



## ADMINISTRATION GUIDE

Lifetime Key Management  
Appliance

DRAFT - DO NOT DISTRIBUTE

# security

LKM Appliance Administration Guide

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

Part number: 30-000311A0 (LKMA 080406)

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 and disclaimer in the source code files and in the documentation and/or other materials provided with the distribution.

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/>).”

## CONTENTS

|                                                     |           |
|-----------------------------------------------------|-----------|
| <b>The Decru Lifetime Key Management Appliance</b>  | <b>6</b>  |
| LKM Appliance Features                              | 6         |
| Deploying the LKM Appliance                         | 6         |
| Enterprise Key Limits                               | 8         |
| Management Interfaces                               | 9         |
| SecureView                                          | 9         |
| <b>Installation</b>                                 | <b>5</b>  |
| Notices and Warnings                                | 5         |
| Power Supply Notice                                 | 5         |
| Dual Power Supply Notice                            | 5         |
| Lithium Battery Notice for Service Personnel        | 6         |
| Rack Mounting the Lifetime Key Management Appliance | 6         |
| Selecting a Location                                | 6         |
| Rack Mounting                                       | 7         |
| Connecting the LKM Appliance                        | 8         |
| System Card Insertion                               | 8         |
| Rear Panel Network Connections                      | 8         |
| Assigning the IP Address                            | 9         |
| Installing the Management Console                   | 11        |
| Management Station Security                         | 11        |
| Running the Installer                               | 12        |
| <b>Initializing an LKM Appliance</b>                | <b>13</b> |
| Running the Setup Wizard                            | 13        |
| <b>Setting up Lifetime Key Management</b>           | <b>23</b> |
| Adding Appliances                                   | 23        |
| Logging into Appliances                             | 26        |
| Connecting DataFort Appliances to LKM               | 29        |
| <b>Decru Management Console Menus</b>               | <b>30</b> |
| Appliance Menu                                      | 31        |
| Configuration Menu                                  | 32        |
| View Menu                                           | 32        |
| Edit Menu                                           | 32        |
| LKM Menu                                            | 33        |
| Help Menu                                           | 33        |

|                                                                    |           |
|--------------------------------------------------------------------|-----------|
| <b>Appliance Management</b>                                        | <b>34</b> |
| Appliance Menu                                                     | 34        |
| Adding an Appliance                                                | 34        |
| Removing an Appliance                                              | 34        |
| Logging into Appliances                                            | 34        |
| Running the Setup Wizard                                           | 35        |
| Verify                                                             | 35        |
| Upgrade                                                            | 35        |
| Back Up                                                            | 35        |
| Trustees                                                           | 36        |
| Link Appliances                                                    | 37        |
| Details                                                            | 37        |
| WebUI                                                              | 37        |
| Command Line                                                       | 37        |
| Collect Tech Support Info                                          | 38        |
| Reboot                                                             | 39        |
| Zeroize                                                            | 39        |
| Exit                                                               | 39        |
| Configuration                                                      | 40        |
| Managing Licenses                                                  | 40        |
| Adding a License                                                   | 41        |
| Managing Administrators                                            | 41        |
| Adding an Administrator                                            | 43        |
| <b>Key Management</b>                                              | <b>46</b> |
| Generating a Key Archive                                           | 47        |
| Generating a Cryptainer Key File                                   | 48        |
| Key Translation                                                    | 49        |
| Translating Cryptainer Keys                                        | 49        |
| Importing and Exporting Keys                                       | 50        |
| Exporting Cryptainer Keys                                          | 50        |
| Importing Exported Cryptainer Keys                                 | 50        |
| <b>Troubleshooting</b>                                             | <b>51</b> |
| Nothing here yet                                                   | 51        |
| <b>CLI Commands</b>                                                | <b>52</b> |
| Specific to LKM appliance management and the Management Console... | 52        |
| <b>Regulatory and Certifications</b>                               | <b>53</b> |
| FCC B Declaration of Conformity                                    | 53        |
| European Union                                                     | 53        |
| Canadian ICES-003                                                  | 54        |
| VCCI Class A Statement                                             | 54        |
| CE Statement                                                       | 54        |

## ■ ■ ■ ■ 1 THE DECRU LIFETIME KEY MANAGEMENT APPLIANCE

The Decru DataFort™ appliance secures data at rest by encrypting it with strong algorithms and storing it in Cryptainer vaults™ managed by DataFort. Keys are generated every time data is encrypted or re-encrypted by DataFort. The presence of these keys is also required in order to decrypt the data. In an environment where multiple DataFort appliances are managing large quantities of data and therefore generating a large number of keys, a robust key management system is required.

The Decru Lifetime Key Management™ appliance (LKM appliance) manages encryption keys for multiple DataFort appliances, ensuring encryption key availability for the life of the secured data. The LKM appliance offers a central location for the administrator to load, view, manage, share and save all keys generated by DataFort appliances in an installation. When used in combination with the separate Decru Decryption Software (DDS), the LKM appliance can also enable authorized administrators to decrypt data outside of the DataFort appliance.

The Decru Management Console provides a powerful tool for managing multiple LKM and DataFort appliances from a single interface. This console displays at-a-glance status for all DataFort and LKM appliances in the installation, as well as providing centralized tools and menu operations for DataFort and LKM appliance management.

### **LKM APPLIANCE FEATURES**

---

The LKM appliance offers the following features:

- Supports all DataFort appliances across the enterprise
- Supports 100+ DataFort appliances and 10 million+ keys per LKM appliance
- Up to 16 LKM appliances can be clustered to support large DataFort deployments (1000+)
- Provides high availability through key replication and redundant components
- Provides centralized management for multiple DataFort and LKM appliances
- Provides global distributed backup, replication, and recovery of encryption keys
- Provides automated key distribution for information sharing
- Leverages FIPS 140-2 level 3-certified Decru SEP for encryption keys
- Provides role-based access controls for administrators
- Provides tamper-evident logging and auditing

### **DEPLOYING THE LKM APPLIANCE**

---

The LKM appliance is positioned on the Ethernet portion of the network where DataFort appliances reside. A secure interface between DataFort and LKM appliances provides a channel for key backup and replication. Once configured to do so, DataFort appliances will automatically send key data to the LKM appliance. DataFort appliance configuration databases will be checked every hour for changes. If changes are found, new configuration data will be sent to LKM appliances.

Multiple LKM appliances can be employed to offer key management across multiple sites, and multiple DataFort cluster locations. A single instance of the Decru Management Console running on the Management Station manages all appliances in use.

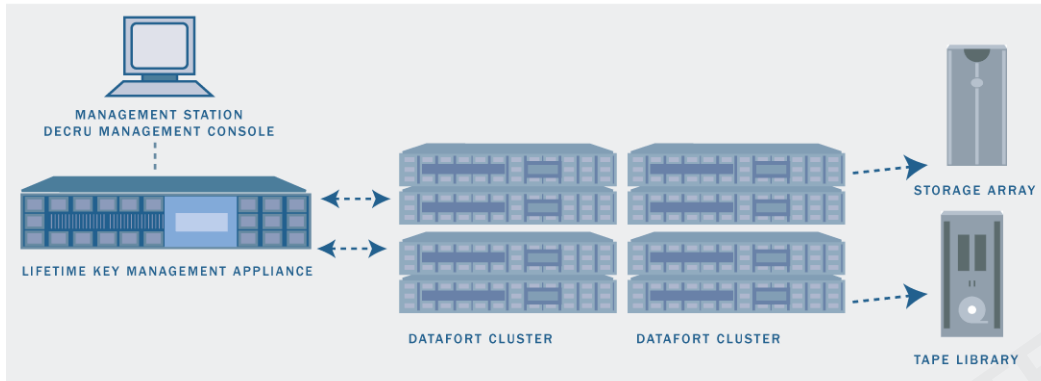


Figure 1-1: The LKM appliance provides centralized management

Multiple LKM appliances can share keys across a large configuration which includes DataFort clusters encrypting data stored on disk and tape. The LKM appliances store all encryption keys for the entire enterprise, and can share them between remote sites. In this type of deployment, the LKM appliances provide seamless key management across the entire enterprise.

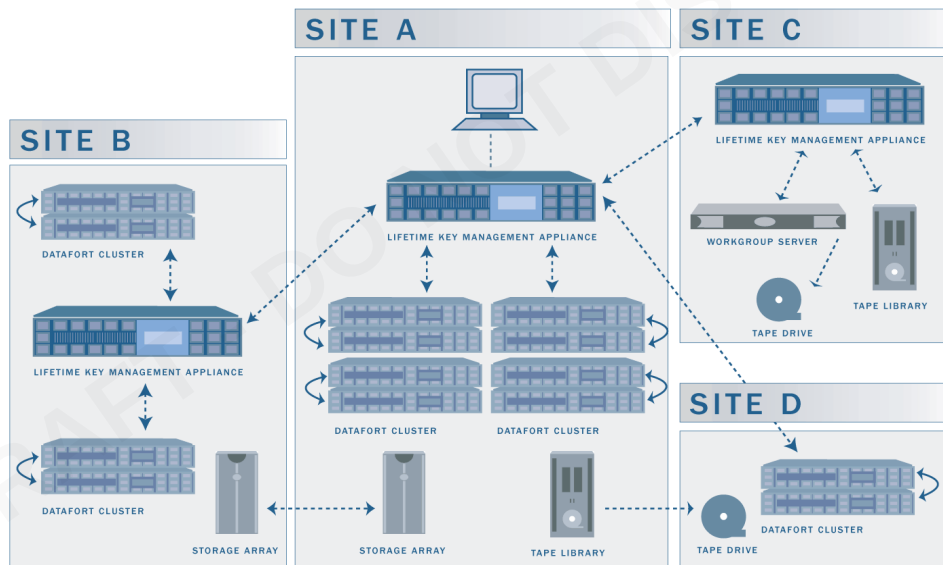


Figure 1-2: Centralized key management for large enterprise deployment

## ENTERPRISE KEY LIMITS

One LKM appliance can support the management of multiple DataFort appliances, and multiple LKM appliances can share key information for the enterprise. The number of DataFort and LKM appliances required across the entire installation will be determined by the frequency of key generation. It is important to understand when keys are generated in order to accurately plan for the number of appliances that should be installed.

