

Dell Encryption Key Manager and Library Managed Encryption

Best Practices and FAQ



Notes and Cautions



NOTE: A NOTE indicates important information that helps you make better use of your computer.



CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

Information in this publication is subject to change without notice.

© 2009–2011 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the DELL logo, and PowerEdge™ are trademarks of Dell Inc. Microsoft®, Windows®, and Windows Server® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. Red Hat® and Red Hat Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® is a registered trademark and SUSE™ is a trademark of Novell Inc. in the United States and other countries.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

Contents

1	Dell Encryption Key Manager and Library Managed Encryption	7
	Best Practices	7
	FAQ	9
	Is Encryption Key Manager (EKM) supported on Microsoft Windows Server 2008 and Windows Server 2008 R2?	9
	Is EKM supported on SUSE Linux Enterprise Server 11?	9
	Is EKM supported on a virtual machine?	9
	How do I upgrade my current EKM to version 2.1?	10
	Can an EKM server running EKM 2.0 and an EKM server running EKM 2.1 be synchronized?	11
	How do I create a redundant EKM based on a primary EKM server?	11
	How do I synchronize the redundant EKM anytime configuration changes (like adding keys, adding key groups, adding drives, and so on) are made to the primary EKM?	12
	How do I locate the TCP port for the EKM server to configure my library?	12
	How do I ensure that EKM restarts automatically if my server reboots?	12
	How do I configure EKM to run as a Windows service in a 32-bit environment?	13
	How do I configure EKM to run as a Windows service in a 64-bit environment?	16

EKM appears to start as a Windows service but shows as stopped when I check or refresh the services	16
How do I uninstall EKM as a Windows service?	17
How do I change my login password?	17
EKM Server is configured to start as a Windows service but it stops after initially starting	18
When I attempt to log into the EKM Server GUI, the GUI returns an error message pop-up reading EKM Server Login Failed: null.	18
How do I configure the EKM CLI client for authentication based on the LocalOS registry?	19
How do I uninstall EKM?	20
How do I reinstall the EKM?	20
I am having issues with a new EKM installation and need to reinstall. How can I determine if the EKM ever provided keys?	21
How do I reuse previously encrypted media as non-encrypted media or as encrypted media with a different encryption key?	21
How do I recover from a forgotten EKM GUI login password?	22
My redundant EKM server does not start and the login fails	23
The <i>Dell Encryption Key Manager User's Guide</i> does not contain details on how the user can edit the EKM configuration files for the server and client	23
My PowerVault TL2000/TL4000 posts an LME Failure when I change the configuration from Library-Managed Encryption to Application-Managed Encryption	24

My PowerVault TL2000/TL4000 is configured for library-managed encryption and my RMU shows an error condition with no associated text.	24
When I attempt to add a drive manually using adddrive in the CLI, it asks for a 12-digit drive serial number. The drive serial number is only 10 digits	24
How is my backup application affected when I configure the library for library-managed encryption?.	24
How does EKM handle the addition of new drives or the replacement of bad drive?	25
How does EKM handle the addition of a new library or the replacement of a bad library?.	25
How is compression affected by encryption and vice versa?.	25
Is there a performance impact with encryption?	25



NOTE: Read the following information before using your Dell PowerVault TL2000, TL4000, or ML6000 tape libraries.

Dell Encryption Key Manager and Library Managed Encryption

This document covers the Dell Encryption Key Manager and Library Managed Encryption used on the Dell PowerVault TL2000, TL4000, and ML6000 tape libraries.

Best Practices

It is not possible to overstate the importance of backing up the key store once it is populated with keys and every time keys are added to the key store. If the keys are lost, the data encrypted with the keys is lost forever.

The key store should be backed up to non-encrypted media. The keys are encrypted within the key store so there is no security concern with this process. The key store should not be backed up to media encrypted with the keys in the key store as the backup is no longer available if the key store is deleted or corrupted. The Dell Encryption Key Manager (EKM) GUI allows for the key store to be backed up every time a configuration change is made.

