance: The Power LED is solid green after the power switch is turned on. If the LED is not lit, the power source may be bad. Check both power cables, and if necessary, plug the power cables into another power source. • On 1U appliance: Check power cable, and if necessary, plug the cable into another power source. • If the front panel LED is not lit, use the power switch to power the appliance on.
There is no output on serial console	• Console should be set to: Speed 9600, Data bits 8, Stop bits 1, Parity None, Hardware or no Flow Control. Check settings on the terminal program. • Verify 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. Verify the cable is connected to the port marked **IOIOI** on the appliance.
Cannot log in via serial connection	• Verify that the login username and password are correct. • Try logging in again using the defaults: User: **user**, Password: **MTKNMTKN**.
Cannot connect to IP address	• Check that IP settings were set and saved after initialization. See Assigning the Appliance IP Address. • Verify the Management Station can reach the appliance IP address on the network.
Cannot connect to domain name of appliance	• The appliance's domain name must be added to the domain by the administrator, and the name must be resolvable by DNS. If not, use the IP address instead.
Cannot clear alert after using CryptoShred button	• The CryptoShred button must be in a normal state to allow operations to be restored. See CryptoShred Button States.
LCD states Intrusion Detected	• Intrusion detection occurs when the chassis of the appliance is opened. Log in to the DMC and reset the tamper detection alert. See Clearing a Defense Alert.
LCD prompts for System, Card or Status LED is red on 2U appliance	• A System Card must be inserted before the appliance is powered on. Once it is powered on, the System Card can be removed. Messages appear about this condition. • For an appliance that has not been configured, power the appliance off, and re-insert the System Card before powering the appliance back on. Verify the System Card is inserted all the way into the front panel slot, with gold contacts facing up and to the back. • A configured appliance may have a security setting in place that halts operations if the appliance is rebooted without a System Card. See Managing Appliance Defense Responses.

TABLE 29: NETWORK CONNECTIONS AND MANAGEMENT INTERFACES (CONTINUED)

Problem	Possible Cause and Solution
Cannot log in to DataFort appliance	• By default, to access the appliance via DMC the Management Station must have access to the Clients NIC. (Note that the administrator can configure the DataFort appliance to be manageable from either NIC.) Ensure the appliance and the Management Station are on the same subnet. • The network switch port connected to the appliance should be set to auto-negotiate. • Verify any firewall for the Management Station is disabled, and that web traffic is not going through a proxy. • In Add/Remove Programs verify the following programs are installed: Decru Management Console, Gemplus Smart Card Reader Tools. • If Secure DMC is enabled, a valid administrator and Admin Card are required to log in. • If Secure DMC is enabled, Terminal Services and Remote Desktop cannot access the DMC. • Some administrators may require login authorization by another administrator. If dual authentication is required for the administrator attempting to log in, an authenticating administrator must log in first. See Requiring Authorization for Login.
Need to clear the saved entries from an incomplete wizard	• Zeroize the appliance. • Delete the setup file from the Management Station. The default location for the file is C:\Program Files\Decru\Decru Management Console\components\setup\prefs. • Run the wizard again.
Cannot log in to appliance CLI	• Verify that the login username and password are correct. • Try logging in again using the defaults: User: **`user`**, Password: **`MTKNMTKN`**. • Check that Secure CLI is disabled.
Login information for sole administrator lost	• Log in using a Recovery Card, and zeroize the appliance. See Emergency Serial Console Port Access.
Need to disable DMC smart card requirement (Secure DMC) via CLI	• If the administrator is unable to access the DMC in order to disable the smart card requirement, this can be done via CLI: • Log in to the CLI and run the command **`system property get sys.security.web.usesmartcard`** to check the setting. A setting of **`1`** requires the Admin Card in order to log in to the DMC; **`0`** disables the requirement. If necessary, run the command **`system property set sys.security.web.usesmartcard 0`** to disable the smart card requirement. A Security or Full Administrator can set this property.
CLI sessions take a long time to establish	• This can occur if the DNS servers are unavailable. Log in through the DMC and change the DNS servers, or wait for the CLI session to establish and then change the DNS servers from the CLI.

CIFS Cryptainers

Table 30 contains troubleshooting tips for CIFS Cryptainers.

Table 30: CIFS Cryptainers

Problem	Possible Cause and Solution
Users are not imported (user registration fails, or user not found when trying to grant access)	• Verify the DataFort domain access user is in the domain. • Note that users are only imported into the DataFort 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 the DataFort appliance (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 the DataFort appliance, an error occurs and users may not appear. Check the time settings. • Configure an NTP server for the DataFort appliance, or reset the time on the DataFort appliance.
	• The DataFort appliance syncs with domain user information. Verify that the domain name is correct and the correct domain controller is specified for the domain.
	• Right-click the domain in the Servers and Portals tab of the DMC and select Validate Domain to test access to the domain.
	• If Group Review is enabled, users do not appear until the administrator reviews and accepts the users.
New CIFS domains cannot be added and existing CIFS domains fail to authenticate	• If there is a time mismatch between the domain controller and the DataFort appliance this can occur. • Configure both the DataFort appliance and domain controller with an NTP server.
Cannot add a CIFS server	• Verify the server is running. Right-click the server in the Servers and Portals tab of the DMC 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 appliance powers up, the DataFort appliance may not be able to add Cryptainers to it. Power servers up before the DataFort appliance. • If the DataFort domain access user is not configured properly, the DataFort appliance is unable to communicate with the server.

TABLE 30: CIFS CRYPTAINERS (CONTINUED)

Problem	Possible Cause and Solution
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 selected share may already contain a .decru file from a previous Cryptainer. Never use the same share for more than one Cryptainer. • Right-click the domain in the Servers and Portals tab of the DMC and select Validate Domain. • Check the share permissions (not just the folder permissions) on the share. • Verify the server is properly configured for sharing.
Cryptainer does not 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 cannot access CIFS Cryptainers	• If the Use Local ACL setting is enabled, the ACL on the DataFort appliance is enforced and there is no unauthorized Cryptainer access through the DataFort appliance. • 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 disabled recently. Users who were connected to a share immediately before User Registration was disabled 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 the client machine and then logging back in. If that does not work, reboot the client machine.
	• Verify mapping is not done 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 the DataFort appliance. • If the DataFort appliance just rebooted, it takes a while for the user and group membership listings to be generated. Wait 30 minutes and try again.
	• Check if the user remained connected to the DataFort appliance while the user was removed from the DataFort configuration (and perhaps added back). In this case, the user may lose access to some Cryptainers through this connection. The user should disconnect from the DataFort appliance, 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, the DataFort appliance cannot perform these operations. The DataFort appliance only supports TCP over UDP.
Cannot create Cryptainer from FAT/FAT32 volume	• FAT/FAT32 volumes are not supported by the DataFort appliance. 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 when such an attempt is made. • Check Group Review settings.

