

KM-Series Appliance 3.0 Release Notes

RELEASE DATE: 2/20/2007

The following are known issues and recommended procedures for the current release of the KM-Series Appliance 3.0 (the Lifetime Key Management Appliance). Please refer to the Lifetime Key Management Appliance Administration Guide for installation, configuration and operation instructions as well as descriptions of how to implement the new features listed below.

CONTENTS

[FIXED NOTES](#)

[DATA DECRYPTION SOFTWARE](#)

[LICENSES](#)

[WIZARD](#)

[NEW FEATURES](#)

[DECRU MANAGEMENT CONSOLE](#)

[KEY TRANSFER TOOL](#)

[LKM APPLIANCE](#)

[WIZARD](#)

[WORKAROUNDS](#)

[DECRU MANAGEMENT CONSOLE](#)

[KEY TRANSLATION](#)

[LKM APPLIANCE](#)

[SETUP WIZARD](#)

[SMART CARDS](#)

[TRUSTEE KEY](#)

FIXED NOTES

DATA DECRYPTION SOFTWARE

- **Preserve Block Size (PBS) on with certain block sizes** Fixed issue where Decru's Data Decryption Software would fail to decrypt tapes formatted with certain block sizes and Preserve Block Size ON. 27210

LICENSES

- **Cluster license not required** Previous versions of the Decru setup wizard required a cluster license when setting up clustered appliances. The cluster license is no longer required during setup. 22290

WIZARD

- **Long hostnames are allowed** Previous versions of the Decru setup wizard did not allow long hostnames. The setup wizard shipped with the LKM appliance allows hostnames up to 80 characters long. 27783

NEW FEATURES

DECRU MANAGEMENT CONSOLE

- **Configuration database storage and retrieval** The LKM appliance supports storage and retrieval of Decru appliance configuration databases. Via the Decru Management Console, the LKM appliance can perform operations previously unavailable with LKM server software including:
 - store configuration databases from peer-linked appliances
 - create an exportable list of available configuration databases
 - export a specific configuration database
 - rename (copy) a configuration database so that a newly saved configuration database does not overwrite existing one 21584

- **Key Management in CLI and DMC** The Decru Management Console integrates DataFort appliance and LKM appliance management, offering a single interface to support the following procedures:

- Key Translation between appliances
- Export and import keys to and from LKM appliance
- Key Recovery [21626](#)

- **SecureView functionality** A SecureView license allows multi-selection of appliances (DataFort and LKM) in the Decru Management Console. This makes a number of multi-select procedures possible, including but not limited to:

- ability to upgrade multiple appliances of the same type at once
- ability to back up configuration databases for multiple appliances at once
- ability to log in and out of multiple appliances at once
- ability to zeroize multiple appliances at once
- ability to perform CLI commands on multiple appliances at once

For more about SecureView, see the LKM Appliance Administration Guide. [22145](#)

- **Tech Support Information** The Decru Management Console provides a menu option to save Tech Support Info to a destination directory. Decru support can use this information to troubleshoot issues. [26260](#)

KEY TRANSFER TOOL

- **Tool for LKM upgrade** Decru's Key Transfer Tool provides the ability to upgrade from LKM software 2.5 to the LKM appliance 3.0. See the LKM Appliance Administration Guide for details. [21860](#)

LKM APPLIANCE

- **Platform management for LKM appliance** The LKM Appliance includes platform management (sensors, SNMP, MIBs, IPMI and RAID management). [21648](#)

- **Support for all Decru product lines** The LKM appliance supports currently shipping Decru product lines (E-Series DataFort version 3.1 and FC-Series DataFort version 2.2). [27718](#)

- **Secure tamper-proof hardware platform** The LKM appliance is a secure, tamper-proof hardware platform. [27719](#)

- **Secure software recovery using DDS and smart cards** The LKM appliance supports secure software recovery using Decru's Data Decryption Software (DDS) and Decru-issued smart cards. [27720](#)

WIZARD

- **Wizard integrated into Decru Management Console** The Decru setup wizard is integrated into the Decru Management Console (DMC). This wizard can be used to initialize a standalone DataFort or LKM appliance as well as initialize a DataFort cluster or add a member to an existing cluster. In addition, the wizard can be used to recover a standalone DataFort or LKM appliance or a DataFort cluster. [22133](#)

WORKAROUNDS

DECRU MANAGEMENT CONSOLE

- **Link DataFort to LKM software via DataFort WebUI** The Decru Management Console can only be used to link DataFort appliances to an LKM appliance, not LKM software. In order to link a DataFort appliance to LKM server software, the DataFort WebUI must be used. For instructions on linking DataFort to an LKM appliance, see the LKM Appliance Administration Guide. For instructions on linking DataFort to LKM server software, see the

