



## ■ ■ ■ ADMINISTRATION GUIDE

DataFort S-Series  
Version 2.2

# security

DataFort Administration Guide for S-Series DataFort

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

Part number: 210-02371 (v. 022207\_S2.2)

Model Numbers: S110

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'ACCÈS.

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

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

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

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

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

**OPPMERKSAMHET:** Apparatet må kun tilkoples jordet stikkontakt.

### Dual Power Supply Notice



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

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

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

### Lithium Battery Notice for Service Personnel

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



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

**ATTENTION :** Il y a danger d'explosion s'il a remplacement incorrect de la batterie. Remplacer uniquement avec une batterie du même type ou d'un type équivalent recommandé par le constructeur. Mettre au rebut les batteries usagées conformément aux instructions du fabricant.

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

### RACK MOUNTING

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



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

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

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

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

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

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

## CONTENTS

|                                                     |           |
|-----------------------------------------------------|-----------|
| <b>Chapter 1 Introduction</b>                       | <b>13</b> |
| About the Decru DataFort Security Appliance         | 14        |
| Components of the Decru Security System             | 14        |
| Encryption                                          | 14        |
| Common Criteria Compliance                          | 14        |
| Hardened Architecture                               | 14        |
| CryptoShred Feature                                 | 14        |
| Key Management                                      | 15        |
| Lifetime Key Management Solutions                   | 15        |
| Configuration Database                              | 15        |
| Authentication Layers                               | 15        |
| DataFort Users                                      | 16        |
| Security Domain                                     | 16        |
| Installation Requirements                           | 17        |
| Conventions Used in this Manual                     | 18        |
| <b>Chapter 2 Planning the Network Configuration</b> | <b>19</b> |
| Planning the Security Domain                        | 20        |
| Decru DataFort Capacity                             | 20        |
| Installation Considerations                         | 20        |
| IPsec in a Cluster                                  | 20        |
| Secure Network Practices                            | 21        |
| Maintaining Configuration Database Backups          | 21        |
| Sending Recovery Cards to Escrow                    | 21        |
| Planning Remote Security Logging                    | 21        |
| Removing the System Card                            | 22        |
| Preparing for Manual Security Responses             | 22        |
| Placing DataFort in the SCSI Network                | 23        |
| <b>Chapter 3 Preparing to Install DataFort</b>      | <b>24</b> |
| Collecting Network Information                      | 25        |
| Preparing the Management Station                    | 25        |
| Management Station Security                         | 26        |
| Enabling TLS                                        | 26        |
| Running the Installer                               | 26        |
| Setting Up Lifetime Key Management                  | 27        |
| <b>Chapter 4 DataFort Appliance Installation</b>    | <b>28</b> |
| Notices and Warnings                                | 29        |
| Power Supply Notice                                 | 29        |
| Dual Power Supply Notice                            | 29        |

|                                                        |           |
|--------------------------------------------------------|-----------|
| Lithium Battery Notice for Service Personnel           | 29        |
| Perchlorate Present                                    | 29        |
| Unpacking the DataFort Appliance                       | 29        |
| Rack Mounting the DataFort Appliance                   | 30        |
| Selecting a Location                                   | 30        |
| Rack Mounting                                          | 30        |
| Connecting the Decru DataFort Appliance                | 31        |
| System Card Insertion                                  | 31        |
| Rear Panel Network Connections                         | 31        |
| Power Connection                                       | 32        |
| Assigning the DataFort IP Address                      | 33        |
| Setting the IP Address Using the LCD                   | 33        |
| Setting the IP Address Using the Serial Console        | 34        |
| Powering Up and Shutting Down                          | 36        |
| <b>Chapter 5 Initializing DataFort Appliances</b>      | <b>37</b> |
| About the Setup Wizard                                 | 38        |
| Setup Wizard Functions                                 | 38        |
| About Smart Cards and Readers                          | 38        |
| Initializing a Standalone DataFort or DataFort Cluster | 39        |
| Connect to Head of Cluster                             | 40        |
| Sign License Agreement                                 | 40        |
| Recover From Database                                  | 40        |
| Create Administrator                                   | 40        |
| Configure Cluster and Recovery Schema                  | 40        |
| Network Settings                                       | 43        |
| Add Licenses                                           | 45        |
| Network and Certificates                               | 46        |
| Insert Recovery Card                                   | 47        |
| Apply Settings                                         | 48        |
| Adding a Member to a Cluster                           | 49        |
| Log in to Head of Cluster                              | 49        |
| Cluster and Recovery Schema                            | 50        |
| Network Settings                                       | 50        |
| Add Licenses                                           | 50        |
| Network and Certificates                               | 50        |
| Insert Recovery Card                                   | 51        |
| Apply Settings                                         | 51        |
| <b>Chapter 6 DataFort Management Interfaces</b>        | <b>52</b> |
| Management Interfaces Overview                         | 53        |
| SecureView                                             | 54        |
| Security Policies                                      | 54        |
| Online Help                                            | 54        |
| Connecting to the DataFort WebUI                       | 55        |

|                                                                  |           |
|------------------------------------------------------------------|-----------|
| Using the DataFort WebUI                                         | 55        |
| Connecting via WebUI                                             | 55        |
| Quick Links and Status                                           | 56        |
| Connecting via WebUI using Dual Authorization                    | 57        |
| Connecting to the DataFort Command Line Interface                | 58        |
| Using the CLI                                                    | 58        |
| Connecting via Standard CLI                                      | 58        |
| Connecting via Secure CLI                                        | 58        |
| Connecting via CLI using Dual Authorization                      | 59        |
| Connecting to CLI via WebUI                                      | 60        |
| Accessing the Decru Management Console                           | 61        |
| Serial Console                                                   | 62        |
| Logging in to the Serial Console Port                            | 62        |
| Configuring IP Settings                                          | 62        |
| Clearing IP Settings                                             | 62        |
| Zeroizing DataFort                                               | 62        |
| DataFort Front Panel LCD                                         | 63        |
| SNMP Settings                                                    | 63        |
| <b>Chapter 7 DataFort Admin Roles and Account Administration</b> | <b>64</b> |
| Administrator Roles                                              | 65        |
| Account Administration                                           | 67        |
| Adding an Administrator                                          | 67        |
| Requiring Authorization for Login                                | 70        |
| Changing the Administrator Password                              | 71        |
| Removing an Administrator                                        | 73        |
| Changing a Card Association                                      | 73        |
| <b>Chapter 8 Before Storage Administration</b>                   | <b>74</b> |
| Checking Cluster State                                           | 75        |
| Configuring Remote Logging                                       | 75        |
| Starting LKM                                                     | 75        |
| LKM Server                                                       | 75        |
| LKM Appliance                                                    | 75        |
| Configuring Tape Settings                                        | 75        |
| Creating Additional Administrators                               | 76        |
| Verifying System Version                                         | 76        |
| Determining the Defense Setting                                  | 76        |
| <b>Chapter 9 Storage Administration</b>                          | <b>77</b> |
| Managing Tape Settings                                           | 78        |
| Pool Settings and Defaults                                       | 78        |
| Tape Settings                                                    | 80        |
| Securing Data on SCSI Devices                                    | 80        |
| View SCSI Devices                                                | 80        |

|                                                           |            |
|-----------------------------------------------------------|------------|
| Assign Keys                                               | 82         |
| Managing SCSI Devices                                     | 83         |
| Storage Management Pane Menu                              | 83         |
| Storage Device Collection Menu                            | 83         |
| SCSI ID Menu                                              | 83         |
| Logical Unit Menu                                         | 84         |
| Managing Tapes                                            | 84         |
| Tapes Management Pane Menu                                | 84         |
| Tape Pool Collection Menu                                 | 84         |
| Tape Pool Menu                                            | 85         |
| Tape Device Menu                                          | 85         |
| Edit Pool Page                                            | 86         |
| Changing SCSI Settings                                    | 87         |
| <b>Chapter 10 Key Administration</b>                      | <b>88</b>  |
| Managing Trustees                                         | 89         |
| Trustee Scenarios                                         | 89         |
| Setting Up Trustees                                       | 89         |
| Importing and Exporting Keys                              | 95         |
| Managing DataFort Defense Responses                       | 96         |
| Defense Triggers and Responses                            | 96         |
| DataFort Defense Setting                                  | 96         |
| Changing the Defense Setting                              | 97         |
| Clearing a Defense Alert                                  | 98         |
| CryptoShred Button States                                 | 98         |
| System Card CryptoShred                                   | 98         |
| Configuring Management Security Settings                  | 100        |
| Managing Recovery Officers and Recovery Cards             | 101        |
| Replacing a Recovery Card                                 | 101        |
| Changing a Recovery Card Password                         | 103        |
| Smart Card Reset                                          | 104        |
| <b>Chapter 11 Backup Administration</b>                   | <b>105</b> |
| Saving Configurations to Lifetime Key Management Software | 106        |
| Best Practices for Secure Backups                         | 106        |
| Configuring Backups to LKM Software                       | 106        |
| Backing Up the Configuration to LKM Software              | 108        |
| Key Purging                                               | 108        |
| Downloading Configurations to a Remote Location           | 109        |
| <b>Chapter 12 Physical Security Administration</b>        | <b>110</b> |
| Setting Date and Time                                     | 111        |
| Configuring and Viewing Logs                              | 111        |
| DataFort Log Storage Guidelines                           | 111        |
| Decru Signed Syslogd (DSS)                                | 112        |

|                                                          |            |
|----------------------------------------------------------|------------|
| Configuring Log Storage                                  | 112        |
| Windows Event Logging                                    | 112        |
| Setting Up Syslog                                        | 114        |
| Viewing the Log                                          | 115        |
| Verifying Signed Log Messages                            | 115        |
| Zeroizing the Decru DataFort                             | 116        |
| Zeroizing After Setup                                    | 117        |
| Zeroization Using the DataFort WebUI                     | <b>117</b> |
| Zeroization Using the CLI                                | 118        |
| Zeroization Using the Serial Console                     | 118        |
| Emergency Serial Console Port Access                     | 118        |
| <b>Chapter 13 Cluster Administration</b>                 | <b>119</b> |
| Cluster Management                                       | 120        |
| Cluster-Wide Management via WebUI                        | 120        |
| Checking the Status of the Cluster                       | 120        |
| Resolving a Cluster Conflict                             | 121        |
| Adding and Removing Cluster Members                      | 121        |
| Adding a Cluster Member                                  | 121        |
| Removing a Cluster Member                                | 121        |
| Replacing a DataFort in a Cluster                        | 122        |
| Recovering a Cluster                                     | 123        |
| Changing Network Properties of a Cluster Member          | 123        |
| Changing the IPsec Secret of a Cluster                   | 123        |
| <b>Chapter 14 Machine Administration</b>                 | <b>124</b> |
| Network Settings                                         | 125        |
| Upgrading DataFort                                       | 125        |
| Setting Security Certificates                            | 126        |
| Setting a Local Security Certificate                     | 126        |
| Setting a Certificate Authority Signed Certificate       | 129        |
| Managing Licenses                                        | 131        |
| SNMP Settings                                            | 132        |
| Enabling SNMP                                            | 132        |
| SNMP Configuration                                       | 132        |
| <b>Chapter 15 DataFort Appliance Settings and Status</b> | <b>134</b> |
| Viewing Settings in the WebUI                            | 135        |
| <b>Chapter 16 Decru Management Console Functions</b>     | <b>137</b> |
| Appliance Management                                     | 138        |
| License and Administration Management                    | 141        |
| Logging Configuration                                    | 143        |
| Decru Management Console Menus                           | 144        |

|                                                          |            |
|----------------------------------------------------------|------------|
| <b>Chapter 17 CLI Administration</b>                     | <b>147</b> |
| Using the CLI                                            | 148        |
| Connecting to the CLI                                    | 148        |
| CLI Help                                                 | 148        |
| Administration Commands                                  | 149        |
| Administrator Roles                                      | 149        |
| Creating a New Administrator Using the CLI               | 149        |
| Cluster Management                                       | 150        |
| System Properties and Log Management                     | 150        |
| Verifying System Logs                                    | 152        |
| Stack Trace Settings                                     | 153        |
| Network Management                                       | 153        |
| Backup Management                                        | 153        |
| <b>Chapter 18 Troubleshooting</b>                        | <b>154</b> |
| Restoring a DataFort Appliance                           | 155        |
| Front Panel LEDs                                         | 156        |
| Power Supply LEDs                                        | 156        |
| Network Connections and Management Interfaces            | 157        |
| SCSI Network                                             | 159        |
| Clusters                                                 | 160        |
| Smart Cards                                              | 161        |
| Hardware Issues                                          | 161        |
| <b>Appendix I Command Line Interface Quick Reference</b> | <b>162</b> |
| Using the CLI                                            | 163        |
| CLI Syntax                                               | 163        |
| CLI Help                                                 | 163        |
| CLI Command Overview                                     | 164        |
| Top Level Commands                                       | 164        |
| Device Commands                                          | 164        |
| Disk Commands                                            | 165        |
| FC Site Commands                                         | 165        |
| KFC Commands                                             | 165        |
| Pool Commands                                            | 165        |
| Tape Commands                                            | 166        |
| CLI Formatting Commands                                  | 166        |
| Help Command                                             | 166        |
| Quit Command                                             | 166        |
| Active-Role Commands                                     | 166        |
| Authorize Command                                        | 166        |
| Password Command                                         | 167        |
| Role Commands                                            | 167        |
| User Commands                                            | 167        |
| Whoami Command                                           | 167        |

|                                                      |            |
|------------------------------------------------------|------------|
| Trustee Commands                                     | 167        |
| Network Commands                                     | 167        |
| Key Management Commands                              | 167        |
| LKM Management Commands                              | 168        |
| Cluster Commands                                     | 168        |
| Database Commands                                    | 168        |
| System Commands                                      | 168        |
| <b>Appendix II Logging Functions</b>                 | <b>170</b> |
| DataFort Log Event and Priority Types                | 171        |
| Log Storage Locations                                | 171        |
| Log Presentation                                     | 172        |
| Temporary Logs                                       | 172        |
| Database Logs                                        | 172        |
| Remote Logs                                          | 173        |
| Log Purging                                          | 174        |
| Log Messages                                         | 177        |
| IFC Logs                                             | 177        |
| Audit Logs                                           | 178        |
| Auth Logs                                            | 179        |
| Security Management Logs                             | 180        |
| Integrity Logs                                       | 186        |
| <b>Appendix III Specifications</b>                   | <b>188</b> |
| Specifications                                       | 189        |
| <b>Appendix IV Partial List of ISO Country Codes</b> | <b>190</b> |
| <b>Appendix V Regulatory and Certifications</b>      | <b>191</b> |
| FCC B Declaration of Conformity                      | 192        |
| European Union                                       | 192        |
| Canadian ICES-003                                    | 192        |
| VCCI Class A Statement                               | 193        |
| CE Statement                                         | 193        |
| <b>Appendix VI Glossary</b>                          | <b>194</b> |
| <b>Index</b>                                         | <b>197</b> |

## ■ ■ ■ ■ 1 INTRODUCTION

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

The Decru DataFort appliance can provide managed, encrypted network storage for NAS, SAN, SCSI and IP networks. Decru DataFort models correspond to the main types of storage architecture:

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

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

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

## ABOUT THE DECRU DATAFORT SECURITY APPLIANCE

---

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

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

**Note:** The S-Series DataFort supports only tape.

## COMPONENTS OF THE DECRU SECURITY SYSTEM

---

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

### ENCRYPTION

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

### COMMON CRITERIA COMPLIANCE

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

### HARDENED ARCHITECTURE

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

### CRYPTOSHRED FEATURE

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

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

## **KEY MANAGEMENT**

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

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

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

## **LIFETIME KEY MANAGEMENT SOLUTIONS**

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

## **CONFIGURATION DATABASE**

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

## **AUTHENTICATION LAYERS**

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

### **System Card**

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

|                       |                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Admin Card</b>     | An Admin Card adds additional optional authentication to the communication between administrator and DataFort. Admin Cards can be used for one or appliances (including a cluster or separate appliances).                                                                                                                                                               |
| <b>Recovery Cards</b> | Recovery Cards are used in sets to restore encrypted data or disabled DataFort appliances, and to replace other smart cards. Each Recovery Card is associated with a Recovery Officer, who is a highly trusted individual in the organization. Officers must present cards and passwords before a recovery procedure that could threaten data security can be performed. |

## **DATAFORT USERS**

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

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DataFort Administrators</b>   | DataFort can be managed by several types of administrators. A Full Administrator can complete all operations necessary to set up, manage and maintain the DataFort appliance. Other administrators can be created that are able to execute a more limited set of functions, targeting specific administration tasks. Every administrator is authenticated with a login name and password. Additionally, administrators can be authenticated with physical possession of an Admin Card. Depending on the organization, it may be desirable to create administrators that require authorization by another administrator in order to manage DataFort. |
| <b>Recovery Officers</b>         | Recovery Officers are trusted individuals responsible for retaining initialized Recovery Cards after DataFort setup is complete. Each Recovery Officer is authenticated by a Recovery Card and its associated password. A set minimum of Recovery Officers must be present with their associated cards in order to complete sensitive operations such as data recovery.                                                                                                                                                                                                                                                                             |
| <b>Physical Security Officer</b> | The Physical Security Officer is an individual responsible for maintaining and checking the physical security of the DataFort appliance prior to insertion of the System Card into the chassis.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## **SECURITY DOMAIN**

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

## INSTALLATION REQUIREMENTS

---

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

- Decru DataFort Appliance
- DataFort Documentation and Software CD-ROM. The documentation and software CD contains software necessary for DataFort operation, such as the smart card reader driver and Decru Management Console installer.
- Custom RJ45 to DB9 adapter and Category 5 cable for a serial connection
- AC power cord or cords appropriate for DataFort model
- DataFort smart cards, including System, Admin and Recovery Cards
- USB smart card reader
- Decru product licenses
- Slide rail mounting kit including hardware and instructions (included in the DataFort package)
- Network cables. Have the requisite number of network cables, of appropriate lengths. Each DataFort will require one standard RJ-45 Ethernet cable.
- Network switch ports. Determine which Ethernet switch ports you will be using to connect the DataFort appliances to your network. Each DataFort has one Ethernet connection, so one switch port per DataFort will be required.
- IP address, Subnet mask and Default Gateway. Each DataFort will require one dedicated IP address. Know what the appropriate subnet mask and appropriate default gateway will be for each dedicated IP address to be used during installation.
- DataFort name. Establish what resolvable system name will be assigned to each DataFort being installed. Associating the specific IP addresses with their associated system names in your DNS configuration prior to installation will simplify IP resolution.
- DNS information. Have the appropriate DNS information (DNS suffix, primary DNS server IP address, secondary DNS server IP address) for each IP address to be used during installation.
- NTP address. Have the appropriate NTP time server information for each dedicated IP address to be used during installation. If you are not using an NTP server for time synchronization then this information is not required.
- Recovery schema. Determine what the recovery schema will be for the DataFort appliance or DataFort cluster. The recovery schema determines how many Recovery Cards and their associated owners must be present for sensitive data recovery operations.

## CONVENTIONS USED IN THIS MANUAL

---

The following typographic conventions are used in this manual:

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

## ■ ■ ■ ■ 2 PLANNING THE NETWORK CONFIGURATION

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

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

- [Planning the Security Domain](#)
- [Decru DataFort Capacity](#)
- [Installation Considerations](#)
- [Secure Network Practices](#)
- [Placing DataFort in the SCSI Network](#)

PLANNING THE SECURITY DOMAIN

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

DECRU DATAFORT CAPACITY

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

TABLE 1: DATAFORT CAPACITY

| Device                                              | Number | Explanation                                                                                                   |
|-----------------------------------------------------|--------|---------------------------------------------------------------------------------------------------------------|
| Number of S-Series DataFort appliances in a cluster | 4      | A DataFort cluster can support up to 4 DataFort appliances.                                                   |
| Attached storage devices                            | 4      | A single DataFort appliance may support no more than 4 attached storage devices.                              |
| Tape keys                                           | 8000   | Once more than 8000 keys have been generated for a cluster keys should be purged from the system upon backup. |

INSTALLATION CONSIDERATIONS

In order to encrypt data moving to storage, DataFort separates the network into cleartext and ciphertext portions. Hosts are connected to the cleartext portion, while storage devices are connected to the ciphertext portion. Separate SCSI ports are available on DataFort to make these connections. DataFort appliances support SCSI daisy-chaining, so a single appliance can encrypt data going to multiple tape libraries. DataFort also supports legacy cleartext tapes, ensuring a seamless transition to a secure environment. DataFort appliances can be deployed in clusters for key sharing.

IPSEC IN A CLUSTER

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

## SECURE NETWORK PRACTICES

---

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

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

### MAINTAINING CONFIGURATION DATABASE BACKUPS

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

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

### SENDING RECOVERY CARDS TO ESCROW

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

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

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

### PLANNING REMOTE SECURITY LOGGING

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

## REMOVING THE SYSTEM CARD

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

## PREPARING FOR MANUAL SECURITY RESPONSES

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

The defense setting determines the DataFort appliance's automatic response to physical intrusion. See [Defense Triggers and Responses](#) on page 96 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 <a href="#">CryptoShred Button States</a> .)                                                                                 |
|                                                                                                                                |                                                                                                     | A Full Administrator can reset DataFort (see <a href="#">Clearing a Defense Alert</a> ).                                                                                                                                  |
| 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 <a href="#">CryptoShred Button States</a> .)                                                                                 |
|                                                                                                                                |                                                                                                     | With Medium and High Level defense, DataFort must be zeroized and then restored using the Setup Wizard, Recovery Officers, and a saved configuration database. See <a href="#">Restoring a DataFort Appliance</a> .       |
| Removing the System Card followed by shutdown and/or reboot (Removing the System Card alone does not stop DataFort operation.) | Stops encryption and decryption immediately.                                                        | If the System Card is available, re-insert it and reboot the DataFort appliance.                                                                                                                                          |
|                                                                                                                                |                                                                                                     | If the System Card was destroyed or lost, DataFort must be zeroized and then restored using the Setup Wizard, Recovery Officers, and a saved configuration database. See <a href="#">Restoring a DataFort Appliance</a> . |

## PLACING DATAFORT IN THE SCSI NETWORK

DataFort can be added to the existing infrastructure of the network without impact on network functions. No re-configuration is necessary for SCSI devices. DataFort supports SCSI daisy-chaining, so a single appliance can encrypt data going to multiple tape libraries. A DataFort cluster can be used for key and bandwidth sharing.

DataFort is placed in the data path between the backup server and the tape device. DataFort S-Series appliances can be deployed in clusters of up to four units for key sharing and availability. Key sharing is done between DataFort appliances via Ethernet.

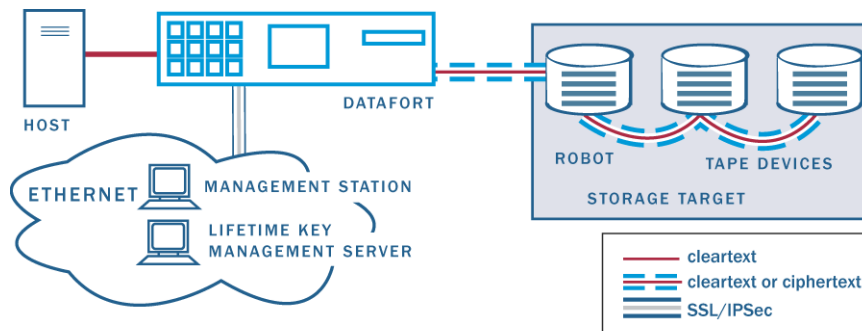


Figure 2-1: DataFort between host and storage

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

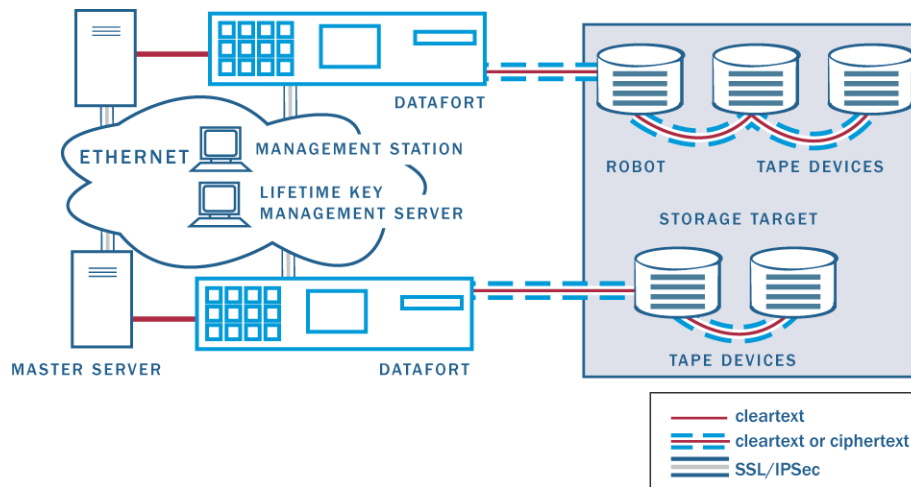


Figure 2-2: DataFort cluster sharing keys and bandwidth

### 3 PREPARING TO INSTALL DATAFORT

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

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

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

Once DataFort is installed, manage the appliance using the DataFort management interfaces. See the [Management Interfaces Overview](#) on page 53 for a list of interfaces and their uses.

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

#### Set up Management Station



#### Set up Lifetime Key Management solution



#### Set up DataFort appliance standalone or cluster



|                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>1</b> Connect PC that will serve as station to network</p> <p>Install smart card reader and Decru Management Console (DMC)</p> <p>Access management interfaces from the management station</p> | <p><b>2</b> Connect LKM appliance or LKM server to network</p> <p>LKM server—Install LKM software</p> <p>LKM appliance—Assemble Recovery Cards and Recovery Officers and run Setup Wizard from Decru Management Console</p> <p>Complete set up of LKM appliances from Decru Management Console</p> | <p><b>3</b> Connect DataFort appliances to network</p> <p>Determine security settings and administrative roles</p> <p>Assemble Recovery Cards and Recovery Officers</p> <p>Run Setup Wizard from Decru Management Console</p> <p>Complete set up of DataFort appliances from DataFort WebUI</p> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## COLLECTING NETWORK INFORMATION

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

### DataFort Network Information

- Resolvable hostname for DataFort appliance
- DNS suffix and DNS server IP address (if DNS is used)
- DataFort Management IP address, Subnet Mask and Gateway. This is initially set when [Assigning the DataFort IP Address](#).
- SCSI ID of the host that will be connected to DataFort

### Cluster Member Information

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

## PREPARING THE MANAGEMENT STATION

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

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

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

**TABLE 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                                                     |
| Browser for DataFort WebUI               | Internet Explorer version 6.0 (Service Pack 1) or greater. TLS must be enabled. |
|                                          | Microsoft JVM or Sun JRE 1.4.2.08 or greater. (DMC installs Sun JRE 1.5_06.)    |

**TABLE 3: MANAGEMENT STATION REQUIREMENTS (CONTINUED)**

| Management Station Requirements |                                                            |
|---------------------------------|------------------------------------------------------------|
| Hardware requirements           | 2Ghz                                                       |
|                                 | 1GB RAM                                                    |
|                                 | 4GB free hard drive space                                  |
|                                 | An available USB port for the smart card reader from Decru |
|                                 | A CD drive for installing software                         |

## MANAGEMENT STATION SECURITY

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

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

## ENABLING TLS

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

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

## RUNNING THE INSTALLER

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

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

## SETTING UP LIFETIME KEY MANAGEMENT

---

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

### **Lifetime Key Management Appliance**

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

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

### **Lifetime Key Management Server Software**

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

If you are using LKM software, install the software on a designated server. Make sure the server is up and its IP address is reachable from the Ethernet network before configuring DataFort appliances. Instructions for enabling automatic updates to LKM servers are provided in [Chapter 11](#).

## ■ ■ ■ ■ 4 DATAFORT APPLIANCE INSTALLATION

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

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

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

## NOTICES AND WARNINGS

---

### POWER SUPPLY NOTICE

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



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

### DUAL POWER SUPPLY NOTICE



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

### LITHIUM BATTERY NOTICE FOR SERVICE PERSONNEL

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



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

### PERCHLORATE PRESENT

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

## UNPACKING THE DATAFORT APPLIANCE

---

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

If an appliance has been tampered with, return it to Decru.