TABLE 30: CIFS CRYPTAINERS (CONTINUED)

Problem	Possible Cause and Solution
Cannot access Cryptainer or share	• The file server may not be running, or may not be sharing correctly. Check the file server to see if it is running correctly and sharing the expected volumes. • The DataFort appliance may have detected an intrusion. Reset intrusion to enable encryption/decryption.
Samba servers do not work in cluster	• When adding a Samba server to a DataFort appliance cluster, the NetBIOS field is required.
Unable to contact domain controller or Unknown RPC failure for Windows Active Directory domain controller	• Ensure that NetBIOS is enabled on the Active Directory Domain Controller. • The DataFort appliance requires NetBIOS / port 139 to be enabled on the Active Directory Domain Controller for SMB / CIFS functionality.
Get filename denied message when attempting to access file through the DataFort appliance	• If a file is written directly to the server or storage system, and not through the DataFort appliance, this message is expected. • Access the file directly on the CIFS server or appliance, and copy or move it to a cleartext location. • Copy the file through the DataFort VIP into the Cryptainer storage vault. This allows accessing the file through the DataFort appliance without error.

Kerberos authentication issues	• The root cause for Kerberos authentication issues is usually misconfigured DNS. While the symptoms may point to a permissions problem, it is strongly recommended to check DNS settings first.
	• Verify that all participating nodes (host, DataFort real and virtual hostnames/IPs, storage, domain controller, etc.) are fully resolvable both ways (name to IP address and vice versa):
	• Log in to the DataFort CLI and run the following commands to confirm:
	`net util host <hostname>`
	`net util host <IP address>`

	• Kerberos problems can be caused by the use of non unicode characters in the username / password fields. Some special characters (letters, and punctuation marks) are not unicode characters.
Cannot join DataFort virtual IP to Windows 2003 Active Directory server.	• If the domain controller has LDAP server signing requirement enabled, log in to the DataFort CLI and run the following command to change the LDAP authentication mode from 0 (GSSAPI, default) to 1 (GSS-SPNEGO): `system property set nas.ldap.authentication.mode 1`

NFS Cryptainers

Table 31 contains troubleshooting tips for NFS Cryptainers.

Table 31: NFS Cryptainers

Problem	Possible Cause and Solution
Unix group memberships are not imported	• If Group Review is enabled, newly imported groups must be confirmed before memberships can be imported.
Cannot create NFS Cryptainer	• The DataFort appliance does not create parent directories. • Check permissions on server and directories. • Verify 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 enabled by default. If the administrator is trying to create a Cryptainer with the root as owner, it fails if the NFS server has rootsquash enabled. Disable rootsquash on the server in order to create a Cryptainer with root as its owner. • When creating a new Cryptainer, verify 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 it cannot be mounted directly, the DataFort appliance cannot mount it either. • Check permissions on the server. • Right-click the server in the Servers and Portals tab of the DMC and select Ping to test access to the server. • If the server can be mounted, 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 mounting the share, try following the Cryptainer path for the failed Cryptainer creation operation. Using the Cryptainer owner as the login, try creating a directory under the Cryptainer path. If this fails, then the DataFort appliance cannot create the Cryptainer directory. Find the cause of this directly on the server and try again from the DataFort appliance. • When creating a new Cryptainer, verify 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 enabled, the user may be awaiting confirmation. To view all users that have access to Cryptainers, run the CLI command `user group list --uflags normal`.
User cannot mount a share from the DataFort appliance	• Make sure a user with UID 0 exists in the DataFort appliance. Typically, client machines use UID 0 when they mount a share, and the DataFort appliance only allows this operation if the user is known to the DataFort appliance.

TABLE 31: 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, the DataFort appliance does 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 system 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 does not work directly, there is a problem with the configuration that is unrelated to the DataFort appliance. If the operation works directly, then look at ACLs on the DataFort appliance and verify the user that is attempting the operation has the necessary permissions. To view the ACL on a Cryptainer, right-click it in the Servers and Portals tab of the DMC and select 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 is 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 the DataFort appliance by running the following CLI commands: • `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 do not see these errors if they did not have access to the share before Cryptainer creation.

iSCSI Cryptainers

Table 32 contains troubleshooting tips for iSCSI Cryptainers.

Table 32: iSCSI Cryptainers

Problem	Possible Cause and Solution
No targets displayed in DMC 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 33 contains troubleshooting tips for DataFort appliance clusters.

TABLE 33: CLUSTERS

Problem	Possible Cause and Solution
Giveback does not work properly	• Select **Configuration > View Cluster Failover** in the DMC. If the clustered DataFort appliances seem to be working, but one of them is serving all VRIDs, try clicking Manual Recover. If this does not work, verify the File Servers NIC cable is plugged in. If it is unplugged, the DataFort appliance does not serve any VRIDs. • In the DMC, select **Configuration > View Cluster Failover** for the DataFort that is not servicing servers and click Manual Recover.
Cluster does not form	• The DataFort cluster license may have expired. Obtain a valid license for each DataFort appliance 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.
Cannot change server-side IP of clustered DataFort appliance	• If the cluster state is not committed/online and the administrator tries to change the server side IP, an error message appears. 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 appliance is permanently offline, it should be replaced. Follow the instructions in Setting Cluster Properties With the CLI. • If the DataFort appliance 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 appliance 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 34 contains troubleshooting tips for working with smart cards.

TABLE 34: SMART CARDS

Problem	Possible Cause and Solution
Management Station does not detect Admin Card	• The Decru software installer places the necessary files on the Management Station. Reinstall the smart card reader software if necessary. • The Management Station must be running Windows 2000, Windows Server 2003 or Windows XP.
	• Verify the Admin Card is properly inserted in the smart card reader. Re-insert the card if necessary. The reader LED should flash and then light continuously.
Need to reset System Card	• The appliance needs a new or reset System Card in order to complete the setup wizard. If the System Card was not inserted into the appliance chassis during zeroization or if it was not properly reset during zeroization, manually reset it. See Resetting Smart Cards.
Lost System Card	• Zeroize, insert a new System Card and run the Setup Wizard.
DMC does not recognize type of card inserted into Management Station smart card reader	• The reader may identify the type of smart card incorrectly. Pull out and re-insert the card. Wait a few seconds for the card reader to detect card insertion (indicated by the status light turning green) before clicking OK. • Disconnect and re-connect the smart card reader.
Lost Admin Card with Secure DMC enabled	• Log in with a different Admin Card and associate a replacement Admin Card with an existing or new administrator. • If all Admin Cards are lost and Secure CLI is not enabled, log in to the CLI and disable Secure DMC by running the CLI command **`system property set sys.security.web.usesmartcard 0`**. Then log in to the DMC and associate a replacement Admin Card with an existing or new administrator. A Security Administrator or Full Administrator can change the system property. A Full Administrator is required to create or change associations with an Admin Card. • If both CLI and DMC login are smart card enabled and all Admin Cards are lost, zeroize the appliance using the serial console.
Problem with multiple smart card readers	• Multiple card readers are not supported for Cluster Recovery operations. Multiple card readers are only supported at the time of cluster formation.
Lost Recovery Card	• Assemble a quorum of Recovery Officers and replace the Recovery Card.
Wrong System Card found error appears on LCD or in logs.	• Appliance software versions require specific smart card versions. A complete compatibility matrix is available from Decru. The version of the smart card is indicated by a sticker on the back of each smart card, for example V147. Check the card version using the following steps: • CLI: Run the command: system version • DMC: Insert the System Card into the smart card reader, then select **Security > Smart Card Utilities**. Check the Smart Card Version field.
Smart card errors appear	• Use an eraser to clean the metal contact on the smart card.

