Dell Encryption Key Manager 3.0
Deployment Guide

Notes, Cautions, and Warnings

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.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2011 – 12

Rev. A00

Contents

1

Overview

Dell Encryption Key Manager (EKM) 3.0 is an encryption utility that secures the data stored on LTO tape cartridges by managing encryption keys for Dell tape automation solutions, including the ML and TL PowerVault series. EKM 3.0 manages the lifecycle of tape encryption keys, including generation, distribution, administration, and deletion.

This guide describes how to install, configure, and perform basic operations in Dell Encryption Key Manager 3.0 (EKM 3.0). Dell recommends reading this document before you install EKM 3.0.

This guide includes information on:

- Hardware and software requirements for EKM 3.0
- Installing and uninstalling EKM 3.0 on Windows and Linux platforms
- Configuring EKM 3.0
- Basic operations in EKM 3.0
- Migrating EKM 2.X during the EKM 3.0 installation and merging EKM 2.X into a configured EKM 3.0 installation
- Frequently asked questions, troubleshooting information, common errors messages, and support contact information

NOTE: EKM 3.0 is based on IBM Tivoli Key Lifecycle Manager (TKLM) V2 FixPack 2, but has been customized to support Dell tape library environments by selecting the relevant subset of TKLM features for tape.

For EKM 3.0 usage information not covered in this guide, refer to the TKLM documentation, which includes the following:

- IBM Tivoli Key Manager 2.0 *Quick Start Guide*
- IBM Tivoli Key Manager 2.0 *Installation and Configuration Guide*
- IBM Tivoli Key Manager 2.0 *Product Overview/Scenario Guide*

For information on how to access the TKLM documentation, see the Documentation and Reference Materials section of the **ReadThisFirst.txt** file on the EKM 3.0 installation media.

Some screens and functionality covered in the IBM TKLM documentation are not enabled in Dell EKM 3.0. EKM 3.0 contains only the subset of features needed to support Dell PowerVault tape libraries.

NOTE: For recommended use and configuration of Dell EKM 3.0, refer to the Best Practices section of the **ReadThisFirst.txt** file on the EKM 3.0 installation media.

NOTE: For the latest information including feature enhancements and bug fixes, refer to the Release Notes at: **support.dell.com/manuals**. Navigate to **Software → Systems Management → Dell Encryption Key Manager** .

Hardware and Software Requirements

Server Hardware Requirements

The minimum hardware requirements for the Key Management Server (the hardware in which EKM 3.0 will be installed) are:

- CPU: 2.3 GHz
- Memory: 4 GB ECC memory

- Available disk storage (for EKM 3.0 installation and typical key storage): 5 GB

NOTE: If the system on which you are installing EKM 3.0 has 24 or more CPUs, refer to the EKM 3.0 Release Notes for details on how to update EKM 3.0 after completing the installation. To access the EKM 3.0 Release Notes, go to **support.dell.com/manuals**, then navigate to **Software → Systems Management → Dell Encryption Key Manager**.

Browser Requirements

EKM 3.0 supports the following browsers:

- Microsoft Internet Explorer, Version 7.0
- Microsoft Internet Explorer, Version 8.0, Compatibility View mode
- Firefox Version 3.0.x (EKM 3.0 does not support Firefox Version 3.5 and above.)

NOTE: JavaScript must be enabled in order for all EKM 3.0 features to function. Refer to your browser's documentation for instructions on enabling JavaScript.

Operating System Requirements

EKM 3.0 supports the following operating systems:

- Windows Server 2003 R2 with Service Pack 2, 32- and 64-bit, Standard and Enterprise Editions
- Windows Server 2008 with Service Pack 2, 32- and 64-bit, Standard and Enterprise Editions
- Windows Server 2008 R2, Standard and Enterprise Editions
- Red Hat Enterprise Linux (RHEL) 4.X, Advanced Server (AS), 32-bit
- Red Hat Enterprise Linux (RHEL) 5.X, 32- and 64-bit
- SUSE Linux Enterprise Server (SLES) 10 with Service Pack 4, 64-bit
- SUSE Linux Enterprise Server (SLES) 11 with Service Pack 1, 64-bit

NOTE: EKM 3.0 does not support VMware or Microsoft Hyper-V Server.

NOTE: For information on the requirements and limitations of setting up a primary/secondary server configuration, refer to Setting up Primary and Secondary EKM 3.0 Servers.

NOTE: EKM 3.0 performs system prerequisite checks before the installation. For more information, refer to System Prerequisite Checks.

2

Installing EKM 3.0

This chapter describes how to install EKM 3.0 on Windows and Linux.

NOTE: If you are currently using EKM 2.X, Dell recommends maintaining your current infrastructure (servers, operating systems, tape libraries, etc. under EKM 2.X protection), unless you are experiencing problems.

EKM 3.0 does not support virtual machines as hosts. If you are using a virtual machine as your EKM 2.X host, you must stay with EKM 2.X or migrate to a physical server.

NOTE: If you are planning to migrate your EKM 2.X into EKM 3.0, refer to Migrating an Encryption Key Manager (EKM) 2.X Version during the EKM 3.0 Installation before you begin the EKM 3.0 installation.

NOTE: Dell recommends that you install EKM 3.0 on a dedicated physical server that is not used for any other services. This will ensure that EKM 3.0's performance and response time is not affected by any other applications running on the same physical server.

CAUTION: EKM 3.0 only supports installation directly from the EKM 3.0 media. Do not copy the EKM 3.0 media's contents to your hard disk.

NOTE: The procedures in this chapter require system administrator-level knowledge.

Preparing for the Installation of EKM 3.0 in Microsoft Windows

This chapter describes the pre-installation steps for Dell Encryption Key Manager 3.0 in Microsoft Windows.

NOTE: The installation procedure takes approximately 45 minutes. Do not turn off the system until the installation completes.

NOTE: You must be logged in as **Administrator** in order to install EKM 3.0.

NOTE: If you do not want to use a complex password for the database, disable the **Password must meet complexity requirements** setting in the operating system before inserting the EKM 3.0 installation media.

1. Insert the EKM 3.0 for Microsoft Windows installation disk into the system on which you want to install EKM 3.0.
2. If your system is set to autorun when a DVD is inserted, wait for a moment for the installer to appear. If your system is not set to autorun, navigate to the DVD drive and double-click the DVD drive or **install.exe** at the root of the DVD drive.