To prevent possible data loss due to an EKM server failure, it is recommended to use a primary and redundant (secondary) EKM server. This configuration provides redundancy in the event the primary EKM server is down or unavailable. For information on configuring a primary and redundant (secondary) EKM server for your library, follow the steps under "How do I create a redundant EKM based on a primary EKM server?" on page 11. If two independent EKMs are installed and configured through the defaults, the key stores cannot be merged later due to identical key aliases.

It is recommended that the primary and redundant EKM servers be synchronized every time changes are made to the primary EKM. In addition, since the two methods of synchronization in the *Dell Encryption Key Manager User's Guide* do not act on the keystore or key groups XML file, both of which are essential to reading encrypted data from the media, they should be copied to the redundant EKM server any time new media is allocated by EKM. For more information, see "How do I synchronize the redundant EKM anytime configuration changes (like adding keys, adding key groups, adding drives, and so on) are made to the primary EKM?" on page 12.

It is recommended that you set the EKM server with a static IP address to avoid changes in the IP address. With the EKM server IP address set to **Dynamic** using a DHCP server, there is the possibility of the E KM server IP address being changed by the DHCP server. When the IP address changes, the library has no way to access the EKM server. All subsequent encrypted backup jobs fail if there is no available EKM server to provide the required keys.

If the library firmware supports key path diagnostics, the diagnostics should be run to validate the EKM connectivity prior to starting normally scheduled backups. This ensures that scheduled backup jobs complete successfully.

If the library firmware does not support key path diagnostics, the firmware can be updated to the most recent version so that key path diagnostics can be used. Test backups can also be used to validate the EKM connectivity.

When using new media, the user must ensure that the tape backup software application recognizes the media as available for backup and is in a valid state prior to encrypting data on the media. This ensures that scheduled backup jobs complete successfully.

To avoid data loss, key path diagnostics should be run on the library to validate that the EKM server or servers are still running. EKM can be configured as a Microsoft Windows service so that it automatically restarts if the system is rebooted. To configure EKM as a Windows service, see "How do I configure EKM to run as a Windows service in a 32-bit environment?" on page 13.

Media portability rules with library-managed encryption are consistent with media portability rules between different types of backup software. Currently media encrypted through library-managed encryption cannot be restored through a standalone drive due to lack of support for standalone drives in EKM. Media encrypted in one Dell PowerVault tape library can be restored through another PowerVault tape library as long as the key store associated with the original library can be accessed by the second library.

To minimize latency in providing keys to the drive, the EKM should be on a localized network. The EKM can be located on a different network or offsite from the library but the network bandwidth should be taken into account.

It is recommended that the audit log file folder be cleaned out periodically. Each audit file log is 1 MB and a new file with a new time stamp is created every time the current file reaches 1 MB. These files are located under `C:\ekm\gui\audit`.

FAQ

Is Encryption Key Manager (EKM) supported on Microsoft Windows Server 2008 and Windows Server 2008 R2?

Support for Windows Server 2008 and Windows Server 2008 R2 was added in EKM version 2.1 available at support.dell.com.

Is EKM supported on SUSE Linux Enterprise Server 11?

Support for SUSE Linux Enterprise Server 11 was added in EKM version 2.1 available at support.dell.com.

Is EKM supported on a virtual machine?

Support for Microsoft Windows Hyper-V and VMWare 4.0 was added in EKM version 2.1 available at support.dell.com. EKM must run on a supported guest operating system.

How do I upgrade my current EKM to version 2.1?

There is no upgrade process for EKM. In order to update to EKM version 2.1, migrate the EKM application. Choose the appropriate option below depending on your operating system environment.