Keys are generated when Cryptainers are created, rekeyed or translated from one DataFort to another. Some environments, such as those where new backup tapes are being created each day, generate many keys. (See the [Example of High Frequency Key Generation](#).) When planning an installation, keep the following [Appliance Key Limits](#) in mind:

**TABLE 1: APPLIANCE KEY LIMITS**

| Appliance Type                    | Item                                                                                                                 | Limit                                   |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| Lifetime Key Management Appliance | Number of DataFort appliances per LKM appliance                                                                      | 100+                                    |
|                                   | Keys per LKM appliance                                                                                               | 10 million+                             |
|                                   | Number of LKM appliances that can be clustered together                                                              | 16                                      |
|                                   |                                                                                                                      |                                         |
| DataFort Appliance                | Keys per DataFort. The DataFort appliance will purge keys from the configuration database when the limit is reached. | 4500 for E-Series<br>8000 for FC-Series |
|                                   | Cluster size key limit. Calculate 8000 key limit per DataFort appliance in the cluster.                              | 2 for E-Series<br>8 for FC-Series       |

The following table provides an example of high frequency key generation by an FC-Series DataFort:

**TABLE 2: EXAMPLE OF HIGH FREQUENCY KEY GENERATION**

| Key Generation                 | Total |
|--------------------------------|-------|
| Keys Generated Per Tape        | 1     |
| Tapes Generated Per Day        | 4     |
| DataFort Appliances in Cluster | 8     |
| Keys Generated Per Day         | 32    |

## MANAGEMENT INTERFACES

To set up an LKM appliance, assign the appliance network settings, install the Decru Management Console on the Management Station, and run the Setup Wizard from the console. Once the appliance has been initialized using the wizard, it can be added to the console for management. Management interfaces available to the LKM appliance administrator are summarized in the following table:

**TABLE 3: MANAGEMENT INTERFACES**

| Interface          | Description                                                                                                                 | Usage                                                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Serial             | A serial connection can be used to enter network settings for an uninitialized appliance.                                   | Set, clear, or reset IP address, gateway and subnet mask. Zeroize when other interfaces are not available.                                                                                      |
| LCD                | The front panel displays message and functions as an interactive touch screen.                                              | View status and throughput information at a glance. Use touch panel buttons to enter initial IP settings and get more information about errors and status.                                      |
| Management Console | A Java tool used for setup and management of the LKM appliance. Can be configured to require the presence of an Admin Card. | The Decru Management Console offers a centralized management tool for all LKM appliances in an installation. It also provides some management functions for DataFort appliances on the network. |
|                    | SecureView feature of Management Console                                                                                    | Feature set enabling many-at-once control of LKM and DataFort appliances. Requires Decru Management Console and optional SecureView license option.                                             |

## 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 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.

## ■ ■ ■ ■ 2 INSTALLATION

LKM appliances must be accessible via Ethernet to all DataFort appliances. Installation steps include:

- [Rack Mounting the Lifetime Key Management Appliance](#)
- [Connecting the LKM Appliance](#)
- [Installing the Management Console](#)

### 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, das die Steckdose einfach zugänglich ist.

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

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

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

**WARNING:** 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 y 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 THE LIFETIME KEY MANAGEMENT APPLIANCE

---

Be sure the following steps are performed when installing the appliance:

- [Selecting a Location](#)
- [Rack Mounting](#)
- [Connecting the LKM Appliance](#)
- [Assigning the IP Address](#)

### SELECTING A LOCATION

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

- Make sure the ambient temperature around the unit (which may be higher than the room temperature) is within the limit specified for the unit:
  - Operating Temperature: +5°C to +35°C (41°F to 95°F)
  - Storage Temperature: -10°C to +60°C (+14°F to 140°F)
- Make sure there is sufficient air flow around the unit. Do not block air flow to fans.
- Make sure electrical circuits are not overloaded - consider the nameplate rating of all the connected equipment, and make sure you have overcurrent protection.
- Make sure the equipment is properly grounded.
- Make sure no objects are placed on top of the unit.
- Do not block access to the front panel smart card slot, LEDs or LCD panel.
- Allow access to rear panel ports and power supplies.
- Avoid dusty or damp locations.



**CAUTION:** TO PREVENT BODILY INJURY WHEN MOUNTING OR SERVICING THE 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 PRODUCT 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 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.

## CONNECTING THE LKM APPLIANCE

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

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

### SYSTEM CARD INSERTION

Insert the System Card **before** powering on the appliance.

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

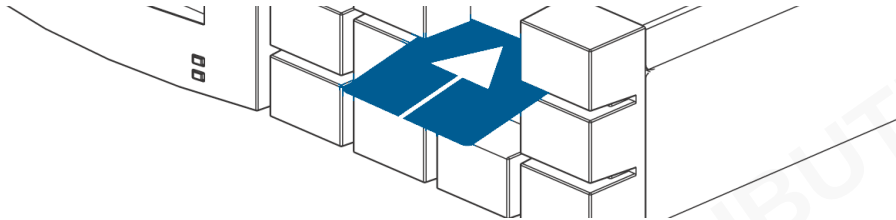


Figure 2-3: The front panel slot housing the System Card

2. Slide the card into the slot firmly, with the gold contacts facing up and towards the back of the appliance. The card should fit snugly all the way into the slot, flush with the front bezel.
3. Leave the System Card inserted until after the appliance boots up.

### REAR PANEL NETWORK CONNECTIONS

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

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

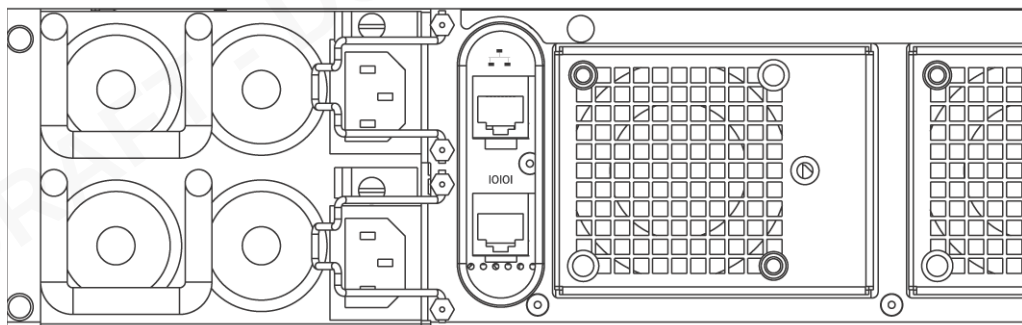


Figure 2-4: Rear panel connections

### Ethernet Connection

Use a Category 6 Ethernet cable to connect the Management Port (the Ethernet port marked with the network icon) to the Ethernet network shared by the PC which will run the Management Console.

### 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 rear panel.

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

### Power Connection

The appliance is equipped with two replaceable power supply/fan modules. Power supplies can be easily removed and replaced and are hot-swappable. For instructions on replacing fans and power supplies, contact Decru.

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

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

2. When the cords are connected, the appliance will power on automatically. Wait two to three minutes. When the LCD messages are completed, the appliance is ready for initialization.

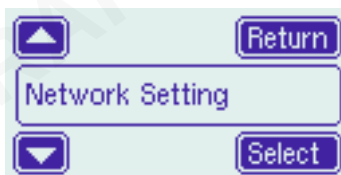
### ASSIGNING THE IP ADDRESS

Assigning an IP address for the LKM appliance Management Port is required so that other devices on the network can send keys to the LKM appliance for storage, and so that the Management Console can connect to the appliance.

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

### Setting the IP Address Using the LCD

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



3. Touch the Select button.
4. Touch the Edit button. The screen displays a keypad of numbers, and selectable fields for the 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.
11. Review the appliance IP settings.
  - If settings are correct, touch Return to exit the menu.
  - If settings are incorrect, touch Edit and enter the settings again. When finished, touch Return to exit the menu.

### Setting the IP Address Using the Serial Console

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

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

- ```

1. Configure Network Interface - not configured
   IP Address                  : (not set)
   Netmask                    : (not set)
   Default Gateway Address    : (not set)

2. Ping Default Gateway

3. Save and Exit

-----

C. Clear Current Settings

Z. Zeroize

Q. Quit

```

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

**Note:** 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.

## INSTALLING THE MANAGEMENT CONSOLE

The Decru Management Console is run on a dedicated PC (the Management Station). This console provides the management interface for the LKM appliance. It also offers some management functions for all DataFort appliances in a given installation. Choose a computer that meets the following requirements to serve as the Management Station:

**TABLE 4: MANAGEMENT STATION REQUIREMENTS**

| Operating System                                                      | Hardware                                                        |
|-----------------------------------------------------------------------|-----------------------------------------------------------------|
| Windows XP Service Pack 2                                             | 2 Ghz                                                           |
| Java 1.5.0_06 (automatically installed with Decru Management Console) | 1GB RAM                                                         |
|                                                                       | 4GB free hard drive space                                       |
|                                                                       | Fixed IP address accessible by all appliances that will use LKM |
|                                                                       | 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. Logons should be limited to authorized administrators, with no remote management enabled.

## RUNNING THE INSTALLER

The installer must be run on the Management Station before an LKM appliance can be configured or managed. This will install the Decru Management Console and the driver for the smart card reader on the Management Station. Use of the smart card reader and console are both required for initial setup of LKM appliances.

1. Insert the LKM CD in a drive on the Management Station.  
The CD will run automatically.
2. Click the installer link.
3. When prompted by the File Download screen to open or save the file, click the Open button to open the file.
4. Follow the prompts to start the installer.
5. Read and accept the terms of the license agreement.
6. Select the model number of your smart card reader. The model number can be found on the underside of the smart card reader (i.e. GemPC413-SL).
7. Select “Yes, I want to restart my computer now” and click Finish to complete installation.
8. Select **Start > Programs > Decru > Decru Management Console** to view the console.

Using the console to initialize an LKM appliance is described in [Chapter 3](#).