   The EKM 3.0 installation wizard **Welcome** screen appears.

   NOTE: If you want to install EKM 3.0 over a network share, do not use a path of the format: **\\<*ip_address*>*EKM_3.0_share***. Instead, map the share to a drive letter. In Windows Explorer, use **Tools** → **Map Network Drive** to make the install path **<*shared_drive_letter*>:\<*EKM_3.0_media*>**.

Continue to Performing the EKM 3.0 Installation Procedure.

Preparing for the Installation of EKM 3.0 in Red Hat Enterprise Linux

This chapter describes the pre-installation steps for Dell Encryption Key Manager 3.0 in Red Hat Enterprise Linux.

NOTE: The installation procedure takes approximately 45 minutes. Do not turn off the system until the installation completes.

To prepare for the installation of EKM 3.0, perform the following steps:

1. Insert the EKM 3.0 installation disk appropriate to your operating system into the system on which you want to install EKM 3.0.
2. If your system is set to autorun when a DVD is inserted, wait for a moment for the installer to appear. If your system is not set to autorun, open a terminal with root access and navigate to the folder where the EKM 3.0 DVD is mounted. Type **./autorun.sh** and press **Enter**.

   NOTE: If SELinux is installed and enabled, disable it before starting the installation. Refer to System Prerequisite Checks.

   NOTE: Red Hat operating systems often have the **noexec** bit set to disable execution of any binaries on the mounted file systems. If the **noexec** bit on the mounted DVD ROM is set to **disable**, then the EKM 3.0 installer will not be launched from the DVD. To launch the EKM 3.0 installer from the DVD, perform the following steps:

   a) Open a terminal session with root access.
   b) Unmount the EKM 3.0 DVD.
   c) Remount the EKM 3.0 DVD as **read-only** with **noexec** disabled by issuing the following commands:

   ```
   mkdir /media/dellmedia
   mount /dev/<EKM 3.0 device><space>/media/dellmedia
   cd /media/dellmedia
   ```

   d) To execute the installer, type **./autorun.sh** and press **Enter**.

   The EKM 3.0 installation wizard **Welcome** screen appears.

Continue to Performing the EKM 3.0 Installation Procedure.

Preparing for the Installation of EKM 3.0 in SUSE Linux Enterprise Server

This chapter describes the pre-installation steps for Dell Encryption Key Manager 3.0 in SUSE Linux Enterprise Server (SLES).

NOTE: The installation procedure takes approximately 45 minutes. Do not turn off the system until the installation completes.

To prepare for the installation of EKM 3.0, perform the following steps:

1. Insert the appropriate EKM 3.0 installation disk for your operating system into the machine on which you want to install EKM 3.0.
2. If your system is set to autorun when a DVD is inserted, wait for a moment for the installer to appear. If your system is not set up to autorun, open a terminal with root access and navigate to the folder where the EKM 3.0 DVD is mounted. Type **./autorun.sh** and press **Enter**.

   The EKM 3.0 installation wizard **Welcome** screen appears.

   NOTE: If SELinux is installed and enabled, disable it before starting the installation.
3. Open port 50000. To do this, perform the following steps:
   a) Navigate to **Computer** → **Places** → **File System** .

b) Double-click **etc**.
c) Double-click **Services**.
d) In the **Services** file, change **50000/tcp** and **50000/udp** to **50100/tcp** and **50100/udp**.
e) Click **Save**.

Continue to Performing the EKM 3.0 Installation Procedure.

Performing the EKM 3.0 Installation Procedure

This chapter describes how to install EKM 3.0.

NOTE: The installation procedure takes approximately 45 minutes. Do not turn off the system until the installation completes.

NOTE: If you are installing EKM 3.0 on a server that will be used as a secondary EKM 3.0 server, the passwords must be the same passwords that you used for the primary EKM 3.0 server's installation.

1. On the EKM 3.0 installation wizard **Welcome** screen, click **Next**.
   The **License Agreement** screen appears.
2. Select the radio button to accept the terms of the license agreement.
3. Click **Next**.

   NOTE: The EKM 3.0 installer runs system prerequisite checks. The installer verifies that the system meets the minimum requirements and configures EKM 3.0 for your system.

   If an error message displays, refer to System Prerequisite Checks.

   The **Reuse Installation Profile** screen appears.
4. *If you are installing EKM 3.0 for the first time*, leave the **Reuse an EKM 3.0 installation profile** check box unchecked.
   If you are reinstalling EKM 3.0 or are installing EKM 3.0 on the secondary server and want to use an installation profile you saved from a previous installation, perform the following steps:
   a) Select the **Reuse an EKM 3.0 installation profile** check box. Selecting the check box activates the **File Location** field.
   b) Click **Choose** and navigate to the installation profile that was created when you previously configured and installed EKM 3.0 (for example, **E:\EKM_config.txt** in Windows, or **/tmp/ekm_config** in Linux).
      You can use a removable drive or a network share to transfer the installation profile from the location where you saved it.

   NOTE: The installation profile populates all of the input fields, with the exception of the passwords, in the installation GUI with the same information that you used in a previous installation. If you are using an installation profile, you must re-enter all passwords.

   NOTE: If you are installing EKM 3.0 on a secondary server, you must reuse the primary EKM 3.0 server's installation profile to ensure that the input parameters are the same.
5. Click **Next**.
   The **Database** screen appears. In this screen, you create the EKM DB2 database administrator account.

   NOTE: This screen and the next two screens each create a different account. Make a note of all user names and passwords that you create for these accounts.
6. The **Database Location** field defaults to a set location. Dell recommends that you keep the default location. This is the location where the installer will install the EKM 3.0 DB2 software.
7. In the **Database User Name** field, enter a user name that conforms to these criteria:
   – Can only include lowercase letters (a–z), numbers (0–9), and the underscore character (_)

- Cannot be longer than eight characters
- Cannot begin with “ibm,” “sys,” “sql,” or a number
- Cannot begin or end with an underscore character (_)
- Cannot be a DB2–reserved word (for example, “users,” “admins,” “guests,” “public,” and “local”) or an SQL-reserved word
- Cannot be a user name of an existing user on the system

This is the ID for the EKM 3.0 DB2 database administrator account. EKM 3.0 creates a local user account on your system with this user name.