- If the existing EKM is running on Microsoft Windows Server 2003, Red Hat Enterprise Linux 4, Red Hat Enterprise Linux 5, SUSE Linux Enterprise Server 9, SUSE Linux Enterprise Server 10—No upgrade is required. EKM version 2.1 does not add any new features to your current installation. Only new operating system support was added.
- If you are upgrading an existing EKM on a new supported operating system using a new server:
 - a** Select the new server and ensure that the new operating system is supported in EKM 2.1.
 - b** Follow the procedure in "How do I create a redundant EKM based on a primary EKM server?" on page 11. However, you do not have to install the primary EKM as mentioned in step 1 as the installation is already completed on the existing server. Make note of the items listed in that step 1. Perform step 7 to step 10 only if you are using a primary and redundant EKM configuration.
 - c** After the EKM is successfully migrated, the original EKM server can be uninstalled. It is recommended that you use key path diagnostics or a test backup to verify the functionality of the new EKM prior to uninstalling the existing EKM.
- If you are upgrading existing EKM on a new supported operating system using the existing server:
 - a** Ensure the new operating system is supported on EKM 2.1.
 - b** Collect the backup files from the existing EKM located in the default directory at `c:\ekm\backup`.
 - c** Record the following settings in the existing EKM: group name, number of keys, key store name, and key store password.
 - d** Install the new operating system and drivers on the existing server.
 - e** Install EKM 2.1. Use the GUI to configure the EKM. The EKM 2.1 settings must be the same as the original EKM - the following items must match: group name, number of keys, key store name, and key store password.

- f Replace the EKM 2.1 files at `C:\ekm\gui` with the files from the original EKM that you backed up in step c.
- g Restart the EKM 2.1 and record the IP address.
- h If required, update the EKM IP address in the library configuration. If this is a primary or redundant EKM configuration, perform step 6 to step 10 in "How do I create a redundant EKM based on a primary EKM server?" on page 11 to complete the configuration.

Can an EKM server running EKM 2.0 and an EKM server running EKM 2.1 be synchronized?

Yes. Ensure that you perform the procedure in "How do I synchronize the redundant EKM anytime configuration changes (like adding keys, adding key groups, adding drives, and so on) are made to the primary EKM?" on page 12.

How do I create a redundant EKM based on a primary EKM server?

- 1 Install the primary EKM server through the install CD. Use the GUI to configure the EKM and make note of the group name, number of keys, key store name, and key store password.
- 2 Install the EKM application for the redundant EKM through the install CD on a different platform. Use the GUI to configure the EKM. The redundant EKM settings must be the same as the original EKM. The following items must match: group name, number of keys, key store name, and key store password.
- 3 Stop the redundant EKM (second EKM installed).
- 4 Collect the backup files from the primary EKM located at `C:\ekm\backup` (default directory).
- 5 Replace the redundant EKM files at `C:\ekm\gui` with the files from the primary EKM (files from step 4).
- 6 Restart the redundant EKM and note the IP address of the redundant EKM.
- 7 Launch the command line interface in the redundant EKM (`C:\ekm\client\startclient.bat`).

- 8 Log in into the EKM by typing (login ekmsuser: EKMAAdmin ekmpassword: changeMe) in the prompt.
- 9 Locate the SSL port in the redundant EKM by typing status.
- 10 Type the command: `sync -all -ipaddr <redundant EKM IP address>:<redundant SSL port> -rewrite.`

How do I synchronize the redundant EKM anytime configuration changes (like adding keys, adding key groups, adding drives, and so on) are made to the primary EKM?

- 1 Stop the redundant EKM.
- 2 Collect the backup files from the primary EKM located at C:\ekm\backup (default directory).
- 3 Replace the redundant EKM files at C:\ekm\gui with the files from the primary EKM (files from step 2).
- 4 Restart the redundant EKM and note the IP address of the redundant EKM.
- 5 Launch the command line interface in the redundant EKM (C:\ekm\client\startclient.bat).
- 6 Log in into the EKM by typing (login ekmsuser: EKMAAdmin ekmpassword: changeMe) in the prompt.
- 7 Locate the SSL port in the redundant EKM by typing status.
- 8 Type the command: `sync -all -ipaddr <redundant EKM IP address>:<redundant SSL port> -rewrite.`

How do I locate the TCP port for the EKM server to configure my library?

