

KM-Series Appliance 3.1 Release Notes

RELEASE DATE: 01/24/2008

CONTENTS

[FIXED NOTES](#)

[WIZARD](#)

[NEW FEATURES](#)

[DMC](#)

[KEY SHARING](#)

[KEY STORAGE](#)

[OPENKEY](#)

[WORKAROUNDS AND LIMITATIONS](#)

[CONFIGDB](#)

[DATA DECRYPTION SOFTWARE](#)

[DECRU MANAGEMENT CONSOLE](#)

[KEY SHARING](#)

[KEY STORAGE](#)

[KEY TRANSLATION](#)

[LKM APPLIANCE](#)

[OPENKEY](#)

[SCSI](#)

[SERIAL CONSOLE](#)

[SETUP WIZARD](#)

[SMART CARDS](#)

[TAPE KEYS](#)

[TRUSTEE KEY](#)

[UPGRADE AND DOWNGRADE](#)

FIXED NOTES

WIZARD

- **64 character hostnames are allowed** Previous versions of the appliance setup wizard incorrectly stated support for 80 character hostnames. The current setup wizard only allows hostnames up to 64 characters long. 28283

NEW FEATURES

DMC

- **New Features in DMC**

The following functionality is now included in DMC:

- Topology pane for E-Series, FC-Series and S-Series DataFort appliances
- Remote Authorization (allows appliance initialization and trustee creation to be established with Recovery Cards at different locations.)
- Custom Groups can now be added to the left hand pane to help sort appliances in DMC
- Appliances can be added to DMC by IP address range
- Remote Association of Admin Cards (allows an administrator to associate an Admin Card to another administrator without having the card present.)
- LKM Link Status pane
- Recovery Card status pane
- Customized Key Find dialog

27549

KEY SHARING

- **Policy Based Key Sharing** Allows non-clustered Decru appliances (DataFort and LKM appliances) and OpenKey clients to share keys through an LKM appliance without manually importing and exporting keys or going through the manual key translation process. The LKM appliance administrator can set up policies to restrict or allow key movement between

individual appliances and OpenKey clients. Note this feature requires links to be established between the client and the LKM appliance. [27516](#)

KEY STORAGE

- **Logging Key Activities** Allows tamper evident logging and auditing of critical key activities such as key sharing, key translation, and writing keys to external storage. [30180](#)
- **Key signatures** Allows detection of unauthorized modification of keys stored in both the KM- Series appliance RAID and external storage. [31623](#)

OPENKEY

- **OpenKey API** Provides key management services to non-DataFort encryption clients through the OpenKey API. [27696](#)

WORKAROUNDS AND LIMITATIONS

CONFIGDB

- **Configuration database backup error reporting** Error reporting of the `db export -l` CLI command is inaccurate. Before zeroizing any DataFort or LKM appliance, double-check that the configuration database has been backed up. Access the directory where the database was saved and ensure the `.xdf` file exists in that location. [33767](#)
- **Configuration database backup interval** The system property `lkm.db.backup.interval` needs to be set twice for the interval to take effect immediately. Alternatively, wait until the current interval elapses. The new interval will automatically take the new value. [34250](#)

DATA DECRYPTION SOFTWARE

- **DDS decryption with encrypted filenames** When using DDS with encrypted filenames, you must specify and decrypt the root Cryptainer which contains the files or folders with encrypted filenames. DDS does not support decryption of encrypted filenames if only the subdirectory is specified. [26521](#)

DECRU MANAGEMENT CONSOLE

- **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](#)
- **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. Access the Decru Management Console, and use the menu options to re-link the appliances. [27727](#)
- **Maintaining KM-Series incremental backups** The "Export Keys..." key backup menu item will fail if the KM-Series appliance has been zeroized between exports. The solution for this is to use a new directory for "Export Keys..." key backups after zeroizing. [28182](#)
- **No pending actions during trustee setup** Setting up a trustee relationship is a sensitive process. Ensure that there are no current or outstanding actions between the two appliances or the trustee creation may fail. Pending trustees should be cleared. Do not reboot either appliance during trustee creation. Do not perform key translation during a trustee setup. [28265](#)
- **Executing DMC on non-English systems** When running DMC or the setup wizard on a non-English system, ensure that all settings in the Control Panels > Regional and Language Options match the target language and location. [29511](#)

- **DMC left hand pane icon status issues** Icons in the left hand pane of DMC may report the incorrect state. If an online appliance appears offline, select View > Refresh in DMC to update its status.