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

## RACK MOUNTING THE DATAFORT APPLIANCE

---

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

- [Selecting a Location](#)
- [Rack Mounting](#)

### SELECTING A LOCATION

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

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



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

### RACK MOUNTING

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



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

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

## CONNECTING THE DECRU DATAFORT APPLIANCE

---

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

- [System Card Insertion](#)
- [Rear Panel Network Connections](#)
- [Power Connection](#)

### SYSTEM CARD INSERTION

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

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

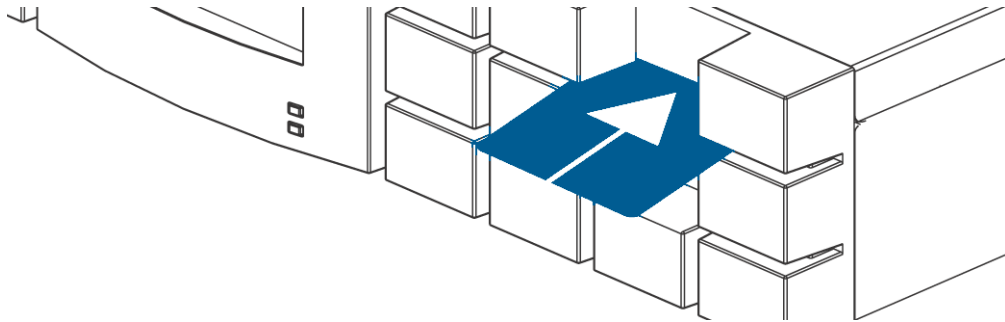


*Figure 4-3: The front panel slot housing the System Card*

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

### REAR PANEL NETWORK CONNECTIONS

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

- [Ethernet Connection](#)
- [SCSI Connection](#)
- [Serial Console Port](#)

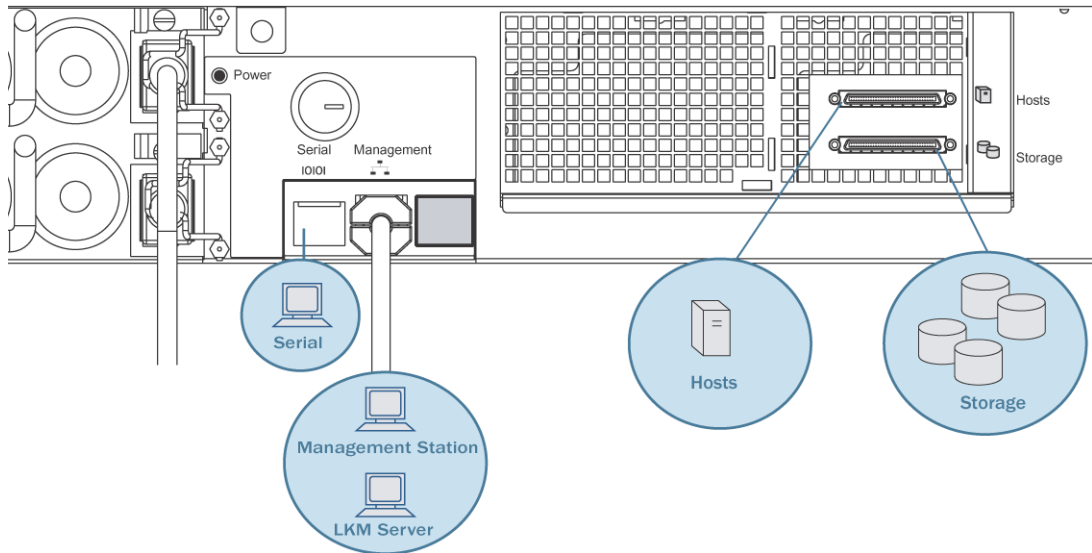


Figure 4-4: Rear panel connections

### Ethernet Connection

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

### SCSI Connection

Connect the host to the DataFort host SCSI port and the storage to the DataFort storage SCSI port. DataFort supports daisy-chaining SCSI devices and can encrypt data sent to all devices on the chain.

**CAUTION:** ONLY USE LVD CABLES TO CONNECT DATAFORT SCSI PORTS.

### Serial Console Port

Use only the supplied RJ45 to DB9 adapter and standard straight through Ethernet cable to connect a workstation or serial switch to the serial console port on the DataFort appliance's rear panel.

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

### POWER CONNECTION

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

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

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

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

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

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

**Note:** Leave DataFort powered on for normal operation. See [Powering Up and Shutting Down](#) on page 36 for instructions on powering off the appliance.

## ASSIGNING THE DATAFORT IP ADDRESS

---

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

### 2U DataFort

Assign the DataFort IP settings using the touch-sensitive buttons on the front panel LCD as described in [Setting the IP Address Using the LCD](#), or the serial console port, as described in [Setting the IP Address Using the Serial Console](#). The LCD can only be used to configure IP settings for an uninitialized DataFort.

### SETTING THE IP ADDRESS USING THE LCD

1. Touch the Details button.
2. Touch the Menu button. The screen shows the NIC Setting entry. (If not, touch either the up or down arrow to scroll the menu to the correct entry.)



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



6. When you have finished entering the Management Port address, touch Next. The touch panel screen displays a keypad of numbers, and selectable fields for the Management Port netmask. A default entry of 255 is in place for the first field.
7. Touch the entry field to highlight it, and then touch the keypad buttons to enter each number.
8. Touch Next. The touch panel screen displays a keypad of numbers and fields for the gateway.
9. Touch the entry field to highlight it, and then touch the keypad buttons to enter each number. Use the decimal point to tab to the next field automatically.
10. Touch Next. Review the DataFort IP settings.



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

### SETTING THE IP ADDRESS USING THE SERIAL CONSOLE

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

The main menu will appear. The serial console menu offers the following options:

- ```
1. Configure Network Interface - not configured
   IP Address                  : (not set)
   Netmask                    : (not set)
   Default Gateway Address    : (not set)
2. Ping Default Gateway
3. Save and Exit
-----
C. Clear Current Settings
Z. Zeroize DataFort
Q. Quit
```
4. Select option **1**, and set an IP address, subnet mask and default gateway.
  5. Select option **3** to save the settings and exit the terminal window.
- Note:** DataFort serial sessions will time out after 90 seconds of inactivity. If this happens before you finish and save your configuration, log in again. Settings will not be saved until the Save and Exit command has been completed.

## POWERING UP AND SHUTTING DOWN

---

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

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

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

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

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

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

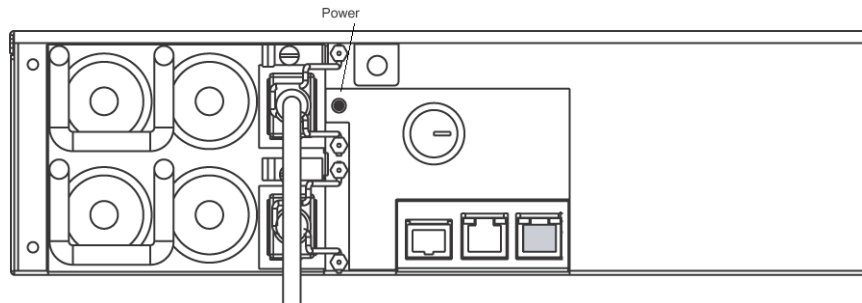


Figure 4-5: Rear panel power port and button

## ■ ■ ■ ■ 5 INITIALIZING DATAFORT APPLIANCES

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

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

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

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

## ABOUT THE SETUP WIZARD

Consider the following when running the wizard:

- Initialization of a new DataFort appliance creates the first Full Administrator for that DataFort or DataFort cluster.
- Security settings established during this procedure require the full team of Recovery Officers. Be sure to have all smart cards and Recovery Officers available for initialization.
- To expedite setup, collect information described in [Collecting Network Information](#) on page 25.

## 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                                                     | <a href="#">Initializing a Standalone DataFort or DataFort Cluster</a> on page 39. The new appliance must be initialized and connected to the network.                                               |
| Set up a new cluster                                                                  | <a href="#">Initializing a Standalone DataFort or DataFort Cluster</a> on page 39. All cluster members must be initialized and connected to the network.                                             |
| Add a new member to an existing cluster                                               | <a href="#">Adding a Member to a Cluster</a> on page 49. A configured standalone appliance must already be set up. The new appliance to be added must be initialized and connected to the network.   |
| Set up a new appliance with an existing saved configuration (restore a configuration) | <a href="#">Restoring a DataFort Appliance</a> on page 155. A saved prior configuration must be accessible to the new appliance. The new appliance must be initialized and connected to the network. |

## ABOUT SMART CARDS AND READERS

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

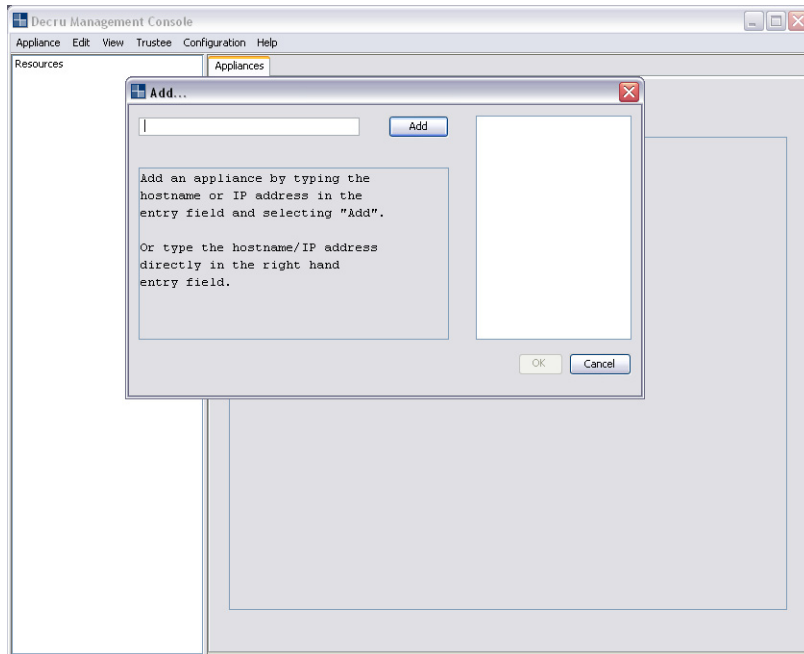
You can choose to connect multiple smart card readers to the Management Station, thereby making it possible to complete the wizard without having to switch cards. For example, if 2 out of 5 cards are required to initialize a cluster and two card readers are connected, both required Recovery Cards can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

## INITIALIZING A STANDALONE DATAFORT OR DATAFORT CLUSTER

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

DMC will start.

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



2. Enter the IP address or hostname of all appliances that will be set up.  
More than one appliance can be added on this screen: enter the IP address or hostname for each appliance in the single field provided and click Add after each, or add all IP addresses or hostnames directly into the pane on the right side of the screen.
3. Click OK when all addresses or hostnames are entered.
4. A certificate validating the connection between each appliance and the Management Console appears, choose to trust the certificate once or always.  
The added appliances will appear in the DMC.
5. From the Resources pane, right-click the first appliance you will configure, and choose Set up.  
The Welcome page of the Wizard appears.
6. Click Start.

## CONNECT TO HEAD OF CLUSTER

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

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

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

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

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

## SIGN LICENSE AGREEMENT

Agree to the license terms to continue the wizard.

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

## RECOVER FROM DATABASE

Use this page of the wizard **ONLY** if this DataFort will replace a previously existing DataFort and a configuration database from that previous DataFort will be used to configure this new DataFort. For information about this feature, see [Restoring a DataFort Appliance](#) on page 155.

- Click Next to skip the Recover from Database screen.

## CREATE ADMINISTRATOR

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

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

1. Enter a username for the administrator.
2. Enter and confirm a password for the administrator 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.

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

## CONFIGURE CLUSTER AND RECOVERY SCHEMA

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

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

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

## Setting the Recovery Schema

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

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

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

Decru Appliance Setup Wizard Step 6 of 12

**Configure Cluster and Recovery Schema**

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

Cluster size is the desired total number of Appliances in the cluster.

IPsec Shared Secret is required for communication within a cluster.

Recovery Schema: 2 out of 5

Cluster Size: Standalone

Shared Secret: (minimum 8 and maximum 30 characters)

Confirm Secret:

Buttons: Cancel, < Back, Next >

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

## Setting the Cluster Size

1. Select standalone or cluster size.

### Standalone

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

### Cluster

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

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

Decru Appliance Setup Wizard Step 6 of 12

**Configure Cluster and Recovery Schema**

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

Cluster size is the desired total number of Appliances in the cluster.

IPsec Shared Secret is required for communication within a cluster.

Recovery Schema: 2 out of 5

Cluster Size: 2

Shared Secret: (minimum 8 and maximum 30 characters)

Confirm Secret:

Buttons: Cancel, < Back, Next >

2. Click Next to proceed.

## NETWORK SETTINGS

Enter the appropriate network settings.

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

### Standalone Network Settings

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

Decru DataFort™ Appliance Setup Wizard - Step 7 of 12

**Introduce Cluster Members**

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

|              |                                            |
|--------------|--------------------------------------------|
| Hostname 1   | <input type="text" value="scsi2"/>         |
| IP Address 1 | <input type="text" value="10.101.17.11"/>  |
| Netmask 1    | <input type="text" value="255.255.248.0"/> |
| Gateway 1    | <input type="text" value="10.101.20.1"/>   |
| SCSI ID 1    | <input type="text" value="7"/>             |

Cancel      < Back      Next >

1. Enter a hostname for this DataFort.  
The IP address, Netmask and Gateway set for the Clients NIC will appear. (These were set when [Assigning the DataFort IP Address](#) on page 33.)
2. Assign a unique SCSI ID to the DataFort. It is recommended that the SCSI ID of the host connected to the DataFort host SCSI port be used. This will ensure that the ID is not being used by any device attached to the DataFort storage SCSI port.
3. Click Next.

## Cluster Network Settings

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

Decru DataFort™ Appliance Setup Wizard Step 7 of 12

**Introduce Cluster Members**

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

Hostname 1: scsi2

IP Address 1: 10.101.17.11

Netmask 1: 255.255.240.0

Gateway 1: 10.101.20.1

SCSI ID 1: 7

Hostname 2:

IP Address 2:

Netmask 2:

Gateway 2:

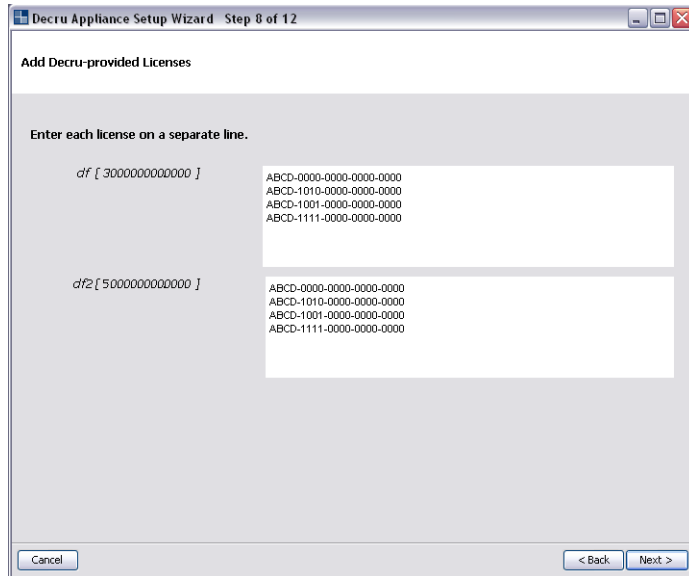
SCSI ID 2:

Cancel < Back Next >

1. Enter a hostname for the first DataFort.  
The IP Address, Netmask and Gateway set for the first DataFort will appear. (These were set when [Assigning the DataFort IP Address](#) on page 33.)
2. Assign a unique SCSI ID to the first DataFort. It is recommended that the SCSI ID of the host connected to the DataFort host SCSI port be used. This will ensure that the ID is not being used by any device attached to the DataFort storage SCSI port.
3. Enter a hostname for additional cluster members.
4. Enter IP Address, Netmask and Gateway information for additional cluster members.
5. Assign a unique SCSI ID to the second DataFort.  
**Note:** When setting up a cluster there may be a delay while the first member is being set up. This can mean that the Next button will not be available for 30 seconds or more.
6. Click Next.
7. Accept the certificate once or always.

## ADD LICENSES

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



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

## NETWORK AND CERTIFICATES

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

### DNS

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

### Certificate

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

1. Enter a name for the appliance.
2. Enter the country code for your location. The country code is limited to two characters in length. For the United States, enter **us**. Other codes are listed in [Partial List of ISO Country Codes](#) on page 190.
3. Enter the rest of the required information about your location.
4. Click Next.

## INSERT RECOVERY CARD

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

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

Decru Appliance Setup Wizard Step 10 of 12

**Initialize Recovery Card**

Ask the Recovery Officer to pick a label and password for this new Recovery Card.  
Use the Security Domain field to help you group related cards.

Card ID: 0900000096e3fffb9bc4b6d86a7e6a446c6ce9e8

Card Label:

Security Domain:

New Password:

Confirm Card Password:

Buttons: Cancel, < Back, Next >

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

### Uninitialized Card

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

### Initialized Card

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

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

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

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

## APPLY SETTINGS

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

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

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

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

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

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

## ADDING A MEMBER TO A CLUSTER

---

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

- You will need the cluster quorum of Recovery Officers with their cards, and the shared secret of the cluster, as well as licenses for all cluster members.
- 1. Choose **Start > Programs > Decru > Decru Management Console**.  
DMC will start.
- 2. From the Resources pane, choose **Appliance > Add** to open the Add... pop-up screen.
- 3. Enter the IP address or hostname of the appliance that will be added to the cluster.  
More than one appliance can be added on this screen: enter the IP address or hostname for each appliance in the single field provided and click Add after each, or add all IP addresses or hostnames directly into the pane on the right side of the screen.
- 4. Click OK when all addresses or hostnames are entered.
- 5. A certificate validating the connection between each appliance and the Management Console appears, choose to trust the certificate once or always.  
The added appliance will appear in the DMC.
- 6. From the Resources pane, right-click an **existing** member of the cluster or a standalone appliance and choose Set up.  
**Note:** Do not select the new DataFort that will be added. Select the already-configured standalone appliance or an existing member of the cluster.  
The Welcome page of the Wizard appears.
- 7. Click Start.

## LOG IN TO HEAD OF CLUSTER

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

## CLUSTER AND RECOVERY SCHEMA

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

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

## NETWORK SETTINGS

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

1. Enter a hostname for the new appliance.
2. Enter IP Address, Netmask and Gateway information for the new appliance.
3. Assign a unique SCSI ID to the appliance. It is recommended that the SCSI ID of the host connected to the DataFort host SCSI port be used. This will ensure that the ID is not being used by any device attached to the DataFort storage SCSI port.

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

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

## ADD LICENSES

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

## NETWORK AND CERTIFICATES

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

### DNS

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

### Certificate

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

1. Enter a name for the appliance.
2. Enter the country code for your location. The country code is limited to two characters in length. For the United States, enter **US**. Other codes are listed in [Partial List of ISO Country Codes](#) on page 190.
3. Enter the rest of the required information about your location and click Next.

### INSERT RECOVERY CARD

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

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

### APPLY SETTINGS

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

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

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

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

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

## 6 DATAFORT MANAGEMENT INTERFACES

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

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

## MANAGEMENT INTERFACES OVERVIEW

After initial setup is complete use the management interfaces to configure and manage the DataFort appliance. The available management interfaces are summarized in Table 5.

**TABLE 5: MANAGEMENT INTERFACES**

| Interface                                                    | Description                                                                                                                                                                                                                                                           | Usage                                                                                                                                                                                   |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure Sockets Layer (SSL)<br>Transport Layer Security (TLS) | A secure HTTP (HTTPS) connection to the DataFort WebUI via a web browser from the Management Station. Can be configured to require smart card authentication in addition to the administrator password. See <a href="#">Connecting to the DataFort WebUI</a> .        | Primary method for creating and managing Cryptainers, DataFort settings, users, etc.                                                                                                    |
| Secure Shell (SSH)                                           | A secure shell connection to DataFort CLI (command line interface) via secure shell client. Can be configured to require smart card authentication in addition to the administrator password. See <a href="#">Connecting to the DataFort Command Line Interface</a> . | Alternative method for creating and managing Cryptainers, DataFort settings, users, etc. Also used for some advanced system configuration.                                              |
| Serial                                                       | A serial connection to DataFort can be used to enter network settings for an uninitialized DataFort. See <a href="#">Serial Console</a> .                                                                                                                             | Set, clear, or reset DataFort IP settings. Zeroize DataFort when other interfaces are not available.                                                                                    |
| LCD                                                          | The DataFort front panel displays messages. The 2U DataFort appliance front panel also functions as an interactive touch screen. See <a href="#">DataFort Front Panel LCD</a> .                                                                                       | View DataFort status and throughput information at a glance. Use 2U DataFort touch panel buttons to enter initial IP settings and get information about errors and status.              |
| SNMP                                                         | Allows an SNMP tool (such as HP OpenView) to get read-only status information from DataFort. The standard MIB-II MIBs are exposed, as well as Decru's proprietary MIB. See <a href="#">SNMP Settings</a> .                                                            | View DataFort status via SNMP tool. No secure information is permitted over this protocol (read only, no set commands).                                                                 |
| Decru Management Console (DMC)                               | A Java tool used for setup and management of LKM and DataFort appliances. DMC provides a centralized management interface for all appliances in an installation. See <a href="#">Accessing the Decru Management Console</a> .                                         | The only way to set up an appliance using the Setup Wizard. The only management interface for the LKM appliance. Provides some additional management functions for DataFort appliances. |
|                                                              | A limited DMC is shipped with each DataFort appliance. The full DMC product supports <a href="#">SecureView</a> .                                                                                                                                                     |                                                                                                                                                                                         |
|                                                              | <a href="#">SecureView</a> feature of Management Console                                                                                                                                                                                                              | Enables many-at-once control of LKM and DataFort appliances. Requires SecureView license on all appliances that will be managed simultaneously.                                         |

## SECUREVIEW

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

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

## SECURITY POLICIES

Security policy settings determine whether an Admin Card is required for logging in to the WebUI or CLI of an appliance. By default, DataFort is set not to require an Admin Card for WebUI or CLI access. To turn on Secure Web or Secure CLI (which require the presence of an Admin Card to log into DataFort), customize the security policy as described in [Configuring Management Security Settings](#) on page 100.

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

## ONLINE HELP

Use the Decru Management Console to access online help for the DataFort appliance. Selecting an appliance in DMC and choosing the Help menu will open an online version of the administrative guide for the selected appliance. See [Decru Management Console Menus](#) on page 144 for details about the DMC Help menu.

## CONNECTING TO THE DATAFORT WEBUI

---

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

### USING THE DATAFORT WEBUI

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

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

### CONNECTING VIA WEBUI

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

1. From Internet Explorer on the Management Station, enter **https://** followed by the IP address or resolvable hostname assigned to DataFort. (Be sure to enter https.)  
**Note:** TLS 1.0 must be enabled as described in [Preparing the Management Station](#) on page 25.
2. Click Yes to acknowledge the security certificate message.
3. Click Yes to agree to load the Decru management applet.

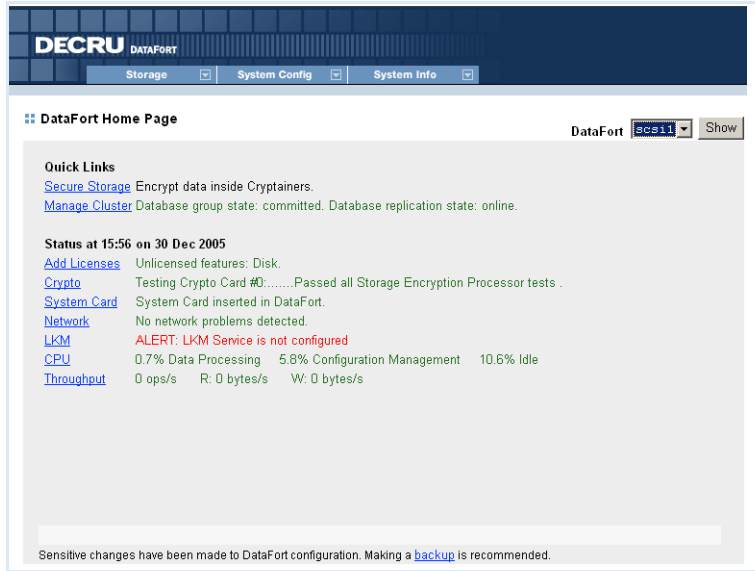
The DataFort Login page appears.

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

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

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

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



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

- D+T** SCSI Devices
- D+B** Back Up Configuration
- D+L** Log
- D+C** LCD
- D+W** WebCLI

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

### QUICK LINKS AND STATUS

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

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

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

**Note:** If the DataFort defense response has been triggered, a warning will appear on the Home page. DataFort will not accept any management commands in this state. To address this warning, see [Clearing a Defense Alert](#) on page 98.

### Cluster Member Access

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

### CONNECTING VIA WEBUI USING DUAL AUTHORIZATION

By default, all administrators created using the DataFort WebUI can log in to the WebUI without additional authorization. By default, administrators created using the CLI will require prior authentication before they can log in to the WebUI or CLI. In addition, if the login privilege is revoked for a given administrator, that administrator will require the presence of an authorizing administrator in order to log in to the WebUI or CLI. See [Requiring Authorization for Login](#) on page 70 for details. The authorizing administrator can be any administrator who does not require authorization.

To log in when dual authentication is required:

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

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

## CONNECTING TO THE DATAFORT COMMAND LINE INTERFACE

---

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

A Full Administrator or Key Administrator can turn on the smart card requirement (Secure CLI) by connecting to the WebUI and accessing the Security Policy settings page, as described in [Configuring Management Security Settings](#) on page 100. Secure CLI requires that a session-specific password be furnished via the WebUI before the administrator can log in.

### USING THE CLI

- See [Using the CLI](#) on page 163 for information about CLI online help.
- As a security measure, the CLI times out after 10 minutes of inactivity.

### CONNECTING VIA STANDARD CLI

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

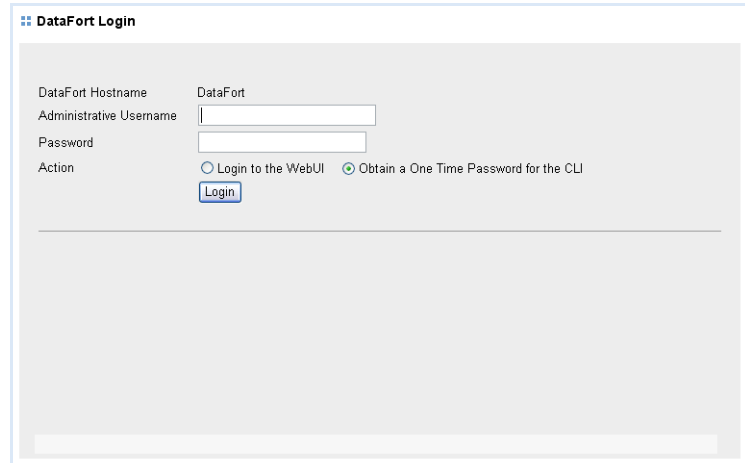
1. Open an SSH client on a workstation connected to the same network as the DataFort.
2. Enter the IP address or hostname assigned to DataFort.
3. In the terminal window, enter the administrator login name and password.

### CONNECTING VIA SECURE CLI

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

1. Insert the Admin Card of a valid administrator into the Management Station smart card reader and access the WebUI Login page from the Management Station as described in [Connecting to the DataFort WebUI](#) on page 55.
2. Click the button: Obtain a One Time Password for the CLI.

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

The image shows a web-based login form titled "DataFort Login". It contains the following fields and options: "DataFort Hostname" with the value "DataFort"; "Administrative Username" with an empty text input field; "Password" with an empty text input field; and "Action" with two radio buttons: "Login to the WebUI" (unselected) and "Obtain a One Time Password for the CLI" (selected). Below the radio buttons is a "Login" button. The form is enclosed in a light gray border with a blue title bar.

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

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

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

### CONNECTING VIA CLI USING DUAL AUTHORIZATION

By default, all administrators created using the DataFort WebUI can log in to the WebUI without additional authorization. By default, administrators created using the CLI will require prior authentication before they can log in to the WebUI or CLI. In addition, if the login privilege is revoked for a given administrator, that administrator will require the presence of an authorizing administrator in order to log in to the WebUI or CLI. See [Requiring Authorization for Login](#) on page 70 for details. The authorizing administrator can be any administrator who does not require authorization.

To log in to CLI when dual authentication is required:

1. First the administrator with authorization privileges must log in. Open an SSH client on a workstation connected to the same network as the DataFort.

2. Enter the IP address or hostname assigned to DataFort.
3. In the terminal window, enter the administrator login name and password.
4. At the prompt, enter:

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

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

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

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

## CONNECTING TO CLI VIA WEBUI

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

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

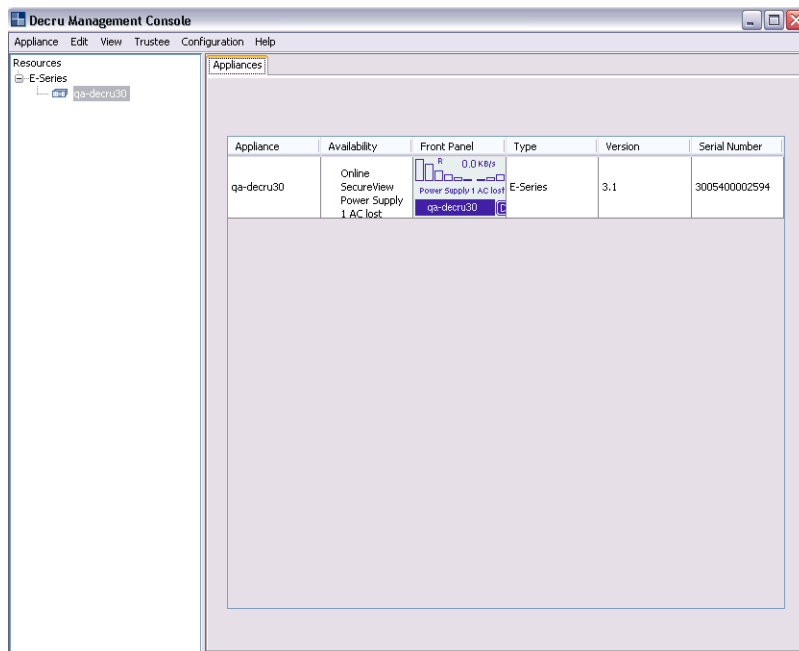
**Note:** WebCLI does not support the following features: command history, command line editing and completion, output paging and context-sensitive help.

