



■ ■ ■ ■ **UPGRADING THE KM-SERIES APPLIANCE FROM 3.0 TO 3.1**

This document describes the procedure to upgrade the Decru Lifetime Key Management™ (LKM) appliance from version 3.0 to version 3.1.

Note: To upgrade from LKM software to the LKM appliance, contact Decru support.

To complete the upgrade, follow these procedures:

- [Upgrading the LKM appliance](#)
- [Upgrading Links](#)

UPGRADING THE LKM APPLIANCE

Update the LKM appliance to version 3.1 using the following procedures.

WARNING: TO UPGRADE WITHOUT ANY LOSS OF SERVICE, EVERY DATAFORT APPLIANCE MUST BE LINKED TO AT LEAST TWO LKM APPLIANCES.

- [Preparing to Upgrade](#)
- [Upgrading to DMC 1.1](#)
- [Exporting Unsigned Keys](#)
- [Applying Upgrade Package](#)
- [Exporting Signed Keys](#)

PREPARING TO UPGRADE

The following are required to upgrade from LKM appliance version 3.0 to 3.1.

- Back up the LKM and DataFort appliance configuration databases to external storage. See the [LKM Appliance Administration Guide](#).
- LKM appliance 3.1 is compatible with DMC 1.1, and DataFort appliance versions E-Series 3.1.1 and FC-Series 2.2.1. The following are required:
 - DMC 1.1 Installer
 - LKM 3.1 upgrade package LKM31_16allSaveEEP_signed.upk. Save this package to a secure location that is accessible to the DMC 1.1 Management Station. To verify that the upgrade package is correct, see the [LKM Appliance Administration Guide](#).

UPGRADING TO DMC 1.1

1. Obtain the DMC 1.1 installer from Decru and launch the installer on the Management Station.
2. In the Select Type screen, select Repair or Update Current Installation and click Next.
3. When the installation is done, click Finish.

This updates DMC and migrates all previously-added appliances. Note that the certificate store will be purged, so users will see a new certificates acceptance window upon login to DMC.

EXPORTING UNSIGNED KEYS

This procedure backs up LKM appliance 3.0 keys.

1. In the DMC, in the appliance tree, select an LKM appliance.
2. From the Keys menu, select Export Keys.
3. On the Select Directory screen, select a folder location and click Select.

A message prompt states the number of keys currently exported from the total number of keys available for export.

Note: Use a separate empty folder for each LKM appliance.

- To pause the export at any time, click the Cancel button.

Note: Resume this procedure anytime by selecting the same appliance and export folder. Any new keys added to the LKM between pausing and resuming the key export are added to the total number of keys available for export in the progress bar.

APPLYING UPGRADE PACKAGE

To prevent upgrades from failing, select the stay logged in option in DMC, otherwise the upgrade session may expire before it is complete. See [Setting Login and Refresh Preferences](#).

1. Save the upgrade package LKM31_16allSaveEEP_signed.upk a location accessible to the Management Station.
2. In the DMC, from the Utilities menu, select Upgrade/Downgrade.
3. Browse to the upgrade package and check to see that the selection to zeroize the appliance is set to No.
4. Click Apply.

Setting Login and Refresh Preferences

1. In the DMC, from the Edit menu, click Preferences.
 - Click the Stay Logged In check box to stay logged in until the DMC session is closed.

Note: As a security measure, the DMC connection to an appliance times out after 30 minutes of inactivity.

- Select the interval to refresh the information on the Appliance tab (up to 20 minutes)
2. Click OK.

EXPORTING SIGNED KEYS

1. In the DMC, in the appliance tree, select an appliance.
2. From the Utilities menu, click Command Line.
3. On the Command Line tab, in the Command field enter the command to sign unsigned keys during export:

```
system property set lkm.appliance.key.sign_unsigned_on_export 1
```

4. Click Execute.
5. From the Keys menu in DMC, select Export Keys to export all keys in the LKM 3.1 signed key export file format.