8. In the **Database Password** field, enter a password for the EKM DB2 database administrator account. In the **Confirm Database Password** field, retype the password.

   NOTE: All passwords are case-sensitive.

   NOTE: Dell recommends the use of strong passwords for all EKM 3.0 user accounts.

9. In the **Database Data Drive** field, enter the database drive location. This is the location where the EKM 3.0 DB2 data will be stored. In Windows, enter a drive letter and colon (:). In Linux, enter a folder location, for example, **/home/ekmdb2**.
10. In the **Database Name** field, enter a name for the EKM 3.0 DB2 database.
11. The **Database Port** field defaults to **50010** in Windows and **50000** in Linux.

    All ports used by EKM 3.0 and set during the EKM 3.0 installation process are preset with the recommended port addresses. Dell strongly recommends that you use these recommended port adresseses. If you plan to use a secondary server and you change a port address when installing EKM 3.0, the port address must be the same for the primary and secondary EKM 3.0 servers.

    NOTE: All ports used during the installation process must be open in order to install EKM 3.0. Verify that they are open:

    To verify that the ports are open in Windows,

    a. Navigate to: **<*root*>:\Windows\System32\drivers\etc**.
    b. Open the **Services** text file.
    c. Review the file and confirm that the port number that you want to use in the **Database Port** field is available. If the port is available, it will not be listed.

    To verify that the ports are open in Linux,

    a. Open the **/etc/services** file.
    b. Review the file and confirm that the port number that you want to use in the **Database Port** field is available. If the port is available, it will not be listed.

12. Click **Next**.

    The **EKM Administrator** screen appears. In this screen, you create the EKM 3.0 Administrator (superuser) account. This account is used for creating new users and new groups and assigning their permissions.

13. In the **Administrator Username** field, enter an EKM 3.0 administrator user name. (This can be any name except **tklmadmin**.)
14. In the **Password** field, enter a password for the EKM 3.0 Administrator account. In the **Confirm Password** field, retype the password.
15. Click **Next**.

    The **Encryption Manager** screen appears. In this screen, you create the EKM 3.0 Encryption Manager (TKLMAdmin) account. This is the regular user account. It is used for daily key management. The **TKLMAdmin Username** field is pre-populated with **tklmadmin**. This is the required EKM Encryption Manager name.

16. In the **TKLMAdmin Password** field, enter a password for the EKM 3.0 Encryption Manager account. In the **TKLMAdmin Confirm Password** field, retype the password.

17. The **EKM Port** defaults to **16310** in Windows and Linux. This is the recommended port. Click **Next**.

    NOTE: If the port provided is used by a different service, then the EKM 3.0 installer will prompt you to select a different port. Use the **netstat** command to determine the ports that are being used, then select a port that is available. Record the port number. You will use this port to access the EKM 3.0 portal.

    The **Migration** screen appears. This screen is used to migrate from EKM 2.X to EKM 3.0.

    If you have an EKM 2.X version that you want to migrate to EKM 3.0, you must migrate it now. Refer to Migrating an Encryption Key Manager (EKM) 2.X Version during the EKM 3.0 Installation.

    NOTE: You can only migrate an EKM 2.X version that has been used to create keys.

    If you do not have an EKM 2.X version to migrate into EKM 3.0,

    a) Leave the **Migrate from EKM 2.X to EKM 3.0** check box unchecked and click **Next**.

       A verification pop-up window appears.

    b) If you have chosen not to migrate an EKM 2.X version, click **Yes** in the pop-up window confirming that you are not migrating an EKM 2.X version.

       The **Configuration Summary** screen appears.

18. In the **Configuration Summary** screen, select the **Save profile** check box.

    The **File Directory** field becomes active.

    NOTE: Dell recommends that you save the installation profile in case EKM 3.0 must be reinstalled in a disaster recovery situation. A saved installation profile is required to create a secondary EKM 3.0 server.

    NOTE: Dell recommends that you use a removable drive as the location. If using a removable drive, you must insert the drive before clicking **Next**. The removable drive must remain inserted until the installation completes. Optionally, you can save the file to a location on the local drive and copy the file to the removable drive later.

    NOTE: The path you enter in this field must include a file name. Do not enter a folder name only. The file path up until the folder name must exist, but the file name used for the installation profile must not exist.

19. In the **File Directory** field, enter the location and file name of the installation profile you are creating or click **Choose** and select a location, then enter a file name.

    This is the location in which you want the installation profile to be saved and the name in which you want it to be saved.

    EKM 3.0 saves the installation profile upon completion of the EKM 3.0 installation. If you are using a primary/secondary server configuration, you must use the primary EKM 3.0 server's installation profile during the installation of the secondary EKM 3.0 server to auto-populate the installation input fields.

    Optionally, if you are reinstalling on the same server and want to use the same fields, you can use this installation profile to auto-populate the installation input fields.

    NOTE: Dell recommends that you capture or print the **Configuration Summary** screen for later reference.

20. In the **Configuration Summary** screen, click **Next**.

    The **Installation Summary** screen appears.

21. Review the information on the **Installation Summary** screen.

22. Click **Install**.

    NOTE: The software install time is approximately 45 minutes. Do not turn off the system until the installation completes.

    NOTE: If you are planning to set up a secondary EKM 3.0 server, do not install EKM 3.0 on the secondary server until the primary server's EKM 3.0 installation is complete.

23. When the installation is complete, click **Done**.

NOTE: If you migrated an EKM 2.X version into the newly-installed EKM 3.0, then Dell strongly recommends that you create a backup of EKM 3.0 to ensure the new keys are not lost. Refer to Creating a Backup of the Keystore.

NOTE: If you are reinstalling EKM 3.0 and the installation fails due to an incomplete uninstall, perform the uninstall manually. Refer to Manually Uninstalling EKM 3.0 in Windows.

3

Setting up Primary and Secondary EKM 3.0 Servers

This chapter describes how to install, use, and uninstall EKM 3.0 on the primary and secondary servers.

CAUTION: To prevent possible data loss due to an EKM 3.0 server failure, Dell recommends using a primary and secondary EKM 3.0 server setup. This configuration provides redundancy in the event that the primary EKM 3.0 server is down or unavailable.

NOTE: You cannot have a primary EKM 3.0 and a secondary EKM 2.X server or vice versa.