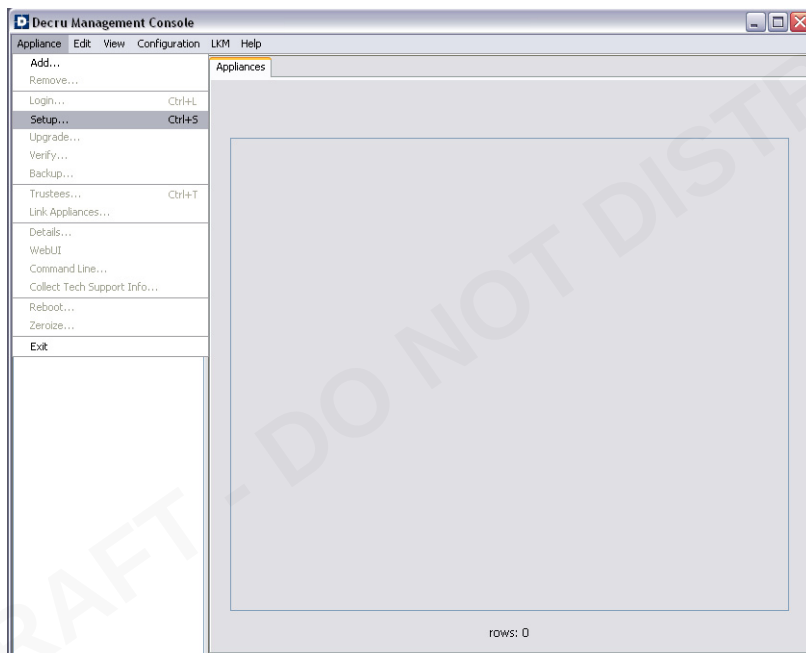
### 3 INITIALIZING AN LKM APPLIANCE

Once the installer has placed the Management Console on the Management Station, use it to run the setup wizard and initialize LKM appliances. This same wizard can also be used to initialize a DataFort appliance. See the [DataFort Administration Guide](#) for information about using the wizard to add a DataFort appliance.

When the console is run for the first time, no appliances will appear in the interface. Use the Setup Wizard to set up uninitialized appliances. Once configured, appliances can be added to the console for further management.

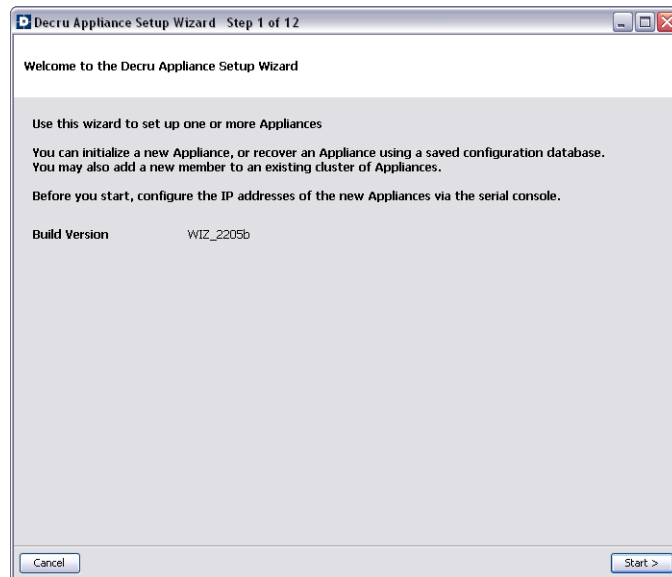
#### RUNNING THE SETUP WIZARD

1. To start the Management Console, choose **Start > Programs > Decru > Lifetime Key Management**.
2. From the Management Console menu, choose **Appliance > Setup**.

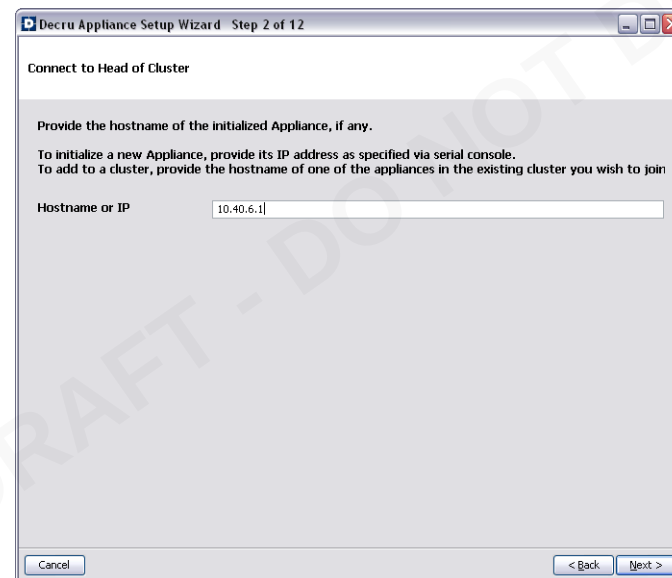


The wizard will begin.

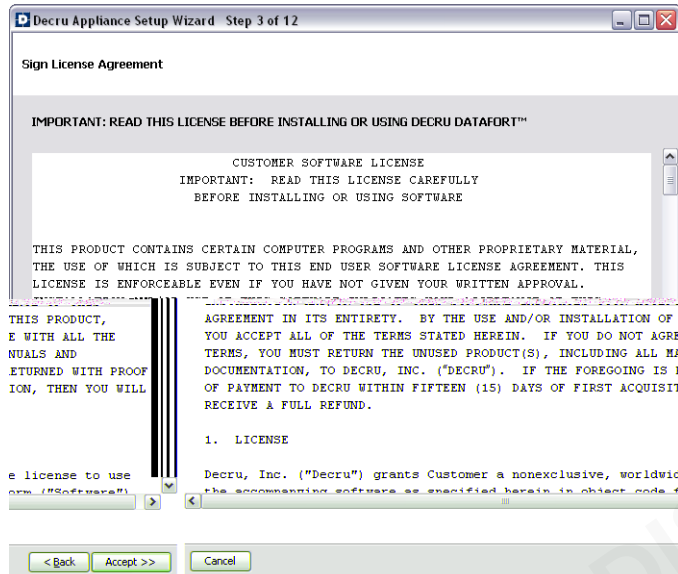
3. Click Start.



4. Enter the IP address of the LKM appliance (as configured using the LCD or serial console during installation). If there is a hostname already associated with that IP address, you may enter the hostname instead.



5. Click Next. The certificate validating the connection between the appliance and the Management Station will appear.
6. Choose whether to trust the certificate once or always.
7. Read and accept the license agreement.



8. Skip the Recover from Database screen by clicking Next.

Decru Appliance Setup Wizard Step 4 of 12

**Recover from Database (Optional)**

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

Path to Configuration Database

The next step creates an administrator for the LKM appliance. After the wizard is completed, additional administrators can be created and associated with Admin Cards.

Decru Appliance Setup Wizard Step 5 of 12

**Create Administrator**

Specify an administrative username and password.

Username

Password  (minimum 8 and maximum 30 characters)

Confirm Password

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

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

11. Click Next.

The next step sets the recovery schema which determines how many Recovery Cards must be present for sensitive data recovery operations.

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

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

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:

Cancel < Back Next >

12. Select the desired data recovery schema.
13. Do not modify the cluster size setting.

**CAUTION:** ONCE THE NEXT BUTTON IS CLICKED ON THIS SCREEN, THIS SETTING WILL BECOME PERMANENT.

14. Click Next.

Decru 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.

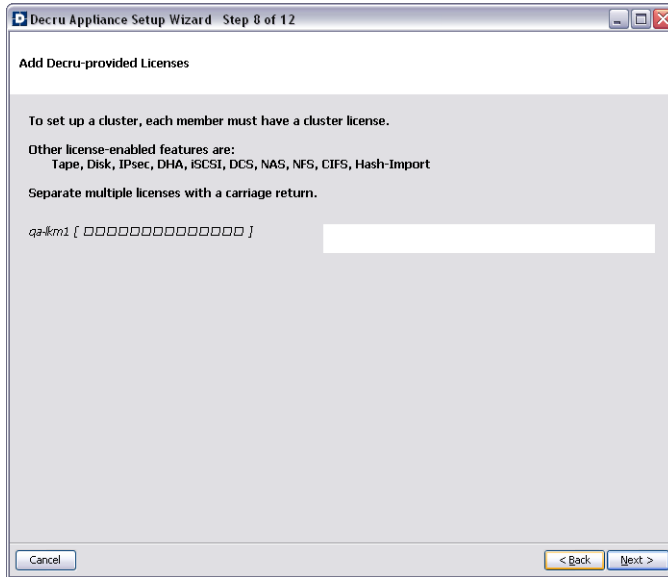
Hostname 1

IP Address 1

Netmask 1

Gateway 1

15. Enter the appropriate network settings.
16. Enter a hostname for this LKM appliance.
17. Click Next.



18. If you have a licensed feature such as SecureView, enter the license on the page.

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.

19. Click Next.

The next step initializes the Recovery Cards associated with this appliance. Recovery Officers responsible for Recovery Cards should be prepared to enter card label and password information into the provided fields.



20. 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.
21. 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.

**Decru Appliance Setup Wizard Step 10 of 12**

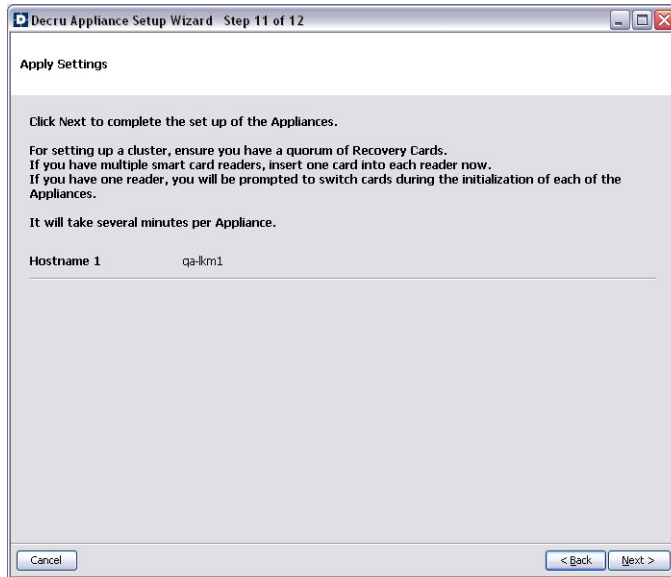
**Recovery Card Authentication**

Authenticate this Recovery Card.

|                  |                 |
|------------------|-----------------|
| Card ID          | 09000000        |
| Card Label       | dr6             |
| Security Domain  | SecurityDomain1 |
| Current Password | *****           |

Buttons: Cancel, < Back, Next >

22. Repeat the previous steps for all the cards specified by the recovery schema.
23. When all cards have been introduced, click Next.
24. Click Next to apply the settings to all appliances that are being configured using the wizard.



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

When the wizard is complete, the final screen appears.

26. Click Finish.

When the wizard is complete, the LKM appliance is ready to be managed by the Decru Management Console. See [Chapter 4](#) for instructions.