HARDWARE

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

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

APPENDIX I COMMAND LINE INTERFACE QUICK REFERENCE

The CLI gives the administrator access to many DataFort management functions, but cannot be used for functions that require the presence of smart cards. The DMC is the only interface that allows management of smart card enabled operations. This chapter includes the following topics:

- Using the CLI
- CLI Command Overview

Refer to the separate *DataFort CLI Reference Guide* for a complete list of commands and parameters.

USING THE CLI

Some CLI commands must be executed in a specific order for desired results. For 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 Command Line Interface on page 80. There are two levels of security that can be set for DataFort CLI login, one of which requires first accessing the DMC before logging into the CLI.
- As a security measure, the CLI times out after 10 minutes of inactivity.

CLI SYNTAX

- In the following pages, an ellipsis (**...**) after an entry indicates that the entry is a hierarchy, rather than a command. The top level commands include **system...** because there is no end command **system** although there is a system hierarchy of commands (**system reboot**, etc.).
- The plus (**+**) symbol indicates that an entry is a command which can take arguments. The command **quit** is not followed by **+** because it does not take arguments.
- Note that **+** and **...** are not intended to be typed in as commands, but serve as indications that more can be typed after a given entry.

CLI HELP

Note: The DMC CLI does not have the same help features as the full CLI. Type **help** to use help in the DMC CLI.

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

CLI Command Overview

Top Level Commands

Type **help** to view top level commands.

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
server...	Server commands...

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 LOGGING FUNCTIONS

The appliance audit function logs security-relevant operations, errors, and warnings as well as many operations, errors and warnings that are not relevant to security.

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

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

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

See Configuring and Viewing Logs on page 189 for information about configuring and viewing logs.

Appliance Log Event and Priority Types

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

Table 35: Log types

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

Log message parameters

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

Table 36: Parameters in log messages

Parameter	Description
<action>	Action taken in response to event, may be: DISABLE_SEP: The SEP was disabled as a result of the event. ZEROIZE_SEP: The SEP was zeroized as a result of the event.
<admin>	This parameter indicates an appliance administrator.
<client>	IFC: The 8 byte WWN of the host requesting the information flow, formatted as 8 hex character bytes: XX:XX:XX:XX:XX:XX:XX:XX
	Audit: IP address from which the user is authenticating
<cryptainer>	The 16 byte ID of the Cryptainer from which the information flow is requested:0xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
<cryptainer_group>	This parameter indicates a group of Cryptainers, as defined by the appliance administrator. The parameter is a text string, up to 31 characters.
<domain>	Domain name of the user that changed the configuration parameter
<host>	This parameter refers to a host, by WWN.

TABLE 36: PARAMETERS IN LOG MESSAGES (CONTINUED)

<host_group>	This parameter indicates a group of hosts, as defined by the appliance administrator. The parameter is a text string, up to 31 characters.
<interface>	Interface to which the user is attempting to authenticate, may be: • CLI—The user is authenticating to the CLI interface. Note that this interface is disabled in the CC evaluated configuration. • DMC—The user is authenticating to the DMC interface. Note that administrators may use the DMC CLI interface after authenticating to the DMC interface. • SERIAL—The user is authenticating to the appliance MenuShell interface.
<pool>	Tape pool.
<pool_group>	Group of tape pools, as defined by the appliance administrator. The parameter is a text string, up to 31 characters.
<prop_name>	Name of a logging facility configuration property.
<reason>	The reason parameter indicates the rule that caused access denial. • port locking rule—the host is not connected via the required port number • authentication rule—the host is not authenticated • authorized flow rule— the host is requesting an unauthorized information flow Reason for authentication failure, may be: • USERPASS—The user entered an incorrect password. • SMARTCARD—The user attempted to authenticate using the wrong smart card.
<serial_number>	Serial number of the appliance that denied or allowed the information flow.
<user>	Name of user that changed a configuration parameter or attempted to authenticate.
<usertype>	ADMIN or USER
<user_target>	This parameter is used for log messages indicating a modification of a user account. In these log messages, <user> is the user that performed the action, while <user_target> is the user that was modified.
<user_domain>	This parameter is used for log messages indicating a modification of a user account. In these log messages, <domain> is the domain of the user that performed the action, while <domain_target> is the domain of the user that was modified.
<wwn>	The 8 byte WWN of the host that is authenticating (DHA), formatted as 8 hex character bytes: XX:XX:XX:XX:XX:XX:XX:XX

LOG STORAGE LOCATIONS

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

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

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

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

TABLE 37: DEFAULT LOG STORAGE LOCATIONS

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

LOG PRESENTATION

- Temporary Logs
- Database Logs
- Remote Logs

TEMPORARY LOGS

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

`/var/log/security`

`/var/log/operations`

`/var/log/performance`

`/var/log/audit`

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

All log messages include:

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

DATABASE LOGS

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

- Viewing database logs via DMC
- Viewing database logs via CLI

Viewing database logs via DMC

The administrator may view log messages stored in the database by selecting **Diagnostics > View System Log** in the DMC. See Configuring and Viewing Logs on page 189 for more information.

All log messages include:

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

Viewing database logs via CLI

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

Log messages are listed in the following format:

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

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

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

<CAT> represents the log containing the message as follows:

- <16.[4,3,2,1,0]>: High priority Security Log
- <16.[7,6]>: Low priority Security Log
- <17.[1,0]>: Operations Alert Log
- <17.4>: Operations Warning Log
- <17.6>: Operations Informational Log
- <17.7>: Operations Debug Log
- <18.[4,3,2,1,0]> High priority Performance Log
- <18.6> Low priority Performance log
- <19.[4,3,2,1,0]> High priority Security Log.
- <19.6> Low priority security log.
- <20.6> Audit Log

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

<MESG> is the log message.

Remote Logs

The formatting for exported log messages corresponds to the syslog protocol as specified in the syslog RFC. Exported log message are listed in the following format:

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

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

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

<MESG> is the log message.

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

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

TABLE 38: APPLIANCE EVENT AND PRIORITY CORRESPONDENCE TO SYSLOG FACILITY AND SEVERITY

Appliance Log	Syslog facility	Syslog priority
High priority Security Log	LOG_LOCAL0 (16)	4,3,2,1,0
Low priority Security Log	LOG_LOCAL0 (16)	6
Operations Alert Log	LOG_LOCAL1 (17)	1,0
Operations Warning Log	LOG_LOCAL1 (17)	4
Operations Informational Log	LOG_LOCAL1 (17)	6
Operations Debug Log	LOG_LOCAL1 (17)	7
High priority performance log	LOG_LOCAL2 (18)	4,3,2,1,0
Low priority performance log	LOG_LOCAL2 (18)	6

Signed Logs

The appliance can be configured to sign log messages. See Configuring and Viewing Logs on page 189 for more information. The configuration option is available separately for each appliance log. If configured, metadata and signature fields are appended to the exported log message:

```
<PRI> <TIME> ' ' <MESG> '[' <MDATA> ' ' <SIG> ' ']
```

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

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

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

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

```
<MESG> ' [' <MDATA>
```

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

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

LOG PURGING

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

- Temporary storage log messages
- Database storage log messages

Temporary storage log messages

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

TABLE 39: SPACE ALLOWANCES FOR TEMPORARILY STORED APPLIANCE LOG MESSAGE

Appliance log	Meaning	Max size
High priority Security Log Low priority Security Log	Combined size of high / low priority security logs	100kB
Operations Alert Log Operations Warning Log Operations Informational Log Operations Debug Log	Combined size of all operations logs	1000kB
High priority Performance Log Low priority Performance Log	Combined size of both performance logs	500kB

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

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

A 10 second timer triggers checks for the previous conditions.