Installing EKM 3.0 on the Primary Server

During the installation of EKM 3.0 on the primary server, you must select the option to save the installation profile. When the installation of EKM 3.0 on the primary server is complete, copy the saved installation profile to a removable drive or a server share. Refer to Installing EKM 3.0.

Using EKM 3.0 on the Primary Server

The primary EKM 3.0 server is where you perform all tasks for the management of encryption keys. By default, the primary EKM 3.0 server is set to **Automatically accept all new device requests for communication**. Refer to Configuring EKM 3.0 to Accept Devices that Contact EKM 3.0 for Keys for details on how to view or configure this setting. Dell recommends regularly backing up the primary EKM 3.0 server. Refer to Performing Backups and Restoring from a Backup.

If the primary EKM 3.0 server must be replaced for any reason, install EKM 3.0 on a new physical server using the installation profile from the original primary EKM 3.0 installation. Restore the new primary EKM 3.0 server with the latest backup, then update all devices to communicate with the new primary EKM 3.0 server for their key requests. Refer to your tape library's user's guide for details on how to change the IP address of the EKM 3.0 server used for key requests. To locate the tape library's user guide, see the Documentation and Reference Materials section of the **ReadThisFirst.txt** file on the EKM 3.0 installation media.

Installing EKM 3.0 on the Secondary Server

NOTE: Do not install EKM 3.0 on the secondary server until the primary server's EKM 3.0 installation is complete.

The system on which EKM 3.0 is installed as a secondary server must have the same version of the operating system that is installed on the primary EKM 3.0 server. EKM 3.0 does not support mixed operating systems between the primary and secondary servers.

Install EKM 3.0 on the secondary server using the procedures in Installing EKM 3.0. Use the installation profile that you saved when you installed EKM 3.0 on the primary server. You must manually enter the same passwords you used when you installed EKM 3.0 on the primary server.

Using EKM 3.0 on the Secondary Server

The secondary EKM 3.0 server is used for redundancy in the event that the primary EKM 3.0 server is down or unavailable.

Use the backup created on the primary EKM 3.0 server to perform the restore operation on the secondary EKM 3.0 server periodically in order to keep the primary and secondary EKM 3.0 servers synchronized. Refer to Performing Backups and Restoring from a Backup.

By default, the secondary EKM 3.0 server is also set to **Automatically accept all new device requests for communication**. Dell recommends changing this setting to **Only accept manually added devices for communication** after every restore operation. This prevents the secondary EKM 3.0 server from serving keys to new devices that are not added to the primary EKM 3.0 server. Refer to Configuring EKM 3.0 to Accept Devices that Contact EKM 3.0 for Keys for details on how to view or configure this setting.

If the primary EKM 3.0 server is temporarily down or unavailable, you must perform the restore operation on the secondary EKM 3.0 server using the last backup created on the primary EKM 3.0 server.

NOTE: When the primary EKM 3.0 server is down or unavailable and the secondary EKM 3.0 server is used to support key requests from devices, Dell recommends that you do not perform any management or operational tasks on the secondary EKM 3.0 server.

Uninstalling EKM 3.0 from the Primary and Secondary Servers

For the procedure to uninstall EKM 3.0 from the primary and secondary servers, refer to Uninstalling EKM 3.0.

4

Performing Backups and Restoring from a Backup

You can perform a backup at any time. Performing a backup creates a backup file that contains the keystore, which contains devices and keys.

Backups do not contain device groups, users, or user groups. The DB2 database contains these.

You can restore from a backup at any time.

NOTE: If keys are not backed up, they will not be served. If keys are not available to be served, encrypted backup jobs will fail.

Creating a Backup of the Keystore

This chapter describes how to back up the keystore.

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.
   The **Welcome to Dell Encryption Key Manager** screen appears.
2. In the navigation pane, navigate to **Dell Encryption Key Manager** → **Backup and Restore** .
   The **Backup and Restore** screen appears.
3. Click **Browse** next to the **Backup repository location** field and navigate to the folder where you want to save the backup file (for example, **C:\EKM_Backup** in Windows, or **/root/EKM_Backup** in Linux).

   NOTE: The folder must exist prior to starting the backup or the backup will fail. If you want to use a new folder, create it before you attempt to create a backup.
4. Click **Select** in the **Browse Directory** pop-up window to return to the **Backup and Restore** screen.
5. Click **Create Backup**.
   The **Create Backup** screen appears.
6. In the **Create password** field, create a password for the backup. This password must not be less than six characters.

   NOTE: Dell recommends the use of strong passwords for all EKM 3.0 related activities.
7. In the **Retype Password** field, re-enter the password.
8. (Optional) In the **Backup description** field, enter a description for the backup file. If you do not enter a description, a default description is added to the backup file.

   NOTE: On some browser versions, the default description field is not editable. For more information, refer to Known Issues and Their Resolutions.
9. Click **Create Backup**.
   A confirmation pop-up window appears.
10. In the confirmation pop-up window, click **OK**. The backup process runs.

    NOTE: Do not use the system while a backup process is running. If the contents of EKM 3.0 are greyed-out for a long period of time, click the web browser's refresh button.

11. When the backup file has been created, an **Information** pop-up window appears, confirming that the file was successfully created. In the pop-up window, click **OK**. The backup file you created displays in the table on the **Backup and Restore** screen.
12. Click **Return home** at the bottom of the screen.

    The **Welcome to Dell Encryption Key Manager** screen appears.

Restoring from a Backup

You can restore from a backup. You can use a backup to create secondary key servers as well as to recreate the EKM 3.0 server in a disaster recovery situation.

CAUTION: Only perform a restore from a backup that was created on the same system or another EKM 3.0 server that was installed using the same installation profile. You cannot restore from a backup that was created on a different system using different installation details.

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.

   The **Welcome to Dell Encryption Key Manager** screen appears.
2. In the navigation pane, navigate to **Dell Encryption Key Manager** → **Backup and Restore** .

   The **Backup and Restore** screen appears.
3. Select the backup from which you want to restore.
4. Click **Restore From Backup** at the top of the table.

   The **Restore From Backup** subwindow appears.
5. Enter the password for the backup file.
6. Click **Restore Backup**.

   A confirmation pop-up window appears.

   CAUTION: Any keys created after you created the backup will be lost along with access to any data encrypted with the keys. Lost or deleted keys cannot be recovered by any means.
7. In the confirmation pop-up window, click **OK**.
8. After restoring from the backup, you must manually stop and start the EKM 3.0 server. Refer to Starting and Stopping the EKM 3.0 Server in Windows or Starting and Stopping the EKM 3.0 Server in Linux.