## ■ ■ ■ ■ 4 SETTING UP LIFETIME KEY MANAGEMENT

After initialization (described in [Chapter 3](#)), both LKM and DataFort appliances can be added to the Decru Management Console for centralized management. Once all appliances have been added, set up the communication channel between DataFort and LKM appliances to automate backups and key management.

In addition to managing the LKM appliance, the Decru Management Console manages some aspects of DataFort functionality, including running the Setup Wizard, adding administrators and manually backing up the configuration database.

If [SecureView™](#) is enabled, these functions can be performed on several appliances at once. SecureView allows the Management Console to manage many appliances at once, making it possible for the administrator to perform management functions on several appliances simultaneously.

The following should be completed to enable LKM appliance key management operations:

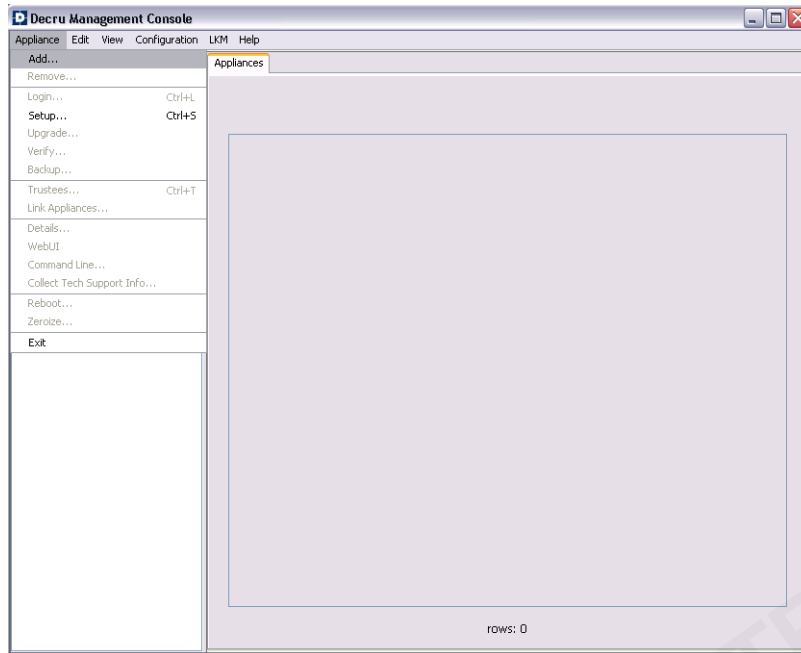
- [Adding Appliances](#)
- [Logging into Appliances](#)
- [Connecting DataFort Appliances to LKM](#)

### ADDING APPLIANCES

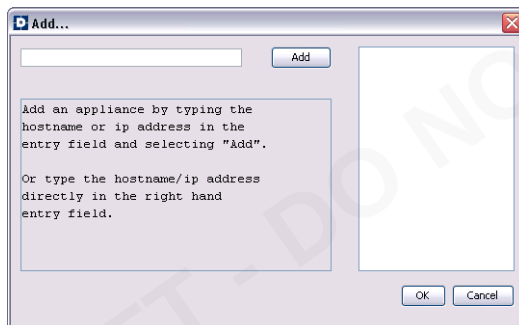
---

Add all LKM and DataFort appliances in the enterprise to the Decru Management Console.

1. To start the Management Console choose **Start > Programs > Decru > Lifetime Key Management**.
2. From the Management Console menu, select **Appliance > Add**.

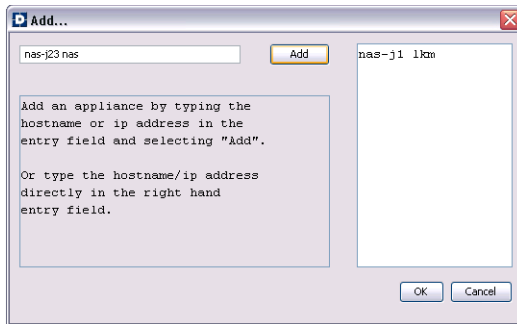


The Add... pop-up screen appears.

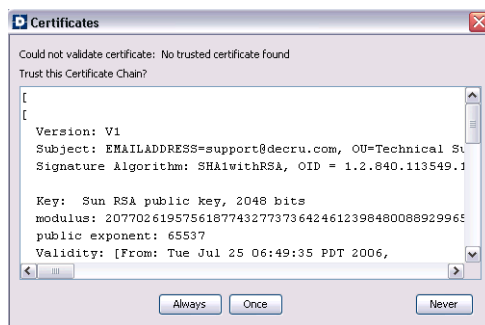


3. Enter the IP address or hostname of the appliance.

More than one appliance can be added on this screen: enter the IP address or hostname for each appliance in the 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.



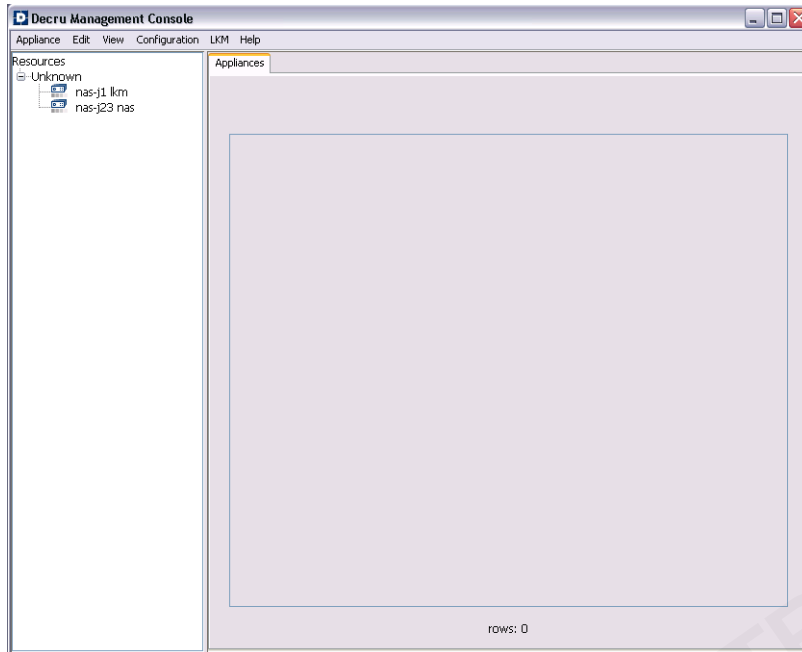
4. Click OK when all addresses or hostnames are entered.  
The certificate warning appears.



5. Choose to trust the certificate once or always.

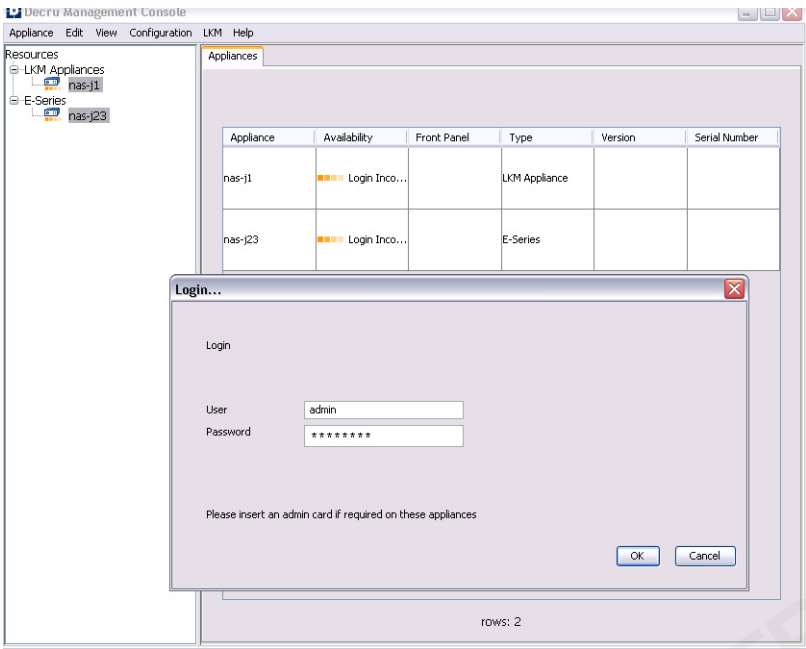
**Note:** If the appliance is not found, no certificate warning will appear. The appliance will be added to the console, but will not appear online.

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

1. Select one or more appliances in the Resources list. Shift-click to select multiple appliances.  
**Note:** You can log into more than one appliance at once if they share a common administrator name and password combination.
2. Right-click and select Login.



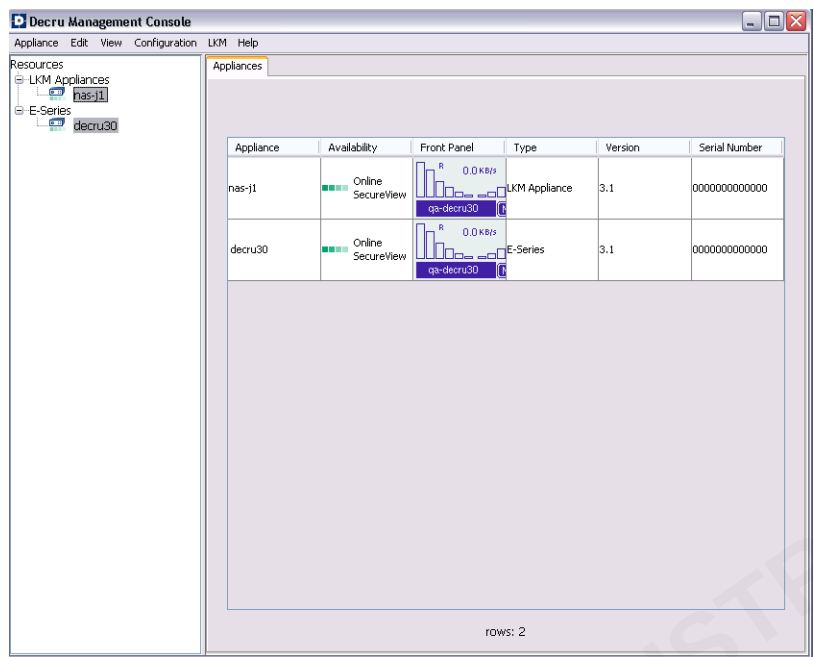
- 3. Enter the administrator name and associated password at the Login... page.
- 4. Click OK.

If the correct credentials were entered and the appliance is correctly configured, the status of the appliance will change to online. The following table shows possible state displays for appliances in the Management Console.