Database storage log messages

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

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

AUDIT CONFIGURATION

The appliance audit function may be configured using either the DMC or the CLI.

- DMC Audit Configuration
- CLI Audit Configuration

DMC Audit Configuration

DMC configuration of the audit function is performed using the DMC. See Configuring and Viewing Logs on page 189 for information.

CLI Audit Configuration

CLI configuration of the audit function is performed by setting the logging system properties. See CLI Administration on page 237 for more about using the CLI.

TABLE 40: AUDIT CONFIGURATION DATABASE PROPERTIES

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

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

TABLE 41: AUDIT FUNCTION CLI CONFIGURATION LIST PARAMETERS

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

TABLE 41: AUDIT FUNCTION CLI CONFIGURATION LIST PARAMETERS (CONTINUED)

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

APPENDIX III 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 the DataFort appliance 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 the antivirus system in the environment. See:

- Considerations Before Configuration
- Preparing the Environment
- Configuring DataFort for Virus Scanning
- Notes for Virus Scanning

Considerations Before Configuration

The following lists some considerations when implementing DataFort appliance support of virus scanning.

- Verify that DataFort Cryptainer Filename Encryption is disabled for Cryptainers that will be scanned for viruses. Virus scanning through the DataFort appliance is not supported when using Cryptainers with encrypted filenames.
- Verify that the administrator has 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) must be created on the DataFort appliance, pending the addition of each AV Scanner. This requires additional IP Addresses on the network.
- Verify that the proper security scheme is in place to administer the possible addition of AV Scanners on your network.
- Consult the NAS array and antivirus software documentation regarding the number of AV Scanners needed in the environment paired with the added resource congestion which may be added to the infrastructure due to these additions.
- If using EMC CAVA software paired with Trend Micro ServerProtect for EMC NAS, consult the EMC CAVA documentation for alternate EMC CAVA installation procedures.

PREPARING THE ENVIRONMENT

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 configuring the DataFort appliance to support virus scanning:

1. Prepare the NAS array (see the documentation for the appropriate type of array):
   - EMC Celerra: Verify 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 the DataFort appliance, 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 requires 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 appliance with hostname DataFort1.
- Two AV scanners with hostnames vscan1 and vscan2.

To configure virus scanning on files to be encrypted by the DataFort appliance complete these steps. This procedure only needs to be completed on one DataFort appliance in a cluster.

1. Log in to the DataFort CLI.
2. Add the AV scanner(s) to the DataFort appliance as a server (in the same domain as the server and DataFort VIP) with the command. If setting up multiple AV Servers, 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 used to route virus scanning traffic to the DataFort appliance. 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 enable that connection.

Two IP addresses must added for each AV scanner that will be used with the DataFort appliance. If setting up multiple AV Servers, 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 setting up multiple AV Servers, 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 the DataFort appliance:

   ```
   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 the DataFort appliance:

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, run the following command:

   ```
   server_file DataMover –put viruschecker.conf viruschecker.conf
   server_viruschk DataMover –update
   ```

6. In CAVA CLI, run the following command:

   ```
   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 the DataFort appliance does not detect a virus file, reboot the AV Scanner.

NetApp VScan

To register the AV scanner with the DataFort appliance:

1. Start the Virus Scanning software (for example: Symantec, McAfee, 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 is done through the DataFort appliance. There are two options for scanning files that are written directly to the NAS array (with data not encrypted by the DataFort appliance):

- For each share that will be accessed directly, create a cleartext Cryptainer on the DataFort appliance 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 deleting a Cryptainer that had an associated **`vscan`** share and then later adding the Cryptainer back, the administrator must manually delete the **`vscan`** share and add it back.

Troubleshooting

Errors may appear 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 the DataFort appliance) 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 IV PORT IDS

The DataFort E-Series appliance uses the following network ports and protocols. Verify that communication on these ports is not blocked in the network environment by firewalls or other filtering mechanisms.

TABLE 1: PORT IDS

Port ID	Transport	Protocol	Appliance Interface	Communication Interface	Communicates over VIP	Programmable Port ID
21	TCP	FTP	For data access over FTP	Mgmt/Client	yes	no
22	TCP	SSH	Secure Shell	Mgmt/Client	no	no
53	UDP	DNS	DNS network client	Mgmt/Client	no	no
69	UDP	TFTP	TFTP traffic	Mgmt/Client, Storage	yes	no
80	TCP	HTTP	For data access over HTTP (not the DMC)	Mgmt/Client	yes	yes See Note
111	TCP	RPC	NFS port lookup	Mgmt/Client, Storage	yes	no
123	UDP	NTP	NTP network client	Mgmt/Client	no	no
139	TCP	netbios-ssn	CIFS traffic	Mgmt/Client, Storage	yes	no
139	TCP	NTAPVS	Virus scanning support for NetApp	Storage, Mgmt/Client	yes	no
161	UDP	SNMP	SNMP client	Mgmt/Client	no	no
443	TCP	HTTPS	DMC	Mgmt/Client	no	no
443	TCP	HTTPs	For data access over HTTPs (not the DMC)	Mgmt/Client	yes	yes See Note
445	TCP	microsoft-ds	CIFS traffic	Mgmt/Client, Storage	yes	no
464	TCP, UDP	kpasswd	For setting machine account password via Kerberos when joining domain	Mgmt/Client	no	no
500	UDP	ISAKMP	DataFort cluster isakmp interface, and NAS clients	Mgmt/Client	yes (for NAS clients)	no

TABLE 1: PORT IDS

514	UDP	Syslog	DataFort remote logging interface	Mgmt/Client	no	no
1023	TCP		NFS Proxy to talk to backend file server	Storage	yes	no
1176	TCP	EMC Cava	Virus scanning support for EMC Cava	Storage, Mgmt/ Client	yes	no
2049	TCP	NFS	NFS traffic	Mgmt/Client, Storage	yes	no
2049	UCP	NFS	NFS traffic	Mgmt/Client, Storage	yes	no
3260	TCP	iSCSI	Anything iSCSI	Mgmt/Client, Storage	yes	no
15360	TCP	IPsec	Cluster heartbeat	Mgmt/Client	no	no
15361	TCP	IPsec	Cluster heartbeat	Mgmt/Client	no	no
16000	TCP	DCS	DCS	Mgmt/Client	no	no
<1024	UDP		NIS client - ypbind, port varies	Mgmt/Client	yes	no
21, >1024	TCP	FTP	FTP network client	Mgmt/Client	no	no
N/A	ICMP	Ping	DataFort Ping Response	Mgmt/Client, Storage	yes	N/A
N/A	ARP	ARP	ARP network broadcast	Mgmt/Client	yes	N/A

A Communication Interface of “Mgmt/Client, Storage” means the appliance listens on the Mgmt/ Client interface, and talks on the Storage interface (but does not listen on it).

A Communication Interface of “Storage, Mgmt/Client” means the DataFort appliance listens on the Storage interface, and talks on the Mgmt/Client interface (but does not listen on it).

Note: Set using the CLI command **`system property set nas.http.port <port>`**

APPENDIX V SPECIFICATIONS

- Supported Systems lists support for components of the DataFort system.
- DataFort Appliance Specifications lists DataFort hardware specifications.