5

Using EKM 3.0

This chapter describes some basic EKM 3.0 operations.

NOTE: EKM 3.0 is based on IBM Tivoli Key Lifecycle Manager (TKLM) V2 FixPack 2, but has been customized to support Dell tape library environments by selecting the relevant subset of TKLM features for tape.

For EKM 3.0 usage information not covered in this guide, refer to the TKLM documentation, which includes the following:

- IBM Tivoli Key Manager 2.0 *Quick Start Guide*
- IBM Tivoli Key Manager 2.0 *Installation and Configuration Guide*
- IBM Tivoli Key Manager 2.0 *Product Overview/Scenario Guide*

For information on how to access the TKLM documentation, see the Documentation and Reference Materials section of the **ReadThisFirst.txt** file on the EKM 3.0 installation media.

Some screens and functionality covered in the IBM TKLM documentation are not enabled in Dell EKM 3.0. EKM 3.0 contains only the subset of features needed to support Dell PowerVault tape libraries.

Logging into the Encryption Key Manager 3.0 Portal

To log into the Encryption Key Manager 3.0 portal, perform the following steps:

1. Open a browser and enter the following URL to open the EKM 3.0 portal:

   http://<*EKM 3.0_server_IP_address*>:<*EKM_3.0_port_number*>

   NOTE: The port number specified is the one you provided during the EKM 3.0 installation. The default is **16310**.

   If you do not know the port number, refer to the following:

In Windows	Refer to the value of the **WC_defaulthost** property in the following file: **<*root*>:\Dell \EKM\profiles\TIPProfile\properties\portdef.props**.
In Linux	Refer to the value of the **WC_defaulthost** property in the following file: **/opt/dell/ekm/ profiles/TIPProfile/properties/portdef.props**.

   NOTE: If an error message displays stating that the page cannot be found, the EKM 3.0 service might not be running. Refer to Starting and Stopping the EKM 3.0 Server in Windows or Starting and Stopping the EKM 3.0 Server in Linux.

   The EKM 3.0 login window appears.

2. Log into EKM 3.0 using the EKM 3.0 Encryption Manager user name (**tklmadmin**) and the EKM 3.0 Encryption Manager password provided during the EKM 3.0 installation.

   The **Welcome to Dell Encryption Key Manager** screen appears.

Creating a Master Keystore

This chapter describes how to create the master keystore. The first time you log into EKM 3.0, you must create the master keystore.

NOTE: If you migrated an EKM 2.X keystore during the EKM 3.0 installation, a keystore is already created, and this procedure will not apply.

NOTE: At a later point, if you want to create additional keys and/or key groups, refer to Creating Key Groups for the Device Group.

To create the master keystore, perform the following steps.

1. In the **Welcome to Dell Encryption Key Manager** screen, click **click here to create the master keystore**.
   The **Keystore** screen appears.
2. Keep the default values for **Keystore type**, **Keystore path**, and **Keystore name**.
   The default values are: **Keystore type**: JCEKS, and **Keystore name**: defaultKeyStore. The default value for the **Keystore path** in Windows is: **<*root*>:\Dell\EKM\products\tklm\keystore**. The default value for the **Keystore path** in Linux is: **/opt/dell/ekm/products/tklm/keystore**.
3. In the **Password** field, create a password for the default keystore. This password must not be less than six characters.
4. In the **Retype Password** field, re-enter the password.
5. Click **OK**.
   The **Keystore** screen confirms that the keystore was created successfully.
6. Create a backup of the keystore. Refer to Performing Backups and Restoring from a Backup.

Enabling the Firewall in the EKM 3.0 Server

NOTE: Refer to your operating system's documentation for instructions on how to configure your firewall.

EKM 3.0 communicates with the tape library over the network. If the firewall is enabled on the system on which EKM 3.0 is installed and the required ports have not been opened, communication between EKM 3.0 and the tape library will fail. If you must enable the firewall on the system on which EKM 3.0 is installed, then perform the following steps to enable communication between EKM 3.0 and the tape library:

NOTE: These are the default ports used by EKM 3.0. If your tape library is configured to use different ports, ensure that you use those port numbers in the firewall settings and in the EKM 3.0 configuration.

NOTE: If you use a primary/secondary server configuration for EKM 3.0, then repeat this procedure for the secondary server.

1. Open the following ports for the corresponding protocols:
   - TCP: 3801
   - SSL: 443
2. If your firewall is configured only to allow specific IP addresses and/or subnet masks to communicate with the above ports, ensure that the tape library's IP address and/or subnet mask are included in the list of allowed IP addresses and/or subnet masks.
   To access the tape library network configuration, log into the tape library remote management unit (RMU) and locate the network settings. For more information, refer to the tape library's user's guide. To locate the tape library's user's guide, see the Documentation and Reference Materials section of the **ReadThisFirst.txt** file on the EKM 3.0 installation media.

3. If at a later point you want to change the port settings for communication between EKM 3.0 and the tape library, ensure that the ports are changed within the tape library's settings, EKM 3.0, and the firewall of the system on which EKM 3.0 is installed.

Configuring EKM 3.0 to Accept Devices that Contact EKM 3.0 for Keys

This chapter describes how to configure the behavior of EKM 3.0 to handle devices that attempt to connect to EKM 3.0 to request keys. Refer to your device's user's guide for details on how to connect to EKM 3.0 for key requests.

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.
   The **Welcome to Dell Encryption Key Manager** screen appears.
2. In the navigation pane, navigate to **Dell Encryption Key Manager** → **Key and Device Management**.
   The **Key and Device Management** screen appears.
3. In the **Manage keys and devices** drop-down menu, select **LTO** and click **Go**.

   NOTE: Refer to TKLM documentation for more details on these settings. For information on how to access the TKLM documentation, see the Documentation and Reference Materials section of the **ReadThisFirst.txt** file on the EKM 3.0 installation media.
4. In the drop-down menu at the bottom of the table, select one of the following:

Automatically accept all new device requests for communication	Keys will automatically be served to new devices. This is the default setting for EKM 3.0. Dell recommends that you keep this setting for the primary EKM 3.0 server, but not for a secondary server if you have configured one.
Only accept manually added devices for communication	Keys will not be served to devices unless the devices are added manually. If you are configuring the secondary EKM 3.0 server, Dell recommends that you use this setting so that the secondary EKM 3.0 server does not automatically serve keys to new devices.
Hold new device requests pending my approval	Devices that contact EKM 3.0 will be added to a pending list.