TABLE 5: APPLIANCE STATUS INDICATORS

| Icon | Color       | Appliance State                                                  |
|------|-------------|------------------------------------------------------------------|
|      | Blue        | Uninitialized: IP address set, but setup wizard not completed    |
|      | Orange      | Login incomplete: administrator name and/or password not correct |
|      | Green       | Online: online with no errors                                    |
|      | Light green | Online with error: check appliance LCD                           |
|      | Red         | Offline                                                          |
|      | Light gray  | Unreachable: appliance may not be on network                     |
|      | Dark gray   | Unknown: no login has taken place                                |

Any appliance added to the console will display with basic information in the console: name, status, messages from the front panel LCD, appliance type, software version and serial number.

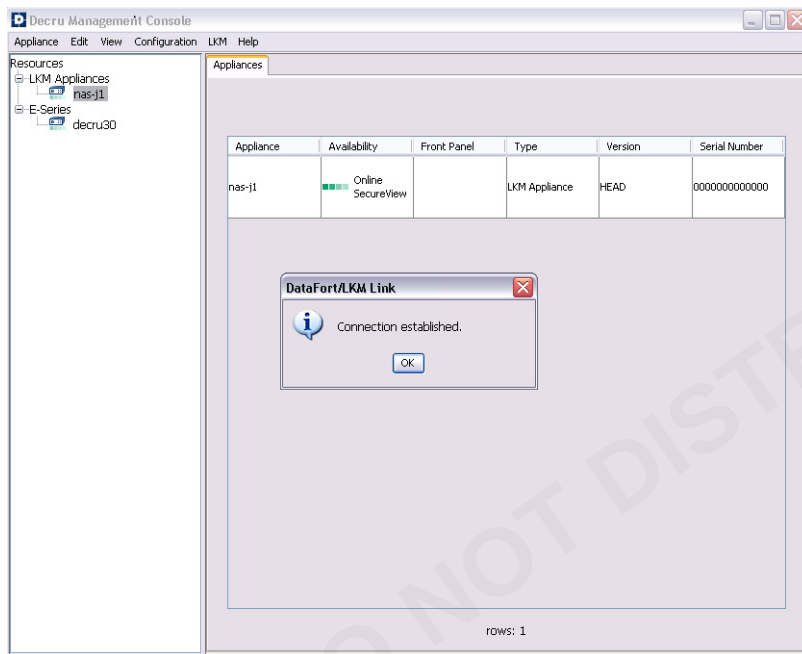


Once LKM and DataFort appliances have been added and you have logged in, connect the appliances. See [Connecting DataFort Appliances to LKM](#).

## CONNECTING DATAFORT APPLIANCES TO LKM

Create a communication channel between all DataFort appliances and the LKM appliance.

1. Select on or more DataFort appliances in the Resources pane. Shift-click to select multiple appliances.
2. Drag the DataFort appliance to the LKM appliance in the Resources pane.  
An alert will appear when the connection has formed.
3. Click OK.



This allows the DataFort appliance to send key information to the LKM appliance.

Once all appliances have been added to the console, and the relationship between LKM and DataFort appliances has been created, you are free to manage appliances and keys using the Decru Management Console Menus. See [Decru Management Console Menus](#) for options.

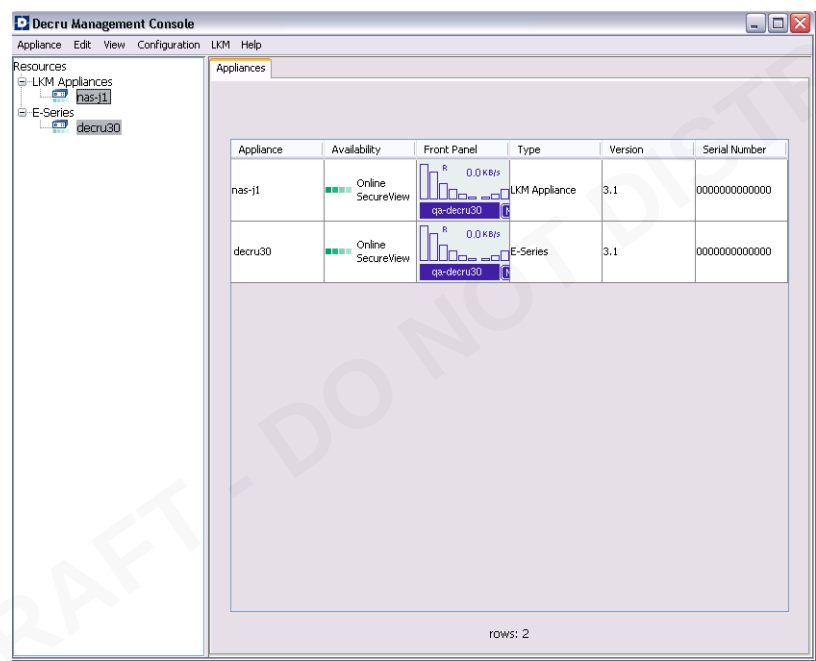
5    **DECRU MANAGEMENT CONSOLE MENUS**

Use the console to manage LKM and DataFort appliances from a central location. The Decru Management Console offers the following drop-down menus:

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

If equipped with SecureView licenses, more than one appliance can be selected at once, and a menu selection applied to all selected appliances.

Some menu options initiate operations which are described in more detail in the [Appliance Management](#) and [Key Management](#) chapters 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 LKM or DataFort appliance. See <a href="#">Adding Appliances</a> on page 23.                                                                                                                                                                                                                                                                                    |
| <b>Remove</b>                    | Remove an appliance from the Management Console. See <a href="#">Removing an Appliance</a> on page 34.                                                                                                                                                                                                                                                                 |
| <b>Login</b>                     | Log in to an appliance as an administrator. See <a href="#">Logging into Appliances</a> on page 26.                                                                                                                                                                                                                                                                    |
| <b>Setup</b>                     | Set up an LKM or DataFort appliance by running the Setup Wizard. See <a href="#">Running the Setup Wizard</a> on page 13.                                                                                                                                                                                                                                              |
| <b>Verify</b>                    | Verify the validity of an upgrade package before upgrading. See <a href="#">Verify</a> on page 35.                                                                                                                                                                                                                                                                     |
| <b>Upgrade</b>                   | Upgrade an appliance. Upgrades should be done only after consulting Decru support. See <a href="#">Upgrade</a> on page 35.                                                                                                                                                                                                                                             |
| <b>Backup</b>                    | Back the configuration database up as a file to a specified location. See <a href="#">Back Up</a> on page 35.                                                                                                                                                                                                                                                          |
| <b>Trustees</b>                  | Create a Trustee relationship between two DataFort appliances. This allows the appliances to share key information. Both appliances must be selected. See <a href="#">Trustees</a> on page 36.                                                                                                                                                                         |
| <b>Link Appliances</b>           | Create a link between a DataFort and LKM appliance so that LKM can manage keys for that DataFort appliance. Both appliances must be selected. See <a href="#">Link Appliances</a> on page 37. The same is achieved by dragging the DataFort appliance icon to the LKM appliance icon as described in <a href="#">Connecting DataFort Appliances to LKM</a> on page 29. |
| <b>Details</b>                   | Shows the system version for the selected appliance. See <a href="#">Details</a> on page 37.                                                                                                                                                                                                                                                                           |
| <b>WebUI</b>                     | Opens the WebUI of the selected appliance (DataFort only). See <a href="#">WebUI</a> on page 37.                                                                                                                                                                                                                                                                       |
| <b>Command Line</b>              | Opens the CLI. Whatever command is run will be executed on all selected appliances. See <a href="#">Command Line</a> on page 37.                                                                                                                                                                                                                                       |
| <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="#">Collect Tech Support Info</a>                                                                                                   |

## CONFIGURATION MENU

---

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

|                       |                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------|
| <b>License</b>        | View licenses. See <a href="#">Managing Licenses</a> on page 40.                        |
| <b>Add License</b>    | Add licenses. See <a href="#">Adding a License</a> on page 41.                          |
| <b>Administrators</b> | View and manage administrators. See <a href="#">Managing Administrators</a> on page 41. |
| <b>Add Admin</b>      | Add an administrator. See <a href="#">Adding an Administrator</a> on page 43.           |

## VIEW MENU

---

The View setting determines how appliances are viewed in the Resources pane. The default setting organizes appliances by type, but the view can be changed to organize the display according to network, and to show type and subnet information. Select an option to sort appliances accordingly, 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.                                                                                        |

## 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.                                                               |
| <b>Refresh</b>    | Repeat search.                                                                                    |

## LKM MENU

---

Select an LKM appliance in the Resources pane. Choose LKM and select from the drop down menu, or right-click an LKM appliance and select from the right-click menu.

|                                              |                                                                                                                                                                                                                                                                     |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cryptainer Keys</b>                       | View all Cryptainer keys stored in LKM. This presents a dialog for filtering Cryptainer keys (find by DataFort, creation date or containing Key ID). The first 100 keys matching the attributes are returned. The Next/Previous Page options retrieve more results. |
| <b>Domain Keys</b>                           | View all Domain keys in the DataFort appliance.                                                                                                                                                                                                                     |
| <b>Recovery Cards</b>                        | View all associated Recovery Cards.                                                                                                                                                                                                                                 |
| <b>Make Key Archive</b>                      | Create a Key Archive. This contains parent key information (Master and Domain key). This does not archive the keys from a single Cryptainer, but from a DataFort or series of DataFort appliances. See <a href="#">Generating a Key Archive</a> on page 47.         |
| <b>Make Cryptainer Key Archive</b>           | Create an archive of Cryptainer Keys. See <a href="#">Generating a Cryptainer Key File</a> on page 48.                                                                                                                                                              |
| <b>Translate Key(s)</b>                      | Translate keys from one DataFort to another DataFort. See <a href="#">Key Translation</a> .                                                                                                                                                                         |
| <b>Next</b>                                  | View next 100 keys in list.                                                                                                                                                                                                                                         |
| <b>Previous</b>                              | View previous 100 keys in list.                                                                                                                                                                                                                                     |
| <b>Export Key File</b>                       | Export Key Files to a local hard drive. The files can then be deleted from the LKM appliance, or imported back into an LKM appliance (the original or another one). Only key information is shared. See <a href="#">Importing and Exporting Keys</a> on page 50.    |
| <b>Import Key File</b>                       | Import Key Files that have been exported from another LKM appliance. <a href="#">Importing and Exporting Keys</a> on page 50.                                                                                                                                       |
| <b>Backup DataFort appliances</b>            | Send a backup of the configuration databases of all DataFort appliances known to this LKM appliance.                                                                                                                                                                |
| <b>Make Cryptainer Key Archive From File</b> | Create a Cryptainer Key Archive from a selected file. The file will be one created by the Export Key File command. This could be used should you need to recover data without the LKM appliance.                                                                    |
| <b>Smart Card Utilities</b>                  | Resets a smart card and displays card information.                                                                                                                                                                                                                  |

## HELP MENU

---

|              |                                                                 |
|--------------|-----------------------------------------------------------------|
| <b>Help</b>  | Opens online help for selected appliance type.                  |
| <b>About</b> | Shows information about this version of the Management Console. |

## 6 APPLIANCE MANAGEMENT

Use the Decru Management Console to manage LKM and DataFort appliances.