SUPPORTED SYSTEMS

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

TABLE 1: SUPPORTED PLATFORMS

Item	Component	Requirement
Management Station	System Requirements	2Ghz 1GB RAM 4GB free hard drive space An available USB port for the smart card reader from Decru (If no USB port is available, a serial smart card reader is available from Decru.) A CD drive for installing software Windows XP SP2 or Windows 2000 SP4 or Windows 2003 SP1
CIFS Protocol	Clients	Windows 2000 Windows Server 2003 Windows XP Windows NT 4.0 SP 6
	File Servers	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

DataFort Appliance Specifications

Table 2: DataFort Appliance Specifications

Item	Detail	Specification	
Hardware	Rack mountable	E515/FC525	Standard 19" EIA rack - 1U
		E510/FC520/ FC1020/S110	Standard 19" EIA rack - 2U
	Weight	E510	14.2 kg (31.3 lbs)
		E515	10.4 kg (22.9 lbs)
		FC520	12.8 kg (28.3 lbs)
		FC525	10.4 kg (22.9 lbs)
		FC1020	16.0 kg/35.3 lbs
		S110	13.7 kg/30.2 lbs
	Size	E515/FC525	43.2 cm W x 48.3 cm D x 4.4 cm H (17.00" W x 19" D x 1.73" H)
		E510/FC520/ FC1020/S110	43.2 cm W x 48.3 cm D x 8.9 cm H (17.00" W x 19" D x 3.5" H)
	Security	SEP FIPS Level 3 Physical Security, Tamper Evident Label, Intrusion Detection Circuit, Optional Chassis Lock, Optional CryptoShred button	
	Network Ports	E510/E515	2 Gigabit Ethernet (IEEE 802.3ab compliant) ports 10/100/1000Base-T, autonegotiation required
		FC520/FC525	1 dual-port HBA for storage network connectivity
		FC1020	5 dual-port HBAs for storage network connectivity
		S110	2 LVD SCSI (one host, one storage supporting daisy chaining)
	Management Ports	2 10/100/1000Base-T Ethernet ports (one used)	
	Serial Port	RJ45 serial console port	
	Power Supply	E510/FC520/ FC1020/S110	2 Redundant/Hot-Swappable/Universal Input 100-240V ~47-63 Hz, 5A
		E515/FC525	1 Cold-Swappable/Universal Input 100-240V ~47-63 Hz, 5A
	Fans	E510/FC520/ FC1020/S110	2 Hot-Swappable
		E515/FC525	1 Cold-Swappable
	LED	Power Status/Network Activity/ Fault Status	
	LCD	E510/FC520/ FC1020/S110	Liquid Crystal Display with touch screen
		E515/FC525	Liquid Crystal Display
	Smart Card	1 smart card reader	
Environment	Temperature	Operating Temperature: 5°C to 40°C (41°F-104°F) Storage Temperature: -10°C to 60°C (14°F-140°F)	
	Humidity	Operating Humidity: 85% RH at 40°C	

TABLE 2: DATAFORT APPLIANCE SPECIFICATIONS

Item	Detail	Specification
Regulatory Compliance	EMC	Canada ICES-003 Class A United States FCC Class A Japan VCCI Class A Korea RRL Class A European Community CE (EN55022 Class A, EN55024, EN61000-3-2 Class A, & EN61000-3-3) Australia/New Zealand AS/NZS 3548 Class A China CCC Taiwan BSMI International IEC 6095 0-1
	Safety	United States UL 60950 - 1 Canada CSA 60950 - 1 Japan IEC 60950 -1 European Community EN60950, TUV R 2845 China CCC International CB IEC 60950 -1

Appendix VI 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
AUSTRALIA	AU
AUSTRIA	AT
BELGIUM	BE
CANADA	CA
CHINA	CN
DENMARK	DK
FINLAND	FI
FRANCE	FR
GERMANY	DE
GREECE	GR
HONG KONG	HK
INDIA	IN
IRELAND	IE
ISRAEL	IL
ITALY	IT
JAPAN	JP
KOREA	KR

Country	Code
MEXICO	MX
NETHERLANDS	NL
NEW ZEALAND	NZ
NORWAY	NO
PANAMA	PA
PHILIPPINES	PH
POLAND	PL
PORTUGAL	PT
PUERTO RICO	PR
SINGAPORE	SG
SPAIN	ES
SWEDEN	SE
SWITZERLAND	CH
TAIWAN	TW
THAILAND	TH
UNITED KINGDOM	GB
UNITED STATES	US

APPENDIX VII REGULATORY AND CERTIFICATIONS

- FCC Declaration of Conformity
- European Union
- Canadian ICES-003
- VCCI Class A Statement
- CE Statement

FCC Declaration of Conformity

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

EUROPEAN UNION

Marking by the symbol CE indicates compliance of this Decru, A NetApp Company device to the EMC directives and the Low Voltage Directives of the European Union.

This is a class A product. In a domestic environment, this product may cause radio interference, in which case, the user may be required to take adequate remedial measures.

CANADIAN ICES-003

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

VCCI Class A Statement

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－ A

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

CE STATEMENT

The standards compliance label on the appliance contains the CE mark which indicates that this system conforms to the provisions of all European Council Directives, laws, and standards.

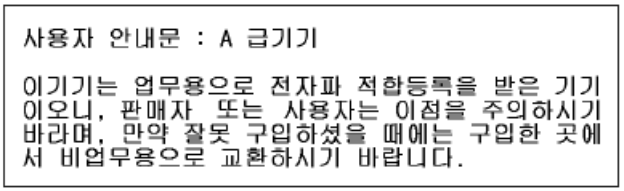
The appliance is in conformity with the provisions of the following EC Directives, including all amendments, and national legislation implementing these directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

The following harmonized standards have been applied:

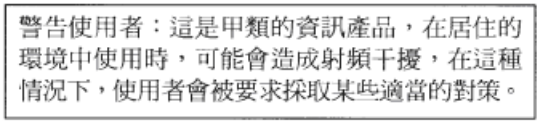
- EN55022: 1998 +A1: 2000 and A2: 2003, CISPR22:1997
- EN61000-3-2 (2000) / IEC 61000-3-2 (2000) Harmonics
- EN61000-3-3 +A1 (2001) / IEC 61000-3-3 (1994) Flicker
- EN55024: 1998 Plus A1: 2000 & A2: 2003, CISPR24:1997
- EN60950-1: 2001+A11: 2004

KOREA MIC



Note that this device has been approved for business purposes with regard to electromagnetic interference. If you find that this device is not suitable for your use, you may exchange it for a non-business device.

TAIWAN BSMI


警告使用者：這是甲類的資訊產品，在居住的
環境中使用時，可能會造成射頻干擾，在這種
情況下，使用者會被要求採取某些適當的對策。

This is a Class A Information Product. When used in residential environment, it may cause radio frequency interference. Under such circumstances, the user may be requested to take appropriate countermeasures.

APPENDIX VIII DATAFORT SERIAL ADAPTER

The Decru serial adapter is configured with the following pinouts.

