

Lifetime Key Management System v2.5

Data Decryption Software v2.5

CONTENTS

NEW FEATURES ADDED SINCE V2.1

BUGS FIXED SINCE V2.1

KNOWN ISSUES AND WORKAROUNDS

UPGRADE INFORMATION

NEW FEATURES ADDED SINCE VERSION 2.1

Separation of LKM and DDS

The LKM and DDS software modules are now individually licensable, enabling customers to purchase and deploy only the features they need for primary, backup, and partner sites.

Support for E Series OS 3.0 and FC Series 2.x

The programs are now completely interoperable with Decru's most recent OS releases, 3.0 for E Series (NAS & iSCSI) and 2.x for FC Series (SAN disk and tape). The software remains interoperable with all previous versions of Decru operating systems and is an effective means of managing keys across heterogeneous environments.

BUGS FIXED SINCE VERSION 2.1

Microsoft SQL Server

In a previous release, the LKM service would not start when using Microsoft SQL Server as the LKM database. That problem has been fixed.

LKM Backups Time Out

Fixed a memory problem that caused backups from the DataFort appliances to the Lifetime Key Management server to timeout.

Cloned Configuration Databases

Fixed a bug where cloned DataFort appliances would overwrite other clones configuration databases causing DataFort recovery wizard to restore the incorrect DataFort.

KNOWN ISSUES AND WORKAROUNDS IN VERSION 2.5

WebUI and Lifetime Key Management

It is recommended that the Decru Lifetime Key Management software not be installed on the same workstation that is used as the Management Stations so that the applications do not both contend for the smart card reader.

Protecting LKM from DoS Attack

For maximum security against denial-of-service attacks against the LKM, Decru recommends putting a firewall in front of the LKM server which is configured to only allow connections from IPs that are valid DataFort Appliances.

MySQL Root Password

By default, MySQL is installed with no root password. It is good practice to set that password to a long, hard-to-guess, string. This can be done by running:

```
mysqladmin -u root password 'newpassword'
```

LKM does not access MySQL as root. LKM accesses the database using the username/password set up during LKM installation.

Deleting Keys in Cloned DataFort Appliances

In a cloned DataFort appliance environment, deleting a key on one of the clones in the LKM GUI will delete that same key on every clone. As best practice, delete keys within a clone only when that key is not needed across the clone set. 20270

DDS and iSCSI Cryptainers

It is possible that after restore using DDS, the data may not appear properly on the target LUN. If this happens, do the following:

- Run 'chkdsk /x' on the target LUN drive
- Refresh from the Windows GUI

Data Decryption Software and NAS Encrypted Filenames

For Data Decryption Software to work properly with DataFort encrypted NAS files with Encrypt Filenames ON, the directory containing the .decru file must be selected in the DDS UI.

Partially Rekeyed NAS Cryptainers

Decru Data Decryption Software does support decryption of partially encrypted NAS cryptainers. This limitation only applies to NAS cryptainers that were partially encrypted during initial encryption of a cleartext share/directory, not to those partially encrypted in re-keying operation .

Two-Byte CIFS Cryptainer Names

Decru Data Decryption Software does not support two-byte CIFS Cryptainer names (e.g. Cryptainer using Japanese or Chinese characters).

Symbolic Links

Decru Data Decryption Software does not resolve symbolic links properly. After decryption, the links will point to nonexistent files. You must correct the links after decrypting the Cryptainer.

UPGRADE INFORMATION

LKM v2.5 has been designed to allow seamless upgrade from previous software versions. Broadly, upgrading requires key export, software upgrade following a simple wizard-based process, and a guided import of the key file.