If an appliance appears to have the incorrect status icon in DMC try:

- 1) Deselect and reselect the appliance; or
- 2) Deselect and reselect the appliance and select View > Refresh; or
- 3) Quit and restart DMC. [31255](#)

- **SmartCard reader not responding** The SmartCard reader(s) are shared between DMC, the setup wizard and the DataFort WebUI. Simultaneous instances of the 3 applications can cause contention with the SmartCard reader. To ensure proper operation of the SmartCard reader, close other applications and web browsers which may be trying to access the reader. [31256](#)

- **Unable to uninstall DMC from Add/Remove Program** A failure to reboot after an install or uninstall may result in InstallShield errors when trying to uninstall the software from the Add/Remove Programs dialog. In this case, run the DMC installer from the supplied CD to uninstall the software.

[32291](#)

- **DMC key translation and key format** Keys with multiple formats need to be translated in separate operations. When translating keys using the Key > Translate Key(s) menu option in DMC, multi- select only keys with the same format for each translation operation.

For information about viewing key formats, see the Adjusting Table Columns topic in the KM-Series administration guide. [32529](#)

- **DMC adding appliances in an IP range** When adding appliances in an IP range, only pingable appliances are added. [33234](#)

- **Incorrect Link Down indication** When using the DMC Appliance > View Link Report option on a newly linked DataFort appliance cluster, sometimes a cluster member will report "Link Down" while another member will report "Link Up". Should this occur, deselect all appliances and select View > Refresh from DMC. [33442](#)

- **DMC Key Import/Export** When using the Keys > Export Keys and Keys > Import Keys functions of DMC, it can take up to 1 minute to show a progress bar. If the export or import is interrupted by shutting down DMC, discard any generated files and restart the operation. [33686](#)

- **KM-Series key viewing** When viewing keys with the Keys > View Data Encryption Keys feature in DMC, the resulting view is limited to 1000 keys. The keys shown can be sorted, but only within the 1000 keys, not the entire result set.

To sort the entire KM-Series key set, ensure that the key selection dialog returns a result set of less than 1000 keys. [34126](#)

- **Restoring Cryptainer vaults with DMC 1.1** To restore a NAS iSCSI Cryptainer using DMC 1.1:

1. Right-click the Targets pane and select the Cryptainer Keys option from menu. Select a key that is to be restored.
2. Right-click and select the Restore... option from the menu.
3. Specify the Target Name, LUN and Owner and optional Cryptainer Name and click apply.

A Cryptainer Restore option is scheduled for a future release of DMC. [34338](#)

- **DMC page sorting** When using DMC to view large numbers of keys, DMC will only page in 1000 keys at a time. Selecting "Next" on the key page will bring in the next 1000 keys. Selecting "Next" many times (>100) will sometimes cause an error that requires DMC to be restarted.

To prevent this, use more selective key attributes to find a smaller set of keys to view.

34535

- **Canceling a Key Export** Canceling a Key Export operation will result in DMC reporting the wrong number of keys exported. An import of the same file will give the true number of keys exported. To complete the interrupted export, start Key Export again and allow it to run to completion. 34984

- **DMC appliance selection, view data, SecureView, and menu enabling** DMC uses the combined selection of appliances in the left hand pane, appliance type, appliance login status and SecureView licensing to control what is shown in the right panes and what is enabled in the menu structure.

If a menu item is not available, ensure that the correct appliance is selected in the left hand pane. If more than one appliance is selected, ensure all appliances have SecureView licenses. If selected appliances are of different types, not all menu selections are available.

35116

- **Appliance password length** DMC incorrectly reports the maximum administrator password length to be 30. The correct password length supported on the KM-Series appliance is 32. 35126

- **Recovery card operations in DMC** The following DMC menu options are only visible when no appliances are selected:

Security > Change Recovery Card Password

Security > Smart Card Utilities

35216

- **Group Review for E-Series DataFort appliances** The Group Review feature is missing in DMC 1.1. Please use the DataFort WebUI, CLI or the DMC CLI to access the Group Review feature. Instructions for CLI Group Review management can be found in the most recent E-Series DataFort Administration Guide. 35290