## ACCESSING THE DECRU MANAGEMENT CONSOLE

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

- Choose **Start > Programs > Decru > Decru Management Console** from the Management Station. Any appliances which have been added to DMC will appear.
- See [Decru Management Console Menus](#) on page 144 for a description of the menu options.

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



## SERIAL CONSOLE

---

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

Use only the supplied crossover RJ45 to DB9 adapter and standard straight through Ethernet cable to connect to the serial console port on the DataFort's rear panel. See [Serial Console Port](#) on page 32 for details.

### LOGGING IN TO THE SERIAL CONSOLE PORT

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

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

### CONFIGURING IP SETTINGS

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

### CLEARING IP SETTINGS

The serial console can be used to temporarily set a new IP address for the DataFort in order to manage it from a new network. After a reboot, the original settings are restored. This feature is meant to be used when DataFort is being moved to a different network but zeroization is not required. When a DataFort is moved to a different network that does not recognize the DataFort IP address, the administrator can temporarily clear the settings so that access via WebUI and CLI are possible. To change the IP settings permanently, see [Network Settings](#) on page 125.

1. At the shell prompt, log in using the administrator name and password assigned to the administrator (note that these entries are space and case sensitive).  
The main menu will appear.
2. Select option **C**.  
The IP settings will be cleared.
3. Select option **3** to save the settings, and exit the terminal window.

### ZEROIZING DATAFORT

Enter the zeroize command from the serial console to return the DataFort appliance to an uninitialized state. See [Zeroization Using the Serial Console](#) on page 118 for details.

DATAFORT FRONT PANEL LCD

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

The left side of the graph indicates the rate (in bytes per second) at which DataFort reads data, or decrypts encrypted data. The right side of the graph depicts the rate at which DataFort writes, or encrypts data.

TABLE 6: READ/WRITE RATE DISPLAY ON 2U DATAFORT APPLIANCES

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

Touch Panel Onscreen Buttons

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

- Menu

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

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

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

SNMP SETTINGS

DataFort supports both MIB II and the read-only private Decru MIB. The Decru MIB is included on the DataFort CD. It provides standard MIB-II as well as Decru MIB messages. All Decru MIBs are read-only for security reasons. See [SNMP Settings](#) on page 132 for details.



## 7 DATAFORT ADMIN ROLES AND ACCOUNT ADMINISTRATION

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

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

ADMINISTRATOR ROLES

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

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

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

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

If desired, compound administrators possessing the characteristics of more than one specialty administrator can also be created. It may be useful for example to have several combined Machine, Storage and Key Administrators, but leave the Security and Account roles for a few highly-trusted individuals. See [Administrator Roles and Privileges](#) on page 65 for details.

TABLE 7: ADMINISTRATOR ROLES AND PRIVILEGES

| Role Name          | Privileges                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full Administrator | The Full Administrator sets up each DataFort or DataFort cluster for the first time by running a setup wizard as described in <a href="#">Initializing DataFort Appliances</a> . The Full Administrator can complete all administrative tasks including: <ul style="list-style-type: none"><li>• <a href="#">Initializing DataFort Appliances</a></li><li>• <a href="#">Account Administration</a></li><li>• <a href="#">Storage Administration</a></li><li>• <a href="#">Key Administration</a></li><li>• <a href="#">Backup Administration</a></li><li>• <a href="#">Physical Security Administration</a></li><li>• <a href="#">Cluster Administration</a></li><li>• <a href="#">Machine Administration</a></li></ul> |

**TABLE 7: ADMINISTRATOR ROLES AND PRIVILEGES (CONTINUED)**

| Role Name               | Privileges                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Accounts Administrator  | <p>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 <a href="#">Account Administration</a>:</p> <ul style="list-style-type: none"> <li>• Add and delete administrators</li> <li>• Create specialty administrators</li> <li>• Change administrator roles</li> <li>• Associate administrators with smart cards</li> <li>• Specify that an administrator requires login authorization</li> </ul>                                                                                                                                                                                                                  |
| Storage Administrator   | <p>A Storage Administrator manages host and storage devices and tape pools. Storage Administrator tasks are described in <a href="#">Storage Administration</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Key Administrator       | <p>A Key Administrator is responsible for applying security-related settings to DataFort appliances as described in <a href="#">Key Administration</a>, as well as the ability to create or delete a Cryptainer as described in <a href="#">Storage Administration</a>. Key Administrator tasks include:</p> <ul style="list-style-type: none"> <li>• <a href="#">Managing Trustees</a> as well as importing and exporting exportable keys</li> <li>• Purging keys upon backup to LKM as described in <a href="#">Key Purging</a></li> <li>• <a href="#">Managing DataFort Defense Responses</a></li> <li>• <a href="#">Configuring Management Security Settings</a></li> <li>• <a href="#">Managing Recovery Officers and Recovery Cards</a></li> </ul> |
| Security Administrator  | <p>A Security Administrator is responsible for applying physical security-related settings to DataFort appliances as described in <a href="#">Physical Security Administration</a>. Security Administrator tasks include:</p> <ul style="list-style-type: none"> <li>• <a href="#">Setting Date and Time</a></li> <li>• <a href="#">Configuring and Viewing Logs</a></li> <li>• <a href="#">Zeroizing the Decru DataFort</a></li> </ul>                                                                                                                                                                                                                                                                                                                  |
| Backup Administrator    | <p>A Backup Administrator is responsible for managing backups of the configuration database, including those to LKM. Backup Administrator tasks described in <a href="#">Backup Administration</a> include:</p> <ul style="list-style-type: none"> <li>• <a href="#">Saving Configurations to Lifetime Key Management Software</a></li> <li>• <a href="#">Downloading Configurations to a Remote Location</a></li> </ul>                                                                                                                                                                                                                                                                                                                                 |
| Machine Administrator   | <p>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 <a href="#">Machine Administration</a> include:</p> <ul style="list-style-type: none"> <li>• <a href="#">Network Settings</a></li> <li>• <a href="#">Upgrading DataFort</a></li> <li>• <a href="#">Setting Security Certificates</a></li> <li>• <a href="#">Managing Licenses</a></li> <li>• <a href="#">SNMP Settings</a></li> <li>• The Machine Administrator can also add cluster members as described in <a href="#">Cluster Administration</a>.</li> </ul>                                                                   |
| Read-Only Administrator | <p>A Read-Only Administrator can view all DataFort settings (see <a href="#">DataFort Appliance Settings and Status</a>) and can view status and logs, but cannot modify settings.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## ACCOUNT ADMINISTRATION

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

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

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

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

### ADDING AN ADMINISTRATOR

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

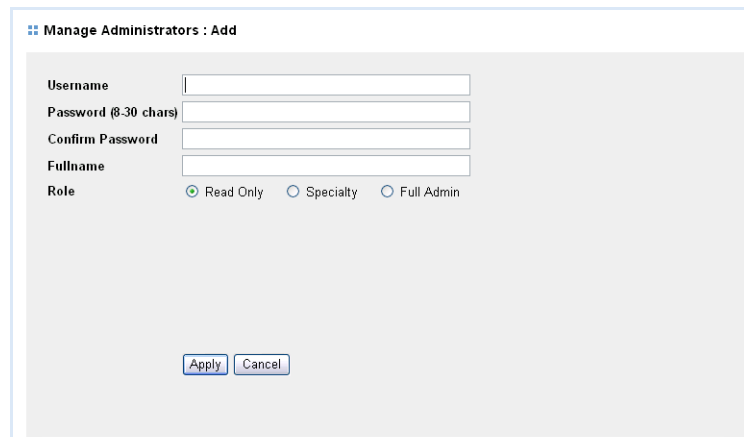
Administrators known to this DataFort appliance are listed.

The screenshot displays the 'Manage Administrators' interface. At the top, it says 'Cluster-wide'. Below this, there's a section titled 'Administrators' with a table. The table has four columns: 'Administrator', 'Fullname', 'Role', and 'Has Card'. The first row shows 'admin' as the administrator, 'admin' as the fullname, 'san-admin' as the role, and 'y' as the has card status. Below the table, there are buttons for 'Add...', 'Edit...', 'Delete', and 'Refresh'. To the right of these buttons are two more buttons: 'Associate Card' and 'Authorize Login'.

| Administrator | Fullname | Role      | Has Card |
|---------------|----------|-----------|----------|
| admin         | admin    | san-admin | y        |

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

3. Click Add.



**Manage Administrators : Add**

Username

Password (8-30 chars)

Confirm Password

Fullname

Role ☒ Read Only ☐ Specialty ☐ Full Admin

4. Enter the name of the new administrator, and a password for that administrator. Strong passwords are an important part of the overall security of the system. Select a password consisting of at least 8 valid, randomly chosen characters.  
  
Passwords may be composed of upper and lower case characters, numbers and special characters. Note that double quotes and backslashes are not permitted.
5. Confirm the password.
6. Enter a full name for the administrator.
7. Select the type of administrator you want to create. The default selection is Read Only. See [Administrator Roles](#) on page 65 for details. You can also require that an administrator be authenticated before being able to log in to DataFort. See [Requiring Authorization for Login](#) on page 70 for more information.

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

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

**Manage Administrators : Add**

Username:

Password (8-30 chars):

Confirm Password:

Full Name:

Role: ☐ Read Only ☒ Specialty ☐ Full Admin

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

8. Click Apply.

**Manage Administrators** Cluster-wide

| Administrator  | Fullname       | Role               | Has Card |
|----------------|----------------|--------------------|----------|
| 321            | 321321321      | san-storage-admin  | n        |
| Security Admin | Security Admin | san-security-admin | n        |
| admin          | admin          | san-admin          | y        |

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

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

## REQUIRING AUTHORIZATION FOR LOGIN

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

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

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

For instructions on creating an administrator requiring prior authentication see:

- [Creating an Administrator Requiring Authorization Using the WebUI](#)
- [Creating a New Administrator Using the CLI](#)

## Protecting Against Insider Attacks

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

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

## Creating an Administrator Requiring Authorization Using the WebUI

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

**Manage Administrators : Edit security administrator**

**Fullname**

**Login** ☐ Direct ☒ Requires Prior Authorization

**Role** ☒ Specialty ☐ Full Admin

☒ Security ☐ Storage ☐ Machine

**Change Password:**

**Current**

**New**

**Confirm**

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

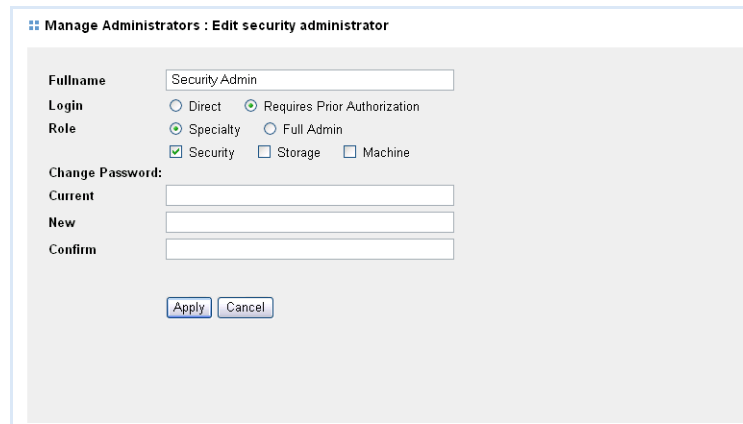
Now this administrator will need authorization to log in to the DataFort. See [Connecting via WebUI using Dual Authorization](#) on page 57 for authorizing WebUI login, and [Connecting via CLI using Dual Authorization](#) on page 59 for authorizing CLI login.

**Note:** To remove the requirement for login authorization, access the same page, deselect Requires Prior Authorization, and click Apply.

### CHANGING THE ADMINISTRATOR PASSWORD

Administrator passwords can be changed periodically if desired as a security measure. The administrator who is logged in can change only his or her own password.

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



The screenshot shows a web form titled "Manage Administrators : Edit security administrator". The form contains the following fields and options:

- FullName:** A text input field containing "Security Admin".
- Login:** Two radio button options: "Direct" (unselected) and "Requires Prior Authorization" (selected).
- Role:** Two radio button options: "Specialty" (selected) and "Full Admin" (unselected).
- Specialty Options:** Three checkboxes: "Security" (checked), "Storage" (unchecked), and "Machine" (unchecked).
- Change Password:** A section with three text input fields labeled "Current", "New", and "Confirm".
- Buttons:** "Apply" and "Cancel" buttons at the bottom.

4. Enter the current password for the administrator.

5. Enter the new password and confirm the entry.

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

6. Click Apply.

The password will be changed.

## REMOVING AN ADMINISTRATOR

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

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

## CHANGING A CARD ASSOCIATION

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

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



## ■ ■ ■ ■ 8 BEFORE STORAGE ADMINISTRATION

DataFort is ready to encrypt data after the Setup Wizard is complete, but you may wish to take additional steps to prepare for data encryption and DataFort operation.

The following should be completed after running the Setup Wizard and before encrypting data:

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

These operations are performed using the WebUI. For login instructions see [Connecting to the DataFort WebUI](#) on page 55. Note that the Decru Management Console (DMC) can also be used to perform some of these operations. See [Chapter 16](#) for DMC menu options.

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

## CHECKING CLUSTER STATE

---

A cluster must be in a committed/online state for proper operation. The DataFort WebUI Home page of any cluster member will display the status of the cluster at the Manage Cluster quick link. See [Checking the Status of the Cluster](#) on page 120 for information about cluster states.

## CONFIGURING REMOTE LOGGING

---

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

- From the WebUI, choose **System Config > General > Configure Log**.
- Determine which log messages should be sent to a remote syslog server on your network. See [DataFort Log Storage Guidelines](#) on page 111 for details.

## STARTING LKM

---

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

- Before configuring DataFort, set up the LKM management solution. See [Setting Up Lifetime Key Management](#) on page 27.

### LKM SERVER

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

- From the WebUI, click the LKM link or choose **System Config > Recovery > LKM Settings**.
- Set the LKM server information for automatic backup. See [Saving Configurations to Lifetime Key Management Software](#) on page 106. All LKM settings are propagated across cluster members, therefore it is sufficient to enter LKM settings once for each cluster.

### LKM APPLIANCE

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

## CONFIGURING TAPE SETTINGS

---

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

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

## CREATING ADDITIONAL ADMINISTRATORS

---

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

It may be desirable to create distinct administrators responsible for certain tasks, as outlined in [DataFort Admin Roles and Account Administration](#).

- From the DataFort WebUI, choose **System Config > System Users > Administrators**.
- Create an additional administrator. If desired, associate one or both administrators with an Admin Card. See [Adding an Administrator](#) on page 67 for instructions.

## VERIFYING SYSTEM VERSION

---

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

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

## DETERMINING THE DEFENSE SETTING

---

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

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

To configure the defense setting:

- From the WebUI, choose **System Config > Security > Defense Settings**.
- Choose the appropriate defense setting. See [Defense Triggers and Responses](#) on page 96.

## ■ ■ ■ ■ 9 STORAGE ADMINISTRATION

This chapter includes instructions for using the DataFort WebUI to manage secure storage. A Full Administrator is assumed to have completed installation and preparation of DataFort appliances. A Full Administrator can perform all of the functions outlined in this chapter.

Once installed, DataFort will monitor backup activity on the SCSI network, after which SCSI devices will appear in the DataFort WebUI automatically, with associated pools assigned. A yellow L icon will indicate the existence of a pool that was learned by DataFort during a backup.

The default tape settings configured using the SCSI Tape Settings Page will be applied to all discovered tapes unless specifically modified on a per tape or per pool basis using the Tape Management menus.

SCSI storage administration involves the following:

- [Managing Tape Settings](#)
- [Securing Data on SCSI Devices](#)
- [Managing SCSI Devices](#)
- [Managing Tapes](#)
- [Changing SCSI Settings](#)

## MANAGING TAPE SETTINGS

Access the **SCSI Tape Settings** page to configure settings for the DataFort, including those for pools and tapes. This page will only appear if a license controlling tape features is installed on DataFort.

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

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

- Right-click in the Tape Management pane and select Settings.
2. Select the desired setting and click Apply to set the changes. Tape settings include:
    - [Pool Settings and Defaults](#)
    - [Tape Settings](#)

The screenshot shows the 'SCSI Tape Settings' page with a 'Cluster-wide' label in the top right. The page is divided into two main sections: 'Pool Settings and Defaults' and 'Tape Settings'. In the 'Pool Settings and Defaults' section, 'Cleartext Default' is set to 'OFF - Auto-detected Pools will be encrypted', 'Default Pool Policy' is set to 'Pool - A key with no expiration is generated per pool', 'Tape Key Lifespans' are both set to '0 Years', 'Key Export' is set to 'ON - Pool Keys will be exportable', and 'Default Read/Write Span' is set to 'Use 0 for No expiration'. In the 'Tape Settings' section, 'Compression' is set to 'ON - If requested by hosts, data will be hardware compressed before it is encrypted'. An 'Apply' button is located at the bottom of the settings area.

### POOL SETTINGS AND DEFAULTS

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

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

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

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cleartext Default</b>   | Determines whether pools that are automatically detected by DataFort will be encrypted or not by default.                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Default Pool Policy</b> | Determines whether keys are generated per tape or per pool by default. Select per-tape to manage key life spans.                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Tape Key Lifespans</b>  | Sets the default read/write life span and read life span of the key used to encrypt tape contents. Read/write represents the span in days that the key may be used for writing. Lifespan is the span in days that the key may be used for reading. Lifespan can be specified in days, months, weeks or years. By default the lifespan of a key is infinite. Lifespan settings should be set only if key expiration is desired. This option is not available when keys are generated per pool. |
| <b>Key Export</b>          | Determines whether keys can be exported to trustees by default. See <a href="#">Managing Trustees</a> on page 89.                                                                                                                                                                                                                                                                                                                                                                             |

## Global Default Pool

The global default pool allows a single pool to be set across all hosts for applications which do not support pools. Using this feature requires that you log into the DataFort CLI and change the default settings of the DataFort appliance.

To override the application pools which are auto-detected in DataFort log in to the DataFort CLI and set `dfc.override_with_default_pool` to True:

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

To create a default pool with the global pool properties:

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

To create a default pool by specifying pool properties, first create a pool, then assign it:

```
pool add [--policy ] [-e, --exportable] [-n, --nokey] [--aclstate ]
  [--days ] [--rw-days ] system property set dfc.default_pool_name
  <pool-label>
```

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

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

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

To return to normal pool mode:

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

## TAPE SETTINGS

Tape settings section of the determine whether compression is on or off by default.

### ACL Learning

By default ACL learning mode is enabled, which on

### Compression

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

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

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

## SECURING DATA ON SCSI DEVICES

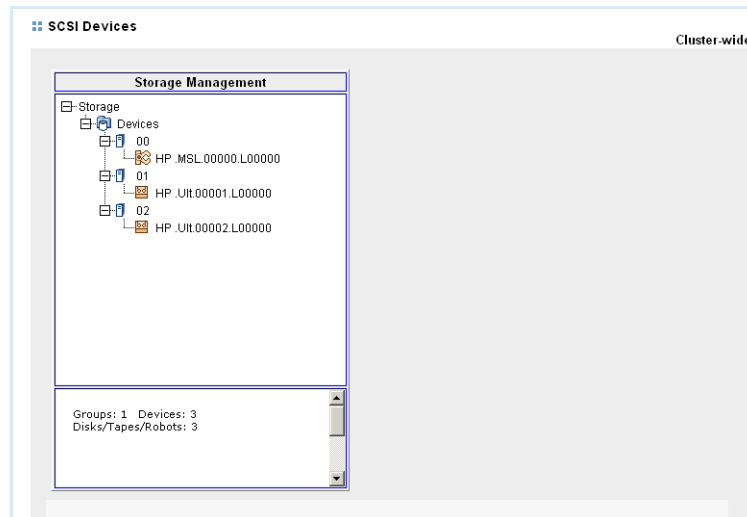
---

Use the SCSI Devices and Manage Tapes WebUI pages to manage encrypted data on SCSI devices. The SCSI Devices page shows all known SCSI devices. The Manage Tapes page is used to manage tapes and encryption keys.

**Note:** If DataFort sees a SCSI storage device but the host does not, this indicates that there is a termination issue on the host side of the DataFort appliance. Forcing termination on the HBA on the host eliminates the termination issue and allows the host to see the storage. Modify termination settings of the Host HBA card using its HBA utility.

### VIEW SCSI DEVICES

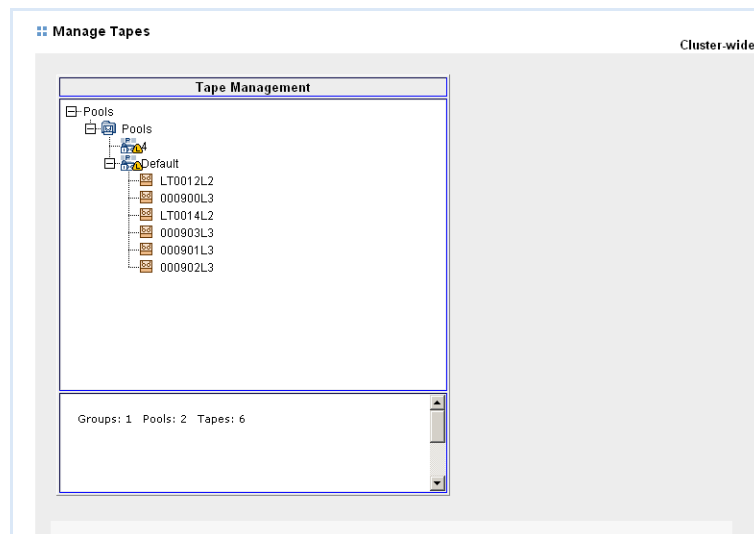
1. Log in to the WebUI as a Full Administrator or Storage Administrator. See [Connecting to the DataFort WebUI](#) on page 55 for login instructions.
2. Select **Storage > SCSI Devices** from the WebUI menu. The page is identified as a Cluster-wide display, meaning that the configuration visible on the page applies to the entire cluster.  
All known SCSI devices will appear on the page.
3. Right-click the Storage Management pane and select Expand All to see the full tree of devices.



4. Make any desired changes to the SCSI device management. See [Managing SCSI Devices](#) on page 83 for information about menu options.

## View Tapes

1. Select **Storage > Manage Tapes** from the WebUI menu.



2. All known tape devices will appear on the page.

The page is identified as a Cluster-wide display, meaning that the configuration visible on the page applies to the entire cluster.

3. Right-click the Tape Management pane and select Expand All to see the full tree of devices.

Pools are auto-created based on the pool numbers that are in use by the backup application. The tape numbers in the pool are IDs assigned to the tape by the backup application.

4. Make any desired modifications to the key management policy. See [Managing Tapes](#) on page 84 for information about menu options.

### **ASSIGN KEYS**

Unless encryption is on by default for all devices, a key must be manually assigned to encrypt data on a SCSI device.

1. Right-click a tape pool and select Assign Key...
2. Apply a new or custom key to encrypt data, or none, to leave data in cleartext form. To use a specific key for the pool, choose custom and enter the ID of the pool key you want to apply.

## MANAGING SCSI DEVICES

Access the SCSI Devices page by selecting **Storage > SCSI Devices** from the WebUI menu. Right-click in the Storage Management pane to use the top level menu.

### STORAGE MANAGEMENT PANE MENU

Use the Storage Management Pane menu to manage the SCSI Devices display.

|                        |                                                                               |
|------------------------|-------------------------------------------------------------------------------|
| Refresh                | Refresh the GUI view of the SCSI network.                                     |
| Expand All             | Expand the tree to display all devices.                                       |
| Collapse All           | Collapse the tree view to top level only.                                     |
| New Collection...      | Create a new collection of SCSI devices.                                      |
| Filter...              | Restricts the WebUI view to only the SCSI devices seen by specified DataFort. |
| Rescan                 | Scans the SCSI network for new SCSI devices.                                  |
| Cluster-wide Rescan... | Forces all DataFort appliances to rescan the SCSI network.                    |
| Purge Unused           | Remove unused devices from the WebUI.                                         |
| Show/Hide Disabled     | Toggle to view or hide disabled devices.                                      |

### STORAGE DEVICE COLLECTION MENU

Right-click a collection of devices to rename or delete it from the WebUI.

|        |                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rename | Select Rename. The name field will open in the lower pane. Enter the new name. To save the change, leave the cursor in the name field and hit Return on the Management Station keyboard. |
| Delete | Right-click the device and select Delete to remove it from the WebUI.                                                                                                                    |

### SCSI ID MENU

Right-click a SCSI ID to move, rename or disable the device in the WebUI.

|         |                                                                                                                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Move to | Move the device to a different collection.                                                                                                                                               |
| Rename  | Select Rename. The name field will open in the lower pane. Enter the new name. To save the change, leave the cursor in the name field and hit Return on the Management Station keyboard. |

|         |                                                                                                                                                                                                                                                                  |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disable | Disable will cause the selected device to disappear from the storage panel. Disabled devices will be grayed out and will not be manageable from the WebUI. To restore disabled images, right-click in the Storage Management Pane and select Show/Hide Disabled. |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### LOGICAL UNIT MENU

Right-click an entry for the logical unit to manage that device.

|           |                                                                                                                                                                                          |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Beacon On | Blink the LED on the physical disk to help identify it on the network.                                                                                                                   |
| Rename    | Select Rename. The name field will open in the lower pane. Enter the new name. To save the change, leave the cursor in the name field and hit Return on the Management Station keyboard. |
| Delete    | Right-click the device and select Delete to remove it from the WebUI.                                                                                                                    |

## MANAGING TAPES

### TAPES MANAGEMENT PANE MENU

Right-click a tape pool collection to view the tape pool collection menu.

|                   |                                                               |
|-------------------|---------------------------------------------------------------|
| Refresh           | Refresh the GUI view of the SCSI network.                     |
| Expand All        | Expand the tree to display all tapes.                         |
| Collapse All      | Collapse the tree view to top level only.                     |
| New Collection... | Create a new collection of tapes.                             |
| New Pool...       | Create a new pool for tapes.                                  |
| Settings...       | Opens the WebUI page where default settings for tape are set. |

### TAPE POOL COLLECTION MENU

Right-click a tape pool to rename or delete the pool collection.

|        |                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rename | Select Rename. The name field will open in the lower pane. Enter the new name. To save the change, leave the cursor in the name field and hit Return on the Management Station keyboard. |
| Delete | Right-click the device and select Delete to remove it from the WebUI.                                                                                                                    |

## TAPE POOL MENU

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

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Assign Key   | <p>A key is assigned to each pool discovered by DataFort. For pools which encrypt per-pool according to the Tape Settings, the key is used to encrypt any data assigned to the pool and is consistent throughout a single tape. For pools which encrypt per-tape, this key is not used for data encryption but rather as a placeholder to keep track of default key attributes for per-tape keys originating from this pool. Note that cleartext cannot be appended to ciphertext on an encrypted tape, nor can ciphertext be appended to a cleartext tape.</p> <p>Apply a new or custom key to encrypt data, or none, to leave data in cleartext form. To use a custom key, enter the ID of the pool key you want to apply.</p> |
| Manage Keys  | <p>If a key is created as an exportable key, it can be imported or exported. See <a href="#">Managing Trustees</a> on page 89 for information.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Move To      | <p>Move the selected pool to a specified collection. Multiple-select device instances by control or shift-clicking them in the Tape Management pane. Right-click and select Move to &gt; New collection...</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Edit         | <p>Opens the Edit Pool page where the Name, Key Policy and Key Export settings can be changed. See <a href="#">Edit Pool Page</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Delete Tapes | <p>Right-click the pool and select Delete Tapes to remove the tapes associated with the pool from the WebUI, but leave the pool.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Delete       | <p>Right-click the pool and select Delete to remove it from the WebUI. All tapes must be deleted before the pool will be removed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## TAPE DEVICE MENU

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

|        |                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------|
| Keys   | <p>Import or export key assigned to tape device. See <a href="#">Managing Trustees</a> on page 89 for information.</p> |
| Delete | <p>Right-click the device and select Delete to remove it from the WebUI.</p>                                           |

EDIT POOL PAGE

Right-click a pool and select Edit to view the Edit Pool page.

Manage Tapes : Edit Pool 21:00:00:e0:8b:07:bc:83\_Pool

Name

21:00:00:e0:8b:07:bc:83\_Pool

Key Policy

☒ Tape

☐ Pool

Key Read/Write Span (Days)

30

(Use 0 for No Expiration)

Key Lifespan (Days)

365

Key Exportable

☒ On

☐ Off

Apply

Cancel

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

|                     |                                                                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                | Change the alias for the pool as it is displayed in the WebUI. Note this does not change the actual pool label which DataFort uses to sync with the backup application. |
| Key Policy          | Select whether the key policy used by this pool is the one set for tapes or for the pool. These policies are defined on the Tape Settings page of the WebUI.            |
| Key Read/Write Span | Sets the read/write life span of the key used to encrypt tape contents. Read/write represents the span in days that the key may be used for writing.                    |
| Key Lifespan        | Sets the lifespan of the key assigned to tapes in the pool. Lifespan represents the span in days that the key may be used for reading.                                  |
| Key Exportable      | Select whether the key for this LUN can be exported to a trustee. See <a href="#">Managing Trustees</a> on page 89.                                                     |

## CHANGING SCSI SETTINGS

Use the SCSI Storage Settings page of the WebUI to changes SCSI ID settings for DataFort. Note that changes to this setting will require a reboot of DataFort.