The library-managed encryption setup is not clear as to what port is to be used in the configuration. The library-managed encryption configuration requires an IP address on the TCP port to access the EKM server. This information can be located on the **Health Monitor** page of the EKM GUI.

How do I ensure that EKM restarts automatically if my server reboots?

EKM should be configured to run as a Windows or Linux-based service to ensure that it restarts automatically if the server reboots.

How do I configure EKM to run as a Windows service in a 32-bit environment?


In a primary and redundant EKM configuration, this needs to be configured for each platform.

- 1 Download the Dell - Application Version Dell EKM Services release for the TL2000/TL4000 or the Dell - Patch/Upgrade for the ML6000 from the Dell Support website at support.dell.com.
- 2 Extract the **LaunchEKMService.exe** file from the release into a temporary directory.


For the service to run properly, some environment variables must be set.

- 3 Create a system variable called **JAVA_HOME**. To do so:
 - a Click **Start**→**Settings**→**Control Panel**.
 - b Double click **System**.
 - c Click the **Advanced** tab, and then click **Environment Variables**.
 - d Under the list of System Variables, click **New**.
 - e Specify **JAVA_HOME** as the variable name and enter the IBM JVM directory.
The default installation is **C:\PROGRA~1\IBM\Java50**.
 - f Click **OK**.

- 4 Edit the system **PATH** variable using this procedure.

 **NOTE:** Setting the **PATH** variable from the command line does not work.

- a Click **Start**→**Settings**→**Control Panel**.
- b Double click **System**.
- c Click the **Advanced** tab, and then click **Environment Variables**.
- d From the list of System Variables, scroll to **Path** variable and click **Edit**.
- e Add the IBM JVM path to the beginning of the **Path** variable.
The default install is **C:\PROGRA~1\IBM\Java50\jre\bin**.

 **NOTE:** Insert a semi colon at the end of the path to differentiate it from other directories in the path list.

- f Click **OK**.

- 5 Verify that you have set the **ClassPath** and **JavaPath** variables correctly. The variables should contain the following paths if they are correct. Pay close attention to the location of the semicolons. Semicolons should only be used between paths.

Class Path

C:\Progra~1\IBM\Java50\lib/ext\IBMKeyManagementServer.jar;C:\Progra~1\IBM\Java50\lib/ext\ibmjssprovider2.jar;C:\Progra~1\IBM\Java50\lib\ibmpkcs.jar;C:\Progra~1\IBM\Java50\lib\ibmpkcs1impl.jar;

JavaPath

C:\Progra~1\IBM\Java50\

- 6 Ensure the paths in your EKM Server Configuration properties file are fully qualified. This file is named `KeyManagerConfig.properties` and is located in the `C:\ekm\gui` directory. All of the following paths inside the file should be checked and updated to make sure they are fully qualified paths (For example, use `C:\ekm\gui\EKMKeys.jck` not `gui\EKMKeys.jck`). See the examples below on what to change the paths to when using a default installation.

Table 1-1 lists the options in the file and the complete path it should point to if using the default installation and key store names.


 **NOTE:** Each of the entries can be found in the `KeyManagerConfig.properties` file.

Table 1-1. Table of the file options and the complete path they must point to, if using the default installation and key store names

Options	Complete Path
config.keygroup.xml.file	FILE:C:/ekm/gui/keygroups/KeyGroups.xml
Admin.ssl.keystore.name	C:/ekm/gui/EKMKeys.jck
TransportListener.ssl.truststore.name	C:/ekm/gui/EKMKeys.jck
Audit.metadata.file.name	C:/ekm/gui/metadata/ekm_metadata.xml
Audit.handler.file.directory	C:/ekm/gui/audit
config.keystore.file	C:/ekm/gui/EKMKeys.jck
TransportListener.ssl.keystore.name	C:/ekm/gui/EKMKeys.jck

Table 1-1. Table of the file options and the complete path they must point to, if using the default installation and key store names (*continued*)

Options	Complete Path
config.drivetable.file.url	FILE:C:/ekm/gui/drivetable/ekm_drivetable.dt
Admin.ssl.truststore.name	C:/ekm/gui/EKMKeys.jck

- 7 The **LaunchEKMServices.exe** file must be run from a command prompt. Navigate to **Start**→**Programs**→**Accessories**→**Command Prompt**.
- 8 From the command prompt, navigate to the temporary directory where the **LaunchEKMService.exe** was extracted.