Creating a Device Group

This procedure creates a device group. If are using a default device group, skip this section.

Device groups are used to manage keys that are served to one or more devices. Dell recommends that you use device groups in order to manage a subset of your devices based on your organization's needs.

To create a new device group, perform the following steps:

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.
   The **Welcome to Dell Encryption Key Manager** screen appears.
2. In the navigation pane, navigate to **Dell Encryption Key Manager** → **Advanced Configuration** → **Device Group**.
   The **Manage Device Groups** screen appears.
3. Click **Create** at the top of the table.
   The **Create Device Group** subwindow appears.

4. Under **Device family**, select the **LTO** radio button.
5. In the **Device group name** field, enter a device group name. Dell recommends that you enter a name that reflects the use of this device group, for example, **Accounting**.
6. Click **Create**.

   An **Information** pop-up window informs you of the device family setting.
7. In the **Information** pop-up window, click **OK**.

   The device group is created. The new device group displays in the list on the **Manage Device Groups** screen.

Creating Key Groups for a Device Group

Key groups are groups of keys for a specific device. This chapter describes how to create and configure key groups for a particular device. Key groups configured for one device cannot be used with another device.

To create key groups for the device group, perform the following steps:

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.

   The **Welcome to Dell Encryption Key Manager** screen appears.
2. In the navigation pane, navigate to **Dell Encryption Key Manager → Key and Device Management**.

   The **Key and Device Management** screen appears.
3. In the **Manage keys and devices** drop-down menu, select the device group name to which you want to add the key group.
4. Next to **Key and Device Management**, click **Go**.

   Within the **Key and Device Management** utility, a page for the device group that you selected displays. This page lists any key groups and devices belonging to that device group.
5. In the table, click **Add**, and then select **Key Group**.

   The **Create Key Group** subwindow appears.
6. In the **Key group name** field, enter the name of the key group.
7. In the **Number of keys to create** field, enter the number of keys to create.
8. In the **First three letters of key name** field, enter any three-letter prefix for the key name.
9. If you want this key group to be the default key group, select the **Make this the default key group** check box.
10. Click **Create Key Group**.

    A **Warning** pop-up window appears.
11. If you want to create a backup, click on the blue link in the **Warning** pop-up window to be directed to the **Backup and Restore** screen. Refer to Performing Backups and Restoring from a Backup. After creating a backup, return to the **Key and Device Management** screen. If you do not want to create a backup at this time, continue to the next step.

    NOTE: Dell recommends creating a backup when you make changes to keys, key groups, or device groups.
12. Click **OK** in the **Warning** pop-up window.

    The key group is created. The **Key and Device Management** screen displays the key groups.
13. This step is optional. Verify that the keys were created by performing the following steps on the **Key and Device Management** screen:
    a) In the drop-down menu at the top of the table, select **View Keys, Key Group Membership and Drives**.

       The keys display in the table.
    b) Scroll down to locate the new keys.

Adding a Device to a Device Group

This chapter describes how to add a device to an existing device group.

NOTE: The default device groups in EKM 3.0 are **FUTURE_DEVICES** and **LTO**.

NOTE: In order to add a device to a device group automatically, you must create a key group and a backup, or the tape library's key path diagnostics will fail and the device will not be added. Refer to Creating Key Groups for a Device Group and Creating a Backup of the Keystore for more information.

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.
   The **Welcome to Dell Encryption Key Manager** screen appears.
2. Under **Key and Device Management**, in the **Manage keys and devices** drop-down menu, select the device group that you want to use.
3. Click **Go**.
   Within the **Key and Device Management** utility, a page for the device group that you selected displays. This page lists any key groups and devices belonging to that device group.
4. From the drop-down menu at the bottom of the page, select **Automatically accept all new device requests for communication**.
5. Configure the tape library to connect to the EKM 3.0 server.
   Refer to the tape library's user's guide for more information. To locate the tape library's user's guide, see the Documentation and Reference Materials section of the **ReadThisFirst.txt** file on the EKM 3.0 installation media.
6. Run key path diagnostics in the tape library's remote management unit (RMU). Refer to the tape library's user's guide for more information.
   The new device displays in the **Key and Device Management** screen.

NOTE: If you want to add a device manually, refer to the TKLM documentation. For information on how to access the TKLM documentation, see the Documentation and Reference Materials section of the **ReadThisFirst.txt** file on the EKM 3.0 installation media.

Adding and Deleting Keys to and from Key Groups

This chapter describes how to add and delete keys to and from key groups.

NOTE: Deleting a key from a key group does not delete the key; it only removes the key from the key group. If you want to delete a single key, refer to Deleting a Specific Key.

NOTE: For instructions on accessing the **Key and Device Management** screen, refer to Creating Key Groups for the Device Group.

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.
   The **Welcome to Dell Encryption Key Manager** screen appears.
2. In the navigation pane, navigate to **Dell Encryption Key Manager → Key and Device Management**.
   The **Key and Device Management** screen appears.
3. In the **Manage keys and devices** drop-down menu, select the device group name to which you want to add the key group.
4. Next to **Key and Device Management**, click **Go**.
   Within the **Key and Device Management** utility, a page for the device group that you selected displays. This page lists any key groups and devices belonging to that device group.

5. Select the key group that you want to modify.
6. Click **Modify** at the top of the table.
   The **Modify Key Group** subwindow appears.
7. In the **Modify Key Group** subwindow, select the desired radio button.
   If you select the **Create additional keys in key group** radio button, enter the number of keys you want to add to the key group in the **Number of keys to create** field. In the **First three letters of key name** field, enter three letters, which will be the prefix of the new keys.
   If you select the **Delete key from key group** field, enter the key alias in the text field.
8. Select **Modify Key Group**.
   The key group is modified to reflect the changes.

Deleting Key Groups

This chapter describes how to delete a key group.

CAUTION: Deleting a key group deletes all of the keys within that key group. Deleting a key is the equivalent of deleting any data protected by that key as the data will no longer be accessible. Deleted keys cannot be recovered by any means for security purposes.

NOTE: You cannot delete the default key group of a device group.