Note: Use a new empty folder for the export; do not use the same folder as was previously used when exporting unsigned keys.

6. From the CLI, in the Command field enter the command to revert the key sign command to the default for 3.1:

```
system property set lkm.appliance.key.sign_unsigned_on_export 0
```

UPGRADING LINKS

After upgrading all LKM and DataFort appliances, upgrade the links between appliances. See the [DataFort Upgrade Guide](#) for instructions on upgrading DataFort appliances.

Note: In LKM appliance version 3.1, keys are archived on the LKM appliance and shared between LKM clients based on link policies. However, appliances must form a trustee relationship with an LKM appliance before creating a link policy.

Begin by upgrading DataFort to LKM appliance links. When that process is complete, upgrade LKM to LKM links.

For LKM to DataFort appliance links:

- Ensure all DataFort appliances have an LKM and a SecureView license.
- Remove appliance links. See [Removing Appliance Links](#) on page 5.
- If a Key Sharing Policy is desired, see [Creating a Trustee Relationship](#) on page 5.
- Create a link policy by selecting a DataFort cluster member and an LKM appliance. See [Creating a Link Policy](#) on page 5.

Note: DMC will automatically link all members within a cluster to a selected LKM appliance.

- View the link report to ensure key sync progress is 100%. See [Viewing Link Report](#) on page 5.
- Move unshared keys into a key sharing group. See [Moving Unshared Keys into a Key Sharing Group](#) on page 5.

For LKM to LKM appliance links:

- Remove appliance links. See [Removing Appliance Links](#) on page 5.
- Before creating a Key Sharing Policy, create a trustee relationship. See [Creating a Trustee Relationship](#) on page 5.
- Create a link policy by selecting two LKM appliances. See [Creating a Link Policy](#) on page 5.
- View the link report to ensure key sync progress is 100%. See [Viewing Link Report](#) on page 5.

REMOVING APPLIANCE LINKS

To upgrade LKM appliance links, you must first remove and then recreate them. This is because in LKM appliance version 3.1 keys are not merely archived on the LKM appliance, they may also be shared between LKM clients based on a selection of link policies, including Archive and Key Sharing Policies. See the [LKM Appliance Administration Guide](#).

CREATING A TRUSTEE RELATIONSHIP

Appliances must form a trustee relationship with an LKM appliance before creating a link policy for a key sharing group. This allows them to share keys without manually importing and exporting keys or going through the key translation process.

Note: A Recovery Card quorum for each appliance is required for setup. The System Card must be inserted into the DataFort appliance in order to fully authorize this cryptographically sensitive procedure. See the [LKM Appliance Administration Guide](#) for instructions on inserting the System Card.

DataFort appliances that do not reside in key sharing groups may continue to share keys by creating an Archive Policy. This requires manually importing and exporting each key for each trustee. See the [DataFort Administration Guide](#).

See the [LKM Appliance Administration Guide](#) for instructions on creating trustee relationships.

CREATING A LINK POLICY

LKM appliance version 3.1 archives key on the LKM appliance and shared between LKM clients based on link policies, including Archive and Key Sharing Policies. Use a Decru Key Sharing Policy when automatic key translation is desired between DataFort appliances. The Decru Archive Policy is used only to store keys wrapped with the source appliance Parent Keys, and to archive configuration data on the LKM appliance. See the [LKM Appliance Administration Guide](#).

VIEWING LINK REPORT

Once appliances are linked to an LKM appliance they are viewable in the link report. The link report shows appliance links and policies including key sharing group affiliations and key synchronization data. See the [LKM Appliance Administration Guide](#).

MOVING UNSHARED KEYS INTO A KEY SHARING GROUP

Use this option for keys that are purged from a DataFort that is being upgraded from an archive link to a key sharing group link. Otherwise the LKM appliance will not be able to share purged keys. See the [LKM Appliance Administration Guide](#).