- [Appliance Menu](#)
- [Configuration](#)

### APPLIANCE MENU

---

#### ADDING AN APPLIANCE

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

1. Select one or more appliances in the Resources pane. Shift-click to select multiple appliances.
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](#).

#### REMOVING AN APPLIANCE

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

1. Select one or more appliances in the Resources list. Shift-click to select multiple appliances.
2. Choose **Appliance > Remove**.

#### LOGGING INTO APPLIANCES

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

1. Select one or more appliances in the Resources pane. Shift-click to select multiple appliances.

**Note:** You can log into more than one appliance at once if they share a common administrator name and password combination.

2. From the Management Console menu select **Appliance > Login**.
3. Enter the administrator name and associated password at the Login page.
4. 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 27 for information about status icons.

## **RUNNING THE SETUP WIZARD**

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

1. Select one or more appliances in the Resources pane. Shift-click to select multiple appliances.
2. From the Management Console menu, choose **Appliance > Setup**.
3. Run the wizard for the appliance. See [Initializing an LKM Appliance](#) on page 13 for detailed instructions.

## **VERIFY**

Verify an upgrade package before running it on the appliance.

1. Select one or more appliances in the Resources pane. Shift-click to select multiple appliances.
2. From the Management Console menu, choose **Appliance > Verify**.
3. Browse to the upgrade file.
4. Click Apply.

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

## **UPGRADE**

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

1. Select one or more appliances in the Resources pane. Shift-click to select multiple appliances.
2. From the Management Console menu, choose **Appliance > Upgrade**.
3. Browse to the upgrade file.
4. Click Apply.

## **BACK UP**

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

1. Select one or more appliances in the Resources pane. Shift-click to select multiple appliances.
2. From the Management Console menu, choose **Appliance > Back Up**.
3. Choose a location for the file to be saved.
4. Click Save.

## TRUSTEES

Select two appliances to form a trustee relationship between them. Creating trustees allows data encryption keys to be shared between DataFort appliances that have no Recovery Cards in common, and may not even be on the same network.

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).

**Note:** Recovery Cards are required during trustee setup.

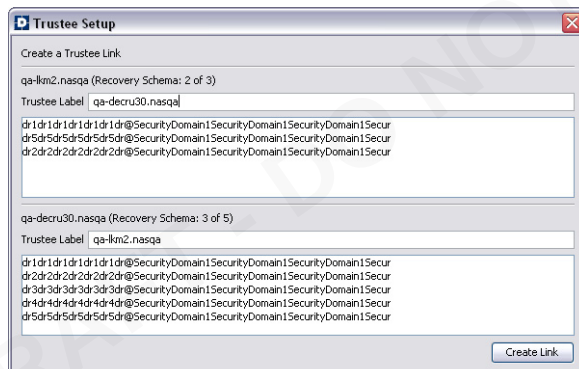
The establishment of trustees enables several enterprise scenarios:

- |                               |                                                                                                                                                                                                                                                                             |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Disaster Recovery Site</b> | In a situation where there is a DataFort appliance off-site, and it is not desirable to form a cluster to share key data (either because there is no network connectivity between the main and off-site 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. Data is protected via Cryptainers, but it is not desirable to share all keys.                                                                                                                     |

To set up a trustee relationship:

1. Select both appliances in the Resources pane of the console.
2. Select **Appliances > Trustees**.

The Trustee Setup page appears. Both appliances appear on the screen.



3. Click Create Link.
4. The TEP wizard will begin. Follow the steps to approve the TEP.

### 5. Procedure not documented...

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.

## LINK APPLIANCES

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

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

Or:

1. Select both appliances in the Resources pane of the console.
2. Drag the icon for the DataFort appliance to the icon for the LKM appliance.
3. An alert will appear when the connection is made.

## DETAILS

Shows the system version information for the appliance.

1. Select one or more appliances in the Resources pane. Shift-click to select multiple appliances.
2. Select **Appliance > Details**.
3. The system version command will be run on the CLI and the output displayed.

## WEBUI

Opens the WebUI for the DataFort appliance.

1. Select a DataFort appliance in the Resources pane.
2. Select **Appliance > WebUI**.

The WebUI for the appliance will open. See the [DataFort Administration Guide](#) for instructions on using the WebUI to manage DataFort appliances.

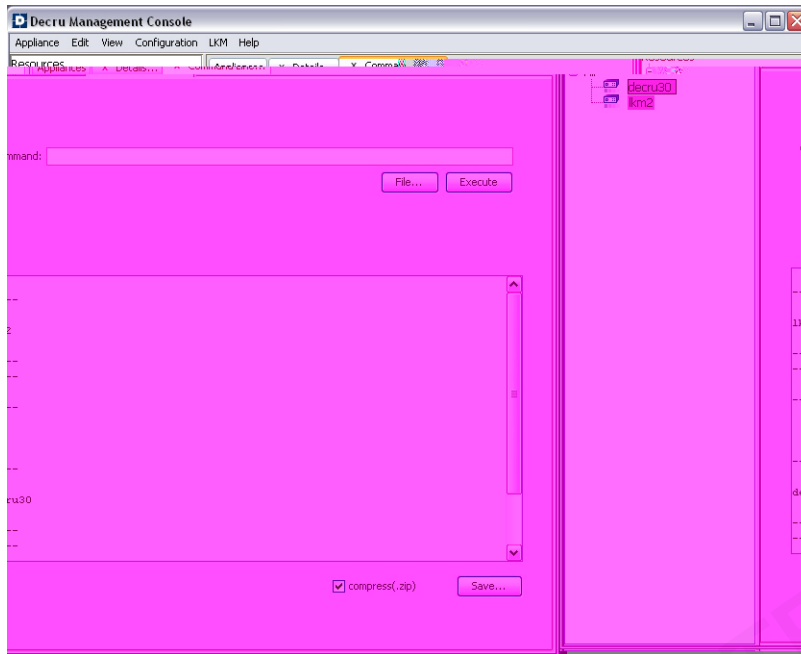
**Note:** This option is only valid for DataFort appliances.

## COMMAND LINE

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

1. Select one or more appliances in the Resources pane. Shift-click to select multiple appliances.
2. Select **Appliance > Command Line**.

The CLI will open. See the [DataFort Administration Guide](#) for instructions on using the CLI to manage DataFort appliances. See [CLI Commands](#) on page 52 for LKM commands.



3. 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.
- To save the output of a command that has been executed, click Save and save the file in a designated location.

### COLLECT TECH SUPPORT INFO

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

1. Select one or more appliances in the Resources pane. Shift-click to select multiple appliances.
2. Select **Appliance > Collect Tech Support Info**
3. Save the exported file to a designated location.

## REBOOT

Reboots all selected appliances.

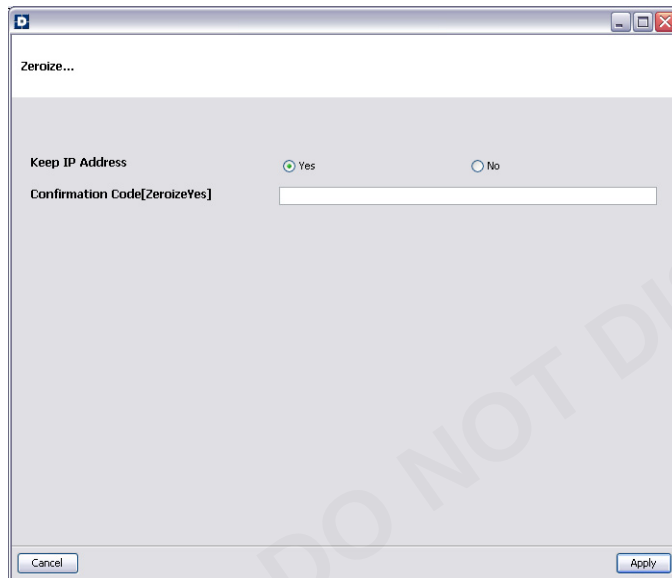
1. Select one or more appliances in the Resources pane. Shift-click to select multiple appliances.
2. Select **Appliance > Reboot**.

The appliance will reboot.

## ZEROIZE

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

1. Select one or more appliances in the Resources pane. Shift-click to select multiple appliances.
2. Select **Appliance > Zeroize**.

A screenshot of a Windows-style dialog box titled "Zeroize...". The dialog has a light gray background. At the top, there is a title bar with standard window controls. Below the title bar, the text "Zeroize..." is displayed. In the center, there are two radio buttons: "Yes" (which is selected) and "No". Below the radio buttons, there is a label "Keep IP Address" and a text input field labeled "Confirmation Code[ZeroizeYes]". At the bottom of the dialog, there are two buttons: "Cancel" on the left and "Apply" on the right. A large, diagonal watermark reading "DO NOT DISTRIBUTE" is visible across the entire dialog box.

3. Choose whether or not to preserve the appliance's IP Address.
4. Enter the conformation code.
5. Click Apply.

## EXIT

Exits the Decru Management Console.