Decru Serial Adapter Pinout

RJ45 (socket) - DB9 (female)

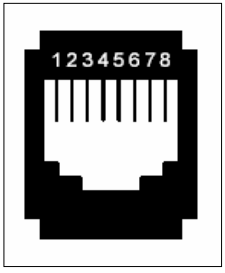
Sort by RJ45

RJ45 (socket)	Color	Signal Name	DB9 (female)
1	Blue	CTS	8
2	Orange	DCD/DSR	6
3	Black	RD	2
4	Red	RI	9
5	Green	SGND	5
6	Yellow	TD	3
7	Brown	DTR	4
8	White	RTS	7

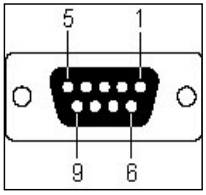
Sort by DB9

RJ45 (socket)	Color	Signal Name	DB9 (female)
3	Black	RD	2
6	Yellow	TD	3
7	Brown	DTR	4
5	Green	SGND	5
2	Orange	DCD/DSR	6
8	White	RTS	7
1	Blue	CTS	8
4	Red	RI	9

RJ45 socket pinout



DB9 female pinout



APPENDIX IX GLOSSARY

ACL — Access Control List. A list of users with permission to access a resource on a network. The DataFort appliance 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 appliance.

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. The DataFort appliance 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, the DataFort appliance requires both a username/password combination and a token to authenticate the DataFort administrator and Recovery Officers. The DataFort appliance can be configured to require only a username and password for management.

chassis — The physical encasement of a device. The DataFort appliance 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 appliances, total system redundancy is increased, reducing the likelihood of any downtime.
Common Criteria Mode	The Common Criteria is an international standard for evaluating information technology security. The ability to run in a mode qualified to meet Common Criteria standards is an enhanced security option for the DataFort appliance.
configuration database	The database stored inside DataFort appliance 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 the DataFort appliance 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 appliance. The CLI allows remote users to log in to the DataFort appliance and administer it by entering text commands over SSH.
Decru Management Console (DMC)	A graphical user interface used to manage the DataFort appliance via an application run on the Management Station over a secure connection.
failover	The ability to withstand the failure of one or several system components by transferring access to data from a failed path to a healthy one.
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 appliances occurs over IPsec; IPsec communication is a licensed option between the DataFort appliance 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 appliance via the Decru Management Console (DMC).
Master Key	The Master Key is generated by the DataFort appliance at initialization time, and is unique to each DataFort appliance. 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 appliance. 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 the DataFort appliance assigns a portion of a high-level cryptographic key to each Recovery Card. A quorum of Recovery Cards is required to reconstitute the key.

Security Domain	A Security Domain defines a distinct group of Recovery Cards. Multiple Security Domains can be used in the enterprise to compartmentalize access to DataFort appliances.
smart cards	Credit card-sized devices with embedded microchips used by the DataFort appliance 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 appliance's hardware encryption/decryption engine, which enables gigabit-speed, full duplex encryption.
System Card	A smart card provided by Decru which is inserted at the front panel of the DataFort appliance for boot-up to enable DataFort encryption services. The System Card may be removed during normal operation to prevent unauthorized use of the DataFort appliance upon reboot.
TLS	Transport Layer Security. A protocol providing secure message transfer over the Internet. Used to secure transmission of data via web browsers.
Trustee	A trustee is a remote DataFort appliance with which a trust relationship has been formed, allowing Cryptainer Keys to be shared. A trustee may import from or export to a trustee.
Trustee Acceptance Package (TAP)	The second message between DataFort appliances when setting up a trustee relationship.
Trustee Establishment Package (TEP)	The first message sent between DataFort appliances when setting up a trustee relationship.
UDP	User Datagram Protocol. User Datagram Protocol is a communications protocol for messages between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP). Services that can be run on both TCP and on UDP (such as NFS) are often deployed with UDP when speed is a concern and deployed with TCP when on a lossy network.

INDEX

A

Access Control List (ACL) 137, 331
  ACL Capture 140
  ACL Preview 114
  ACL Sync 114
  CIFS 100
  Cryptainer ACL management 139
  end user Cryptainer ACL management 151
  NFS 249
  Use Local ACL 180
adapter, crossover RJ45 to DB9 83
adding and removing cluster members 207
Admin Card 22, 23, 331
administrator 23, 331
  add 90, 95
  change password 92
  change the card association 93
  delete profile 92
  log in to CLI 80
  login to WebUI 79
  number recommended 90
  require login authorization 91
  roles outlined 87
  Security Administrator 122
  specialty administrator, create 91
administrator roles, CLI 239
AES 19, 331
alert, clearing 174
appliance
  CLI, connecting to 80
  defense setting 173, 174
  licenses 219
  menu 229
  recovery 273
  remove, custom group 223
  restoring a previous configuration 273
  upgrading 218
  zeroizing 197
appliance sensors, sensors 225
ARP table 243
auditing DataFort logs 194
authentication 22, 331
authorization for login 91
authorizing administrator 91
auto giveback 206, 215
automatic domain sync 136
automatic domain sync disabled 136

B

back up
  appliance configuration 32, 168, 171
Backup Methods 40
backup, data
  planning 40
battery v, 48

C

Category 5 cable 24, 53
certificates
  setting security certificate 201
certificates lost after zeroization 197
change password
  administrator 92
change password, Recovery Card 186
changing media type 244
changing the user's password 150
chassis 20, 331
  intrusion 173
CIFS 18, 331
  administration example 257
  CIFS message signing 118
  data access example 146
  DataFort domain access user 46
  domain types 98
  groups 259
  SMB signatures 118
  supported clients and file servers 318
  User Registration 149
ciphertext 19, 331
ciphertext and cleartext 28, 146, 331
clear all appliance settings 197
clear an intrusion (defense alert) 174
clear smart cards 187
cleartext 19, 331
CLI 80
  command help 238, 288

commands and admin roles 239
connect from SSH client 80
disable Secure DMC 277
DMC access 82
documentation 238, 288
general information 238, 288
help 294
log in 80
login 152
permissions 237
quick reference 287
quit 294
system commands 241, 297
time-out 288
top level commands 289
CLI login with dual authentication 81
Clients NIC
changing IP address in cluster 210
Clients NIC Management Access 179
connecting to client subnet 53
interface for unencrypted data 53
cluster 332
adding member 207
auto (crypto) failover 214
auto giveback property 215
change configurations 207
change IP address of member 210
change network 204
change to standalone 207
check cluster state 95
check failover status 206
commands, CLI 296
configuration 29
configure for STP 214
conflict 206
disable command 240
failover 29, 38, 207
forming, after initial setup 207
heartbeat 29, 296
intrusion detection 214
IPsec tunnel 29
load balancing 29
management 203
management using CLI 240
manual failover 204
recover from failover 206
recovery guidelines 209
remove member 207
replace an offline member 208
requirements 207
resolving conflict 206
restore previous configuration 209
set properties with CLI 214
size 203
state 205
troubleshooting 284
VRID 212
cluster-wide operations 205
Command Line Interface
log in 80
Common Criteria 20
Common Internet File System (CIFS) 18
configuration
menu 231
configuration backup 171
configuration database 21, 332
applied to new appliance 273
back up using DMC 171
backup to LKM 169
changes synchronized in cluster 29
contents 168
event log capacity 189
size 170
used for recovery 273
Configuring switch ports for VLAN support 267
configuring table columns 228
create
custom group 223
Cryptainer 332
Access Control menu 113
access, inherited from group 136
access, NFS, with CLI 249
ACL 113, 137, 139
add, with DMC 106
aliases 263
before creating 94
cleartext 112, 249
create (add), with DMC 111
create CIFS, with CLI 260
create multi-protocol, with CLI 256
create NFS, with CLI 249
Data Encryption 112
defined 20
encryption key 21
Filename Encryption 112
icon with no lock 112