1. Access the page by choosing **Storage > SCSI Settings**.

The current SCSI setting will appear.

2. Enter the new SCSI ID and click Apply.
3. Select **System Config > General > WebCLI**.
4. Enter the CLI command to power cycle DataFort:

```
system reboot -p
```



## ■ ■ ■ ■ 10 KEY ADMINISTRATION

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

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

- [Managing Trustees](#)
- [Managing DataFort Defense Responses](#)
- [Managing Recovery Officers and Recovery Cards](#)

Any administrator can reset smart cards:

- [Smart Card Reset](#)

## MANAGING TRUSTEES

---

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

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

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

### TRUSTEE SCENARIOS

The establishment of trustees enables several enterprise scenarios:

- |                               |                                                                                                                                                                                                                                                                           |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Disaster Recovery Site</b> | 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). |
| <b>HQ with branches</b>       | In a situation where there are many branch offices and it is desirable to share a different encryption key with each branch exclusively.                                                                                                                                  |
| <b>Vendors/Third parties</b>  | In a situation where a vendor and supplier both have DataFort appliances, but it is not desirable to share all keys.                                                                                                                                                      |

### SETTING UP TRUSTEES

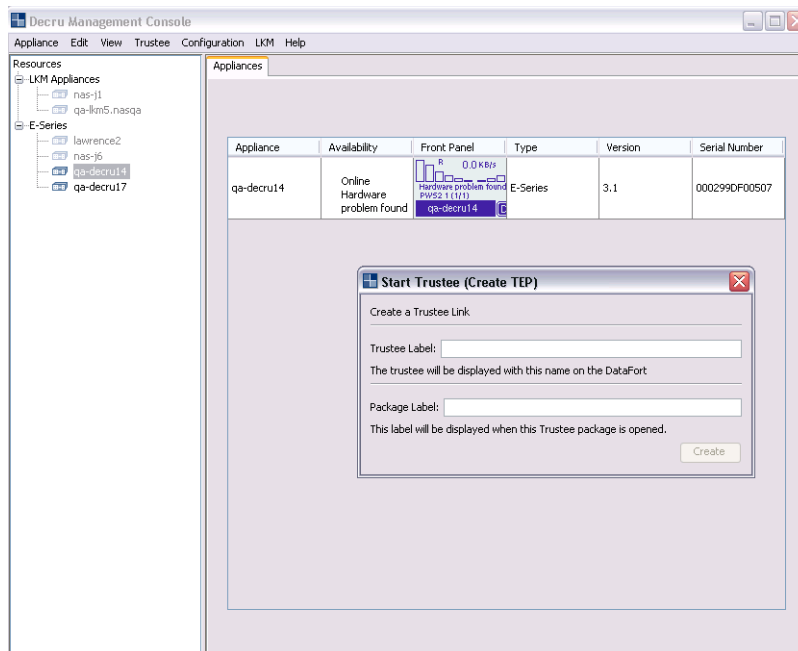
This example describes a trustee relationship between a main and a remote site. Setting up trustees requires:

- A Key or Full Administrator (with permissions to create trustees) at each site.
- The quorum of Recovery Officers and their Recovery Cards at each site/for each appliance. If the Security Setup requires 2 out of 5 cards, for example, two people will have to be present to insert their cards and enter the label name and password for the card, in order to establish trustees.
- Files and information will need to be provided by the main site administrator so that the remote site administrator can import the trust package.

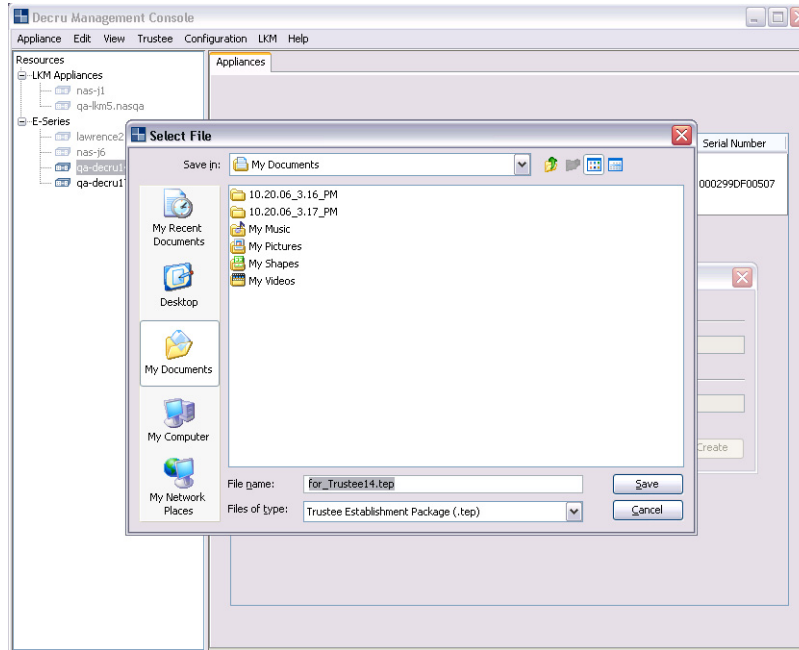
### Create the Trustee Link

Trustee management requires the use of the Decru Management Console (DMC). See [Decru Management Console Functions](#) on page 137 for information about this interface.

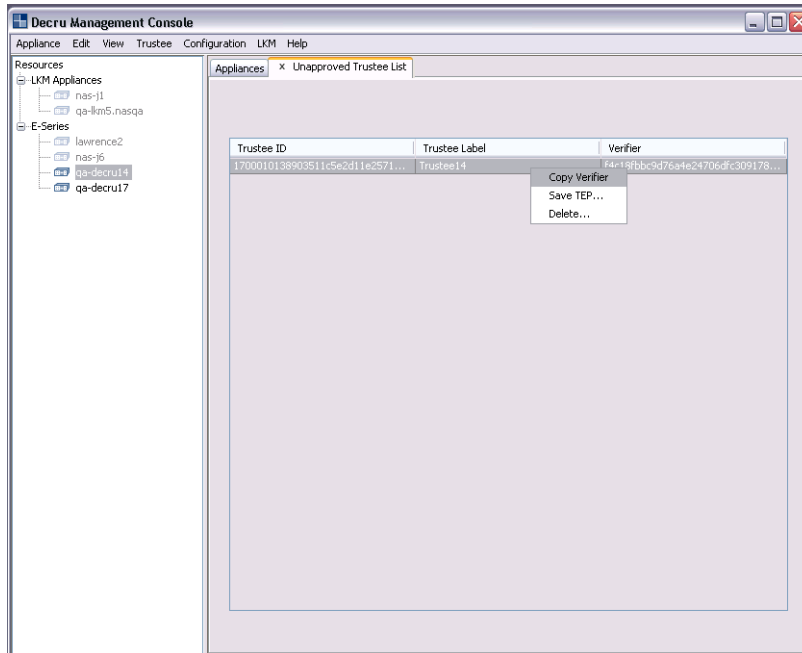
1. Choose **Start > Programs > Decru > Decru Management Console**.
2. From the Resources pane, select the first DataFort that will become a trustee.
3. From the Trustee menu, select **Start Trustee Creation**.



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



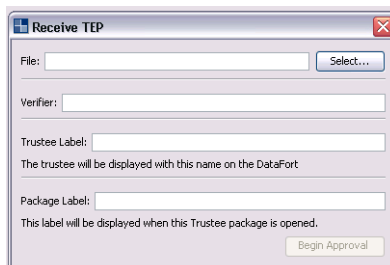
5. In the Select File window, keep the default name and choose a directory in which to save the TEP file.
6. From the Trustee menu, select Unapproved Trustee list.
7. Right-click the newly-created trustee and select Copy Verifier.



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

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

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



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

The approve TEP panel appears.

**Approve TEP**

Name: Trustee17

Verifier: F4c18fbbc9d76a4e24706dfc3091784104e11c07dad796fcd5613e921214c1d

Please select and/or insert a quorum of Recovery Cards.

Recovery Officers:

Alan@Finance@Finance  
Jim@Finance@Finance  
Bob@Finance@Finance

Card Label:

Security Domain:

Password:

Verify Password

Card Label:

Security Domain:

Password:

Verify Password

Start

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

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

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

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

**Approve TEP**

Name: Trustee17

Verifier: f4c18fbbc9d76a4e24706dfc3091784104e11c07dad796fc6d5613e921214c1d

Please select and/or insert a quorum of Recovery Cards.

Recovery Officers:

- Alan@Finance@Finance
- Jim@Finance@Finance
- Bob@Finance@Finance

Card Label: Jim@Finance

Security Domain: Finance

Password: \*\*\*\*\*

Verify Password

Card Label:

Security Domain:

Password:

Verify Password

Start

15. Click Start.  
Wait for the progress bar to appear. Approval is being obtained from the card. Do not remove it from the reader.
16. If using a single card reader, when prompted insert the other card and click Start.  
Wait for the progress bar to appear.
17. In the Select File box, keep the default file name and choose a directory in which to save the TAP file.
18. From the Trustee menu, select Unapproved Trustee list.
19. Right-click the newly-created trustee and select Copy Verifier.
20. Paste the verifier into a text file.
21. Communicate the file and the verifier to the administrator of the other appliance, if there is a different administrator.
22. Select the first DataFort again.
23. From the Trustee menu, select Receive TAP
24. In the Receive TAP window, for the File field, select the TAP file saved in step 17. For the Verifier field, paste the verifier ID copied in step 20.
25. In the Approve TAP window, insert or select Recovery Cards and enter the passwords.

26. Click Start.

When finished, a Trustee created message will appear.

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

### IMPORTING AND EXPORTING KEYS

Once a trustee relationship is established, use the right-click menu options of the DataFort WebUI Manage Tapes page to import and export keys.

To Import or export a key, right-click the pool or device the key will be imported to or exported from.

- Pool: Right-click the pool and select **Manage Keys > Export** or **Manage Keys > Import**.
- Device: Right-click the device and select **Keys > Export** or **Keys > Import**.

To import, browse to the saved key package from the remote trustee and click Upload.

To export, select the trustee that the key will be exported to and click Export.

MANAGING DATAFORT DEFENSE RESPONSES

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

DEFENSE TRIGGERS AND RESPONSES

A defense response can be triggered by the following:

- Chassis Intrusion**
- If DataFort is opened, this causes an automatic defense response. If chassis intrusion has been detected, there should be physical evidence (such as scratches, a broken lock or a stolen chassis key).
- Loss of Power**
- If DataFort is left without power for a long time (more than 3 weeks) a defense response can be triggered.
- CryptoShred Button**
- If DataFort is equipped with a CryptoShred button, pressing the button activates the defense response.

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

- The first response level disables the SEP and makes the DataFort unusable for cryptographic operations. It will still be possible to access management interfaces and view logs, but encrypted data will be inaccessible. To resume normal operation and data access you can perform an administrative reset (see [Clearing a Defense Alert](#) on page 98).
- The second response level protects the data by automatically clearing all encryption keys in the DataFort. Recovery from this response requires zeroization and data recovery.

When encryption keys are cleared (Medium and High levels) all encrypted data becomes immediately unusable. Zeroization is required before DataFort can be restored to a previous configuration.

The DataFort battery powers the intrusion-detection circuit even when DataFort is switched off. When this battery becomes low (because DataFort has been powered off for extended periods), DataFort may not detect or signal a physical intrusion.

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

DATAFORT DEFENSE SETTING

Defense levels are summarized in Table 8. If in doubt, choose the Basic level.

TABLE 8: DATAFORT DEFENSE SETTINGS

| Setting | When Used                                                        | Intrusion Trigger                          | Response                            | Operation Resumes                                                              |
|---------|------------------------------------------------------------------|--------------------------------------------|-------------------------------------|--------------------------------------------------------------------------------|
| Basic   | When it is sufficient to warn the administrator of an intrusion. | Internal chassis intrusion detected.       | Encryption and decryption disabled. | After administrator determines the cause of the intrusion and resets DataFort. |
|         |                                                                  | CryptoShred button pressed.                |                                     |                                                                                |
|         |                                                                  | Battery too low when system is powered on. |                                     |                                                                                |

**TABLE 8: DATAFORT DEFENSE SETTINGS (CONTINUED)**

| Setting       | When Used                                                                                                                               | Intrusion Trigger                                                  | Response                                                        | Operation Resumes                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|-----------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <b>Medium</b> | 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. |
| <b>High</b>   | When it is necessary to clear encryption keys immediately at the possibility of intrusion, whether a physical intrusion or low battery. | Internal chassis intrusion detected.                               | Encryption and decryption disabled and encryption keys cleared. | After DataFort zeroization and restoration using Setup Wizard and Recovery Cards. |
|               |                                                                                                                                         | CryptoShred button pressed.                                        |                                                                 |                                                                                   |
|               |                                                                                                                                         | Battery too low when system is powered on.                         |                                                                 |                                                                                   |

## CHANGING THE DEFENSE SETTING

To change the defense setting after setup:

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

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

3. Click Apply.

**Defense Settings**

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

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

| Administrative Procedures for Recovery                  |                                                                                                                                                                                                     |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="radio"/> <b>Basic Level</b><br> | For all defense-triggering events, clear the alert and reboot DataFort.                                                                                                                             |
| <input type="radio"/> <b>Medium Level</b><br>           | For a low battery condition, clear the alert and reboot DataFort.<br>For all other defense-triggering events, zeroize and restore DataFort from a backup configuration and a set of Recovery Cards. |
| <input type="radio"/> <b>High Level</b><br>             | For all defense-triggering events, zeroize and restore DataFort from a backup configuration and a set of Recovery Cards.                                                                            |

\* **Defense-triggering events** :

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

Apply

## CLEARING A DEFENSE ALERT

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

- On the front panel LCD
- On every page of the WebUI
- After CLI login
- In the DataFort logs

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

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

## Resetting a Defense Alert via WebUI

1. Click the Reset link from the Home page, or from the bottom of any page.
2. Click OK to dismiss the message alerting you about the reset.  
The DataFort will reboot, clearing the alert.
3. Close the connection to the DataFort.

## CRYPTOSHRED BUTTON STATES

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

### Normal State

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

### Activated State

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

## SYSTEM CARD CRYPTOShRED

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

1. Remove the System Card and store it in a safe place. To make it more difficult to access encrypted data after emergency shutdown, destroy or shred the card instead of storing it.

2. Power off DataFort by pressing the switch on the rear panel.

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

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

**Restore Operation if System Card was Destroyed:** To return DataFort to normal operations, DataFort will have to be zeroized and reconfigured with the wizard and Recovery Officers. See [Zeroizing the Decru DataFort](#) on page 116. A new System Card will have to be initialized. DataFort can be restored to the last configuration that was downloaded or backed up.

## CONFIGURING MANAGEMENT SECURITY SETTINGS

---

DataFort offers configurable levels of security for DataFort management interfaces.

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

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

**Security Settings** Cluster-wide

**Restrict management of the DataFort**

**Secure Web** ☒ OFF - The Admin Card is not needed in order to access the DataFort WebUI  
☐ ON - A valid Admin Card is required in order to access the DataFort WebUI

**Secure CLI** ☒ OFF - The Admin Card is not required for accessing the DataFort CLI  
☐ ON - The administrator must access the WebUI with a valid Admin Card to obtain a one time password

## MANAGING RECOVERY OFFICERS AND RECOVERY CARDS

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

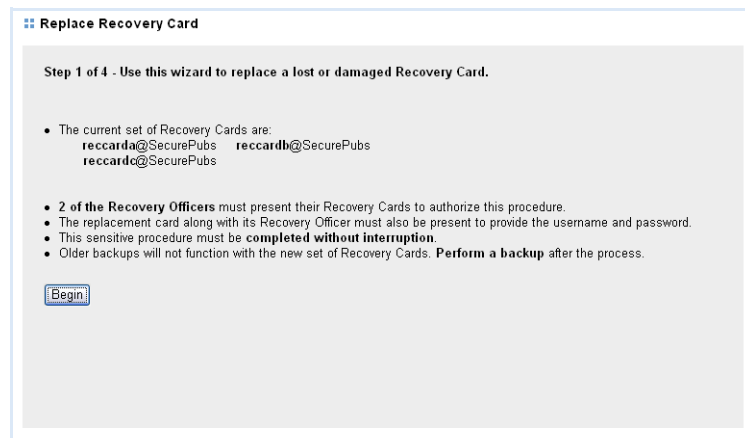
**Note:** Card replacement procedures are sensitive, and should not be interrupted by any other configuration or activity.

Card replacement procedures require:

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

### REPLACING A RECOVERY CARD

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



The current set of cards is displayed.

2. Click Begin.

**Replace Recovery Card**

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

**Known Recovery Cards**

| <u>Label</u> | <u>Security Domain</u> | <u>Card ID</u>                           |
|--------------|------------------------|------------------------------------------|
| reccarda     | SecurePubs             | 0900000048de53bc3ae10c52cfc0ab3ba7eb9a82 |
| reccardb     | SecurePubs             | 090000007ac343cfaea4225cd5d26ab8451a2886 |
| reccardc     | SecurePubs             | 09000000942c8759f682dee01061ce123c0b9d25 |

3. In the Known Recovery Cards window select the card that will be replaced and click Mark for Deletion.
4. Insert the card that will replace the deleted card into the Management Station smart card reader.
5. Click Introduce.  
The wizard will indicate how many cards are required to authenticate the replacement.
6. Insert a Recovery Card from the original set which included the card that is now being replaced and click Begin.  
The system will prompt for the old Recovery Cards. Recovery Officers should insert their cards as prompted, and enter the label and password information for each card. A quorum of Recovery Officers must present cards. Each card owner must supply the password for his or her card.
7. When prompted, insert the remaining cards from the set one by one, clicking OK when prompted.
8. Enter the password for each card and click Log In.
9. Repeat for as many cards as are needed.
10. When prompted that the replacement card is authorized, insert it into the reader and click OK.
11. Enter the label and password information for the card and click Log In.
  - If an uninitialized card is being used as a replacement, enter a card label and password, then click Log In.
  - If an initialized card is being used as a replacement card, existing values will appear. You cannot change the Security Domain of an initialized card. Enter the password information for the existing card, then click Log In.
12. Complete a configuration database backup.

## CHANGING A RECOVERY CARD PASSWORD

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

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

**Recovery Officers**

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

|                     |                                                                                                                                |                     |                     |                     |  |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------|---------------------|---------------------|---------------------|--|
| Recovery Schema     | 2 out of 3                                                                                                                     |                     |                     |                     |  |
| Recovery Cards      | <table><tr><td>reccarda@SecurePubs</td><td>reccardb@SecurePubs</td></tr><tr><td>reccardc@SecurePubs</td><td></td></tr></table> | reccarda@SecurePubs | reccardb@SecurePubs | reccardc@SecurePubs |  |
| reccarda@SecurePubs | reccardb@SecurePubs                                                                                                            |                     |                     |                     |  |
| reccardc@SecurePubs |                                                                                                                                |                     |                     |                     |  |

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

Card Label

Security Domain

Current Password

New Password  (8 - 30 characters)

Confirm Password

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

## SMART CARD RESET

---

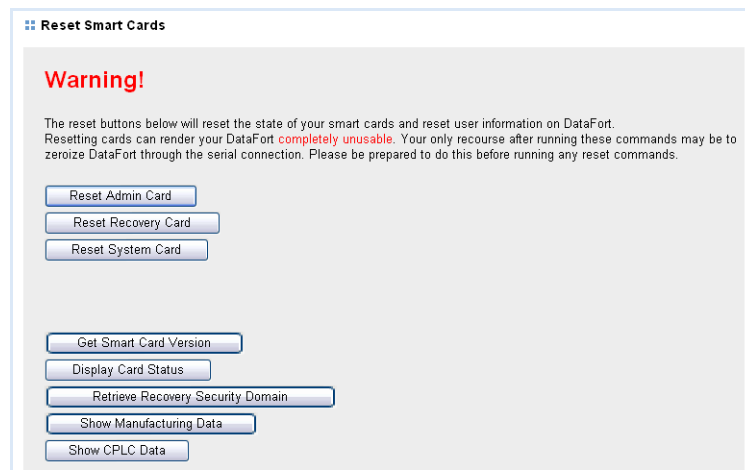
It is possible to completely reset a smart card using a special DataFort Reset Smart Cards page. This page also allows the administrator to check smart card versions and status.

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

1. Enter the following path into the browser window:

<https://<nameofDataFort>/resetcards.htm>

The Reset Smart Card page will appear.



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

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

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

4. After clicking the Reset button, confirm the transaction.



## ■ ■ ■ ■ 11 BACKUP ADMINISTRATION

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

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

- [Saving Configurations to Lifetime Key Management Software](#)
- [Downloading Configurations to a Remote Location](#)

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

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

## SAVING CONFIGURATIONS TO LIFETIME KEY MANAGEMENT SOFTWARE

---

The LKM software will manage keys for an entire cluster, offering a centralized approach to consolidating all encryption key information, for the purpose of emergency data recovery. LKM keeps all encryption keys even if the original keys are purged from DataFort or the source DataFort is decommissioned. LKM maintains an encrypted copy of all encryption keys, providing a single key management and data recovery solution for the cluster. See LKM documentation for more information.

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

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

### BEST PRACTICES FOR SECURE BACKUPS

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

- The system is designed to ensure that rollbacks to prior state is not possible.
- Only a single copy of the most recent LKM database must exist.
- This backup must be stored per organizational retention guidelines.
- Old copies must be considered sensitive and must be shredded per media shredding guidelines.
- Backups must not be transmitted over channels that retain data. Email must not be used but SSH can be used.
- DataFort should not back up keys in any other form other than sending them to LKM.

### CONFIGURING BACKUPS TO LKM SOFTWARE

Use this procedure to set up regular automatic backups to LKM software. DataFort supports up to four servers for the LKM system. Backups will be sent to all LKM servers at the same time. Enter the IP addresses for each LKM server as described below.

**Note:** These instructions only apply to LKM software. For LKM appliance operation, refer to the [LKM Appliance Administration Guide](#).

DataFort supports automated configuration backups to four LKM servers.

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

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

**Software Lifetime Key Management (LKM) Settings**

DataFort

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

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

Label

Description  (Optional)

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

| IP Address    | Port  | Using SSL |
|---------------|-------|-----------|
| 10.101.13.108 | 15362 | 0         |
| 10.101.13.93  | 15362 | 0         |

- Click Add.

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

**Software Lifetime Key Management (LKM) Settings : Add Software LKM Server**

Software LKM IP

Server Port

Using SSL Connection ☒ On ☐ Off

Shared Secret

Confirm Secret

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

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

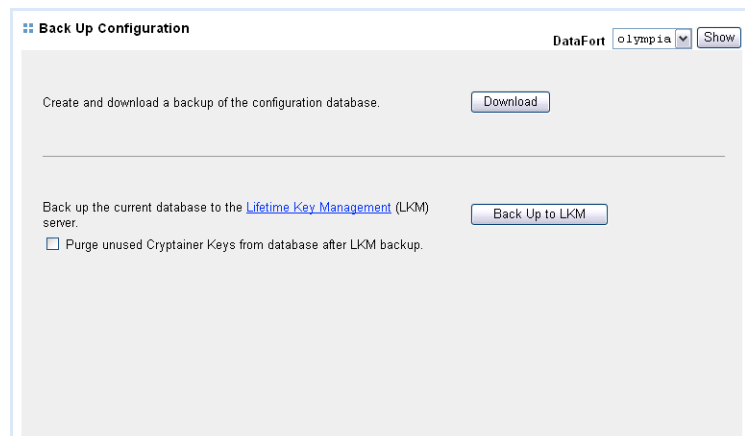
To configure DataFort to communicate with the LKM server across a secure SSL connection, leave Using SSL Connection enabled.

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

## BACKING UP THE CONFIGURATION TO LKM SOFTWARE

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

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



2. Choose whether or not to purge unused keys after backup to LKM.  
Keys for deleted or re-keyed data can be removed from the configuration database after a copy of the database has been backed up to an LKM server. Removing keys can help control the size of the DataFort configuration database. Since LKM is designed to retain all keys, it is not necessary to keep them in the DataFort configuration database as well.
3. Click Back Up to LKM.  
The configuration will be sent to the LKM server, connecting to the ports configured on the LKM Settings page, and using SSL if that option was selected.

## KEY PURGING

Keys are automatically backed up to LKM when LKM is in use. When backing up to LKM manually, you have the option to purge keys by checking the Purge unused Cryptainer keys... box on the Back Up Configuration page of the WebUI. This removes unused keys from the DataFort database, and stores them only in LKM.

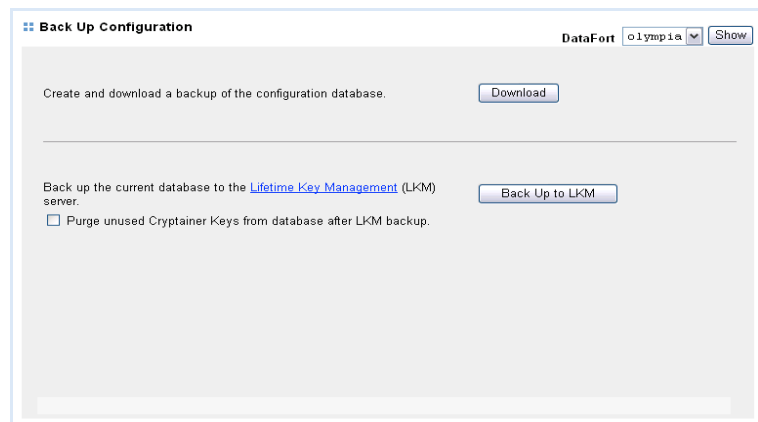
Only keys that are no longer current (meaning they are not assigned to Cryptainers) are allowed to be purged. In a large installation, it is a good idea to check the size of the configuration database using

the CLI command `db size`. This command will return a table of entries and a percent full number. Should the database be more than 75% full, consider purging keys. The `keyman purgekeys` command allows you to specify which keys are purged at backup. Using the `keyman purgekeys start -a` command allows you to define the age of the keys to be purged in days.

## DOWNLOADING CONFIGURATIONS TO A REMOTE LOCATION

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

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



The screenshot shows a web interface titled "Back Up Configuration". In the top right corner, there is a "DataFort" label, a dropdown menu currently showing "olympia", and a "Show" button. The main content area has a light gray background and contains the following elements:

- A text instruction: "Create and download a backup of the configuration database." followed by a "Download" button.
- A horizontal separator line.
- Text: "Back up the current database to the [Lifetime Key Management](#) (LKM) server." followed by a "Back Up to LKM" button.
- A checkbox labeled "Purge unused Cryptainer Keys from database after LKM backup." which is currently unchecked.

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



## ■ ■ ■ ■ 12 PHYSICAL SECURITY ADMINISTRATION

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

- [Setting Date and Time](#)
- [Configuring and Viewing Logs](#)
- [Zeroizing the Decru DataFort](#)

## SETTING DATE AND TIME

---

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

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

## CONFIGURING AND VIEWING LOGS

---

DataFort logs events in these categories:

- Security
- Operations
- Performance

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

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

**Note:** It is recommended that logs be stored in more than one location. See [Recommended Configuration](#) on page 112 for an example of a secure logging configuration.

For more about logging, see [Logging Functions](#) on page 170.

## DATAFORT LOG STORAGE GUIDELINES

Keep in mind the following when configuring DataFort logging:

- Decru recommends that you redirect all logs to a remote syslog server, and that you turn the Decru Signed Syslog feature on for remote logs. Remote log storage is supported for a system running a standard syslogd configured to accept log data from the DataFort.
- Decru recommends that critical operations be logged both locally and remotely.
- Remote logs should be verified using the remote log verification utility.
- Note that log information stored in the configuration database is encrypted by DataFort, while the remote syslog is not encrypted and is not secure.
- The DataFort configuration database can retain up to 2,500 events at a time. When this number is exceeded, old log information is purged. Logs exported via syslog will remain on the syslog host subject to its log rotation and storage policies.

### DECRU SIGNED SYSLOGD (DSS)

Log signatures can be turned on if remote logging is being used. Signed logs offer a way to authenticate log messages and verify that the log is complete. The logs are sortable for missing messages and can be verified using CLI commands. The feature is applicable only to remote syslogd.

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

- Verify that a given log message is authentic.
- Verify the source and timestamp of log messages.
- Verify that no messages are missing from the log.

Note that in a regular syslogd the source and timestamp are generated by the remote daemon and therefore cannot be trusted.

### CONFIGURING LOG STORAGE

1. To configure the storage location for log information, choose **System Config > General > Configure Log**.
2. The default settings are in effect until they are changed. If you want log information to be stored remotely, indicate the storage location according to the instructions below.
3. Select the desired settings and then click Apply. Clicking Reset restores the default settings.

### Setting and Enabling a Remote Storage Address

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

### Recommended Configuration

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

- Enable remote logging for all types of logging messages.
- Enable Decru Signed Syslog (DSS) for Security, Operations and Performance messages.
- Store High Security, High Performance and Error and Warning Operations log messages both locally in the configuration database, and remotely.