CONFIGURATION

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

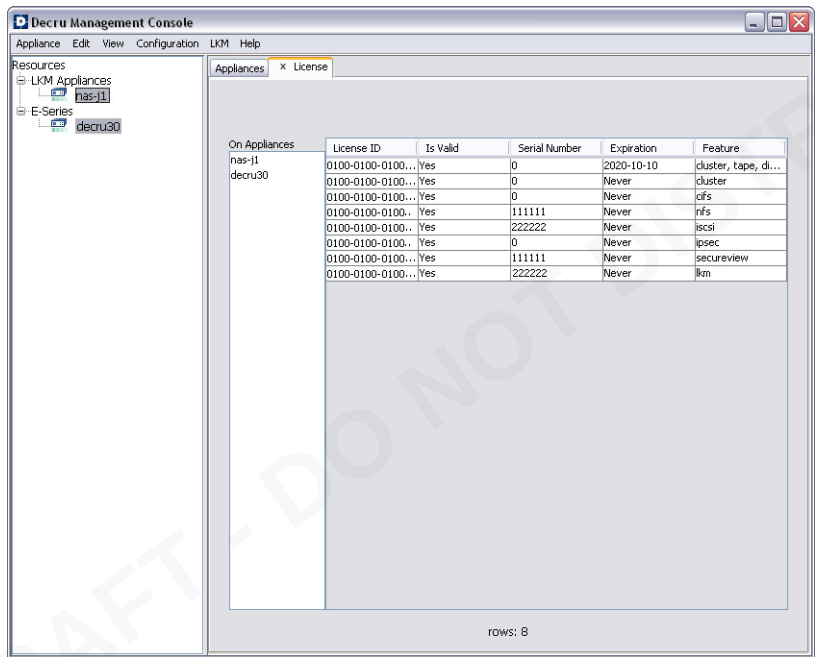
- [Managing Licenses](#)
- [Adding a License](#)
- [Managing Administrators](#)
- [Adding an Administrator](#)

If SecureView licences are in use, these functions can be applied to several appliances simultaneously.

MANAGING LICENSES

To view the licenses on selected appliances:

1. Select the appliance or appliances in the Resources pane. Shift-click to multi-select.
2. Choose **Configuration > License**.

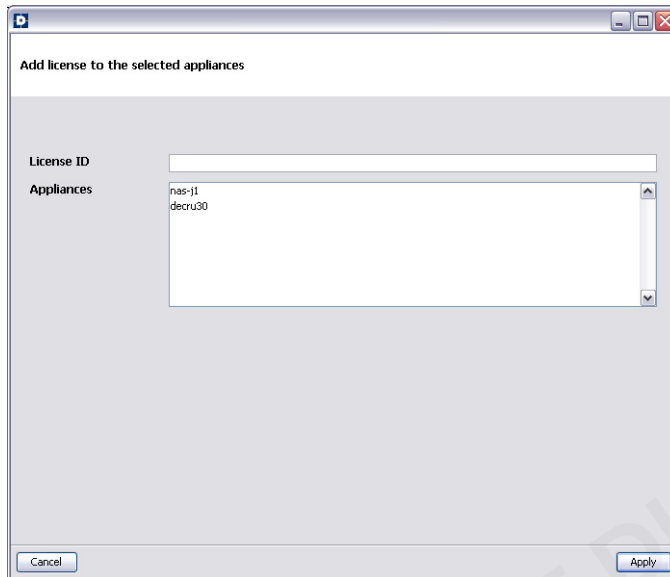


All known licenses for the selected appliances appear.  
Licenses can be removed by right-clicking the license on-screen and selecting Delete.

## ADDING A LICENSE

To add licenses to selected appliances:

1. Select the appliance or appliances in the Resources pane. Shift-click to multi-select.
2. Choose **Configuration > Add License**.
3. Enter the license into the provided field.

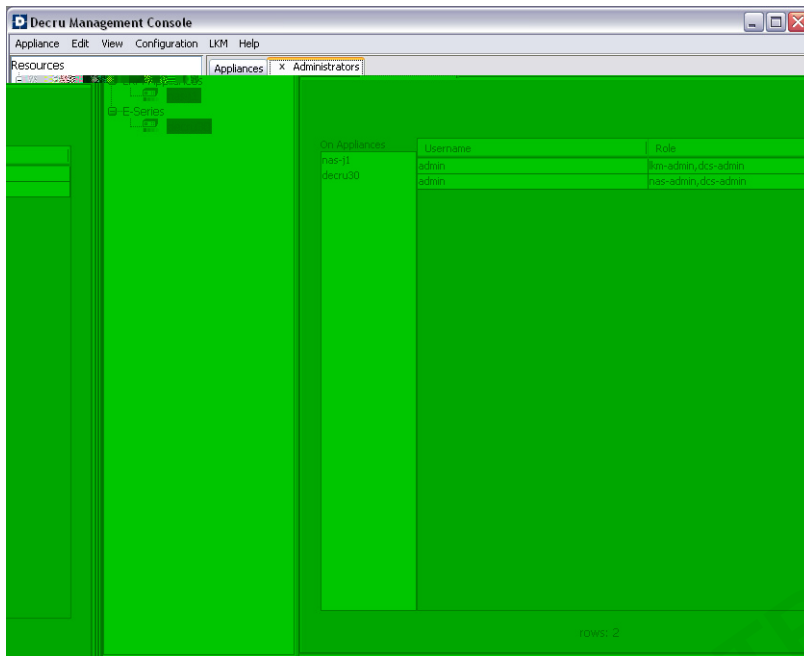


4. Click Apply.  
All known licenses for the selected appliances appear.

## MANAGING ADMINISTRATORS

To view the administrators with permission to manage selected appliances:

1. Select the appliance or appliances in the Resources pane. Shift-click to multi-select.
2. Choose **Configuration > Administrators**.

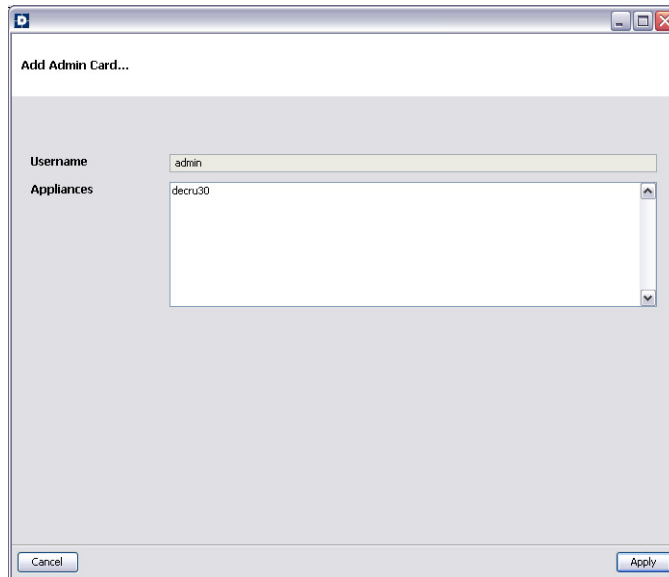


All known administrators for the selected appliances appear.

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

1. On the Administrators page, right-click an administrator (or shift-click to multi-select and then right click).
2. Select Add Admin Card.



**Add Admin Card...**

Username: admin

Appliances: decru30

Cancel Apply

### Removing an Admin Card from an Administrator

1. On the Administrators page, right-click an administrator (or shift-click to multi-select and then right click).
2. Select Remove Admin Card.

### Deleting an Administrator

1. On the Administrators page, right-click an administrator (or shift-click to multi-select and then right click).
2. Select Delete.

### ADDING AN ADMINISTRATOR

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

1. Select the appliance or appliances in the Resources pane. Shift-click to multi-select.
2. Choose **Configuration > Add Admin**.

**Add Administrator for selected appliances**

Username

Password

Confirm Password

Role ☒ Read Only ☐ Specialty ☐ Full Admin

Appliances

The Add Administrator page appears.

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

#### **Read-only**

Select this to create an administrator who can view DataFort settings, but cannot modify them.

#### **Specialty**

Select this to create specialized administrators. With Specialty selected, you can check multiple special types to combine permissions for one administrator.

#### **Full Admin**

Select this to create a Full Administrator role.

**Note:** Full Admins 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.

**Add Administrator for selected appliances**

Username:

Password:

Confirm Password:

Role: ☐ Read Only ☒ Speciality ☐ Full Admin

Speciality Role: ☐ Key ☐ Security ☐ Accounts ☐ Storage ☐ Backup ☐ Machine

Appliances:

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. The administrative types are:

|                       |                                                                                                                                                 |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Key Admin</b>      | Responsible for applying security-related settings to appliances.                                                                               |
| <b>Security Admin</b> | Responsible for applying physical security-related settings to appliances.                                                                      |
| <b>Accounts Admin</b> | Can add, delete and manage administrators.                                                                                                      |
| <b>Storage Admin</b>  | Can add and delete hosts/clients and storage in order to create Cryptainers                                                                     |
| <b>Backup Admin</b>   | Responsible for managing backups of the configuration database                                                                                  |
| <b>Machine Admin</b>  | Responsible for managing system properties and non-security sensitive cluster operations. This administrator can change local network settings. |

See the [DataFort Administration Guide](#) for more information about administrator roles.

6. Select the appliance to associate with this administrator.
7. Click Apply.

**Note:** To associate and Admin Card with this administrator, see [Adding an Admin Card to an Administrator](#).

## 7 KEY MANAGEMENT

The LKM appliance and the Management Console provide tools for managing keys in the enterprise. Use LKM Menus in the console to create archive files of encryption keys that can make data recovery possible even if a DataFort or LKM appliance is made unavailable. The LKM appliance uses special file types to save and share encryption keys. The following keys are in use::

|                               |                                                                                                                   |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Cryptainer Keys</b>        | Encrypt data within Cryptainers.                                                                                  |
| <b>Domain Keys</b>            | Shared between clustered DataFort appliances.                                                                     |
| <b>Parent Keys</b>            | Encrypt all Cryptainer keys within a DataFort appliances.                                                         |
| <b>Key Archive</b>            | A file (.ka) which contains parent key information.                                                               |
| <b>Cryptainer Key Archive</b> | A file (.cka) which contains Cryptainer Keys. For use with DDS when decrypting data without a DataFort appliance. |
| <b>Translated Key</b>         | Keys that have been made available by one DataFort to another.                                                    |
| <b>Exported Key File</b>      | A key list exported from an LKM appliance and stored in a file (.klf).                                            |
| <b>Imported Key File</b>      | A key list Imported to an LKM appliance from a .klf file.                                                         |
| <b>Backup DataFort File</b>   | A configuration backup from all DataFort appliances linked to LKM.                                                |

LKM functions provide the necessary components of emergency data recovery including:

|                            |                                                                                                                                                                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Key Archive</b>         | A Key Archive should be created for every DataFort after it is initialized. A new Key Archive is needed only if the DataFort is zeroized and subsequently reinitialized. The archive is used to recover encrypted data if the original DataFort is no longer available. See <a href="#">Generating a Key Archive</a> . |
| <b>Cryptainer Key File</b> | LKM can generate a Cryptainer Key File for a single Cryptainer or all Cryptainers in a DataFort configuration. <a href="#">Generating a Cryptainer Key File</a> is an intermediate component of data recovery. A Cryptainer Key File is used by the separate Decru Data Decryption Software (DDS) to recover data.     |
| <b>Translate Keys</b>      | The <a href="#">Key Translation</a> enables all Cryptainers on a selected DataFort to be accessible from another DataFort.                                                                                                                                                                                             |
| <b>Import/Export Keys</b>  | Used to export and import encryption keys from one LKM appliance to another. See <a href="#">Importing and Exporting Keys</a> .                                                                                                                                                                                        |

**CAUTION:** GENERATION OF KEY ARCHIVES AND CRYPTAINER KEY FILES SHOULD BE EXECUTED ONLY ON A SECURE MANAGEMENT STATION THAT HAS BEEN SCANNED FOR VIRUSES AND THOROUGHLY CHECKED FOR THE PRESENCE OF MALICIOUS CODE THAT COULD COMPROMISE THE SECURITY OF ENCRYPTED DATA. DECRU RECOMMENDS REBOOTING THE MANAGEMENT STATION AFTER ANY KIND OF KEY ARCHIVE HAS BEEN CREATED.