Initial Encryption 112
IP address restriction 113, 114
IPsec, require for client 115
key 113
manage CIFS, with CLI 257
manage multi-protocol, with CLI 252, 255
manage NFS, with CLI 245, 248
manage, using DMC 113
mount, NFS 147
multi-protocol 102
NFS with root access, CLI 249
NFS, view ACL with CLI 250
options when creating 112
owner 106
owner (NFS), CLI 249
Rekey 113, 115
Require IPsec 112
Restore command, DMC 111, 131
restoring 262
share level or sub-share level 100, 101
troubleshooting CIFS 278
troubleshooting NFS 281, 283
Cryptainer ID 133
Crypto Failover 214
cryptographic test 225
CryptoShred 20, 173, 176
CryptoShred button 20, 173, 174, 175
states 175
custom group
create 223
remove 223
remove appliance 223

D

data
encryption 21
migration 148
DataFort
assigning IP settings 55
capacity 27
connecting ports to network 53
DataFort Password 149, 180
DATAFORT_ADMIN domain 137
deployment 36
diagram, back panel 52
Domain Access User 46
domains 97
emergency shutdown 176
groups 137
LDAP User 46
licenses 65
management interfaces 75
specifications 319
users 136
WebUI, connecting to 79
where installed 19
DataFort CLI 332
DataFort CLI Reference Guide 237, 287
DataFort HBAs 319
DataFort hostname limitations 42
DataFort Password 180
DataFort WebUI 79
login 79
date and time
setting from DMC 188
date and time settings, time and date settings 225
DCS
requirement on Cryptainer 250, 260
decru file 146
Decru licenses 65
Decru Management Console 23, 75, 77, 226
defined 332
dual authorization 78
logging in 77
menus 226
Secure 78
Standard 77
Decru MIB 85
Decru Signed Syslogd (DSS) 189
default security setting 179
defense
alert, clearing 174
response 173
triggers 173
defense setting 33, 173
changing after setup 173
summary 174
deleted Cryptainer
restore 121, 133
deleting targets 131
diagnostic
menu 236
disable automatic domain sync 136
disabling a cluster member 240
display

state 227
DMC 23, 75, 77, 226
access to cluster members 205
defined 332
dual authorization 78
logging in 77
menus 226
Secure 78
Standard 77
DMC CLI 82
DNS 24
domain 97
add CIFS, with CLI 257
add multi-protocol, with CLI 252
add NFS, with CLI 245
add, with DMC 104
join VIP to CIFS domain 182
manage CIFS, with CLI 257
manage multi-protocol, with CLI 253
manage NFS, with CLI 246
name 104
select for user registration 149, 150
types and subtypes 98
userless 99
domain access user 46
domain controller
and DataFort 136
dual authentication login, CLI 81
dual authorization 78, 81, 91

E

edit
menu 230
emergency shutdown 176
emergency zeroization via serial console 200
encrypted file, viewing 146, 147
encryption 19
end user
access to Cryptainers 31
login to CLI 152
login to WebUI 151
manage Cryptainer ACL 151
notification 145
Windows password 149, 150
escrow service 32
event logs 189
export, NFS 101, 245

F

failover 29, 331, 332
Ethernet switch configuration 39
recovering a cluster 206
status 206
fan modules, replacing 286
fan specifications 319
feature licenses 65
Fibre Channel
networks 18
File Servers NIC
changing IP address in cluster 211
connecting to file servers subnet 53
interface for encrypted data 53
file servers subnet 53
filename encryption 112
Floating 105, 130
front panel
display 84
LCD used to assign IP address 55
LEDs 274
System Card slot 51
FTP 155
commands, CLI 291
home directory 155
full database 170

G

global default pool 120
Group Review 138, 179
accept changes 138
groups, imported from domain controller 136

H

hardware maintenance 286
hardware specifications 319
help
menu 236
hidden .decru file 146
hidden shares, naming 100
Home page
returning to 79
hostname limits for DataFort 42
HTTP 153, 291

I

IKE 332
initial encryption of Cryptainer 112

installation
in rack 49
planning 28
precautions v, 50
requirements 24
International Organization for Standardization (ISO) 202, 321
Internet Explorer
for accessing WebUI 79
intrusion detection 173, 174
in cluster 214
IP address 24
additional for server 110, 129
DataFort, assigning 55
IP restriction 113, 114
of CIFS server, in configuration database 258
IP settings
assigning from LCD 55
changing, with DMC 217
DataFort, assigning from serial console 56
IPsec 29, 332
add rules to DataFort, with CLI 182, 265
configure Solaris clients 183
configure VIP, with DMC 130
configure VIP, with WebUI 117
configure Windows clients 183
Kerberos rule for Windows clients (CLI) 181
require for clients 112
support 181
iSCSI node name 20
ISO 321
IT power systems iv, 48

J

join CIFS domain 182
jumbo frames 244

K

Kerberos authentication 265
client to DataFort requires joining domain 182
configure DataFort, with CLI 181, 265
used without IPsec 182
with LDAP server 46
key
encryption key 113
key, chassis 173
keys 332
encryption keys 20
key escrow service 32
menu 232
purge 169

L

LCD 75, 84, 225
assigning DataFort IP settings 55
bar graph 84
buttons 84
display 225
touch panel interface 75
LDAP 332
supported server schemas 98
User for DataFort 46
with CIFS or NFS domains 98
LEDs 274
power supply 275
licenses 24
IPsec 265
managing 219
Lifetime Key Management (LKM) 21, 333
limited administrator 91
Limits
Number of DataFort appliances in a cluster 27
Lithium battery v, 48
LKM 32
appliance setup 45
number of supported servers 169
software setup 45
LKM servers
number supported 169
load balancing 29
with IP addresses 117
Local domain 99
log types 189
login
CLI 80
CLI, dual authorization 81
CLI, end-user 152
WebUI, end-user 151
logs 189
configuring storage location 190
Decru Signed Syslogd (DSS) 189
syslog mapping table 193
temporary file mapping 193

viewing, with DMC 194
logs, DataFort
auditing 194

M

management console installation 44
Management Station
requirements 318
management station 22, 333
management console installer 44
requirements 43
security 43
Master Key 21, 333
media type 244
menu
appliance 229
configuration 231
diagnostic 236
edit 230
help 236
keys 232
security 234
topology 233
trustee 235
utilities 233
view 230
MIB 85, 333
mounting DataFort in rack 49
mounting shares, NFS 147
MPIO 124, 125, 130
multi-appliance management 226
multi-protocol Cryptainer 102
ACL Sync after restore 121
add, with DMC 106
create and manage, with CLI 252
owner 106
multi-protocol server
add, with DMC 104
multi-protocol share
add, with DMC 105
virtualize, with DMC 106

N

NAS 18, 333
network diagram 19, 36
NAS Topology view 102, 124
nas-admin 137
nas-user 137
NDMP (Network Data Management Protocol) 40
network
diagram, NAS 19, 36
information needed for setup 42
manage, with CLI 243
planning backup and restore 40
settings, changing 217
Network Attached Storage (NAS) 18
network commands, CLI 243
Network File System (NFS) 18
network switch ports 24
network time servers 188
network, IP Settings 217
NFS 18, 292, 333
administration example 245
Cryptainer ACL 249
data access example 147
domain types 98
groups 249
preparing the network 101, 245
supported clients and file servers 318
NIS 98
node name 20
NTP time server 24, 188