Run the **LaunchEKMService.exe** file using the following options below as a reference.

```
LaunchEKMService {-help | -i config_file | -u}
```

- **help** – Displays the usage information.
- **i** – Installs the Encryption Key Manager as a Windows service. This option requires full path name of the configuration properties file to be passed in as an argument. The default path and filename are C:\ekm\gui\KeyManagerConfig.properties.
- **u** – Uninstalls the key manager Windows Service if you no longer need to run it as a service. Note that the EKMServer service must be stopped before it is uninstalled. When running this command, you may also see the following error message: `Could not remove EKMServer. Error 0`. However, the service may still be uninstalled.

To install Encryption Key Manager as a Windows service, issue:

```
LaunchEKMService.exe -i config_file
```

- 9 Once the service is installed, **EKMServer** shows up in the **Service Control Panel**.




NOTE: You must start the **EKM Windows Service** manually the first time it is used by using the control panel.


- 10 Once the **Dell Encryption Key Manager** is installed as a Windows service with the above command, it can be started and stopped from the **Service Control Panel**.

How do I configure EKM to run as a Windows service in a 64-bit environment?

In a primary and redundant EKM configuration, this needs to be configured for each platform.


 **NOTE:** There is a known issue with the `LaunchEKMService.exe` file which causes it to fail to start in a Windows 64-bit environment. The current **LaunchEKMService** is a 32-bit application and is not be able to execute a call to a 64-bit application.

- 1 Locate the `StartServer.bat` file in your EKM directory.

 **NOTE:** The default directory is `C:\ekm\ekmservice`.

- 2 Right click the `StartServer.bat` file, select **send to**, and then select **desktop (create short cut)**.
- 3 Navigate to **Start**→ **Programs**→ **Startup**.
Right click **Startup** and select **Open**.
- 4 Copy the shortcut created in the desktop into the startup folder.
- 5 To test, stop the EKM server by selecting **Stop Server** in the EKM GUI. Then navigate to **Start**→ **Programs**→ **Startup** and click **Shortcut** to start the Server.

Verify your EKM server is once again running.

 **NOTE:** In a 64-bit Windows environment, the user account where the shortcut was created must remain logged in for the EKM service to remain running. If the user account logs out, backup jobs requiring encryption keys fail due to the lack of an EKM server to service the key requests. This issue does not occur in a 32-bit Windows environment.

EKM appears to start as a Windows service but shows as stopped when I check or refresh the services

Most likely there is an issue with the path variables due to an incorrect/invalid entry. Verify that you have set the `ClassPath` and `JavaPath` variables correctly in the registry. The variables should contain the following paths if they are correct. Pay close attention to the location of the semicolons. Semicolons should only be used between paths.

- 1 Click **Start**→ **Settings**→ **Control Panel**.
- 2 Double click **System**.

- 3 Click the **Advanced** tab, and then **Environment Variables**.
- 4 Scroll down the list of System Variables to the **ClassPath** and **JavaPath** variables.

ClassPath

C:\Progra~1\IBM\Java50\lib/ext\IBMKeyManagementServer.jar;C:\Progra~1\IBM\Java50\lib/ext\ibmjssprovider2.jar;C:\Progra~1\IBM\Java50\lib\ibmpkcs.jar;C:\Progra~1\IBM\Java50\lib\ibmpkcs1impl.jar;


JavaPath

C:\Progra~1\IBM\Java50\

How do I uninstall EKM as a Windows service?

- 1 Stop the EKM server through the GUI and exit the EKM application or kill the **java.exe** process in **Windows Task Manager**.
- 2 At a command prompt, type `LaunchEKMService.exe -u`.
-u – Uninstalls EKM windows service if you no longer need to run EKM as a service.