### WINDOWS EVENT LOGGING

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

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

**Logging Configuration** Cluster-wide

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

| Source      | Priority        | Location                            |                                     |                                                 | Signed                                                                            |
|-------------|-----------------|-------------------------------------|-------------------------------------|-------------------------------------------------|-----------------------------------------------------------------------------------|
|             |                 | Temporary Database                  | Remote Logging Host                 | Event Log Host                                  |                                                                                   |
| Security    | Low (6)         | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> 10.10.21.49 | <input type="checkbox"/> <input type="text"/> <input checked="" type="checkbox"/> |
|             | High (4)        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> 10.10.21.49 | <input type="checkbox"/> <input type="text"/> <input checked="" type="checkbox"/> |
| Operations  | Trace (7)       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> 10.10.21.49 | <input type="checkbox"/> <input type="text"/> <input checked="" type="checkbox"/> |
|             | Information (6) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> 10.10.21.49 | <input type="checkbox"/> <input type="text"/> <input checked="" type="checkbox"/> |
|             | Warning (4)     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> 10.10.21.49 | <input type="checkbox"/> <input type="text"/> <input checked="" type="checkbox"/> |
|             | Error (1)       | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> 10.10.21.49 | <input type="checkbox"/> <input type="text"/> <input checked="" type="checkbox"/> |
| Performance | Low (6)         | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> 10.10.21.49 | <input type="checkbox"/> <input type="text"/> <input checked="" type="checkbox"/> |
|             | High (4)        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> 10.10.21.49 | <input type="checkbox"/> <input type="text"/> <input checked="" type="checkbox"/> |

- Set up the Event User by clicking Edit User.

**Logging Configuration : Windows Event Log User**

This information will be used for Windows Event Logging.

Domain:   
 User:   
 Password:   
 Confirm Password:

- Enter information about the user who will log into the Windows host to generate the events including the domain to which that user belongs, and the name and password of the user. This user must have permission to log events to that host.
- Click Apply.
- Choose **System Config > General > Configure Log**.
- In the Event Log Host column, check each box that should be logged to the Windows host and enter the IP address of the Windows host in these boxes.

**Note:** It is a good practice to enter the same IP address for all event log host fields. Enter different IP addresses only if the user login is the same for all entered IP addresses.

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

SETTING UP SYSLOG

1. On a system running a syslog daemon configured to accept syslog messages from remote hosts (specifically DataFort), create an empty file to store the system log. You can use any name, but in this example it is DataFort1.
- Note:** The configuration information from DataFort is consistent with the standard syslog.conf format supported on a majority of Unix systems, but is also applicable to syslogd implementations available for other systems.
2. Edit the syslog.conf file and add these lines:

local0.\* /var/log/DataFort1

# local0 is for Security messages

local1.\* /var/log/DataFort1

# local1 is for Operations messages

local2.\* /var/log/DataFort1

# local2 is for Performance messages
3. Signal syslogd to start receiving messages from DataFort.

Syslogd Mapping

Table 9 shows the Descriptive Name, System Property Name, Syslog Facility and Level mapping for DataFort logs.

TABLE 9: LOG MAPPING

| Descriptive Name       | System Property Name             | Syslog Facility and Level |
|------------------------|----------------------------------|---------------------------|
| security low           | sys.proc.syslogd.conf.sec_minor  | local0.info               |
| security high          | sys.proc.syslogd.conf.sec_major  | local0.warning            |
| operations information | sys.proc.syslogd.conf.op_info    | local1.info               |
| operations warning     | sys.proc.syslogd.conf.op_warning | local1.warning            |
| operations error       | sys.proc.syslogd.conf.op_error   | local1.alert              |
| performance low        | sys.proc.syslogd.conf.perf_minor | local2.warning            |
| performance high       | sys.proc.syslogd.conf.perf_major | local2.info               |

Temporary Files Mapping

Table 10 describes the mapping for temporary logs.

**TABLE 10: TEMPORARY LOG MAPPING**

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

## VIEWING THE LOG

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

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

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

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

## VERIFYING SIGNED LOG MESSAGES

It is possible for log data to be changed at the server or missed during a network transmission. To verify the correctness of the log, ensure that log source and global sequence numbers appear in correct order (with no log messages missing).

Logs that are missing from the sequence could be caused by the following:

- Log messages were deleted intentionally from the remote server to hide activity.
- Messages were dropped across the UDP connection between DataFort and the remote server.
- syslogd died on the remote server.

If logs appear to be missing, compare the logs saved to separate remote locations (logs can be sent to up to four locations, as indicated in [Recommended Configuration](#) on page 112) to verify breaks in the log are replicated. Remote logs can also be compared to the internal DataFort log.

The administrator can use the CLI to verify the correctness of the log using the **system log verify** command. See [Verifying System Logs](#) on page 152.

## ZEROIZING THE DECRU DATAFORT

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

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 11: KEY RECOVERY AND ZEROIZATION**

| Key Type                                                                     | Example                                                                                                               | Recovered by Setup Wizard                                                                                                 |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Keys that protect user data                                                  | <ul style="list-style-type: none"><li>• Cryptainer keys</li><li>• Parent keys which encrypt Cryptainer keys</li></ul> | Recovered using the wizard, in order to ensure data can be decrypted by the recovered DataFort.                           |
| Keys that authenticate one DataFort to another, or a DataFort to an end user | <ul style="list-style-type: none"><li>• SSL keys</li><li>• SSH keys</li><li>• IPsec keys</li></ul>                    | Not recovered, in order to prevent one DataFort appliance from falsely appearing to be a different DataFort appliance.    |
| Secrets belonging to DataFort users                                          | <ul style="list-style-type: none"><li>• User passwords</li></ul>                                                      | Recovered using the wizard, in order to allow the same users to access a recovered DataFort without recreating passwords. |

**WARNING:** SSL PRIVATE KEYS ARE CLEARED BY ZEROIZATION, AND MAY NOT BE BACKED UP OR TRANSFERRED TO OTHER APPLIANCES. IF SIGNED CERTIFICATES HAVE BEEN PURCHASED, THEY WILL HAVE TO BE REPLACED.

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

Depending on the DataFort defense setting, zeroization and recovery may be required after the chassis has been opened or if another defense response is triggered. Zeroization and recovery are required after loss or destruction of the System Card.

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

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

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

## ZEROIZING AFTER SETUP

If after running the Setup Wizard, you discover that the initial configuration is incorrect, or you must zeroize for some other reason, it is best to do so before creating Cryptainers. Log into the WebUI and complete steps to zeroize as described below. If necessary, you may also need to reset smart cards initialized during the Setup Wizard, as described in [Configuring and Viewing Logs](#) on page 111.

## ZEROIZATION USING THE DATAFORT WEBUI

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

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

**Zeroize**

DataFort **qa-decru16** Show

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

*Details*

Zeroizing the DataFort appliance "qa-decru16":

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

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

*Steps*

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

☒ **Keep DataFort IP addresses**

Zeroize...

3. Click Zeroize.
4. Type the provided code into the popup box to verify that you want to zeroize this DataFort.  
After providing the code in the popup box, you will be automatically logged out of the WebUI and redirected to the login screen.  
DataFort will reboot.
5. If IP settings were not preserved by checking the Keep DataFort IP addresses box, assign the DataFort IP settings as described in [Assigning the DataFort IP Address](#) on page 33.
6. Complete the configuration by running the Setup Wizard.

## ZEROIZATION USING THE CLI

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

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

1. Log in to the CLI with a valid administrator username and password.
2. Execute the `system zeroize` command. To preserve the existing IP address, use the `system zeroize [-k, --keep_ip]` command. You will be prompted to enter a confirmation code.
3. Enter the command again, followed by the code.  
`system zeroize [confirmation-value]`
4. Wait while the System Card is reset, and the DataFort reboots.
5. If they were not preserved, reassign the DataFort IP settings as described in [Assigning the DataFort IP Address](#) on page 33.
6. Complete the configuration by running the Setup Wizard.

## ZEROIZATION USING THE SERIAL CONSOLE

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

1. Connect the serial console port (see [Serial Console Port](#) on page 32).
2. Log in to the serial console with a valid administrator username and password.
3. To zeroize DataFort, enter option `Z`.
4. Enter a confirmation code when prompted.  
The DataFort will reboot.
5. Assign the DataFort IP settings. See [Assigning the DataFort IP Address](#) on page 33.
6. After the DataFort has been assigned IP settings, complete the configuration by running the Setup Wizard.

## EMERGENCY SERIAL CONSOLE PORT ACCESS

If all Admin Cards and passwords for a DataFort are lost, it will not be possible to log in to its WebUI or CLI. However it is still possible to connect to the DataFort serial console using a valid Recovery Card from the set used when that DataFort was initialized. This will allow the DataFort to be zeroized so it can be reset for future use.

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

## ■ ■ ■ ■ 13 CLUSTER ADMINISTRATION

A cluster is created using the Setup Wizard. See [Chapter 5](#) for instructions on completing the wizard. Note that standalone DataFort appliances cannot be joined together to form a cluster.

An S-Series DataFort cluster can include up to 4 DataFort appliances. All cluster members maintain configuration information for the entire cluster.

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

Cluster administration tasks include:

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

## CLUSTER MANAGEMENT

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

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

If one DataFort in the cluster goes offline, the remaining appliance will automatically take over operations. All cluster members keep the same configuration database.

## CLUSTER-WIDE MANAGEMENT VIA WEBUI

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

## CHECKING THE STATUS OF THE CLUSTER

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

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

If the cluster is not in a committed/online state, some action may be required in order to resolve the cluster condition. Check Table 12 for a description of cluster states.

**TABLE 12: CLUSTER STATES**

| Replication State | Group State                                                                                                                                                                                   |                                                                                                                                                                                                |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | committed                                                                                                                                                                                     | aborted                                                                                                                                                                                        |
| <b>online</b>     | <b>committed/online</b><br>The cluster is stable. This is the only state in which changes to the configuration are permitted. A standalone DataFort will also show this as its cluster state. |                                                                                                                                                                                                |
| <b>recover</b>    | <b>committed/recover</b><br>Cluster members are synchronizing configuration information. When the process is complete the state will change to committed/online.                              | <b>aborted/recover</b><br>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. |
| <b>conflict</b>   | <b>committed/conflict</b><br>There is a conflict between configuration databases that cannot be automatically resolved.                                                                       |                                                                                                                                                                                                |

## RESOLVING A CLUSTER CONFLICT

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

1. Determine which cluster member has an incorrect database. This may require logging into the conflicted DataFort appliances and examining the configuration properties to determine which database is correct.
2. Log into the WebUI of the cluster member with the incorrect database. An alert will appear on the Home page near the Manage Cluster link.
3. Click the Manage Cluster link on the Home page or choose **System Config > Cluster > Manage Cluster**.
4. Highlight a DataFort with the correct database, and click Pull Information.
5. The database pull starts automatically. The process of updating the incorrect database and reforming the cluster can take up to five minutes. When complete, the cluster state will change to “committed/online.”

## ADDING AND REMOVING CLUSTER MEMBERS

---

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

A DataFort can also be removed from the cluster at any time. See [Removing a Cluster Member](#). Keep in mind that in most cases once a DataFort is removed from the cluster, it must be zeroized and reintroduced to the cluster using the Setup Wizard.

### ADDING A CLUSTER MEMBER

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

- A DataFort must be uninitialized when added to a cluster. Initialized standalone DataFort appliances cannot be joined to form a cluster. To zeroize an initialized DataFort so it can be added as a new cluster member, see [Zeroizing the Decru DataFort](#) on page 116.
- 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 will continue to function as a standalone device.

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

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

### REPLACING A DATAFORT IN A CLUSTER

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

- A new or zeroized DataFort.
  - A DataFort remaining from the original cluster.
  - The minimum set of Recovery Officers and Recovery Cards as determined by the recovery schema of the cluster.
  - A valid cluster license from Decru for each DataFort that will be in the new cluster.
1. Power down the offline DataFort and remove it from the network, disconnecting the cables.
  2. Log in to the WebUI of an online member of the cluster and click the Manage Cluster link on the Home page (or choose **System Config > Cluster > Manage Cluster**).
  3. Select the offline DataFort in the Cluster Membership Information window and click Remove.
  4. Click Add. To leave the shared secret unchanged, click Next. To change the shared secret for the cluster, enter it and click Set.
  5. Click Add. In the popup window, enter the IP address of the member that will be added. Click OK.
  6. Click Next.
  7. Make a note of the instructions on the page, and click OK.
  8. Log out of the WebUI of the online DataFort.
  9. Replace the removed DataFort with the new, uninitialized DataFort.
  10. Assign an IP address to that DataFort and connect it to the network.
  11. Run the Setup Wizard for the new DataFort.

## RECOVERING A CLUSTER

---

Follow the cluster recovery procedures to return an entire cluster to a previous configuration or to replace all members of a cluster. This procedure is used to replace missing or damaged clustered DataFort appliances. The replacement DataFort appliances must be uninitialized or zeroized (see [Zeroizing the Decru DataFort](#) on page 116).

- 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 121. Use the wizard to restore the first member of a cluster only if all members have been lost.
- If no cluster members are online, run the wizard on one DataFort, using a saved configuration database from a lost cluster member, then add the second cluster member.

This procedure requires:

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

## CHANGING NETWORK PROPERTIES OF A CLUSTER MEMBER

---

The network settings can be changed for a cluster member.

- [Changing the IPsec Secret of a Cluster](#)

### CHANGING THE IPSEC SECRET OF A CLUSTER

A Full Administrator can change the IPsec secret of a cluster. The most direct way to make this change is to use the CLI. The change must be made manually for each member of a cluster.

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

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



## ■ ■ ■ ■ 14 MACHINE ADMINISTRATION

Machine administration includes tasks that allow network properties to be set and DataFort upgrades to be executed.

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

**Note:** A specified Machine Administrator can also add a new member to a cluster, as described in [Cluster Administration](#) on page 119.

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

- [Network Settings](#)
- [Upgrading DataFort](#)
- [Setting Security Certificates](#)
- [Managing Licenses](#)

Only a Full Administrator can manage SNMP:

- [SNMP Settings](#)

**Note:** DataFort appliance Date and Time can only be set by a Full or Security Administrator. See [Setting Date and Time](#) on page 111.

## NETWORK SETTINGS

---

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

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

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

## UPGRADING DATAFORT

---

From time to time, Decru offers upgrades for DataFort. Each upgrade package comes with its own set of instructions from Decru. Download the provided software package to the Management Station (or another local machine) and complete the steps outlined in the upgrade instruction packet. Upgrades can be completed by accessing the **System Config > General > Upgrade** page of the WebUI and browsing to the Upgrade file from Decru. There is also an option to upgrade from the WebUI of a zeroized DataFort by using the link provided in the setup wizard.

**Note:** While the DataFort appliance is being upgraded, there is a small window of time during which the appliance's intrusion detection is disabled. Upgrades should only be performed when the administrator can maintain physical security of the DataFort.

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

## SETTING SECURITY CERTIFICATES

Internet Explorer will notify you any time a secure connection is made certified by an unrecognized authority. To eliminate this warning, and to protect against security attacks that could occur between DataFort and the Management Station, a locally signed certificate is generated during the Setup Wizard. After the certificate is set and installed, the security warning will not appear when logging in to the DataFort unless there has been a change made to the IP address or hostname of the DataFort, or cryptographic operations have been disabled. It may be desirable to install a certificate signed by a certificate authority as described in [Setting a Certificate Authority Signed Certificate](#) on page 129. Keep the following in mind:

- A certificate must be generated independently for each DataFort in a cluster.
- Create the certificate and then use it until its expiration date.
- Only a Full Administrator can set the security certificate

### SETTING A LOCAL SECURITY CERTIFICATE

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

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

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

2. Click Use Self-Signed.

**DataFort Certificate : Self-Sign & Set**

DataFort poly Show

Generate a self-signed certificate.

Common Name olympia

Country Code

Province/State

City/Town

Organization Name

Organization Unit

Contact Email

Sign and Set as Certificate Cancel

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

3. Enter the information for the locally signed certificate. This information will appear when certificate details are viewed.

**Note:** Country codes are established by the International Organization for Standardization (ISO). For a partial list of country codes, see [Partial List of ISO Country Codes](#) on page 190.

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



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

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

## SETTING A CERTIFICATE AUTHORITY SIGNED CERTIFICATE

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

**DataFort Certificate** DataFort: poly Show

The local certificate is self-signed.

|                   |                         |  |
|-------------------|-------------------------|--|
| <b>Valid From</b> | Jun 6 01:00:05 2003 GMT |  |
| <b>Valid Till</b> | Jun 5 01:00:05 2006 GMT |  |

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

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

2. Click Use CA-Signed.

**DataFort Certificate : Request & Set** DataFort: poly Show

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

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

Generate Request

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

Set as Certificate Cancel

3. Enter the required information into the fields provided and click Generate Request. This generates a PEM-encoded request which can be submitted to a known certificate authority such as VeriSign or a local certificate authority.

**Note:** Country codes are established by the International Organization for Standardization (ISO). For a partial list of country codes, see [Partial List of ISO Country Codes](#) on page 190.

4. When you receive the signed request from the CA, paste it into the box provided. Cut and paste the entire contents of the certificate file, including the BEGIN and END lines.

5. Click Set as Certificate.
6. Log out of the WebUI.
7. Open an HTTPS connection to the DataFort.  
The certificate warning appears.
8. Click View Certificate.

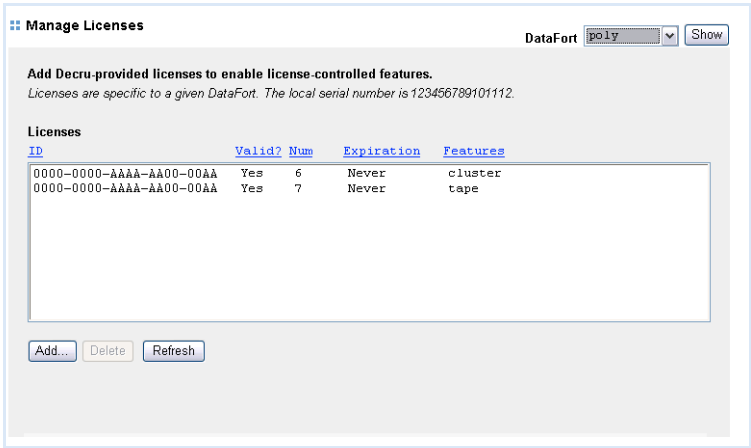


9. Click Install Certificate.
10. Complete the Install Certificate Wizard.  
The certificate has been installed. When you connect to the WebUI, no security certificate warning should appear.

MANAGING LICENSES

DataFort features (such as clustering) require a software license issued by Decru before they can be enabled. A Security Administrator or Full Administrator is required when adding or removing a license.

- 1. To view the license for a DataFort, choose **System Config > General > Licensing**.



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

## SNMP SETTINGS

---

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

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

For a complete list of DataFort MIBs and SNMP alarms, contact Decru. Decru MIBs fall into the following categories:

|                       |                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Crypto Alerts</b>  | Useful for monitoring the status of the crypto subsystem for the DataFort appliance (crypto interrupts, crypto status, etc.). |
| <b>Chassis Alerts</b> | Useful for monitoring the physical status of the DataFort appliance (fan speeds, temperatures, battery voltages, etc.).       |
| <b>System Alerts</b>  | Useful for monitoring the software running on the DataFort (number of processes, file system usage, etc.).                    |

## ENABLING SNMP

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

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

## SNMP CONFIGURATION

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

|                        |                                                                                                                                                                                           |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System location</b> | sysLocation.0 under MIB-II. A description of the physical location where the device is installed or operating.                                                                            |
| <b>System contact</b>  | sysContact.0 under MIB-II. The contact information for the person or organization responsible for managing the device.                                                                    |
| <b>SNMP parameters</b> | Read Community: community string used to read SNMP MIB.<br>Trap Host: hostname (or IP address) which SNMP traps are sent to.<br>Trap Community: community string used to send SNMP traps. |

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

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

**System**

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

**Trap**

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

**Version**

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

## ■ ■ ■ ■ 15 DATAFORT APPLIANCE SETTINGS AND STATUS

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

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

## VIEWING SETTINGS IN THE WEBUI

---

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

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

### View DataFort Logs

Choose **System Info > Log**. To filter the view by time, select a display period from the drop-down menu at the left. Events can be displayed from the last minute, 5 minutes, 15 minutes, 1 hour, 1 day, or 1 week. To select a single type of event to view, select Security, Operations or Performance from the Source drop-down menu. To select only events of certain priorities, select the priority level from the Priority Limit drop-down menu. To configure logs see [Configuring Log Storage](#) on page 112.

### View DataFort Throughput and CPU Usage

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

### View Storage Diagnostics

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

### View DataFort Date and Time Setting

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

### View DataFort System Users

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

### View DataFort Network Settings

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

**View Crypto Status of DataFort**

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

**View Information About DataFort**

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

**View DataFort Sensors**

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

**View DataFort LCD in WebUI**

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



## ■ ■ ■ ■ 16 DECROU MANAGEMENT CONSOLE FUNCTIONS

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

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

The DMC console menus provide tools for the following:

- [Appliance Management](#)
- [License and Administration Management](#)
- [Logging Configuration](#)

See [Decru Management Console Menus](#) for an overview of DMC menus.

APPLIANCE MANAGEMENT

The Decru Management Console is installed on the Management Station so the DataFort setup wizard can be run, as described in [Initializing DataFort Appliances](#).

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

Once an appliance is added to the Decru Management Console, icons show appliance status. [Table 13](#) shows possible state displays.

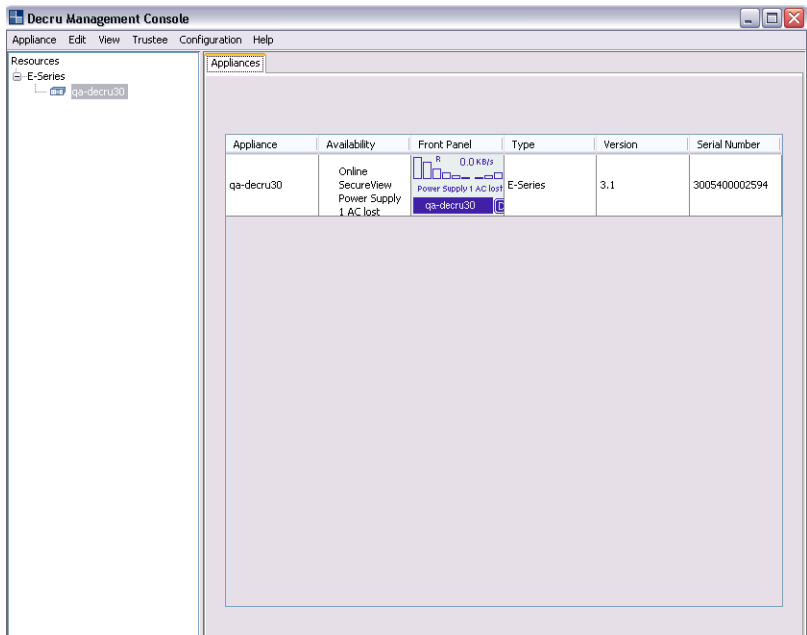


TABLE 13: APPLIANCE STATUS INDICATORS

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

### ADDING AN APPLIANCE

Use the Appliance menu to add an LKM or DataFort appliance so it can be managed by the console.

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

2. Choose **Appliance > Add**.

The Add... pop-up screen appears.

3. Enter the IP address or hostname of the appliance.

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

4. Click OK when all addresses or hostnames are entered.

The certificate warning appears.

5. Agree to trust the certificate once or always.

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

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

### LOGGING INTO APPLIANCES

Log into each appliance after adding it to DMC.

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

If the correct credentials were entered and the appliance is correctly configured, the status of the appliance will change to online. See [Appliance Status Indicators](#) on page 138 for information about status icons.

### REMOVING AN APPLIANCE

Remove an appliance from the Management Console.

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

### RUNNING THE SETUP WIZARD

Use the wizard to configure LKM and DataFort appliances.

1. Select an appliance in the Resources list and choose **Appliance > Setup**.
2. Run the wizard for the appliance. See [Initializing DataFort Appliances](#) on page 37 for detailed instructions.

### VERIFYING AN UPGRADE PACKAGE

Verify an upgrade package before running it on the appliance.

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

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

## UPGRADING AN APPLIANCE

Upgrade the appliance version with an upgrade package from Decru.

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

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

## BACKING UP AN APPLIANCE

Back up the configuration database of the selected appliance.

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

## CREATING TRUSTEES

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

Use the DMC to set up trustees. See [Managing Trustees](#) on page 89 for instructions.

## VIEWING DETAILS

Shows the system version information for the appliance.

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

## ACCESSING DATAFORT WEBUI

Opens the WebUI for the DataFort appliance.

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

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

## ACCESSING COMMAND LINE INTERFACE

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

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

The CLI will open. See [CLI Administration](#) on page 147 for commonly-used commands.

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

### COLLECTING TECH SUPPORT INFO

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

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

### REBOOTING APPLIANCES

Reboots selected appliance.

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

### ZEROIZING APPLIANCES

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

**Note:** Read the cautions outlined in [Zeroizing the Decru DataFort](#) on page 116 before zeroizing an appliance.

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

### EXITING THE CONSOLE

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

## LICENSE AND ADMINISTRATION MANAGEMENT

---

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

- [Managing Licenses](#)
- [Adding a License](#)
- [Managing Administrators](#)
- [Adding an Administrator](#)

### MANAGING LICENSES

To view the licenses on selected appliances:

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

All known licenses for the selected appliances appear.

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

## ADDING A LICENSE

To add licenses to selected appliances:

1. Select an appliance in the Resources pane and choose **Configuration > Add License**.
2. Enter the license into the provided field and click Apply.  
All known licenses for the selected appliances appear.

## MANAGING ADMINISTRATORS

To view the administrators with permission to manage selected appliances:

1. Select an appliance in the Resources pane and choose **Configuration > Administrators**.  
All known administrators for the selected appliance appear.  
Administrators can be managed from this view. See [Adding an Admin Card to an Administrator](#), [Removing an Admin Card from an Administrator](#) and [Deleting an Administrator](#).

### Adding an Admin Card to an Administrator

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

### Removing an Admin Card from an Administrator

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

### Deleting an Administrator

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

## ADDING AN ADMINISTRATOR

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

1. Select an appliance in the Resources pane choose **Configuration > Add Admin**.  
The Add Administrator page appears.
2. Enter the name of the administrator to be added to the selected appliance.
3. Enter and confirm the password for the administrator.
4. Select the type of administrator to add.

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

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

Specialty administrators can be used to separate tasks for increased security. The roles have separately defined permissions, ensuring that administrators only have permission to execute certain designated commands. If desired, compound administrators possessing the characteristics of more than one specialty administrator can also be created. See [Administrator Roles](#) on page 65 for more information about administrator roles.

## LOGGING CONFIGURATION

---

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

- Security
- Operations
- Performance

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

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

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

For more about logging, see [Logging Functions](#) on page 170.

1. Select an appliance in the Resources pane and choose **Configuration > Log Configuration**.  
The Logging Configuration page will appear.
2. Select the desired settings and then click Apply.