O

online help 76
owner, of Cryptainer 106

P

Parent Key 21
password
administrator, changing 92
end-user DataFort password 149, 180
one-time, CLI 80
Recovery Card, changing 186
password and label limitations 66
port
Clients 53
File servers 53
forwarding 264
power
precautions iv, 48
power button 57
power cord 24
power supply
LEDs 275
notice iv, 48

replaceable 286
power supply specifications 319
primary filer 40
protect against insider attacks 91

Q

quorum 23, 32, 185, 187, 333

R

rack installation 49
rack mounting kit 24
Real NAS Elements 102, 124
real server
add and manage CIFS, with CLI 258
add and manage multi-protocol, with CLI 253
add and manage NFS, with CLI 247
add, with DMC 104
manage, with DMC 110
Recovery Cards 22, 185, 333
change password 186
lost 185
replace 185
Recovery Officers 23, 333
required for forming cluster 209
required for replacing appliance 273
required for replacing DataFort 208
required for replacing Recovery Card 158
required for Setup 59
rekey jobs, status 115
remote authorization 60
Remote Desktop 277
remote filer 40
remove
custom group 223
replacing an offline cluster member 208
reset appliance 197
reset smart cards 187
reset System Card 285
Restore Cryptainer 111, 131
restore, planning 40
Reviewing the Cluster Load Balance 215
RJ45 to DB9 adapter 24, 53

S

SAN 18
secret share 333
Secure CLI 76, 179
login 80
Secure CLI default setting 177
Secure DMC 76, 179
enable/disable via CLI 277
Secure DMC default setting 179
Secure Password Update 180
secure shell (SSH) support 75
Secure Sockets Layer (SSL) 75
Secure Web default setting 177
SecureView 23, 75
security
menu 234
Security Administrator 122
security certificate
certificate authority signed, generating request 202
certificate authority signed, installing 202
self-signed, installing 201
warning 61
security certificate, setting 201
security domain 23, 334
planning 28
Security Policy
customize 178
pre-configured levels 177, 178
security policy
planning 32
security, implementing and maintaining 28
Security, Management Security 177, 178
security, zeroize 198
SEP 20, 214, 334
serial console 75, 83
assigning DataFort IP settings 56
clearing IP Settings 83
connecting serial port 53
emergency access 200
interface 75
zeroizing appliance 83
serial console port
adapter 83
log in 83
serial number 225
server
add CIFS, with CLI 258
add multi-protocol, with CLI 253
add NFS, with CLI 247
add, with DMC 104
manage CIFS, with CLI 258
manage multi-protocol, with CLI 253

manage NFS, with CLI 247
manage, with DMC 110
multi-protocol 104
servicing appliance 286
set
SNMP options 221
share
add CIFS, with CLI 259
add multi-protocol, with CLI 254
add NFS, with CLI 248
add, with DMC 105
CIFS 100
icons 106
manage CIFS, with CLI 259
manage multi-protocol, with CLI 254
manage NFS, with CLI 248
manage, with DMC 111
multi-protocol 105
view CIFS shares 146
view NFS shares 147
virtualize CIFS, with CLI 259
virtualize multi-protocol, with CLI 255
virtualize NFS, with CLI 248
virtualize, with DMC 106
size of the configuration database 170
smart card reader 22, 24
using multiple 59
smart cards 24, 334
checking versions and status 187
reset procedure 187
summary 22
troubleshooting 285
SMB signatures 118
SnapDrive 123, 131
SnapMirror 40
snapshot 40
SNMP 75, 334
chassis alerts 220
configuration 220
crypto alerts 220
MIB 85
options 220
set options 221
system alerts 220
spanning-tree protocol 39, 214
specifications 317
SSH 75, 334
CLI access 80, 81, 238
SSL 153, 334
stack trace 243
standard CLI 80
standard rack mount 49
state displays 227
status and settings 224
Storage Area Network (SAN) 18
Storage Encryption Processor (SEP) 20
STP 39, 214
supported platforms 318
switch connections in a cluster 30
syslog, syslogd (syslog daemon) 189, 192
System Card 22, 334
inserting 51
removing, in emergency 176
resetting 285
system log, appliance logs 225
system logs, verifying 242
system properties, CLI 241
system requirements 318
system users, administrators 95

T

tab
appliance 228
table columns
configuring 228
TAP 158
TEP 158
Terminal Services 277
TFTP 156, 292
time and date
setting from DMC 188
time servers 188
time-out
CLI 80
DMC 77
serial session 83
WebUI 79
topology
menu 233
troubleshooting 272
CIFS Cryptainers 278
clusters 284
management interfaces 276
network connections 276
NFS Cryptainers 281, 283
smart cards 285

trustee
  managing 158
  menu 235
Trustee Acceptance Package 158
Trustee Acceptance Package (TAP) 160
Trustee Establishment Package 158
Trustee Establishment Package (TEP) 159, 160, 161, 163, 164
trustee relationship
  approve TAP, on local network 161
  approve TAP, on remote network 165, 166
  approve TEP, on local network 160
  approve TEP, on remote network 163, 164
  authorizing trustees locally to approve TEP/TAP, on a local network 159
  create TEP, on remote network 162
  create trustee link, on local network 159
  create, on local network 159
  create, on remote network 162
  delete unapproved TAP trustee 166
  initiating remote authorization to approve TAP, on local network 161
  initiating remote authorization to approve TAP, on remote network 165
  initiating remote authorization to approve TEP, on local network 160
  initiating remote authorization to approve TEP, on remote network 164
  receive TAP, on remote network 165
  receive TEP, on remote network 162
types of keys recovered during a restore 197

U

UDP 334
Upgrade 218
upgrading appliances 218
USB 24
Use Local ACL 180
user management of Cryptainer ACL 151
User Mapping 99, 180
user notification 145
User Registration 149, 179
user updating password information 150
userless domain 99
users and groups
  CIFS, manage with CLI 259
  manage access 136, 139
  NFS, manage with CLI 248, 249
utilities
  menu 233

V

view
  menu 230
Virtual LAN setup 266
Virtual NAS Elements 102, 124
virtual server (VIP)
  add NFS, with CLI 247
  configure IPsec 117, 130
  manage CIFS, with CLI 258
  manage multi-protocol, with CLI 254
  manage NFS, with CLI 247
  manage, with DMC 117, 130
  planning 31
  set certificate 117, 130
virtualize
  CIFS share, with CLI 259
  multi-protocol share, with CLI 255
  NFS share, with CLI 248
  share, with DMC 106
VLAN commands, CLI 293
VLAN setup 266
VLAN support
  configuring VLAN access 268
  restricting admin access to specified VLAN 270
  switch port configuration 267
VRID 29
  changing 212
VRRP (Virtual Router Redundancy Protocol) 29

W

WAN 29
Web Access 153
WebDAV 153, 154
WebUI
  accessing 79
  login 79, 151
  time-out 79
  user registration 149
Windows
  domain access user for DataFort 46
Windows event logging 191
Windows Event Viewer 191

Z

zeroization without admin card 200
zeroizing appliance 197
    using DMC or CLI 198
    using serial console 200