How do I change my login password?

- 1 In the **EKM GUI** window, stop the EKM server and log out of the GUI.
- 2 Open a command prompt window.
- 3 Navigate to the EKM directory through `C:\cd ekm`.
 **NOTE:** `C:\ekm` is the default directory.
- 4 Navigate to the **EKMServer** directory through `C:\cd ekmserver`.
- 5 Start the EKM server by typing `startServer`.
- 6 Navigate to the **ekmclient** folder through `C:\cd` then `C:\cd ekmclient`.
- 7 Start EKM client by typing `startClient`.

- 8 Login to the EKM client by typing `login ekmsuser : EKMAAdmin`
`ekmpassword: changeMe`.
- 9 Change the password by typing `chgpasswd -new changeME2`
where *changeME2* is the desired new password.
Once logged in, the user can use the command line interface to complete operations not supported in the GUI.
- 10 Type `exit` to logout. This returns the user to the command prompt.

EKM Server is configured to start as a Windows service but it stops after initially starting

OR

When I attempt to log into the EKM Server GUI, the GUI returns an error message pop-up reading EKM Server Login Failed: null

This issue can occur if the `EKMkey.jck` file is empty or not fully populated. The `EKMkey.jck` file is created during the initial configuration of the EKM Server and resides in the `C:\ekm\gui` subdirectory. This file is the key store file. A possible reason for the file to become empty is if the installation or configuration process is interrupted.

If a backup exists of the `EKMkey.jck`, restore the file. The default backup file directory on a Windows server is `C:\ekm\gui\BackupFiles`.

Backed up files are prefixed with a date and time stamp, example:
`2008_11_26_10_59_41_EKMKeys.jck`.

Rename the file to `EKMKeys.jck` and copy it back to `C:\ekm\gui` directory.

Alternatively, uninstall and re-install the EKM service (if installed) and EKM Server. For more information, see "How do I uninstall EKM as a Windows service?" on page 17.

How do I configure the EKM CLI client for authentication based on the LocalOS registry?

In a primary and redundant EKM configuration, this needs to be configured for each platform.

By default, the EKM CLI client is authenticated to the EKM Server as user EKMAAdmin and a default password located in the EKM documentation.

The EKM CLI clients can also be authenticated based on LocalOS registry.



NOTE: The EKM server must be off and the EKM GUI must be closed when making these changes to the EKM configuration file

To turn this feature on in Windows:

- 1 Locate the **KeyManagerConfig.properties** file. (C:\ekm\gui is the default directory).
- 2 Open the file with the text editor of your choice.



NOTE: The recommended text editor is WordPad.

- 3 Locate the **Server.authMechanism** string. If this string is not present, add it to the file in this exact format **Server.authMechanism=LocalOS**.
- 4 Save the file.

Now your user name and password for the EKM server matches the OS user account. Note that only users allowed to login and submit commands to the server and have administrator privileges can manage the EKM server.

To turn this feature on in a Linux-based system:

- 1 Download Dell - Patch/Upgrade for the ML6000 or the Dell - Application Version Dell EKM Services release for the TL2000/TL4000 from the Dell Support website at support.dell.com.
- 2 Locate the LocalOS directory in the download.

- 3** Copy the appropriate libjaasauth.so for your platform to the `jre/bin` directory.
 - On 32-bit Intel Linux environments, copy the `LocalOS-setup/linux_ia32/libjaasauth.so` file to the `<JAVA_HOME>/jre/bin/` directory where `JAVA_HOME` is typically `<java_install_path>/IBMJava2-i386-142` for a 32-bit Intel Linux kernel running the 1.4.2 JVM.
 - On 64-bit AMD64 Linux environments, copy the `LocalOS-setup/linux-x86_64/libjaasauth.so` file to the `<JAVA_HOME>/jre/bin/` directory where `JAVA_HOME` is typically `<java_install_path>/IBMJava2-amd64-142` for a 64-bit AMD Linux kernel running the 1.4.2 JVM.