- **Linked cluster member doesn't appear in DMC immediately** If only one member of a cluster is linked to an LKM appliance using the Decru Management Console (DMC), the other cluster members will automatically be added to DMC as well. However, the other cluster members will not appear in the Resources pane of DMC until the view type is changed (using the DMC View menu), or if DMC is restarted. 26361

- **Searching by keys from filter only searches cluster coordinator** DMC includes a *keys from* filter when searching for Cryptainer keys. When using the *keys from* filter in DMC to search for Cryptainer keys in a cluster, the search will only show the cluster coordinator, which may or may not be the cluster member that was initially added to DMC. 26363

- **Cluster member partially links to LKM appliance** DMC will prompt to connect all cluster members when one member of the cluster is linked to an LKM appliance. If *No* is selected at this prompt, the LKM appliance will still be partially linked to the other cluster member. 26429

- **Unable to link LKM appliance to DataFort cluster member** An administrator must be logged into all members of a DataFort cluster via DMC in order to link any of the cluster members to an LKM appliance. Attempts to link a DataFort cluster member to an LKM appliance if the administrator is not logged in to all cluster members via DMC will result in the error *ERROR: Unable to link 10.x.x.x and 10.x.x.x! ERROR: Unauthorized command: 'lkm'*.

Log in to all appliances before trying to link them. 26455

- **Need to re-link appliances after Recovery Wizard** After the Recovery Wizard is completed on an appliance (LKM or DataFort) that was linked to an LKM appliance, the appliance must be re-linked to the LKM appliance. Log in to the CLI of each appliance that was linked to the LKM appliance and issue the following command:

```
lkm server remove
```

Access the Decru Management Console, and use the menu options to re-link the appliances. 27727

- **Removing a peer link from LKM appliance** To remove a peer link from an LKM appliance, log into the CLI of each peer-linked appliance and enter the following command:

```
lkm server remove
```

27741

KEY TRANSLATION

- **Translated key not saved after translation** At the end of a key translation procedure a Key Translation Results message appears. If the administrator's login times out before OK is clicked on this message, the following error will appear: *Error Saving Key(s). 'x' key(s) could not be saved.* Keys will not have been translated.

If this occurs, the administrator must log back in and redo the key translation, making sure to click OK to the Key Translation Results message before the login times out. 27341

LKM APPLIANCE

- **Key resync required after zeroization of peer** If a peer-linked LKM appliance is zeroized using the CLI command `lkm zeroize` command, the `lkm key resync` command must be executed on its linked peers. Log into the CLI of the LKM appliance linked to the zeroized appliance and execute:

```
lkm key resync 26515
```

- **LCD shows Setup Wizard and software error** If the LKM appliance LCD shows *WARNING: The Setup Wizard has not been completed* and *Software problem found: PRC3 20*, reboot the appliance. 26619

- **Occasional error after zeroization** On occasion, after zeroizing the LKM appliance by issuing the `lkm zeroize` command and then checking the status of the appliance using the `lkm status` command, the following error will appear: *ERROR: Connection refused*

To clear the error, restart the appliance by issuing the `lkm restart` command. 27553

- **Ampersand in Cryptainer name prevents key backup** If a Cryptainer name includes an ampersand, its encryption key will not be backed up to the LKM appliance. In addition, other Cryptainer keys of the same type may not be backed up. To confirm which Cryptainer keys may fall into this category, execute the `cry key list` command on the DataFort appliance and view the result. Any Cryptainer appearing in the list after the one containing the ampersand in its name will not have its key backed up. 27567

SETUP WIZARD

- **Cluster member ID order preserved after recovery** After recovering a DataFort cluster, the member ID ordering for the cluster members will be preserved.

1. Run Setup Wizard for primary DataFort (DF1) and secondary DataFort (DF2). DF1 has member ID 0 and DF2 has member ID 1.
2. Save the configuration databases for both DataFort appliances (DF1 and DF2).
3. If DF1 was the primary appliance, but you use the configuration database from DF2 to recover the cluster, DF1 will be assigned member ID 1 and DF2 will be assigned member ID 0.

To preserve the Member IDs for the cluster members, use the configuration database from the primary DataFort to restore the cluster. 25144

SMART CARDS

- **One-time password option not available** If Secure CLI is turned ON for an appliance, a one-time password must be generated to allow access to the management interface. The one-time password option is not available unless Secure WebUI is turned ON also.

One-time password can be made available by setting the following system properties in the CLI:

```
system property set sys.security.ssh.usesmartcard = 1
system property set sys.security.web.usesmartcard = 1
27170
```

TRUSTEE KEY

- **Exported Trustee key gets overwritten** An exported Trustee key will be overwritten if exported within a minute of a previous export. To avoid this, wait 2 minutes between each Trustee Key Export. 26544