## DECRU MANAGEMENT CONSOLE MENUS

---

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

- [Appliance Menu](#)
- [Edit Menu](#)
- [View Menu](#)
- [Trustee Menu](#)
- [Configuration Menu](#)
- [Help Menu](#)

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

### APPLIANCE MENU

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

|                     |                                                                                                                                                         |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Add</b>          | Add an appliance to the Management Console. See <a href="#">Adding an Appliance</a> on page 139.                                                        |
| <b>Remove</b>       | Remove an appliance from the Management Console.                                                                                                        |
| <b>Log in</b>       | Log in to an appliance as an administrator. See <a href="#">Logging into Appliances</a> on page 139.                                                    |
| <b>Log out</b>      | Log out of an appliance as an administrator.                                                                                                            |
| <b>Set up</b>       | Set up an LKM or DataFort appliance by running the Setup Wizard. See <a href="#">Initializing a Standalone DataFort or DataFort Cluster</a> on page 39. |
| <b>Verify</b>       | Verify the validity of an upgrade package before upgrading. See <a href="#">Verifying an Upgrade Package</a> on page 139.                               |
| <b>Upgrade</b>      | Upgrade an appliance. Upgrades should be done only after consulting Decru support. See <a href="#">Upgrading an Appliance</a> on page 140.              |
| <b>Back up</b>      | Back the configuration database up as a file to a specified location. See <a href="#">Backing Up an Appliance</a> on page 140.                          |
| <b>Details</b>      | Shows the system version for the selected appliance. See <a href="#">Viewing Details</a> on page 140.                                                   |
| <b>WebUI</b>        | Opens the WebUI of the selected appliance (DataFort only). See <a href="#">Accessing DataFort WebUI</a> on page 140.                                    |
| <b>Command Line</b> | Opens the CLI. Whatever command is run will be executed on all selected appliances. See <a href="#">Accessing Command Line Interface</a> on page 140.   |

|                                  |                                                                                                                                                                                                                                                                                      |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Collect Tech Support Info</b> | Creates a file containing information useful to technical support when troubleshooting for the selected appliance. The file is by default placed in the tech support folder of the Decru Management Console directory. See <a href="#">Collecting Tech Support Info</a> on page 141. |
| <b>Reboot</b>                    | Reboot the selected appliance. See <a href="#">Rebooting Appliances</a> on page 141.                                                                                                                                                                                                 |
| <b>Zeroize</b>                   | Zeroize the selected appliance. See <a href="#">Zeroizing Appliances</a> on page 141.                                                                                                                                                                                                |
| <b>Smart Card Utilities</b>      | Resets a smart card and displays card information.                                                                                                                                                                                                                                   |
| <b>Exit</b>                      | Exit the Management Console. See <a href="#">Exiting the Console</a> on page 141.                                                                                                                                                                                                    |

## EDIT MENU

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

|                   |                                                                                                   |
|-------------------|---------------------------------------------------------------------------------------------------|
| <b>Find</b>       | Searches for text in the active pane of the Management Console. The search is not case sensitive. |
| <b>Find Again</b> | Finds next instance of same search.                                                               |

## VIEW MENU

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

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

## TRUSTEE MENU

A trustee relationship between two appliances allows encryption keys to be shared between those appliances even if they have no Recovery Cards in common, and are not on the same network. Trustees send messages to establish a relationship before key sharing. The first message is the Trustee Establishment Package (TEP). The second message is the Trustee Acceptance Package (TAP).

|                               |                                                                                                                          |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Start Trustee Creation</b> | Starts the process of creating a trustee for selected appliance. See <a href="#">Creating Trustees</a> on page 140.      |
| <b>Receive TEP</b>            | Allows selected appliance to receive a Trustee Establishment Package. See <a href="#">Creating Trustees</a> on page 140. |

|                                |                                                                                                                          |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Receive TAP</b>             | Allows selected appliance to receive a Trustee Acceptance Package. See <a href="#">Creating Trustees</a> on page 140.    |
| <b>Unapproved Trustee List</b> | Displays list of trustees not yet approved (waiting to accept a TAP). See <a href="#">Creating Trustees</a> on page 140. |
| <b>Trustee List</b>            | Displays list of trustees. See <a href="#">Creating Trustees</a> on page 140.                                            |

## CONFIGURATION MENU

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

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>License</b>                  | View licenses. See <a href="#">Managing Licenses</a> on page 141.                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Add License</b>              | Add licenses. See <a href="#">Adding a License</a> on page 142.                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Administrators</b>           | View and manage administrators. See <a href="#">Managing Administrators</a> on page 142.                                                                                                                                                                                                                                                                                                                                                       |
| <b>Add Admin</b>                | Add an administrator. See <a href="#">Adding an Administrator</a> on page 142.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Log Configuration</b>        | See <a href="#">Logging Configuration</a> on page 143                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Replace Recovery Officer</b> | <p>The Configuration Menu offers the Replace Recovery Officer menu. This allows you to replace a Recovery Card in the set, thereby replacing the associated Recovery Officer as well.</p> <p>See <a href="#">Removing an Administrator</a> on page 73 for instructions on using the DataFort WebUI to manage administrators.</p> <p>To replace a recovery card using DMC, refer to the <a href="#">LKM Appliance Administration Guide</a>.</p> |

## HELP MENU

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



## ■ ■ ■ ■ 17 CLI ADMINISTRATION

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

**Note:** The CLI cannot be used to replace smart cards, manage keys, or recover data.

A Full Administrator logged in to the CLI can execute all CLI commands; specialty administrators will be restricted to executing commands associated with their role.

A list of top-level commands can be found in the [Command Line Interface Quick Reference](#) on page 162 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](#)

## USING THE CLI

---

Some CLI commands must be executed in a specific order for desired results. The command line will provide usage guidelines when [CLI Help](#) is used. For some commands, it is good practice to execute a verification command (such as `list`) after an action that adds an item to the database. Always perform a backup of the database after any changes.

### CONNECTING TO THE CLI

Connect to CLI from an SSH client (see [Connecting to the DataFort Command Line Interface](#) on page 58). By default, DataFort is set for standard CLI. It is recommended that only one WebUI or CLI session be open per cluster at one time.

### CLI HELP

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

## ADMINISTRATION COMMANDS

---

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

- [Administrator Roles](#)
- [Creating a New Administrator Using the CLI](#)
- [Cluster Management](#)
- [System Properties and Log Management](#)
- [Stack Trace Settings](#)
- [Network Management](#)

### ADMINISTRATOR ROLES

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

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

1. Log in as the specialty administrator whose permitted commands you want to see and enter:

```
cli doc -n
```

The list of commands executable by the type of administrator who is currently logged in appears.

2. Enter the name of the current administrator into the `system property get` command to see the current values of system properties, preceded by permissions for the named administrator role. RW indicates that the administrator logged in has read and write permission, R- indicates read-only permission. A lower-case w indicates a property that can only be changed via WebUI.

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

### CREATING A NEW ADMINISTRATOR USING THE CLI

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

To create an administrator using the DataFort CLI:

1. Log in to the CLI as a Full Administrator.
2. To create an administrator for a single DataFort, add a user, indicating the type from the list of [Administrator Roles](#) in the `<group>` field:

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

3. To create an administrator that is replicated to cluster partners add a user with the `--replicate` flag, indicating the type from list of [Administrator Roles](#) in the `<group>` field:

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

4. To add the authorizer role to the newly created administrator so that dual authentication is not required when logging in:

```
user role grant authorizer@DATAFORT_ADMIN username@DATAFORT_ADMIN
```

## CLUSTER MANAGEMENT

The following commands are useful when managing clusters.

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>cluster status</code>  | Shows the status of a DataFort cluster, as well as a list of member DataFort appliances, their IPs and member IDs. Shows current status of the cluster as well as the IP addressees of each cluster member.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <code>cluster config</code>  | Cluster configuration commands.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <code>cluster enable</code>  | Enables clustering. This command breaks any pre-existing cluster connectivity and forces a re-negotiation of the cluster.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <code>cluster rexec</code>   | Allows commands to be issued remotely to all other DataFort appliances in the cluster as identified by IP address or name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>cluster rsh</code>     | Connects directly to another member of the cluster as identified by IP address or name. The <code>ctl-d</code> command breaks out of this into the previous shell.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <code>cluster disable</code> | <p>Allows the temporary removal of a cluster member without having to run a wizard in order to reintroduce the cluster member. This is useful if a DataFort appliance needs to be moved or isolated for servicing. There is no indication in the WebUI that the member has been disabled.</p> <p>To disable a member, log into another member of the cluster and execute the <code>cluster disable &lt;member-ip or name&gt;</code> command, identifying the DataFort to be removed by name or IP address. To allow the member back into the cluster, execute the <code>cluster enable &lt;member-ip or name&gt;</code> command from another cluster member.</p> |

## SYSTEM PROPERTIES AND LOG MANAGEMENT

Use the CLI to view system logs, search for messages, and to aid in [Verifying System Logs](#).

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>system property get</code> | <p>View the current values of system properties, and see permissions for the administrator currently logged in.</p> <p>To view the current values of system properties in a detailed view that shows permissions for the administrator logged in, and lists all the administrator roles permitted to change (set) those properties use:</p> <pre>system property get -d</pre> <p>Output will be of the form: <code>security-admin RW global sys.security.web.usesmartcard: 0</code></p> |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**system property get**

View the current values of system properties, and see permissions for the administrator currently logged in.

This output means that Security Administrators and up will be able to modify the property, in this case Secure Web. Only a Full Administrator is above a Security Administrator. RW indicates that the administrator logged in has read and write permission, R- indicates read-only permission. A lower-case w indicates that the property can be changed from the web only. The output (after the colon) shows the current value of the property. In this case 0 indicates that Secure Web is off.

**system selftest**

Performs a series of tests on the DataFort and configured servers.

**system utility lcdmessages**

Displays text of any warnings currently on the DataFort LCD.

**system version**

Displays current system version, including Platform Serial Number, Platform Firmware Version, Platform Firmware Build ID, database version, HBA firmware information, SEP information and System Card information.

**system reboot**

Reboots DataFort. Adding the **-p** flag to **system reboot** will power cycle the box. This is necessary after upgrades.

**system log list**

Lists system logs in the database. Various filtering options are available, for example:

Search for messages of priority 1 and type SEC:

```
system log list -p 1 -t SEC
```

Search for messages starting from 2002/1/17 1pm to 2pm (the interval **i** is in seconds):

```
system log list -b '2002-01-17 13:00:00' -i 3600
```

To search for messages of the last 24 hours:

```
system log list -b now -i -86400
```

To search for the last 10 messages:

```
system log list -o -10
```

## VERIFYING SYSTEM LOGS

1. To verify a signed log message, where the `<mesg>` parameter is a log message to be verified `"mesg-text [meta-data signature]"`:  
`system log verify <mesg>`
2. Single quotes, double quotes, and backslashes in the message must be preceded with a backslash and the entire message must be surrounded by double quotes. For example, to verify the following log message, execute the `system log verify` command that follows the log message:

```
2004-02-10 16:21:22 Local1.Info 10.20.21.163 Feb 10 16:21:22
boxmanager: Executed: share virtual add --ip "his" \\\his\\chi
"nas-hiro1" (sess id: 228933632) [AAAAAEMAAAFAAAAgnUpQA== 3NKQl8/
5r3x6n+Rw]

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

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

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

This returns:

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

The output indicates the validity of the message, and provides a trusted timestamp and counters to help verify that no messages are missing.

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

## STACK TRACE SETTINGS

DataFort has the capability to dump a trace of the platform execution stack in the event of a kernel panic. This stack trace information is useful for debugging, but may expose DataFort state information. Decru does not believe that this information poses a security risk or leaks any user or critical data, as no function arguments are leaked in the trace. However, the administrator should determine whether or not stack trace dumps should be enabled. To change the stack trace setting, log into the CLI and execute the appropriate **system property** command:

Stack trace is on by default. To disable stack trace:

```
system property set sys.stacktrace.enabled 0
```

To enable stack trace:

```
system property set sys.stacktrace.enabled 1
```

To retrieve a stack trace:

```
system util stacklog
```

## NETWORK MANAGEMENT

The following network commands are useful in managing the network:

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

## BACKUP MANAGEMENT

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

|                  |                                                                                                                                                                                                                                                                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>db export</b> | The CLI command <b>db export</b> can be used for manual configuration database backups, such as to the LKM server or another designated site. Enter <b>db export ?</b> to see the options, and see LKM documentation for more information. Using the interactive backup mode ( <b>db export -u</b> ) will require that a user name and password be entered. |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



## ■ ■ ■ ■ 18 TROUBLESHOOTING

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

- [Restoring a DataFort Appliance](#)
- [Front Panel LEDs](#)
- [Power Supply LEDs](#)
- [Network Connections and Management Interfaces](#)
- [SCSI Network](#)
- [Clusters](#)
- [Smart Cards](#)
- [Hardware Issues](#)

## RESTORING A DATAFORT APPLIANCE

---

If a standalone DataFort is lost, a saved configuration database from that DataFort can be used to configure a replacement DataFort. The recovered DataFort will then be able to retrieve data that was encrypted using the previous DataFort. The Setup Wizard assigns a new DataFort the configuration from a pre-existing DataFort. The replacement DataFort will retain all parameters stored in the configuration database of the original DataFort, including network, Cryptainer, access control and encryption key information.

If a cluster member is lost, it should not be restored using the wizard. It should be deleted from the cluster and replaced as described in [Adding a Cluster Member](#) on page 121. Use the wizard to restore the head of a cluster only if all members have been lost.

The procedure is conducted by a Full Administrator. The recovery procedure requires:

- A new or reset System Card.
  - A new or zeroized DataFort.
  - The minimum set of Recovery Officers and Recovery Cards as determined by the recovery schema of the cluster.
  - A saved database from the DataFort that is to be restored.
1. Connect the new or zeroized DataFort to the network and assign it the IP settings of the old DataFort. See [Assigning the DataFort IP Address](#) on page 33.
  2. Start the wizard. See [Initializing DataFort Appliances](#) on page 37.
  3. At the Recover from Database page, browse to the saved configuration database.  
DataFort will need the minimum number of Recovery Cards required for recovery procedures (as set in the original configuration). You will be prompted to insert Recovery Cards from the original DataFort configuration.
  4. Complete the wizard.

## FRONT PANEL LEDs

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

**TABLE 14: FRONT PANEL DUAL LEDs - 2U**

| LED Name    | Position | Color | Behavior | Indication                                                    |
|-------------|----------|-------|----------|---------------------------------------------------------------|
| Status LED  | Top      | Green | Solid    | DataFort on network, no errors                                |
|             |          | Red   | Solid    | Error Alarm; DataFort not functional. Check LCD for messages. |
| Network LED | Bottom   | Green | Blinking | Network link, activity                                        |
|             |          |       | Solid    | Network link, idle                                            |
|             |          | Red   | Solid    | Network error                                                 |

## POWER SUPPLY LEDs

The power supply module on the 2U model DataFort provides a single external bicolor LED to indicate the status of the power supply. When AC is applied to the power supply unit and standby voltages are available, the LED will blink green. The LED will be solid green to indicate that all the power outputs are available. It will be solid amber to indicate that the power supply has failed, there is a shutdown due to over-current, over-temperature, or if the unit is indicating a predictive failure.

**TABLE 16: POWER SUPPLY LEDs**

| Power Supply Condition                                         | Power Supply LED |
|----------------------------------------------------------------|------------------|
| No AC power to all power supply units                          | Off              |
| No AC power to this power supply unit only                     | Amber            |
| AC present / Only standby outputs on                           | Blink green      |
| Power supply DC outputs ON and OK                              | Green            |
| Power supply failure (includes over voltage, over temperature) | Amber            |
| VRM failure (voltage regulator module - cage related)          | Blink green      |
| 240VA limit (cage related)                                     | Blink green      |
| Current limit                                                  | Amber            |

## NETWORK CONNECTIONS AND MANAGEMENT INTERFACES

[Table 17](#) contains troubleshooting tips for the network and management connections to DataFort.

**TABLE 17: NETWORK CONNECTIONS AND MANAGEMENT INTERFACES**

| Problem                                                      | Possible Cause and Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No Ethernet network connection                               | <ul style="list-style-type: none"> <li>• Check the LCD on the front panel for messages. Check that the management port is connected.</li> <li>• DataFort must have an IP address assigned. See <a href="#">Assigning the DataFort IP Address</a>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Power not on                                                 | <ul style="list-style-type: none"> <li>• On 2U DataFort: The Power LED is solid green after the power switch is turned on. If the LED is not lit, the power source may be bad. Check both power cables, and if necessary plug the power cables into another power source.</li> <li>• Check power cable and if necessary plug the cable into another power source.</li> <li>• If the front panel LED is not lit, use the power switch to turn DataFort on.</li> </ul>                                                                                                                                                                                                                                                    |
| There is no output on serial console                         | <ul style="list-style-type: none"> <li>• 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.</li> <li>• Be sure the COM port connected to the serial cable is on and working correctly. Use a different workstation if the COM port is not functioning.</li> <li>• Check cabling. Use only the connector provided by Decru and a straight-through cable to connect to the serial port. Make sure the cable is connected to the port marked <b>IOIOI</b> on DataFort.</li> </ul>                                                                                                                                           |
| Cannot log in via serial connection                          | <ul style="list-style-type: none"> <li>• Check that you are logging in with a valid username and password.</li> <li>• Try logging in again using the defaults: User: <b>user</b>, Password: <b>MTKNMTKN</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Cannot connect to IP address                                 | <ul style="list-style-type: none"> <li>• Check that IP settings were set and saved after initialization. See <a href="#">Assigning the DataFort IP Address</a>.</li> <li>• Make sure the DataFort IP address is reachable on the network from the Management Station.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Cannot connect to domain name of DataFort                    | <ul style="list-style-type: none"> <li>• The DataFort domain name must be added to the domain by the administrator, and the name must be resolvable by DNS. If not, use the IP address instead.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Cannot clear alert after using CryptoShred button            | <ul style="list-style-type: none"> <li>• The CryptoShred button must be in a normal state to allow operations to be restored. See <a href="#">CryptoShred Button States</a>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| LCD says Intrusion Detected                                  | <ul style="list-style-type: none"> <li>• Intrusion detection occurs when the chassis of the DataFort is opened.</li> <li>• Log in to the DataFort WebUI and reset the tamper detection alert. See <a href="#">Clearing a Defense Alert</a>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| LCD asks for System Card or Status LED is red on 2U DataFort | <ul style="list-style-type: none"> <li>• A System Card needs to be inserted before DataFort is powered on. Once DataFort is powered on, the System Card can be removed, but messages will appear about this condition.</li> <li>• For a DataFort that has not been configured, switch DataFort off, and re-insert the System Card before switching it back on. Make sure the System Card is inserted all the way into the front panel slot, with gold contacts facing up and to the back of the slot.</li> <li>• A configured DataFort may have a security setting in place that will halt operations if the DataFort is rebooted without a System Card. See <a href="#">Collecting Network Information</a>.</li> </ul> |

**TABLE 17: NETWORK CONNECTIONS AND MANAGEMENT INTERFACES (CONTINUED)**

| Problem                                                               | Possible Cause and Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cannot log in to DataFort WebUI                                       | <ul style="list-style-type: none"> <li>• To access the DataFort WebUI you must have access to the DataFort's IP address from the Management Station. Make sure DataFort and the Management Station are on the same network.</li> <li>• If Secure Web is turned on, a valid administrator name and Admin Card are needed when logging in.</li> <li>• TLS 1.0 must be explicitly enabled in Internet Explorer. See <a href="#">Preparing the Management Station</a>.</li> <li>• If Secure Web is on, Terminal Services or Remote Desktop cannot be used to access the WebUI.</li> <li>• Some administrators are created requiring login authorization by another administrator. If dual authentication is required for the administrator attempting to log in, an authenticating administrator must log in first. See <a href="#">Requiring Authorization for Login</a>.</li> </ul> |
| Establishing the initial connection to the WebUI is slow or times out | <ul style="list-style-type: none"> <li>• In the Internet Explorer Tools &gt; Internet Options &gt; Advanced &gt; Security menu, uncheck the "Check for publisher's certificate revocation option." When checked, Internet Explorer will connect to companies that provide certificate revocation checking and download a CRL (Certificate Revocation List) file. If the Management Station has no connection to the Internet, this may time out.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Cannot log in to DataFort CLI                                         | <ul style="list-style-type: none"> <li>• Check that you are logging in with a valid username and password.</li> <li>• Try logging in again using the defaults: User: <b>user</b>, Password: <b>MTKNMTKN</b>.</li> <li>• Check that Secure CLI is not on.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Lost login information for only administrator                         | <ul style="list-style-type: none"> <li>• Log in using a Recovery Card and zeroize the appliance. See <a href="#">Emergency Serial Console Port Access</a>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Need to turn off WebUI smart card requirement (Secure Web) via CLI    | <ul style="list-style-type: none"> <li>• If you are unable to access the WebUI in order to turn off the smart card requirement, you can do so via CLI:</li> <li>• Log in to the CLI and enter: <b>system property get sys.security.web.usesmartcard</b> to check the setting. A setting of <b>1</b> requires the Admin Card in order to log in to the WebUI; <b>0</b> disables the requirement. If necessary, enter: <b>system property set sys.security.web.usesmartcard 0</b> to disable the smart card requirement. A Security or Full Administrator can set this property.</li> </ul>                                                                                                                                                                                                                                                                                         |
| CLI sessions take a long time to establish                            | <ul style="list-style-type: none"> <li>• This can occur if the DNS servers are unavailable. Log in through WebUI and change the DNS servers, or wait for the SSH to connect and then change the DNS servers from the CLI.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

SCSI NETWORK

Table 18 contains troubleshooting tips for SCSI environments.

TABLE 18: SCSI NETWORK

| Problem     | Possible Cause and Solution                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SCSI ID     | <ul style="list-style-type: none"><li>• Verify that each device has a unique SCSI ID that is unique to both on the host-side and the storage-side SCSI chain to avoid a SCSI ID conflict. Note that the DataFort storage-side HBA can have the same SCSI as the host since it presents itself as the host to the storage.</li></ul>                                                                                      |
| Termination | <ul style="list-style-type: none"><li>• Verify that each SCSI chain is properly terminated and that physical terminators are securely connected and screwed into place. An improperly terminated SCSI chain prevents the DataFort appliance from properly seeing devices on the chain.</li><li>• Access the host's HBA configuration and force termination, or introduce a physical terminator into the chain.</li></ul> |
| LVD         | <ul style="list-style-type: none"><li>• Verify all devices in each SCSI chain are LVD (Low Voltage Differential) devices. If an HVD device is present, a converter must be used.</li></ul>                                                                                                                                                                                                                               |
| Cabling     | <ul style="list-style-type: none"><li>• Confirm that the cables used are securely connected at both ends and that the connector screws are screwed into place.</li><li>• Verify cables are in good working order. When running into inconsistent performance or connectivity issues, replace the cables with a set of known good ones.</li></ul>                                                                         |

CLUSTERS

Table 19 includes troubleshooting tips for cluster management issues.

TABLE 19: CLUSTERS

| Problem                                              | Possible Cause and Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cluster won't form to start with                     | <ul style="list-style-type: none"><li>• If the cluster will not form (it remains in an aborted/recover state), verify network settings of all DataFort devices.</li><li>• Be sure each DataFort has a valid, unexpired license for clustering.</li><li>• Execute <code>cluster stat</code> on each of the members in the cluster.</li><li>• If there are two members that are not communicating, disable both of them and then bring them back one at a time, making sure that the cluster forms with each addition. Use the <code>cluster disable</code> command for this.</li><li>• Check for other problem with a cluster member that will not join the cluster, including any crypto errors.</li></ul> |
| Cluster member goes down and cluster will not reform | <ul style="list-style-type: none"><li>• Check that the loss of the cluster member has not dropped the number of devices in the cluster below quorum.</li><li>• Use the <code>cluster disable</code> command to remove an offline member from the cluster and redefine the number of members required for the quorum.</li></ul>                                                                                                                                                                                                                                                                                                                                                                             |

## SMART CARDS

[Table 20](#) contains troubleshooting tips for working with smart cards.

**TABLE 20: SMART CARDS**

| Problem                                                                                           | Possible Cause and Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Management Station doesn't detect Admin Card                                                      | <ul style="list-style-type: none"> <li>The DataFort installer places the necessary files on the Management Station. Reinstall the smart card reader software if necessary.</li> <li>The Management Station must be running Windows 2000, Windows Server 2003 or Windows XP and IE 6.0 or greater.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Lost System Card                                                                                  | <ul style="list-style-type: none"> <li>Be sure the Admin Card is properly inserted in the smart card reader. Re-insert the card if necessary. The reader LED should flash and then light continuously.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| DataFort WebUI does not recognize type of card inserted into Management Station smart card reader | <ul style="list-style-type: none"> <li>Zeroize, insert a new System Card and run the Setup Wizard.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Lost Admin Card when Secure WebUI is turned on                                                    | <ul style="list-style-type: none"> <li>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.</li> <li>Disconnect and re-connect the smart card reader.</li> <li>Close and open the web browser.</li> <li>Do not open the WebUI for more than one DataFort at a time on a single Management Station.</li> </ul>                                                                                                                                                                                                                                                                                                                                                          |
| Lost Admin Card when Secure WebUI is turned on                                                    | <ul style="list-style-type: none"> <li>Log in with a different Admin Card and associate a replacement Admin Card with an existing or new administrator.</li> <li>If all Admin Cards are lost and Secure CLI is not on, log in to the CLI and turn off Secure Web by entering: <code>system property set sys.security.web.usesmartcard 0</code> to disable the smart card requirement for the WebUI. Then log in to the WebUI and associate a replacement Admin Card with an existing or new administrator. A Security Administrator or Full Administrator can change the system property. A Full Administrator is required to create or change associations with an Admin Card.</li> <li>If both CLI and WebUI login are smart card enabled and all Admin Cards are lost, you will have to zeroize DataFort using the serial console.</li> </ul> |
| Problem with multiple smart card readers                                                          | <ul style="list-style-type: none"> <li>Multiple card readers are not supported for Cluster Recovery operations. Multiple card readers are only supported at the time of cluster formation.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Lost Recovery Card                                                                                | <ul style="list-style-type: none"> <li>Assemble a quorum of Recovery Officers and replace the Recovery Card.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Smart card errors appear                                                                          | <ul style="list-style-type: none"> <li>Use an eraser to clean the metal contact on the smart card.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## HARDWARE ISSUES

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

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



## ■ ■ ■ ■ **APPENDIX I    COMMAND LINE INTERFACE QUICK REFERENCE**

The CLI gives the administrator access to many DataFort management functions, but cannot be used for functions that require the presence of smart cards. The DataFort WebUI is the only interface that allows management of smart card enabled operations. This chapter includes the following topics:

- [Using the CLI](#)
- [CLI Command Overview](#)

Refer to the separate [DataFort CLI Reference Guide](#) for a complete list of commands and parameters.

## USING THE CLI

---

Some CLI commands must be executed in a specific order for desired results. For some commands, it is good practice to execute a verification command (such as **list**) after an action that adds an item to the database. Always perform a backup of the database after any changes.

- For login instructions, see [Connecting to the DataFort Command Line Interface](#) on page 58. There are two levels of security that can be set for DataFort CLI login, one of which requires first accessing the DataFort WebUI before logging into the CLI.
- As a security measure, the CLI will time out after 10 minutes of inactivity.

### CLI SYNTAX

- In the following pages, an ellipsis (...) after an entry indicates that the entry is a hierarchy, rather than a command. The top level commands include **system...** because there is no end command **system** although there is a system hierarchy of commands (**system reboot**, etc.).
- The plus (+) symbol indicates that an entry is a command which can take arguments. The command **quit** is not followed by + because it does not take arguments.

Note that + and ... are not intended to be typed in as commands, but serve as indications that more can be typed after a given entry.

### CLI HELP

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

## CLI COMMAND OVERVIEW

---

### TOP LEVEL COMMANDS

Type `?` to view the top level commands.

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

### DEVICE COMMANDS

Type `device ?` to view the device commands

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

## DISK COMMANDS

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

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

## FC SITE COMMANDS

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

|                  |                                                                 |
|------------------|-----------------------------------------------------------------|
| <b>list +</b>    | List all the FC sites in the configuration database             |
| <b>remove +</b>  | Delete the FC site settings for the specified DataFort          |
| <b>replace +</b> | Make the local DataFort a replacement for the specified FC site |

## KFC COMMANDS

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

|                       |                                                      |
|-----------------------|------------------------------------------------------|
| <b>config</b>         | Configure FC kernel                                  |
| <b>fw...</b>          | SAN kernel firmware commands...                      |
| <b>list +</b>         | Display SAN kernel statistics                        |
| <b>link...</b>        | SAN kernel link commands...                          |
| <b>request...</b>     | SAN kernel Request commands...                       |
| <b>reservation...</b> | SAN kernel Reservation commands...                   |
| <b>sync</b>           | Query the fabric to update the status of all devices |
| <b>util...</b>        | SAN kernel utility commands...                       |
| <b>vp...</b>          | SAN kernel virtual port commands...                  |
| <b>wwn...</b>         | Fibre Channel primary port node/port WWN utils...    |

## POOL COMMANDS

Type **pool ?** to view pool commands.

|                |                             |
|----------------|-----------------------------|
| <b>add +</b>   | Add a pool                  |
| <b>grant +</b> | Grant pool access to a host |

|                       |                                |
|-----------------------|--------------------------------|
| <code>group...</code> | Pool group commands...         |
| <code>key...</code>   | Pool key commands...           |
| <code>list +</code>   | List pools                     |
| <code>perm...</code>  | List pool permissions...       |
| <code>remove +</code> | Remove a pool                  |
| <code>revoke +</code> | Revoke pool access from a host |
| <code>set +</code>    | Set pool settings              |

## TAPE COMMANDS

Type `tape ?` to view tape commands.

|                        |                        |
|------------------------|------------------------|
| <code>history +</code> | List tape keys history |
| <code>list +</code>    | List tapes             |
| <code>remove +</code>  | Remove a tape          |

## CLI FORMATTING COMMANDS

Type `cli ?` to view CLI formatting commands.

|                              |                                                                                             |
|------------------------------|---------------------------------------------------------------------------------------------|
| <code>complete +</code>      | Command line completion                                                                     |
| <code>cshelp...</code>       | CLI context-sensitive help commands...                                                      |
| <code>documentation +</code> | Print CLI documentation (cli documentation according to the role of user that is logged in) |
| <code>format +</code>        | Change CLI display format                                                                   |
| <code>pager +</code>         | Turn on/off screenful CLI output display pager                                              |

## HELP COMMAND

Type `help` to view the top level command list.

|                     |                         |
|---------------------|-------------------------|
| <code>help +</code> | Command line usage help |
|---------------------|-------------------------|

## QUIT COMMAND

Type `quit` to quit the CLI session.

|                   |                                 |
|-------------------|---------------------------------|
| <code>quit</code> | Quit the current client session |
|-------------------|---------------------------------|

## ACTIVE-ROLE COMMANDS

Type `active-role to` to view active role commands.

|                       |                             |
|-----------------------|-----------------------------|
| <code>add +</code>    | Activate an authorized role |
| <code>list</code>     | List active roles           |
| <code>remove +</code> | Remove an active role       |

## AUTHORIZE COMMAND

Type `authorize` to authorize an admin login

|                        |                          |
|------------------------|--------------------------|
| <code>authorize</code> | Authorize an admin login |
|------------------------|--------------------------|

## PASSWORD COMMAND

Type **password** to change an admin password.

**password +** Change password

## ROLE COMMANDS

Type **role** to view role commands.

**list +** List roles

**path...** Role path commands...

## USER COMMANDS

Type **user** to view user commands.

**add +** Add a user account

**list +** List all users in database

**remove +** Remove a user from the database

**role...** User role commands...

**set +** Set user settings

## WHOAMI COMMAND

Type **whoami** to see the current user ID.

**whoami** Display effective user ID

## TRUSTEE COMMANDS

Type **trustee ?** to view trustee commands.

**delete +** Remove trustee from the system

**keys..** Trustee key export and import commands...

**list +** List all the approved trustees in the system

**unapproved..** Trust establishment commands for unapproved trustees...

## NETWORK COMMANDS

Type **net ?** to view network management commands.

**apply +** Apply network changes

**connection...** Network connection administration commands...

**interface...** Network interface commands...

**status +** Display network status

**util...** Network utilities...

## KEY MANAGEMENT COMMANDS

Type **keyman** to view key management commands.

**cryptainerkeys +** Query Cryptainer Keys

**lkmkeys +** LKM key management commands...

|                     |                                         |
|---------------------|-----------------------------------------|
| <b>masterkeys +</b> | Query Master Keys                       |
| <b>purgekeys</b>    | Purge unused Cryptainer and Master Keys |

## LKM MANAGEMENT COMMANDS

Type **lkm** to view Lifetime Key Management commands.

|                 |                                                                 |
|-----------------|-----------------------------------------------------------------|
| <b>status</b>   | Check the status of the connection to the configured LKM System |
| <b>erver...</b> | Server commands...                                              |

## CLUSTER COMMANDS

Type **cluster ?** to view the cluster commands.

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

## DATABASE COMMANDS

Type **db ?** to view database management commands.

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

## SYSTEM COMMANDS

Type **system** to view system commands.

|                     |                             |
|---------------------|-----------------------------|
| <b>agreement...</b> | Agreement commands...       |
| <b>crypto...</b>    | Crypto commands...          |
| <b>check +</b>      | Perform basic system checks |
| <b>date...</b>      | Date commands...            |
| <b>httpd...</b>     | HTTPD commands...           |
| <b>license...</b>   | License commands...         |
| <b>log...</b>       | System log commands...      |

|                          |                                                            |
|--------------------------|------------------------------------------------------------|
| <code>ntpd...</code>     | NTPD commands...                                           |
| <code>property...</code> | Property commands...                                       |
| <code>reboot +</code>    | Reboot the system                                          |
| <code>selftest +</code>  | Perform system selftest                                    |
| <code>sensors</code>     | Display system sensors                                     |
| <code>serial</code>      | Display DataFort serial number                             |
| <code>snmp...</code>     | SNMP commands...                                           |
| <code>sshd...</code>     | SSHD private key commands...                               |
| <code>tamper...</code>   | Tamper commands...                                         |
| <code>timers...</code>   | System timer commands...                                   |
| <code>timezone...</code> | Timezone commands...                                       |
| <code>upgrade +</code>   | Upgrade the system                                         |
| <code>util...</code>     | System utilities...                                        |
| <code>version +</code>   | Display the version of all system components               |
| <code>zeroize +</code>   | Zeroize all key material and delete configuration database |

## ■ ■ ■ ■ ■ APPENDIX II LOGGING FUNCTIONS

The DataFort audit function logs security relevant operations, errors, and warnings and many non-security relevant operations, errors and warnings.

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

Log purging is defined independently for each of the log storage locations. Note that the same log may be stored in more than one of the storage locations, or none of the storage locations (in which case the log message is not produced). See the following sections for information about logging:

- [DataFort Log Event and Priority Types](#)
- [Log Storage Locations](#)
- [Log Presentation](#)
- [Log Messages](#)

**Note:** This appendix contains references to Common Criteria mode configuration and settings specifically supported in that mode. The Common Criteria is an international standard for evaluating information technology security. The ability to run in a mode qualified to meet Common Criteria standards is an enhanced security option for DataFort. See separate documentation on operating in Common Criteria mode for more information.

DATAFORT LOG EVENT AND PRIORITY TYPES

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

**Note:** In Common Criteria mode only the Security logs are enabled. The operations logs and performance logs are not enabled.

The following logs are maintained:

TABLE 21: LOG TYPES

|                  |                               |
|------------------|-------------------------------|
| Security Logs    |                               |
|                  | High priority security log    |
|                  | Low priority security log     |
| Operations Logs  |                               |
|                  | Operations alert log          |
|                  | Operations warning log        |
|                  | Operations informational log  |
|                  | Operations debug log          |
|                  | Operations alert log          |
| Performance Logs |                               |
|                  | High priority performance log |
|                  | Low priority performance log  |
|                  | High priority performance log |

LOG STORAGE LOCATIONS

For each of the DataFort logs, the administrator may select multiple storage locations. Whenever a new log message is generated, it is written to storage location(s) as configured for the log the message belongs to. The following storage options are available:

- Temporary storage

Logs stored in the temporary storage location are written to RAM within the DataFort appliance. Note that log messages of the same event type (but different severity) are aggregated in temporary storage (i.e. Security logs, Operations logs, Performance logs).
- Database storage

Logs stored in the database storage location are written to the DataFort appliance configuration database.
- Remote storage

The DataFort appliance forwards a log message to a remote syslog host whenever a generated log message is of an event and priority type for which the administrator has specified remote storage. For remotely stored logs, the administrator may also optionally specify log message signing, in which case the DataFort appliance appends a signature to the exported log message.

**TABLE 22: DEFAULT LOG STORAGE LOCATIONS**

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

## LOG PRESENTATION

---

### TEMPORARY LOGS

The administrator may view log messages stored in RAM by issuing the `sys util cat` CLI command, with one of the following parameters:

```

/var/log/security
/var/log/operations
/var/log/performance
/var/log/audit

```

The logs shown for each selectable location are dependent on the configuration options the administrator has chosen for temporary storage locations.

All outputted log messages include:

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

### DATABASE LOGS

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

#### Viewing database logs via CLI

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

Log messages are listed in the following format:

```
<SEQ> <DATE> <CAT> <MSG>
```

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

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

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

- <16.[4,3,2,1,0]>: High priority Security Log
- <16.[7,6]>: Low priority Security Log
- <17.[1,0]>: Operations Alert Log
- <17.4>: Operations Warning Log
- <17.6>: Operations Informational Log
- <17.7>: Operations debug Log

<MSG> is the log message.

### Viewing database logs via WebUI

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

All outputted log messages include:

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

### REMOTE LOGS

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

**<PRI> <TIME> ' ' <MSG>**

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

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

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

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

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

**TABLE 23: DataFort EVENT AND PRIORITY CORRESPONDENCE TO SYSLOG FACILITY AND SEVERITY**

| DataFort Log                  | Syslog facility | Syslog priority |
|-------------------------------|-----------------|-----------------|
| High Priority Security Log    | LOG_LOCAL0 (16) | 1,0             |
| Low Priority Security Log     | LOG_LOCAL0 (16) | 4,3,2,1,0       |
| 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) | <<>>            |
| Low priority performance log  | LOG_LOCAL2 (18) | <<>>            |

The administrator may configure the DataFort to sign log messages. The configuration option is available separately for each DataFort log. If configured, metadata and signature fields are appended to the exported log message:

```
<PRI> <TIME> ' ' <MSG> '[' <MDATA> ' ' <SIG> ' ']
```

The <MDATA> field includes the following base 64 encoded bytes:

```
0x0000000000 padding
4 bytes local sequence number
4 bytes global sequence number
4 bytes timestamp
```

The local sequence number is the message sequence number with respect to the specific DataFort log. The global sequence number is the message sequence number with respect to all DataFort generated logs. Note that the DataFort maintains sequence numbers across power cycles.

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

```
<MSG> ' ' '[' <MDATA>
```

The computed signature is the first 12 bytes of a SHA\_1 based HMAC. The 12 byte signature is then appended to the message. The following are example <MDATA> and <SIG> fields:

```
[AAAAAKxXAAC4FWAA6tgoQg== b/hPTEecqTCpD/Mk]
[AAAAAHAdAAC5FWAA69goQg== fN1evQzBytL/ulfz]
```

## LOG PURGING

DataFort purges stored log messages depending on what type of storage location is selected for the log type. The purging operation is independent for the same message stored in multiple locations.

### Temporary storage log messages

DataFort checks for maximum space requirements on log messages stored in RAM at 5 minute intervals. Separate checks are performed for each aggregation of log messages.

**TABLE 24: SPACE ALLOWANCES FOR TEMPORARILY STORED DATAFORT LOG MESSAGE**

| DataFort log                                                                                           | Meaning                                            | Max size |
|--------------------------------------------------------------------------------------------------------|----------------------------------------------------|----------|
| High priority security log<br>Low priority security log                                                | combined size of high / low priority security logs | 100kB    |
| Operations alert log<br>Operations warning log<br>Operations informational log<br>Operations debug log | combined size of all operations logs               | 1000kB   |
| High priority performance log<br>Low priority performance log                                          | combined size of both performance logs             | 500kB    |

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

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

A 10 second timer triggers checks for the previous conditions.

#### Database storage log messages

The log database has a saturation limit of 2500 events. When that limit is hit, the system should delete old events based on the following criteria.

Log messages should be deleted so that the last 925 high priority and 1330 low priority messages remain in the log database.

#### Audit configuration

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

#### WebUI configuration

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

#### WebCLI configuration

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

**TABLE 25: 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     |

**TABLE 25: AUDIT CONFIGURATION DATABASE PROPERTIES (CONTINUED)**

|                                  |                               |
|----------------------------------|-------------------------------|
| 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 26: AUDIT FUNCTION WEBCLI CONFIGURATION LIST PARAMETERS**

| Audit function configuration list parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ldb                                         | If present in the comma separated list, logs of this type will use the database storage location.                                                                                                                                                                                                                                                                                                                                                                                                         |
| @<hostname>                                 | If present in the comma separated list, logs of this type will be forwarded to a remote syslog host, as indicated by the <hostname> parameter. Note, the DataFort will resolve hostnames before allowing the configuration change to occur. Multiple hosts may be specified in separate comma separated list entries.                                                                                                                                                                                     |
| \$<filepath>                                | If present in the comma separated list, logs of this type will be stored to a temporary file in a ram based file system. Valid options for <filepath> include:<br>· /var/log/security<br>· /var/log/operation<br>· /var/log/performance<br>· /var/log/audit (E-Series product only)<br>If a configuration is specified using a filepath not in the previous list, the audit function configuration will not be changed. Note that any of the previous filepaths may be specified for any syslog property. |
| sign                                        | If present in the comma separated list, logs of this type will be signed by the DataFort, before export to a remote syslog host. The parameter has no effect on the audit function if no remote hosts are specified. Specifying the sign parameter with no log storage destinations is not a valid input, and the audit configuration will not be changed.                                                                                                                                                |
| disabled                                    | If present in the comma separated list, logs of this type will be disabled. Specifying the disable option with any other parameters is not a valid input, and the audit configuration will not be changed.                                                                                                                                                                                                                                                                                                |

## LOG MESSAGES

This section lists all log messages that may be issued by the DataFort when running in the Common Criteria evaluated configuration. Log messages are broken into the following categories:

- [IFC Logs](#)
- [Audit Logs](#)
- [Auth Logs](#)
- [Security Management Logs](#)
- [Integrity Logs](#)

For each category, a table lists parameters that may appear in log messages for that category. Any log message parameters not described in this table are described with the log message.

### IFC Logs

IFC log messages are generated when Information Flow Control rules either deny an unauthorized information flow, or allow an authorized information flow. See:

- [Generic parameters in IFC function log messages](#)
- [IFC function log messages](#)

**TABLE 27: GENERIC PARAMETERS IN IFC FUNCTION LOG MESSAGES**

| Parameter       | Description                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <client>        | 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                                                                                                                                                                                                                                                      |
| <cryptainer>    | The 16 byte ID of the Cryptainer from which the information flow is requested: 0XXXXXXXXXXXXXXXXXXXXXXXXXXXXX                                                                                                                                                                                                                                                                |
| <reason>        | The reason parameter indicates the IFC rule that caused access denial.<br><reason> may be: <ul style="list-style-type: none"> <li>• port locking rule—the host is not connected via the required port number</li> <li>• authentication rule—the host is not authenticated</li> <li>• authorized flow rule—the host is requesting an unauthorized information flow</li> </ul> |
| <serial_number> | Serial number of DataFort that denied or allowed the information flow                                                                                                                                                                                                                                                                                                        |

**TABLE 28: IFC FUNCTION LOG MESSAGES**

| Log Message   | Log Message description |                                                                                                                                   |
|---------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| ACCESS_DENIED | Level                   | WARNING                                                                                                                           |
|               | Message                 | <client> was denied access to Cryptainer <cryptainer> because it violated the <reason> at DataFort <serial_number>                |
|               | Description             | A host made a request that either violated an access rule (port locking, DHA) or would have resulted in illegal information flow. |

## Audit Logs

Audit logs are generated by the DataFort audit function when modifications to its configuration or state are made. See:

- [Generic parameters in audit function log messages](#)
- [Audit function log messages](#)

**TABLE 29: GENERIC PARAMETERS IN AUDIT FUNCTION LOG MESSAGES**

| Parameter       | Description                                                      |
|-----------------|------------------------------------------------------------------|
| <serial number> | Serial number of the DataFort that generated the log message     |
| <user>          | Username of the user that changed the configuration parameter    |
| <domain>        | Domain name of the user that changed the configuration parameter |
| <prop_name>     | Name of a logging facility configuration property (see Table 4). |

**TABLE 30: AUDIT FUNCTION LOG MESSAGES**

| Log Message        | Log Message description |                                                                                                                                                                  |
|--------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUDIT_STARTED      | Level                   | INFO                                                                                                                                                             |
|                    | Message                 | Audit function started at DataFort <serial_number>                                                                                                               |
|                    | Description             | This log message is issued when the DataFort audit function starts: when the machine boots, when the audit configuration changes, or on issuing sys log restart. |
| AUDIT_STOPPED      | Level                   | INFO                                                                                                                                                             |
|                    | Message                 | Audit function stopped at DataFort <serial_number>                                                                                                               |
|                    | Description             | This log message is issued when the machine shuts down, when the audit configuration is changes, or on issuing sys log restart.                                  |
| AUDIT_CONF_ADDED   | Level                   | INFO                                                                                                                                                             |
|                    | Message                 | <user>@<domain> added audit configuration <prop_name> and set to <prop_value> at DataFort <serial_number>                                                        |
|                    | Description             | This log message is issued when a new audit configuration is added. This should not occur in runtime operation, but may occur during the course of an upgrade.   |
| AUDIT_CONF_CHANGED | Level                   | INFO                                                                                                                                                             |
|                    | Message                 | <user>@<domain> changed audit configuration <prop_name> to <prop_value> at DataFort <serial_number>                                                              |
|                    | Description             | This log message is issued when the administrator changes one of the database properties.                                                                        |

**TABLE 30: AUDIT FUNCTION LOG MESSAGES (CONTINUED)**

|                    |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUDIT_LOG_REPEATED | Level       | Varies, depending on repeated log message level                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                    | Message     | last message repeated <n> times                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                    | Description | This message is displayed if a log message is repeated with no intermediary log message. If a message is repeated, log output is held for 30 seconds to capture additional repeat messages. The AUDIT_LOG_REPEATED message is displayed when a different log message is generated, or at the end of the 30 second hold period. If the same message is repeated for more than 30 seconds, the interval is increased to 120 seconds, and after 120 seconds to 600 seconds. The interval is reset to 30 seconds when the first non-repeat message is generated. |

## AUTH LOGS

Auth logs are generated to record authentication requests and decisions made by the DataFort appliance. See:

- [Generic parameters in audit function log messages](#)
- [Authentication function log messages](#)

**TABLE 31: GENERIC PARAMETERS IN AUDIT FUNCTION LOG MESSAGES**

| Parameter   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <usertype>  | ADMIN or USER                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <user>      | Username of the user that attempted to authenticate                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <interface> | Interface to which the user is attempting to authenticate, may be: <ul style="list-style-type: none"> <li>• CLI—The user is authenticating to the CLI interface. Note that this interface is disabled in the CC evaluated configuration.</li> <li>• WEBUI—The user is authenticating to the WebUI interface. Note that administrators may use the WebCLI interface after authenticating to the WebUI interface.</li> <li>• SERIAL—The user is authenticating to the DataFort MenuShell interface.</li> </ul> |
| <client>    | IP address from which the user is authenticating                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <reason>    | Reason for authentication failure, may be: <ul style="list-style-type: none"> <li>• USERPASS—The user entered an incorrect password.</li> <li>• SMARTCARD—The user attempted to authenticate using the wrong smart card.</li> </ul>                                                                                                                                                                                                                                                                          |
| <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                                                                                                                                                                                                                                                                                                                                                                                         |

**TABLE 32: AUTHENTICATION FUNCTION LOG MESSAGES**

| Log Message      | Log Message description |                                                                                                                     |
|------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------|
| AUTH_DENIED      | Level                   | WARNING                                                                                                             |
|                  | Message                 | <usertype> <user> <interface> login from <client> failed due to <reason> at DataFort <serial>                       |
|                  | Description             | A user authentication failed. Note that there are no non-ADMIN users in the FC-Series DataFort.                     |
| AUTH_GRANTED     | Level                   | INFO                                                                                                                |
|                  | Message                 | <usertype> <user> <interface> login from <client> succeeded at DataFort <serial>                                    |
|                  | Description             | A user authentication succeeded. Note that there are no non-ADMIN users in the FC-Series DataFort.                  |
| AUTH_DENIED_DHA  | Level                   | WARNING                                                                                                             |
|                  | Message                 | Host <wwn> DHA login failed <count> time(s) at DataFort <serial>                                                    |
|                  | Description             | A host failed the DHA protocol. <count> indicates the number of failures that have occurred in the last 60 seconds. |
| AUTH_GRANTED_DHA | Level                   | INFO                                                                                                                |
|                  | Message                 | Host <wwn> DHA login succeeded at DataFort <serial>                                                                 |
|                  | Description             | A host successfully ran the DHA protocol.                                                                           |

## SECURITY MANAGEMENT LOGS

Security Management logs are generated to record changes to authentication policies. See:

- [Generic parameters in Security management function log messages](#)
- [Authentication function log messages](#)

**TABLE 33: GENERIC PARAMETERS IN SECURITY MANAGEMENT FUNCTION LOG MESSAGES**

| Parameter     | Description                                                                                                                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <usertype>    | ADMIN or USER                                                                                                                                                                                                                                |
| <user>        | username                                                                                                                                                                                                                                     |
| <domain>      | Domain (usually null or DataFort)                                                                                                                                                                                                            |
| <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. |
| <admin>       | This parameter indicates a DataFort administrator.                                                                                                                                                                                           |

**TABLE 33: GENERIC PARAMETERS IN SECURITY MANAGEMENT FUNCTION LOG MESSAGES (CONTINUED)**

|                    |                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <cryptainer>       | The 16 byte ID of the Cryptainer from which the information flow is requested: 0XXXXXXXXXXXXXXXXXXXXXXXXXXXXX                                   |
| <cryptainer_group> | This parameter indicates a group of Cryptainers, as defined by the DataFort administrator. The parameter is a text string, up to 31 characters. |
| <host>             | This parameter refers to a host, by WWN.                                                                                                        |
| <host_group>       | This parameter indicates a group of hosts, as defined by the DataFort administrator. The parameter is a text string, up to 31 characters.       |
| <pool>             | This parameter refers to a tape pool.                                                                                                           |
| <pool_group>       | This parameter indicates a group of tape pools, as defined by the DataFort administrator. The parameter is a text string, up to 31 characters.  |

**TABLE 34: AUTHENTICATION FUNCTION LOG MESSAGES**

| Log Message                        | Log Message description |                                                                                                                                                                                                                                                      |
|------------------------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SECMAN_USER_CREATED                | Level                   | INFO                                                                                                                                                                                                                                                 |
|                                    | Message                 | <user>@<domain> created new <usertype> <user_target>@<domain_target> in group <group> at DataFort <serial>                                                                                                                                           |
|                                    | Description             | This log message is issued when a new user is created. Note that in the FC-Series DataFort, all users are of usertype ADMIN, and in the domain DATAFORT_ADMIN. The group of an administrator corresponds to the role assigned to that administrator. |
| SECMAN_USER_DELETED                | Level                   | INFO                                                                                                                                                                                                                                                 |
|                                    | Message                 | <user>@<domain> deleted <usertype> <user_target>@<domain_target> in group <group> at DataFort <serial>                                                                                                                                               |
|                                    | Description             | This log message is issued when a user is deleted. <user>, <domain>, and <usertype> correspond to the user that performed the action. <user_target>, <domain_target>, and <group> correspond to the user that was deleted.                           |
| SECMAN_USER_CHANGED                | Level                   | INFO                                                                                                                                                                                                                                                 |
|                                    | Message                 | '\$type' <user>' '\$attr' changed by <user>_admin'                                                                                                                                                                                                   |
|                                    | Description             | Not used                                                                                                                                                                                                                                             |
| SECMAN_FCHOST_DHA_PASSWORD_CHANGED | Level                   | INFO                                                                                                                                                                                                                                                 |
|                                    | Message                 | Host <host> DHA password changed by administrator <admin> at DataFort <serial>                                                                                                                                                                       |
|                                    | Description             | A DataFort administrator changed the DHA password of a host.                                                                                                                                                                                         |

**TABLE 34: AUTHENTICATION FUNCTION LOG MESSAGES (CONTINUED)**

|                                                   |             |                                                                                                                                                                           |
|---------------------------------------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SECMAN_FCHOST_DHA_PASSWORD_REMOVED                | Level       | INFO                                                                                                                                                                      |
|                                                   | Message     | Host <host> DHA password removed by administrator <admin> at DataFort <serial>                                                                                            |
|                                                   | Description | A DataFort administrator disabled the DHA requirement for a host.                                                                                                         |
| SECMAN_FCHOST_RAID_ADMIN_MODE_CHANGED             | Level       | INFO                                                                                                                                                                      |
|                                                   | Message     | Host <host> RAID administrator mode changed to <state> by administrator <admin> at DataFort <serial>                                                                      |
|                                                   | Description | A DataFort administrator granted or revoked RAID administrator access to a host. <state> may be either OFF or ON.                                                         |
| SECMAN_FCHOST_PORT_LOCK_MODE_CHANGED              | Level       | INFO                                                                                                                                                                      |
|                                                   | Message     | Host <host> port locking changed to <state> by administrator <admin> at DataFort <serial>                                                                                 |
|                                                   | Description | A DataFort administrator turned the port locking requirement ON or OFF for a host.                                                                                        |
| SECMAN_FCCRYPTAINER_CREATED                       | Level       | INFO                                                                                                                                                                      |
|                                                   | Message     | Cryptainer <cryptainer> on LUN <host_port_wwn>, <disk_port_wwn>, <lun> created by administrator <admin> at DataFort <serial>                                              |
|                                                   | Description | A DataFort administrator added a Cryptainer. <host_port_wwn>, <disk_port_wwn>, <lun> are the parameters specified by the administrator in the Cryptainer creation command |
| SECMAN_FCCRYPTAINER_ACCESS_PERMISSION_GRANTED     | Level       | INFO                                                                                                                                                                      |
|                                                   | Message     | Cryptainer <cryptainer> allowed information flows changed by administrator <admin> : granted access to Host <host> at DataFort <serial>                                   |
|                                                   | Description | A DataFort administrator added an authorized information flow to a Cryptainer.                                                                                            |
| SECMAN_FCCRYPTAINER_ACCESS_PERMISSION_REVOKED     | Level       | INFO                                                                                                                                                                      |
|                                                   | Message     | Cryptainer <cryptainer> allowed information flows changed by administrator <admin> : revoked access from Host <host> at DataFort <serial>                                 |
|                                                   | Description | A DataFort administrator removed an authorized information flow from a Cryptainer.                                                                                        |
| SECMAN_FCCRYPTAINER_ACCESS_PERMISSION_REVOKED_ALL | Level       | INFO                                                                                                                                                                      |
|                                                   | Message     | Cryptainer <cryptainer> allowed information flows changed by administrator <admin> : revoked access from all Hosts at DataFort <serial>                                   |
|                                                   | Description | A DataFort administrator removed all authorized information flows from a Cryptainer.                                                                                      |

**TABLE 34: AUTHENTICATION FUNCTION LOG MESSAGES (CONTINUED)**

|                                                     |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SECMAN_FCCRYPTAINER_DCS_CHANGED                     | Level       | INFO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                                                     | Message     | Cryptainer <cryptainer> allowed information flows changed by administrator <admin> : DCS requirement set to <requirement> at DataFort <serial>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                                     | Description | <p>A DataFort administrator changed the authentication requirements for access to a specific Cryptainer. The requirements may be one of:</p> <ul style="list-style-type: none"> <li>• off—No authentication requirements for this Cryptainer (an authentication requirement may still be placed on a SAN host)</li> <li>• DHA—This Cryptainer requires that any accessing host be authenticated with DHA</li> <li>• dcs—this requirement indicates that any accessing host be running the Decru DCS software. Note that no DCS configuration options are not part of the CC evaluated configuration.</li> </ul> |
| SECMAN_FCCRYPTAINER_GROUP_ACCESS_PERMISSION_GRANTED | Level       | INFO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                                                     | Message     | Cryptainer group <cryptainer_group> allowed information flows changed by administrator <admin> : granted access to Host group <host_group> at DataFort <serial>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                                                     | Description | A DataFort administrator granted authorized information flows for a group of Cryptainers. Authorized flows were created for each host that is a member of the <host_group> host group.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SECMAN_FCCRYPTAINER_GROUP_ACCESS_PERMISSION_REVOKED | Level       | INFO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                                                     | Message     | Cryptainer group <cryptainer_group> allowed information flows changed by administrator <admin> : revoked access from Host group <host_group> at DataFort <serial>                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                                                     | Description | A DataFort administrator removed information flows from a group of Cryptainers. Authorized flows were removed for each host that is a member of the <host_group> host group.                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**TABLE 34: AUTHENTICATION FUNCTION LOG MESSAGES (CONTINUED)**

|                                          |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SECMAN_FCCRYPTAINER_GROUP_DCS_CHANGED    | Level       | INFO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                          | Message     | Cryptainer group <cryptainer_group> allowed information flows changed by administrator <admin> : DCS requirement set to <requirement> at DataFort <serial>                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                          | Description | A DataFort administrator changed the authentication requirements for access to a all Cryptainers within the Cryptainer group <cryptainer_group>. The requirements may be one of:<br><ul style="list-style-type: none"> <li>• off—No authentication requirements for this Cryptainer (an authentication requirement may still be placed on a SAN host)</li> <li>• DHA—This Cryptainer requires that any accessing host be authenticated with DHA.</li> <li>• DCS—This requirement indicates that any accessing host be running the Decru DCS software.</li> </ul> |
| SECMAN_FCPPOOL_CREATED                   | Level       | INFO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                          | Message     | Pool <pool> created by administrator <admin> at DataFort <serial>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|                                          | Description | A DataFort administrator created a new tape pool.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SECMAN_FCPPOOL_ACCESS_PERMISSION_GRANTED | Level       | INFO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                          | Message     | Pool <pool> allowed information flows changed by administrator <admin> : granted access to Host <host> at DataFort <serial>                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                                          | Description | A DataFort administrator added an authorized information flow for the tape pool <pool> and the host <host>.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SECMAN_FCPPOOL_ACCESS_PERMISSION_REVOKED | Level       | INFO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                          | Message     | Pool <pool> allowed information flows changed by administrator <admin> : revoked access from Host <host> at DataFort <serial>                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                                          | Description | A DataFort administrator removed an authorized information flow for the tape pool <pool> and the host <host>.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SECMAN_FCPPOOL_KEY_POLICY_CHANGED        | Level       | INFO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                          | Message     | Pool <pool> key policy is changed to <policy> by administrator <admin> at DataFort <serial>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                                          | Description | A DataFort administrator changed the pool key policy attribute for the tape pool <pool>. <policy> may be one of:<br>tape—The policy is set to one key per tape for this tape pool.<br>pool—The policy is set to one key per pool for this tape pool.<br>host—The policy is set to one key per host for this tape pool.                                                                                                                                                                                                                                           |

**TABLE 34: AUTHENTICATION FUNCTION LOG MESSAGES (CONTINUED)**

|                                                  |                              |                                                                                                                                                                                       |
|--------------------------------------------------|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SECMAN_FCPOOL_ACL_LEARNING_MODE_PROPERTY_CHANGED | Level                        | INFO                                                                                                                                                                                  |
|                                                  | Message                      | Pool ACL learning is <state> by administrator <admin> at DataFort <serial>                                                                                                            |
|                                                  | Description                  | A DataFort administrator changed enabled or disabled (indicated by <state>) the global DataFort learning mode attribute.                                                              |
| SECMAN_FCPOOL_ACL_LEARNING_MODE_CHANGED          | Level                        | INFO                                                                                                                                                                                  |
|                                                  | Message                      | Pool <pool> ACL learning mode is changed to <mode> by administrator <admin> at DataFort <serial>                                                                                      |
|                                                  | Description                  | A DataFort administrator changed ACL learning mode for the tape pool <pool>. <mode> may be: <ul style="list-style-type: none"> <li>• Clear</li> <li>• Learn</li> <li>• Set</li> </ul> |
| SECMAN_FCPOOL_GROUP_ACCESS_PERMISSION_GRANTED    | Level                        | INFO                                                                                                                                                                                  |
|                                                  | Message                      | Pool group <pool_group> allowed information flows changed by administrator <admin> : granted access to Host group <host_group> at DataFort <serial>                                   |
|                                                  | Description                  | A DataFort administrator added an authorized information flow for the tape pool <pool> and all hosts in the host group <host_group>.                                                  |
| SECMAN_FCPOOL_GROUP_ACCESS_PERMISSION_REVOKED    | Level                        | INFO                                                                                                                                                                                  |
|                                                  | Message                      | Pool group <pool_group> allowed information flows changed by administrator <admin> : revoked access from Host group <host_group> at DataFort <serial>                                 |
|                                                  | Description                  | A DataFort administrator removed all authorized information flows for the tape pool <pool> and the hosts in host group <host_group>.                                                  |
| SECMAN_CLI_EXECUTED                              | Level                        | INFO                                                                                                                                                                                  |
|                                                  | Message                      | <principal> executed CLI command <command> at DataFort <serial>                                                                                                                       |
|                                                  | Description                  | DataFort automatically logs the invocation of some CLI commands. <principal> refers to a user and domain: <user>@<domain>.                                                            |
|                                                  | CLI commands that are logged | system util stacklog                                                                                                                                                                  |

## INTEGRITY LOGS

Integrity Logs are generated to record events that might modify the integrity of the DataFort appliance (for example clock or tamper settings). See:

- [Generic parameters in Integrity function log messages](#)
- [Integrity function log messages](#)

**TABLE 35: GENERIC PARAMETERS IN INTEGRITY FUNCTION 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  |

**TABLE 36: INTEGRITY FUNCTION LOG MESSAGES**

| Log Message        | Log Message description |                                                                                                                                         |
|--------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| INT_CLOCK_CHANGED  | Level                   | INFO                                                                                                                                    |
|                    | Message                 | <user>@<domain> changed clock at DataFort <serial> from <old time> to <new time>                                                        |
|                    | Description             | This message is issued when an administrator changes the DataFort clock.                                                                |
| INT_TAMPERED       | Level                   | WARNING                                                                                                                                 |
|                    | Message                 | DataFort <serial> detected potential intrusion: <action> at DataFort <serial>                                                           |
|                    | Description             | This message is issued when DataFort detects a chassis intrusion event, or the intrusion function of the SEP is triggered.              |
| INT_SEP_SHREDDED   | Level                   | WARNING                                                                                                                                 |
|                    | Message                 | DataFort <serial> activated Defense Setting. All key material has been deleted: <defense_level>                                         |
|                    | Description             | An intrusion event triggered the zeroization function.                                                                                  |
| INT_SEP_SHRED_MODE | Level                   | WARNING                                                                                                                                 |
|                    | Message                 | DataFort <serial> will use <defense_level> defense level henceforth                                                                     |
|                    | Description             | The administrator configured the CryptoShred defense setting.                                                                           |
| INT_SEP_ERROR      | Level                   | WARNING                                                                                                                                 |
|                    | Message                 | DataFort <serial> detected SEP hardware error at DataFort <serial>                                                                      |
|                    | Description             | A hardware error occurred within the SEP of the specified DataFort. Note, the SEP will disable itself in the event of a hardware error. |

**TABLE 36: INTEGRITY FUNCTION LOG MESSAGES (CONTINUED)**

|                                 |             |                                                                                                                                                                                                                                    |
|---------------------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| INT_SEP_ZEROIZED                | Level       | WARNING                                                                                                                                                                                                                            |
|                                 | Message     | <user>@<domain> zeroized SEP at DataFort <serial>                                                                                                                                                                                  |
|                                 | Description | A DataFort administrator issued a command to zeroize the SEP.                                                                                                                                                                      |
| INT_SYSCARD_ZEROIZED            | Level       | WARNING                                                                                                                                                                                                                            |
|                                 | Message     | <user>@<domain> zeroized System Card at DataFort <serial>                                                                                                                                                                          |
|                                 | Description | A DataFort administrator issued a command to zeroize the DataFort System Card.                                                                                                                                                     |
| INT_CLUSTER_MEMBER_DISCONNECTED | Level       | WARNING                                                                                                                                                                                                                            |
|                                 | Message     | DataFort <serial> detected cluster is aborted because of disconnection of cluster member <ip>                                                                                                                                      |
|                                 | Description | The DataFort failover cluster was aborted due to failure to reach a cluster member at IP address <ip>. The cluster will automatically begin reformation.                                                                           |
| INT_CLUSTER_ABORTED             | Level       | WARNING                                                                                                                                                                                                                            |
|                                 | Message     | DataFort <serial> cluster status transitioned from committed to aborted                                                                                                                                                            |
|                                 | Description | The DataFort cluster transitioned to an aborted state.                                                                                                                                                                             |
| INT_CLUSTER_ONLINE              | Level       | INFO                                                                                                                                                                                                                               |
|                                 | Message     | DataFort <serial_number> detected cluster is committed online with <num_members> member(s)                                                                                                                                         |
|                                 | Description | The DataFort cluster transitioned to an online state. <num_members> indicates the number of DataFort appliances that are members of the currently established cluster.                                                             |
| INT_TIME_RESET                  | Level       | INFO                                                                                                                                                                                                                               |
|                                 | Message     | DataFort <serial_number> reset time by NTP: <num_secs> second(s)                                                                                                                                                                   |
|                                 | Description | The DataFort clock was changed by the NTP daemon by <num_secs> seconds.                                                                                                                                                            |
| INT_TIME_RESET_FAILED           | Level       | WARNING                                                                                                                                                                                                                            |
|                                 | Message     | DataFort <serial_number> failed to reset time by NTP because of too large offset <num_secs> second(s)                                                                                                                              |
|                                 | Description | The NTP daemon failed to change the DataFort clock. The NTP daemon will only change the DataFort clock if the current clock error is within an allowable range. This error occurs when the current clock is too far out of bounds. |



## ■ ■ ■ ■ **APPENDIX III SPECIFICATIONS**

- [Specifications](#) lists DataFort hardware specifications.

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

SPECIFICATIONS

TABLE 37: DATAFORT S110 SPECIFICATIONS

| Item                  | Detail          | Specification                                                                                                                                                                                                                                                          |
|-----------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hardware              | Rack mountable  | Standard 19" EIA rack (2U height)                                                                                                                                                                                                                                      |
|                       | Weight          | 13.7 kg/30.2 lbs                                                                                                                                                                                                                                                       |
|                       | Size            | 43.2 cm (17.00") W x 8.8 cm (3.46") H x 48.2 cm (19") D                                                                                                                                                                                                                |
|                       | Security        | Chassis: Pick-resistant Medeco lock, intrusion detection                                                                                                                                                                                                               |
|                       | Data Ports      | 2 LVD SCSI (one host, one storage which supports daisy chaining)                                                                                                                                                                                                       |
|                       | Management Port | 1 10/100/1000Base-T Ethernet port                                                                                                                                                                                                                                      |
|                       | Serial Port     | RJ45 serial console port                                                                                                                                                                                                                                               |
|                       | Power Supply    | 2 Universal: 100-240V/6A, 50/60 Hz, Hot swappable                                                                                                                                                                                                                      |
|                       | LED             | Power status, network activity                                                                                                                                                                                                                                         |
|                       | LCD             | Liquid Crystal display with touch-panel capability                                                                                                                                                                                                                     |
|                       | Smart Card      | 1 internal smart card reader                                                                                                                                                                                                                                           |
| Environment           | Temperature     | Operating Temperature: 5°C to 40°C (41°F-104°F)<br>Storage Temperature: -10°C to 60°C (14°F-140°F)                                                                                                                                                                     |
|                       | Humidity        | Operating Humidity: 85% RH at 35°C                                                                                                                                                                                                                                     |
| Regulatory Compliance | EMC             | Canada ICES-003 Class B<br>United States FCC Class B<br>Japan VCCI Class B<br>Korea RRL Class B<br>European Community CE (EN55022 Class B, EN55024, EN61000-3-2 Class A, & EN61000-3-3)<br>Australia/New Zealand AS/NZS 3548 Class B<br>International CISPR 22 Class B |
|                       | Safety          | Canada CSA 60950<br>United States UL 60950<br>Japan IEC60950 A4<br>European Community EN60950, TUV<br>International IEC 60950                                                                                                                                          |

## ■ ■ ■ ■ APPENDIX IV PARTIAL LIST OF ISO COUNTRY CODES

The country codes that are used when setting SSL security certificates are established by the International Organization for Standardization (ISO). A full list of country codes can be found on their website. A partial list of codes is shown below.

**TABLE 38: ISO COUNTRY CODES**

| Country   | Code | Country        | Code |
|-----------|------|----------------|------|
| AUSTRALIA | AU   | MEXICO         | MX   |
| AUSTRIA   | AT   | NETHERLANDS    | NL   |
| BELGIUM   | BE   | NEW ZEALAND    | NZ   |
| CANADA    | CA   | NORWAY         | NO   |
| CHINA     | CN   | PANAMA         | PA   |
| DENMARK   | DK   | PHILIPPINES    | PH   |
| FINLAND   | FI   | POLAND         | PL   |
| FRANCE    | FR   | PORTUGAL       | PT   |
| GERMANY   | DE   | PUERTO RICO    | PR   |
| GREECE    | GR   | SINGAPORE      | SG   |
| HONG KONG | HK   | SPAIN          | ES   |
| INDIA     | IN   | SWEDEN         | SE   |
| IRELAND   | IE   | SWITZERLAND    | CH   |
| ISRAEL    | IL   | TAIWAN         | TW   |
| ITALY     | IT   | THAILAND       | TH   |
| JAPAN     | JP   | UNITED KINGDOM | GB   |
| KOREA     | KR   | UNITED STATES  | US   |



## ■ ■ ■ ■ **APPENDIX V REGULATORY AND CERTIFICATIONS**

- [FCC B Declaration of Conformity](#)
- [European Union](#)
- [Canadian ICES-003](#)
- [VCCI Class A Statement](#)
- [CE Statement](#)



## FCC B DECLARATION OF CONFORMITY

---

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

In order to maintain compliance with FCC regulations, shielded cables must be used with this equipment. Operation with non-approved equipment or unshielded cables is likely to result in interference to radio and TV reception. The user is cautioned that changes and modifications made to the equipment without the approval of manufacturer could void the user's authority to operate this equipment.

## EUROPEAN UNION

---

This equipment is intended to operate under the following environmental conditions with respect to EMC:

1. A separate defined location under user's control.
2. Earthing and bonding shall meet the requirements of ETS 300 253 or CCITT K27.
3. Where applicable, AC power distribution shall be one of the following types: TN-S and TN-C [as defined in IEC 364-3] In addition, if equipment is operated in a domestic environment, interference may occur.

## CANADIAN ICES-003

---

This Class A digital apparatus meets all requirements of the Canadian ICES-003 Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

## VCCI CLASS A STATEMENT

---

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用する  
と電波妨害を引き起こすことがあります。この場合には使用者が適切な対策  
を講ずるよう要求されることがあります。

VCCI- A

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take corrective actions. VCCI-A

## CE STATEMENT

---

The standards compliance label on the appliance contains the CE mark which indicates that this system conforms to the provisions of all European Council Directives, laws, and standards.

The appliance is in conformity with the provisions of the following EC Directives, including all amendments, and national legislation implementing these directives:

- 89/336/EEC
- 93/68/EEC
- 73/23/EEC

The following harmonized standards have been applied

- EN55022: 1998 Plus A1: 2000 & A2: 2003
- EN61000-3-2: 2001
- EN61000-3-3: 1995 Plus A1: 2001
- EN55024: 1998 Plus A1: 2000 & A2: 2003
- EN60950-1: 2001+A11: 2004

## ■ ■ ■ ■ ■ APPENDIX VI GLOSSARY

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>administrator</b>        | 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.                                                                                                                                                                                |
| <b>Admin Card</b>           | A smart card used to authenticate a DataFort administrator. An individual possessing the Admin Card and the username and password for that card has privileges of a DataFort administrator. DataFort detects the presence of this card in the smart card reader attached to the Management Station.                                                                                                                                            |
| <b>AES</b>                  | 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.                                                                                                                                                                                                              |
| <b>authentication</b>       | The process by which identity is established on a network. Typically, identity is established with username/password combinations (logging in to a computer) or using physical tokens (keys, smart cards). By default, DataFort requires both a username/password combination and a token to authenticate the DataFort administrator and Recovery Officers. DataFort can be configured to require only a username and password for management. |
| <b>chassis</b>              | The physical encasement of a device. DataFort is designed to resist and detect any attempt to open the chassis.                                                                                                                                                                                                                                                                                                                                |
| <b>ciphertext</b>           | 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.                                                                                                                                                                                               |
| <b>cleartext</b>            | Data before encryption. Unencrypted data is clear in the sense that anyone with access to the data can read it.                                                                                                                                                                                                                                                                                                                                |
| <b>cluster</b>              | A cluster is a set of interconnected devices. If one fails, the other can continue providing the service. By clustering DataFort devices, total system redundancy is increased, decreasing the probability of any downtime.                                                                                                                                                                                                                    |
| <b>Common Criteria Mode</b> | The Common Criteria is an international standard for evaluating information technology security. The ability to run in a mode qualified to meet Common Criteria standards is an enhanced security option for DataFort.                                                                                                                                                                                                                         |

|                                      |                                                                                                                                                                                                                                                            |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>configuration database</b>        | The database stored inside DataFort hardware which contains network and security information, ACLs and encrypted key material.                                                                                                                             |
| <b>Cryptainer</b>                    | A Cryptainer is a specially designated directory. Data within a Cryptainer can be encrypted by DataFort with a Cryptainer Key, using AES.                                                                                                                  |
| <b>cryptography</b>                  | 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.                                             |
| <b>DataFort CLI</b>                  | The command line interface used to manage the DataFort device. The CLI allows remote users to log in to DataFort and administer it by entering text commands over SSH.                                                                                     |
| <b>DataFort WebUI</b>                | A graphical user interface used to manage the DataFort device via a web browser using SSL. Commands are entered by selecting from drop-down menus and filling out web forms.                                                                               |
| <b>failover</b>                      | 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.                                                                                                               |
| <b>IPsec</b>                         | Internet Protocol Security. A standard for secure network communication. Communication between clustered DataFort devices occurs over IPsec; IPsec communication is a licensed option between DataFort and clients.                                        |
| <b>key</b>                           | 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.                               |
| <b>Lifetime Key Management (LKM)</b> | Decru's proprietary solution for encryption key management. LKM software and the LKM appliance both store key information.                                                                                                                                 |
| <b>Management Station</b>            | A Windows PC equipped with a smart card reader, from which a DataFort administrator can manage the DataFort via the DataFort WebUI.                                                                                                                        |
| <b>Master Key</b>                    | The Master Key is generated by DataFort at initialization time, and is unique to each DataFort. It is ultimately required in order to decrypt other keys in the configuration database.                                                                    |
| <b>MIB</b>                           | Management Information Base. A set of network objects that can be managed using the Simple Network Management Protocol (SNMP).                                                                                                                             |
| <b>NTP</b>                           | Network Time Protocol, used to synchronize computer clocks on the Internet.                                                                                                                                                                                |
| <b>quorum</b>                        | The minimum number of Recovery Officers required to complete sensitive DataFort management procedures.                                                                                                                                                     |
| <b>Recovery Cards</b>                | 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. |

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Recovery Officers</b>                   | Recovery Officers are entrusted with keeping Recovery Cards and their associated passwords safely. Recovery Officers must present their cards and passwords to initialize a new DataFort. A quorum of Recovery Officers is required for other sensitive options such as data recovery, cluster authentication, and Recovery Card replacement.                                                         |
| <b>secret sharing</b>                      | A split knowledge procedure, whereby several parties are each given a portion of some secret data. In order to recover the data, a predetermined number of parties must combine their portions. In the DataFort system, this process is used when DataFort assigns a portion of a high-level cryptographic key to each Recovery Card. A quorum of Recovery Cards is required to reconstitute the key. |
| <b>Security Domain</b>                     | A Security Domain defines a distinct group of Recovery Cards. Multiple Security Domains can be used in the enterprise to compartmentalize access to deployed DataFort appliances.                                                                                                                                                                                                                     |
| <b>smart cards</b>                         | Credit card-sized devices with embedded microchips used by DataFort for authentication procedures.                                                                                                                                                                                                                                                                                                    |
| <b>SNMP</b>                                | Simple Network Management Protocol. A protocol for network management and monitoring of network devices.                                                                                                                                                                                                                                                                                              |
| <b>SSH</b>                                 | 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.                                                                                                                                                                                                                                  |
| <b>SSL</b>                                 | Secure Sockets Layer. A protocol providing secure message transfer over the Internet. Used to secure transmission of data via web browsers.                                                                                                                                                                                                                                                           |
| <b>Storage Encryption Processor (SEP)</b>  | DataFort's hardware encryption/decryption engine, which enables gigabit-speed, full duplex encryption.                                                                                                                                                                                                                                                                                                |
| <b>System Card</b>                         | A smart card provided by Decru which inserted at the front panel of DataFort for boot-up to enable DataFort encryption services. The System Card may be removed during normal operation to prevent unauthorized use of DataFort upon reboot.                                                                                                                                                          |
| <b>Trustee</b>                             | A trustee is a remote DataFort with which a trust relationship has been formed, allowing exportable Cryptainer Keys to be shared. A trustee may import from or export to a trustee.                                                                                                                                                                                                                   |
| <b>Trustee Acceptance Package (TAP)</b>    | The second message between DataFort appliances when setting up a trustee relationship.                                                                                                                                                                                                                                                                                                                |
| <b>Trustee Establishment Package (TEP)</b> | The first message sent between DataFort appliances when setting up a trustee relationship.                                                                                                                                                                                                                                                                                                            |

## INDEX

### A

- access control for tape 78
- Adding and Removing Cluster Members 121
- Admin Card 15, 16, 194
  - associate with administrator 69
- administrator 16, 194
  - add 67
  - associate card 69
  - associate with Admin Card 69
  - change password 71
  - change the card association 73
  - delete profile 73
  - dual authorization, login 57
  - login to CLI 58
  - login to WebUI 55
  - new 76
  - number recommended 67
  - require login authorization 70
  - roles outlined 65
  - Security Administrator 88, 105, 110
  - specialty administrator, create 68
- administrator roles 65
- administrator roles, CLI 149
- AES 14, 194
- alert, clearing 98
- appending ciphertext 85
- appending cleartext 85
- ARP table 153
- associate Admin Card with administrator 69
- authentication 15, 194
- authorization for login 70
- authorizing administrator 70
- Auto-detected pools 78

### B

- backup
  - DataFort configuration 21, 105
- battery iv, 29

### C

- Category 5 cable 17, 32
- certificates
  - Management Station to DataFort 126

- certificates lost after zeroization 116
- change password
  - administrator 71
- change password, Recovery Card 103
- chassis 14, 194
  - intrusion 96
- ciphertext 14, 194
- ciphertext and cleartext 20, 194
- clear all DataFort settings 116
- clear an intrusion (defense alert) 98
- clear smart cards 104
- cleartext 14, 79, 194
- cleartext pools 79
- cleartext tape 23
- CLI 58
  - command help 148, 163
  - commands and admin roles 149
  - connect from SSH client 58
  - general information 148, 163
  - help 166
  - login 58
  - permissions 147
  - Quick Reference 162
  - quit 166
  - system commands 150, 168
  - time-out 163
  - top level commands 164
  - turn off Secure Web 158
  - WebUI access 60
- CLI documentation 148, 163
- CLI login with dual authentication 59
- cluster 194
  - change to standalone 121
  - commands, CLI 168
  - forming, after initial setup 121
  - IPsec tunnel 20
  - management 119
  - management using CLI 150
  - recovery guidelines 123
  - remove member 121
  - replace an offline member 122
  - requirements 121
  - resolving conflict 121

- restore previous configuration 123
  - state 120
  - state after wizard 75
- cluster conflict 121
- cluster disable command 150, 160
- cluster size 119
- cluster troubleshooting 160
- cluster-wide operations 120
- Common Criteria 14, 170, 171
- configurable security levels 100
- configuration database 15, 195
  - applied to new DataFort 155
  - backup to LKM 75, 106
  - backup using WebUI 109
  - changes synchronized in cluster 20
  - commands, CLI 168
  - contents 105
  - event log capacity 111
  - purging unused keys after backup 108
  - size 108
  - used for recovery 155
- Cryptainer 195
  - before creating 74
- Cryptainer encryption key 15
- cryptographic test 136
- CryptoShred 14, 98
- CryptoShred button 14, 96, 98
  - states 98

## D

- data
  - encryption 15
- DataFort
  - administrators 135
  - assigning IP settings 33
  - back panel connections 31
  - capacity 20
  - CLI, connecting to 58
  - Defense Setting 96
  - emergency shutdown 98
  - licenses 45, 131
  - recovery 155
  - Recovery Officers 135
  - restoring a previous configuration 155
  - specifications 189
  - troubleshooting 154
  - upgrading 125
  - users 16

- WebUI, connecting to 55
  - where installed 14
  - zeroizing 116
- DataFort CD-ROM 17
- DataFort CLI 58, 195
  - login 58
- DataFort CLI Reference Guide 147, 162
- DataFort Throughput 135
- DataFort WebUI 55, 195
  - login 55
- DCS
  - administrator roles 149
- Decru licenses 45, 131
- Decru Management Console 137
  - menus 137
- Decru MIB 63, 132
- Decru Signed Syslogd (DSS) 112
- defense
  - alert, clearing 98
  - response 96
  - triggers 96
- Defense Setting
  - changing after setup 96
  - summary 96
- defense setting 22, 96
- deleted Cryptainer
  - purge unused keys 108
- disabling a cluster member 150
- DMC 137
- documentation 17
- dual authentication login, CLI 59
- dual authentication login, WebUI 57
- dual authorization 57, 59, 70

## E

- emergency shutdown 98
- emergency zeroization via serial console 118
- Enabling SNMP 132
- enabling TLS 26
- encryption 14
- escrow service 21
- Ethernet cable 17
- event logs 111

## F

- failover 194, 195
- fan modules, replacing 161
- feature licenses 45

- Fibre Channel 13
- front panel
  - display 63
  - LCD used to assign IP address 33
  - LED 156
  - System Card slot 31
- Front Panel Dual LEDs - 2U 156
- Front Panel LEDs - 1U 156
- full database 109

## G

- Global Default Pool 79

## H

- hardware maintenance 161
- Home page
  - returning to 55
- Host Default Pools 78

## I

- installation
  - in rack 30
  - planning 20
  - precautions iv, 30
  - requirements 17
- International Organization for Standardization (ISO) 129, 190
- Internet Explorer
  - for accessing WebUI 55
- intrusion detection 96, 98
- IP address 17
  - DataFort, assigning 33
  - DataFort, current 135
  - preserve during zeroization 117
- IP settings
  - assigning from LCD 33
  - assigning from serial console 62
  - changing, with WebUI 125
  - DataFort, assigning from serial console 34
- IPsec 20, 195
- ISO 190
- IT power systems iii, 29

## K

- key 195
  - encryption key 14
  - escrow 21
- Key Purging 106

- key, chassis 96

## L

- LCD 63, 136
  - assigning DataFort IP settings 33
  - bar graph 63
  - buttons 63
  - touch panel interface 53
  - web page 136
- LED 156
- LEDs
  - power supply 156
- legacy cleartext tape 23
- licenses 17, 131
  - managing 131
- lifespan of tape keys 79, 86
- Lifetime Key Management (LKM) 15, 195
- limited administrator 70
- Limits
  - Number of DataFort appliances in a cluster 20
- Lithium battery iv, 29
- LKM 21, 106
  - server saves latest configuration backup 21
  - server, specifying settings in WebUI 75, 106
- LKM appliance setup 27, 75
- LKM servers
  - number supported 106
- LKM software setup 27
- LKM using SSL 107
- login
  - CLI 58
  - CLI, dual authorization 59
  - requiring authorization 70
  - WebUI 57
  - WebUI, dual authorization 57
- logs, DataFort 111
  - configuring storage location 112
  - Decru Signed Syslogd (DSS) 112
  - filtering 115, 135
  - guidelines 111
  - syslog mapping table 114
  - temporary file mapping 114
  - viewing, with WebUI 115

## M

- Management Console 53
- Management Console installation 26
- Management Port

- connecting to Ethernet network 32
- Management Station 15, 195
  - Management Console installer 26
- Management Station requirements 25
- Management Station security 26
- Master Key 15, 195
- metadata 112
- MIB 63, 132, 195
- mounting DataFort in rack 30
- Multi ID 80
- multi-appliance management 137

## N

- NAS 13
- network
  - connection to DataFort ports 31
  - information needed for setup 25
  - manage, with CLI 153
  - settings, changing 125
- Network Attached Storage (NAS) 13
- network commands, CLI 153
- Network switch ports 17
- NTP time server 17

## O

- online help 54, 146

## P

- Parent Key 15
- password
  - administrator, changing 71
  - one-time, CLI 58
  - Recovery Card, changing 103
- pools and tapes 78
  - settings 78
- port
  - Management 32
- power
  - precautions iii, 29
- power button 36
- power cord 17
- power down DataFort 36
- power supply
  - LEDs 156
  - notice iii, 29
  - replaceable 161
- powering down 36
- powering up 36

- protect against insider attacks 70
- purging keys 108

## Q

- quorum 16, 21, 101, 102, 104, 160, 195

## R

- rack installation 30
- rack mounting kit 17
- Recovery Cards 15, 101, 195
  - change password 103
  - replacement procedure 101
- Recovery Officers 16, 196
  - required for forming cluster 123
  - required for replacing DataFort 122, 155
  - required for replacing Recovery Card 89, 101
  - required for Setup 38
- Remote Desktop 55, 158
- replacing a Recovery Card 101
- replacing an offline cluster member 122
- requiring login authorization 70
- reset DataFort 116
- reset smart cards 104
- restore a previous DataFort configuration 155
- RJ45 to DB9 adapter 17, 32

## S

- SAN 13
- secret share 196
- Secure CLI 54, 100
  - login 58
- Secure Web 54, 55, 100
  - turn on and off via CLI 158
- SecureView 54
- Security Administrator 88, 105, 110
- Security Certificate 126
  - Certificate Authority Signed, installing 129
  - self-signed, installing 126
- Security Domain 16, 196
  - planning 20
- Security Policy
  - planning 21
- Security Settings 100
- security, implementing and maintaining 20
- Sensors 136
- SEP 14, 136, 196
- serial console 62
  - assigning DataFort IP settings 34

- clearing IP Settings 62
  - connecting serial port 32, 62
  - emergency access 118
  - menu options 62
  - zeroizing DataFort 62
  - serial number 136
  - servicing DataFort 161
  - shutting down 36
  - size of the configuration database 108
  - smart card reader 15, 17
  - Smart Card Reset 104, 111
  - smart cards 17, 196
    - checking versions and status 104
    - reset procedure 104
    - summary 15
    - troubleshooting 161
  - SNMP 132, 196
    - MIBs 132
    - setting with WebUI 132
    - turning on and off 132
    - version 133
  - software CD-ROM 17
  - specialized administrators 65
  - specifications 188
  - SSH 53, 196
    - CLI access 58, 59, 148
  - SSL 107, 196
  - stack trace 153
  - Standard CLI 58
  - standard rack mount 30
  - status and settings 134
  - Storage Area Network (SAN) 13
  - Storage Diagnostics 135
  - Storage Encryption Processor (SEP) 14
  - syslog, syslogd (syslog daemon) 111, 114
  - System Card 15, 196
    - inserting 31
    - removing, in emergency 98
  - System Config menu (WebUI)
    - General, Upgrade 125
    - Network, IP Settings 125
    - Network, SNMP Agent 132
    - Recovery, Backup 109
    - Recovery, Replace Recovery Card 101
    - Security, Zeroize 117
    - System Users 135
    - System Users, Administrators 76
    - view settings 135
  - System Info menu (WebUI)
    - Status 136
    - Status, Log 115, 135
    - system properties, CLI 150
    - system users 135
- ## T
- TAP 89, 145
  - tape key 79, 86
    - deletion 79, 86
    - expiration 79, 86
    - lifespan 79, 86
  - tape pool types 78
  - Tape Settings 78
  - TEP 89, 145
  - Terminal Services 55, 158
  - time and date
    - setting from WebUI 111
  - time servers 111
  - time-out
    - CLI 58
    - serial session 62
    - WebUI 55
  - trap 133
  - troubleshooting 154
    - network connections 157
    - smart cards 161
  - Trustee Acceptance Package 89, 145
  - Trustee Establishment Package 89, 145
  - Trustees 89
  - types of keys recovered during a restore 116
- ## U
- upgrading DataFort 125
  - USB 17
- ## V
- Verifying System Logs 152
- ## W
- WebCLI 60
  - WebUI
    - accessing 55
    - keyboard shortcuts 56
    - login 55
    - login with Secure Web 55
    - required display setting 55
    - time-out 55

- WebUI access to cluster members 120
- WebUI login with dual authentication 57
- Windows event logging 112
- Windows Event Viewer 112

## Z

- zeroization without admin card 118
- zeroizing DataFort 116
  - using serial console 118
  - using WebUI or CLI 117