After the installation is complete, you can start the EKM server.

The EKM client can now login with the OS-based user name and password. Note that only userids allowed to login and submit commands to the server is the userid under which the server is running and which also has superuser/root authority.

How do I uninstall EKM?

First, use the instructions under "How do I uninstall EKM as a Windows service?" on page 17 to uninstall EKM as a Windows service if configured.

- 1** Open **Windows Task Manager** and locate the `javaw.exe` process.
- 2** End the `javaw.exe` process if found.
- 3** Uninstall the IBM Java application.
- 4** Delete the full `ekm` directory (`C:\ekm`).

How do I reinstall the EKM?

Put the EKM CD in the drive and run through the installer again. The EKM Quick Start Guide can be used as a reference.

I am having issues with a new EKM installation and need to reinstall. How can I determine if the EKM ever provided keys?

- 1** Open a command prompt and navigate to the audit log file directory (cd C:\ekm\gui\audit).
- 2** Copy the current audit log file to a temporary file so it can be opened. The current audit log file is active and cannot be opened while being updated.
- 3** Open the temporary copy in WordPad. Search for Drive Serial Number. If there is an entry, a key has been provided. If the volser is blank, this is the result of key path diagnostics and the file should be searched for additional entries associated with the drive serial number to be certain.
- 4** If keys have been provided, the data on the affected media should be restored in clear text if possible prior to the EKM uninstall and re-installation.

How do I reuse previously encrypted media as non-encrypted media or as encrypted media with a different encryption key?

Reusing previously encrypted media requires the use of a working EKM configuration containing the keys for the tapes to be reused and a PowerVault TL2000 or TL4000. Tapes cannot be overwritten in this manner in the PowerVault ML6000. Tapes can be migrated from an ML6000 to a TL2000 or TL4000 for this purpose. The TL2000 or TL4000 then needs to be pointed to the appropriate EKM.

- 1** Ensure that the EKM server is running, and configured properly.
- 2** Login to the RMU GUI for the TL2000/TL4000 (admin/service login required).
- 3** Navigate to **Configure Library**.
- 4** Navigate to **Encryption**.
- 5** Change the Encryption Policy settings to **Internal Label - Selective Encryption**.
- 6** Submit a write job (For example, quick erase, long erase, backup) to the media to be reused.

To verify that the encryption has been overwritten:

- 1 Login to the RMU GUI for the TL2000/4000.
- 2 Navigate to **Monitor Library**, and then to **Inventory**.
- 3 Click the drop down menu for the appropriate magazine.
- 4 Verify that the Comment section shows **Not Encrypted**.

Only after all desired media is un-encrypted can EKM be removed or uninstalled. It is recommended that a backup critical files be performed in the EKM GUI and the files backed up to an external source like a USB key. This allows EKM to be restored if additional tapes must be un-encrypted. To restore the EKM, follow step 4 to step 9 of "How do I create a redundant EKM based on a primary EKM server?" on page 11.

How do I recover from a forgotten EKM GUI login password?

- 1 Go to the **Windows Task Manager** and locate the **javaw.exe**.
- 2 End the **javaw.exe** process.
- 3 Uninstall the IBM Java application.
- 4 Navigate to the **C:\EKM\gui\backup** files (this is the default directory).
- 5 Make a copy of the last backup file set (this step can be skipped if you do not want to preserve the keys).
- 6 Delete the full **ekm** directory (**C:\ekm** is the default directory).
- 7 Reinstall the application and use the redundant EKM installation instructions if the user needs to preserve the previously created keys.
- 8 If applicable, restore the backed up files as follows:
 - a Stop the EKM service or stop the server through the EKM Server GUI.
 - b Copy the backup files to their respective file directory without the date and time stamp prefix. Table 1-2 details the respective file names and directory paths for restoration:

Table 1-2. Table of file names and directory paths

File name	Directory Path
Key Store	C:\ekm\gui\EKMKeys.jck
Audit	C:\ekm\gui\audit\kms_audit.log
Meta Data	C:\ekm\gui\metadata\ekm_metadata.xml
Drive Table File	C:\ekm\gui\drivetable\ekm_drivetable.dt
Key Groups	C:\ekm\gui\keygroups\Keygroups.xml



NOTE: The `kms_audit.log` file is not a vital file for EKM Server restoration.