KEY SHARING

- **Generic key import errors** Occasionally when restoring a Cryptainer on a DataFort appliance, you may see *Generic LKM error* or *LKM key not found*. This generic message indicates the key was not found by the DataFort on the requested LKM appliance. In either case, check that the key has been properly imported or translated onto the destination LKM appliance. 30029

- **Key ID format** The stored key id on a DataFort appliance is longer than the stored key ID on an LKM appliance. Thus, when manually restoring a key onto a DataFort appliance using `keyman lkmkeys import -- ck-id`, pre-pend the LKM appliance key id with `01000000`. 32607

- **LKM appliance intrusion behavior** If an intrusion is detected on an LKM appliance, cryptographic operations will halt. This will block Policy Based Key Sharing over Key Sharing Links. However, any Key Archival Links will still be active. This is because cryptographic operations are not necessary on such links at the LKM appliance end. A DataFort appliance linked to an LKM appliance with an intrusion alert will still be able to save keys and configuration databases to that LKM appliance, and the DataFort appliances will continue to be able to restore Cryptainers that it created. It will not be able to restore Cryptainers created by another DataFort however. 34215

- **Full Admin required for Trustee Link** Only a Full Administrator can create a Trustee Link. If a Key Administrator wants to set up Policy Based Key Sharing, a Full Administrator must first set up the Trustee Link before the Key Sharing Policy can be set up. 35100

KEY STORAGE

- **Key purging** The system property `lkm.appliance.key.purge.name` is ignored in LKM 3.1. Its value is always `purge_time`. This means that any key that has a `purge_time` attribute with a positive integer value less than current epoch time will be purged. 32309

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

OPENKEY

- **LKM 3.0 does not support OpenKey** To protect OpenKey keys, a KM-Series appliance running LKM 3.0 is not allowed to sync keys off of a KM-Series appliance running LKM 3.1. Decru recommends all KM-Series appliances be upgraded to LKM 3.1. 31333

SCSI

- **DDS does not support Adaptec 29160 SCSI HBA with block size greater than 63kbytes** When the host writes a xK block through the DataFort appliance, the block becomes (x+1)K on tape with the DataFort appliance's metadata. When DDS is used to read the 'xk block', it needs to read (x+1)K (xK + 1K metadata) in order to decrypt correctly. When x equals 64, DDS will need to read 64 + 1 which requires 17 elements in the HBA's scatter-gather list since Windows has a 4k page size. Adaptec 29160 has a SG setting of 16 which supports up to 64k size. On the Adaptec 29320A-R, the SG limit is set by a registry value with a maximum of 255. 29815

SERIAL CONSOLE

- **Incorrect display on serial console** The LKM serial console may incorrectly state NO CARRIER (even though a valid ethernet cable is attached) or may appear to not allow the subnet mask to be set (value stays at 0.0.0.0). If this occurs, log out and log back into the serial console to resolve the issue. 32979

SETUP WIZARD

- **Recreating links after setup wizard** After running the Cluster Wizard or Recovery Wizard on a DataFort or LKM appliance, it is necessary to re-establish the links between all appliances. Only the SSL link needs to be re-established. Recovery Cards will not be required in order to re-link. 33421

- **RAID drives** When running the Recovery Wizard on a KM-Series appliance, the RAID drives must be inserted into the appliance. Otherwise, customers will see `crypto module error`. 34188

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
```

- **Zeroizing LKM appliances during emergency login** Remove the Recovery Card from the LKM appliance prior to zeroization during emergency serial login. Zeroizing the LKM appliance will also zeroize any card inserted into the appliance. 35292

TAPE KEYS

- **Discrepancies between pool and tape key labels** LKM may not display historical pool and tape labels for all stored keys. Pools or tapes which share the same encryption key will only show labels for the most recent usage of that key. All tapes will still be able to be restored using this key. Queries in DMC for keys by pool or tape label may not yield the desired results. 31568

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

UPGRADE AND DOWNGRADE

- **Downgrade only supported in CLI** Downgrading a KM-Series appliance from LKM 3.1 to LKM 3.0 is not supported from DMC. You must use the CLI. Note that downgrading to LKM 3.0 from 3.1 requires a zeroize. 32704

- **Key downgrade** When downgrading a KM-Series appliance from LKM 3.1 to LKM 3.0, the CLI command `lkm key downgrade` may take up to two hours for every 1000 keys. During this period, the CLI session will be lost. To verify that the key downgrade procedure was successful, check the LKM appliance logs for `lkm.key.downgraded`. 34643