To delete a key group, perform the following steps:

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.
   The **Welcome to Dell Encryption Key Manager** screen appears.
2. In the navigation pane, navigate to **Dell Encryption Key Manager → Key and Device Management**.
   The **Key and Device Management** screen appears.
3. In the **Manage keys and devices** drop-down menu, select the device group name to which you want to add the key group.
4. Next to **Key and Device Management**, click **Go**.
   Within the **Key and Device Management** utility, a page for the device group that you selected displays. This page lists any key groups and devices belonging to that device group.
5. Verify that the key group you want to delete is not the default key group. If it is the default key group, modify the key group so that it is not the default key group:
   a) In the **Key Group** table, right-click on the key group that you want to delete.
      A pop-up menu appears.
   b) In the pop-up menu, select **Modify**.
      The **Modify Key Group** subwindow appears.
   c) Uncheck the **Make this the default key group** check box.
   d) Click **Modify Key Group**.
      The **Key and Device Management** screen appears.
6. Select the key group that you want to delete to highlight it, then click **Delete**.
   A confirmation pop-up window appears.
7. Click **OK** in the confirmation pop-up window.
   The key group and all the keys associated with the key group are deleted.

Verifying the Server Certificate

This chapter describes how to verify that the server certificate that you want to use is the certificate in use. To do this, perform the following steps:

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.

   The **Welcome to Dell Encryption Key Manager** screen appears.
2. In the navigation pane, navigate to **Dell Encryption Key Manager** → **Advanced Configuration** → **Server Certificates**.

   The **Administer Server Certificates** screen appears.
3. Confirm that there is a check mark in the **In Use** column for the certificate you want to use.

   *If the **In Use** column for the desired certificate has a check mark in it,* this procedure is complete.

   *If the **In Use** column for the certificate you want to use does not have a check mark in it,* perform the following steps:

   a) Click on the certificate you want to use to highlight it.
   b) Click **Modify** at the top of the table.

      The **Modify SSL/KMIP** subwindow appears.
   c) Select the **Current certificate in use** check box.
   d) Click **Modify Certificate**.

      A **Warning** pop-up window appears.
   e) Click **OK** in the **Warning** pop-up window.
   f) Stop and restart the server. Refer to Starting and Stopping the EKM 3.0 Server in Windows or Starting and Stopping the EKM 3.0 Server in Linux.

   NOTE: Other than setting a certificate to be **In Use**, you cannot modify a certificate.

Viewing the Server Certificate Details

If you want to view the certificate details, perform the following steps:

1. Click on the certificate to highlight it.
2. Click **Modify** at the top of the table.

   The **Modify SSL/KMIP Certificate** subwindow appears.
3. View the certificate details. You can also click **Optional Certificate Parameters** to view any optional parameters.

Logging onto the WebSphere Server

Some procedures in this guide require you to log onto the WebSphere server. This chapter describes how to log onto the WebSphere server in Windows and Linux. You only need to log onto the WebSphere server if directed to do so in another procedure.

To log onto the WebSphere server with the **wsadmin** command:

1. *In Windows,* in a command prompt, navigate to **<*root*>:\Dell\EKM\bin**. *In Linux,* in a terminal session, navigate to **/opt/dell/ekm/bin**.
2. *For Windows,* enter the following command:

   ```
   wsadmin -username tklmadmin -password <tklm password> -lang jython
   ```

   For Linux, enter the following command:

   ```
   ./wsadmin.sh -username tklmadmin -password <tklm password> -lang jython
   ```

Press **Enter**. The command runs for a short amount of time, and the **wsadmin** command prompt appears.

NOTE: The commands are case-sensitive. There are no spaces around the parenthesis or brackets. Do not enter the less than and greater than symbols (< >) around variables.

NOTE: To log out of the WebSphere server, type **Exit** and press **Enter**.

Starting and Stopping the EKM 3.0 Server in Windows

This chapter describes how to start and stop the EKM 3.0 server in Windows.

1. In a command prompt, navigate to **<*root*>:\Dell\EKM\bin**.
2. To start the server, enter the following command:
   ```
   startserver server1
   ```
   To stop the server, enter the following command:
   ```
   stopserver server1
   ```
3. Press **Enter**.
   The command runs and the command prompt displays the confirmation message:
   ```
   Server server1 open for e-business
   ```
   or
   ```
   Server server1 stop completed
   ```

Starting and Stopping the EKM 3.0 Server in Linux

This chapter describes how to start and stop the EKM 3.0 server in Linux.

NOTE: You must log in as a root user to start and stop the server.

1. In a terminal session, navigate to **/opt/dell/ekm/bin**.
2. To start the server, enter the following command:
   ```
   ./startserver.sh server1
   ```
   To stop the server, enter the following command:
   ```
   ./stopserver.sh server1
   ```
   NOTE: You will be prompted for the EKM 3.0 Administrator login and password in order to stop the server.
3. Press **Enter**.
   The command runs and the terminal session displays the confirmation message:
   ```
   Server server1 open for e-business
   ```
   or
   ```
   Server server1 stop completed
   ```

6

Migration and Merge

During the EKM 3.0 installation, you can migrate EKM 2.X into EKM 3.0.

After the EKM 3.0 installation, you can merge EKM 2.X into EKM 3.0.

This chapter describes the merge and migration procedures.

NOTE: You can only migrate or merge an EKM 2.X version that has been used to create keys.

Migrating an Encryption Key Manager (EKM) 2.X Version during the EKM 3.0 Installation

Perform this procedure only if you are configuring the **Migration** screen during the EKM 3.0 installation. The **Migration** screen is used to migrate an Encryption Key Manager (EKM) 2.X version into EKM 3.0.

NOTE: If you are currently using EKM 2.X, Dell recommends maintaining your current infrastructure (servers, operating systems, tape libraries, etc. that are under EKM 2.X protection), unless you are experiencing problems.

If you must migrate an EKM 2.X version into EKM 3.0, Dell recommends that you migrate it now.

NOTE: If you are using EKM 2.X with a virtual machine as the EKM 2.X host, you must stay with EKM 2.X or migrate to a physical server. EKM 3.0 does not support virtual machines as hosts.

NOTE: During EKM 3.0 installation, you can only migrate a single EKM 2.X version. If you have more than one EKM 2.X version to port into EKM 3.0, migrate the first one using this procedure, then after the installation is complete, refer to Merging Additional EKM 2.X Versions into EKM 3.0 to merge the additional versions.