## GENERATING A KEY ARCHIVE

---

DataFort uses a parent key to encrypt each Cryptainer Key in a configuration. In the event that both a DataFort and its associated Recovery Cards are unavailable, LKM can use a Key Archive to supply the keys needed to decrypt data.

A Recovery Key Archive should be created after every DataFort is initialized in order to ensure key availability. The Key Archive is generally valid for the life of the DataFort. A new Key Archive is needed only if the DataFort is zeroized and subsequently reinitialized.

**CAUTION:** BECAUSE THE KEY ARCHIVE COMPROMISES THE DISTRIBUTED SECURITY DESIGN OF THE SYSTEM AND RECOVERY CARDS, A RECOVERY KEY ARCHIVE SHOULD BE CREATED AND USED FOR ONLY TWO PURPOSES: IMMEDIATE DATA RECOVERY IF A DATAFORT IS NO LONGER FUNCTIONING, AND PLACEMENT IN KEY ESCROW OR ANOTHER FORM OF TRUSTED LONG-TERM STORAGE, FOR USE IN AN EMERGENCY.

Generating a Recovery Key Archive requires:

- The quorum of Recovery Officers and Recovery Cards (as configured during DataFort setup). Each Recovery Officer will be required to present a Recovery Card and its password.
  - A passphrase that the security administrator will supply in the course of generating the Key Archive to encrypt the Key Archive.
1. From the Decru Management Console, right-click a DataFort appliance.
  2. Choose Make Key Archive from the LKM menu.  
You are informed of the quorum of Recovery Cards required for the selected DataFort.
  3. A scrollbar lists the Recovery Cards in the Security Domain. If desired, control-click to select the particular Recovery Cards you will present to speed up the process. Click Next.
  4. When prompted, a Recovery Officer should insert a Recovery Card in the smart card reader, and click OK.
  5. Enter the Recovery Card password. Click Next.  
The previous two steps are repeated for all the Recovery Cards in the quorum.
  6. When prompted for a passphrase for the Recovery Key Archive, enter it twice and make a note of it. Click Next.
  7. Enter a comment or identifying name to help identify the Key Archive, and browse or enter the path to the directory where the file should be saved.
  8. Enter a descriptive filename and click Save.
  9. Click Finish.
  10. Move the Key Archive file to escrow or secure long-term storage, making sure you store the passphrase as well.

**CAUTION:** DELETE EVERY KEY ARCHIVE IMMEDIATELY AFTER USE OR SUBMISSION TO ESCROW. DO NOT LEAVE RECOVERY KEY ARCHIVE FILES ON ANY ACCESSIBLE LOCATION, AS THEY MAY COMPROMISE THE SECURITY OF ENCRYPTED DATA.

## GENERATING A CRYPTAINER KEY FILE

---

A Cryptainer Key File contains passphrase-encrypted Cryptainer or tape keys. These keys allow the recovery of encrypted data under special circumstances without a DataFort appliance.

Before a Cryptainer Key can be used, the Recovery Key must be introduced. This is done by presenting either a quorum of Recovery Cards or a Recovery Key Archive file.

Generate a Cryptainer Key File for a single Cryptainer, or for all Cryptainers in a configuration database.

- To generate an archive for all Cryptainers associated with a DataFort, right-click the DataFort, and choose Generate Key File.
  - To generate an archive for a single Cryptainer, select the DataFort in the left pane. A list of Cryptainers is shown on the right. Right-click the Cryptainer you wish to recover, and choose Generate Key File.
1. Select the method by which the Recovery Key will be introduced.
    - If you are using Recovery Cards to supply the Recovery Key, you are told how many Recovery Cards will be required. Pre-selecting the Recovery Cards that will be used speeds up the process. Recovery Officers should follow the screen prompts to insert Recovery Cards in the smart card reader and authenticate them with their passwords. Click OK.
    - Alternatively, if you are using the Recovery Key Archive to supply the Recovery Key, browse to locate the Recovery Key Archive file, and enter the Recovery Key Archive passphrase. Click Next.
  2. Whether you used Recovery Cards or the Recovery Key Archive, enter and confirm a passphrase for LKM to use to encrypt the archive.
  3. Click Next.
  4. Browse or enter a location for storing the archive.
  5. Enter a filename, and click Save.
  6. Click Finish.

The file is stored in the designated location.

## KEY TRANSLATION

Key Translation transfers encryption keys between DataFort appliances. In the event that one DataFort is unavailable or has been reassigned (for example to secure data for a different group), an administrator may transfer the Cryptainers protected by that DataFort (the source DataFort) to another DataFort (the target). Key Translation does not disable the Cryptainer Keys from the source DataFort.

Key Translation can be performed for one or more Cryptainers, and the target can be one or more DataFort appliances. Key translation can be performed for all Cryptainers at once, or one at a time.

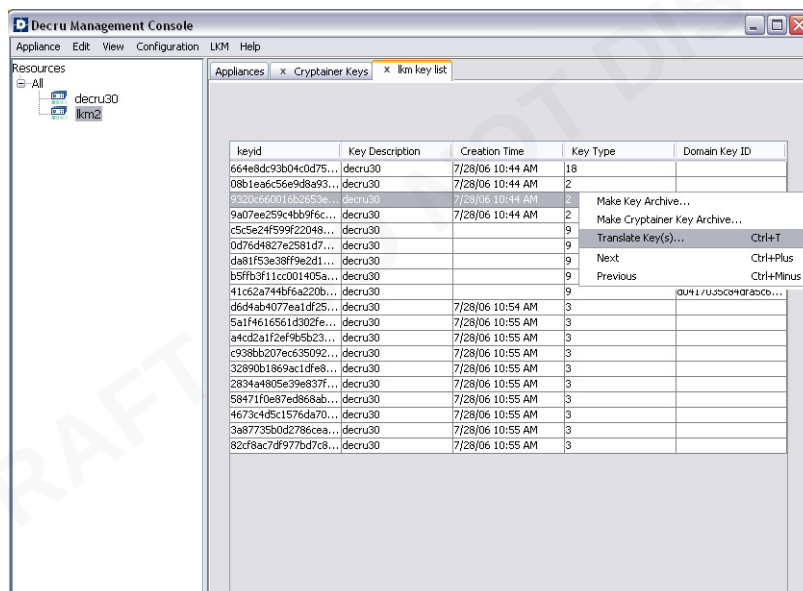
Key Translation is initiated from the LKM appliance that contains key information for both the source and target DataFort appliances. It requires a quorum of Recovery Officers and Recovery Cards for both the source and target DataFort, if they are secured by different individuals and cards.

After the key or keys are translated to the target DataFort, the administrator must perform a Cryptainer Restore operation on each of the translated Cryptainers, in order to make them accessible from the target DataFort. The steps are outlined below.

### TRANSLATING CRYPTAINER KEYS

Key translation can be authenticated either with Recovery Cards or Recovery Key Archives. In the first case, assemble the Recovery Officers and Recovery Cards for both the source DataFort and the target DataFort. In the second case, obtain Recovery Key Archives for the source and target DataFort.

1. Select the LKM appliance in the Resources pane.
2. Right-click a key or shift-click and then right-click to select more than one key in the LKM key list pane.



3. Highlight a destination key (target DataFort appliance) and click OK.
  4. Choose the method of authenticating the Key Translation and click Next. (Choose Use Recovery Cards unless you have already created a Recovery Key Archive.)
    - If you choose Use Recovery Cards, the quorum of Recovery Cards will be needed (from both DataFort appliances). When prompted to insert Recovery Cards, Recovery Officers insert their Recovery Cards in the smart card reader, and enter their passwords.
    - If you choose Use Key Archives, browse or enter the path to the Key Archive for the source DataFort, and enter the Recovery Key Archive passphrase. Click Next. Browse or enter the path to the Key Archive for the target DataFort, and enter its passphrase. Click Next.
- A message confirms that the keys have been successfully translated.

## IMPORTING AND EXPORTING KEYS

---

Importing and exporting keys can be helpful when maintaining an off-site clone of a DataFort appliance. LKM can be used to selectively export and import Cryptainer Keys.

### EXPORTING CRYPTAINER KEYS

1. Select the LKM appliance in the Resources pane and select **LKM > Export Key File**.
2. Enter and then confirm a passphrase in the dialog that follows.
3. Click Choose Save Location.
4. Specify a location to save the export file. Enter a new filename or accept the default filename (which is based on the DataFort name or key name), and click Save.

### IMPORTING EXPORTED CRYPTAINER KEYS

The saved export file can be imported into another LKM installation.

1. Select the LKM appliance in the Resources pane and select **LKM > Import Key File**.
2. Enter the passphrase you supplied when you exported the Cryptainer Keys. Click Choose File Location.
3. Browse to the export file you saved in the previous procedure, and click Open.

The imported keys now appear in the right pane, associated with the appropriate DataFort.





## ■ ■ ■ ■ APPENDIX I CLI COMMANDS

SPECIFIC TO LKM APPLIANCE MANAGEMENT AND THE MANAGEMENT CONSOLE...

DRAFT - DO NOT DISTRIBUTE

## ■ ■ ■ ■ APPENDIX II 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 Lifetime Key Mangement™ 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