My redundant EKM server does not start and the login fails

Most likely the primary EKM files were improperly copied to the redundant EKM directory.

To correct this issue, see "How do I uninstall EKM?" on page 20 and "How do I create a redundant EKM based on a primary EKM server?" on page 11.

The *Dell Encryption Key Manager User's Guide* does not contain details on how the user can edit the EKM configuration files for the server and client

The *Dell Encryption Key Manager User's Guide* tells the user that the `KeyManagerConfig.Properties` file and the `KeyManagerConfig_Client.properties` file must be modified on some occasions. To edit the files:

- 1 Stop the EKM server.
- 2 Open the properties file that needs to be updated using the text editor of your choice.
- 3 Make the necessary updates. Make sure to follow the instructions in the *Dell Encryption Key Manager User's Guide*.
- 4 Save the document.
- 5 Restart the EKM server.

My PowerVault TL2000/TL4000 posts an LME Failure when I change the configuration from Library-Managed Encryption to Application-Managed Encryption

This is a false failure. The IP address field is cleared when the configuration is changed. This field is required for library-managed encryption and the failure is generated when it is cleared. This field is not required for application-managed encryption.

My PowerVault TL2000/TL4000 is configured for library-managed encryption and my RMU shows an error condition with no associated text

Most likely an LME failure has occurred. The failure message is not posted on the RMU. It can be viewed through the RMU by navigating to the warning log in the unit. To clear the error, it must be acknowledged in the OCP.

This issue was fixed in the 7.40 version of the library firmware (version A07 on support.dell.com).

When I attempt to add a drive manually using adddrive in the CLI, it asks for a 12-digit drive serial number. The drive serial number is only 10 digits

Two leading zeroes must be added to the 10 digit drive serial number to make up the 12 digit serial number entered when using adddrive.

Example: Drive serial number is 1234567891. Use 001234567891 for drive serial number in adddrive.

How is my backup application affected when I configure the library for library-managed encryption?

Setting changes are made in the drive after library-managed encryption is enabled on the library. The backup application services must be stopped and restarted after library-managed encryption is enabled to ensure the backup application recognizes the encryption setting in the drive.

The tape backup application does not show encryption as enabled if library-managed encryption is used. The tape backup application only shows encryption as enabled if the application is providing the keys to the drive (application-managed encryption).

How does EKM handle the addition of new drives or the replacement of bad drive?

New or replacement drives can be added to the EKM through auto discovery or manually. To auto discover the drives, check the auto discovery checkbox on the EKM Server Configuration tab in the EKM GUI. To add the drives manually, follow the instructions in the Encryption Key Manager User's Guide to add the drives through the command line interface.

It is recommended to use auto discovery as the 12-digit drive serial number (10 digit serial number plus two leading zeros) must be entered to add the drive manually. If security is a concern, auto discovery can be turned on and test backups run to add the necessary drives to the drive table. Then auto discovery can be turned off to prevent new drives from obtaining keys.

As long as EKM can authenticate the drive digital signature assigned to the drive at the factory, EKM accepts the key request. The keys are grouped in the key store in key groups and the key groups can be associated with the new/replacement drives after the drives are added.

How does EKM handle the addition of a new library or the replacement of a bad library?

In library-managed encryption, the library is only a proxy. Libraries can be added or replaced and keys provided as long as the EKM can authenticate to the digital signature on the drive.

How is compression affected by encryption and vice versa?

The data is compressed prior to being encrypted as encrypted data is generally uncompressible. Therefore compression has no effect on encryption and vice versa.

Is there a performance impact with encryption?

There can be a slight performance impact with encryption but it should not cause an increase in the backup window.

EC number: M10948A

IBM Part number: 46X4059

(1P) P/N:46X4059