It is possible to *merge* the EKM 2.X version into EKM 3.0 after the EKM 3.0 installation is complete using the EKM 2.X to EKM 3.0 merge tool, but Dell strongly recommends that you perform the migration at this time.

NOTE: If you are using a primary/secondary EKM 3.0 server configuration, then you must perform the migration procedure only on the primary EKM 3.0 server.

When the migration is complete, perform a backup of the primary EKM 3.0 server and use the backup to restore the secondary EKM 3.0 server to match the primary EKM 3.0 server.

To migrate from EKM 2.X during the EKM 3.0 installation process, continue to EKM 2.X to EKM 3.0 Migration Procedure.

EKM 2.X to EKM 3.0 Migration Procedure

To migrate an EKM 2.X version into EKM 3.0 from the **Migration** screen during the EKM 3.0 installation, perform the following steps:

1. Log into the EKM 2.X console, back up the EKM 2.X keystore, stop the EKM 2.X server, and exit from the EKM 2.X console. Refer the EKM 2.X user's guide for more information.
2. Copy the EKM 2.X folder:

   If your EKM 2.X server is installed on a different machine than your target EKM 3.0 installation machine, copy the EKM 2.X folder on the EKM 2.X server to a temporary folder on the EKM 3.0 server (for example, **C:\temp\MyEKM2** in Windows, or **/opt/myekm2** in Linux).

   If your EKM 2.X server is installed on the same machine as your target EKM 3.0 installation machine, you must still make a copy of the EKM 2.X folder on that machine.
3. In the EKM 3.0 installation **Migration** screen, place a check mark in the **Migrate from EKM 2.X to EKM 3.0** check box.
4. Click **Choose** and navigate to the directory where you copied the EKM 2.X folder previously. Do not select anything below this folder.

   CAUTION: If your EKM 2.X server is installed on the same machine as your target EKM 3.0 installation machine, then do not navigate to the directory where EKM 2.X is installed, because the EKM 3.0 installer deletes the folder used for migration. Navigate to the copy of the EKM 2.X directory that you created previously.
5. Click **Next**.

   The **Configuration Summary** screen appears.

NOTE: If an error message displays, verify the path to your EKM 2.X directory.

6. Continue with the EKM 3.0 installation. Refer to Performing the EKM 3.0 Installation Procedure.

NOTE: The password for the new EKM 3.0 keystore is the same password that was associated with the EKM 2.X keystore used for migration.

CAUTION: Do not delete EKM 2.X after you have migrated its keys to EKM 3.0 since EKM 3.0 references the keystore that is in the EKM 2.X folder. In order to prevent EKM 2.X from issuing keys, log into the EKM 2.X console, back up the EKM 2.X keystore, stop the EKM 2.X server, and exit from the EKM 2.X console. Dell strongly recommends that you back up the EKM 2.X files prior to using EKM 3.0. Refer the EKM 2.X user's guide for more information.

Merging Encryption Key Manager (EKM) 2.X into EKM 3.0 after Installing EKM 3.0

This chapter describes the post-installation EKM 2.X to EKM 3.0 merge procedure for Windows and Linux. This procedure uses the EKM 2.X to EKM 3.0 merge tool.

Use this procedure if EKM 3.0 is already installed and configured and you want to merge EKM 2.X into EKM 3.0.

NOTE: If you are using a primary/secondary EKM 3.0 server configuration, then you must perform the merge procedure only on the primary EKM 3.0 server. After the merge procedure is complete on the primary EKM 3.0 server, perform the backup procedure, and then restore the backup file on the secondary EKM 3.0 server. Refer to Performing Backups and Restoring from a Backup.

NOTE: If EKM 3.0 is not yet installed, Dell recommends migrating EKM 2.X into EKM 3.0 during the EKM 3.0 installation. Refer to Performing the EKM 3.0 Installation Procedure.

The examples in this document use standard Windows paths (for example, **C:\<*foldername*>**). Substitute the appropriate root drive letter or Linux path for your system.

Merge Tool Prerequisites

Before running the merge tool, verify that the following requirements are met:

- EKM 3.0 must be installed and the master keystore must be created or the merge procedure will fail. Refer to Creating a Master Keystore.
- When merging from EKM 2.X to EKM 3.0, EKM 2.X and EKM 3.0 must be installed on the same operating system version.
- If you have previously merged or migrated EKM 2.X into EKM 3.0, the **ekmcert** certificate from the previous merge or migration will still exist on the EKM 3.0 server, and may exist even if you have restored from a previous backup. You must remove the **ekmcert** certificate from the EKM 3.0 server before performing the merge procedure. Refer to Deleting the ekmcert Certificate, Keys, and Key Groups, and Renaming Devices.
- You must rename the duplicate keys, key groups, and devices in EKM 2.X before merging them into EKM 3.0. Refer to the EKM 2.X user's guide.
  - There cannot be duplicate key aliases/names from the source EKM 2.X with the target EKM 3.0. Each incoming key must have a unique alias/name, otherwise the merge procedure will fail.
  - There cannot be duplicate key *group* aliases/names from the source EKM 2.X with the target EKM 3.0. Each incoming key group must have a unique alias/name, otherwise the merge procedure will fail.
  - There cannot be duplicate devices from the source EKM 2.X with the target EKM 3.0, otherwise, the merge procedure will fail.

EKM 2.X to EKM 3.0 Merge Procedure

Perform the following steps to run the merge tool:

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.

   The **Welcome to Dell Encryption Key Manager** screen appears.
2. On the EKM 3.0 server, create a backup of EKM 3.0. Refer to Performing Backups and Restoring from a Backup for the procedure on creating backups.

   If the merge tool fails or corrupts any EKM 3.0 data, you can use the backup to recover any lost information.
3. Log out of EKM 3.0.
4. Stop the EKM 3.0 server before running the merge tool. Refer to Starting and Stopping the EKM 3.0 Server in Windows or Starting and Stopping the EKM 3.0 Server in Linux.
5. In the root of the EKM 3.0 server, create a suitable folder (for example, **C:\EKM_Files** in Windows, or **/opt/EKM_Files** in Linux).
6. Log into the EKM 2.X console, back up the EKM 2.X keystore, stop the EKM 2.X server, and exit from the EKM 2.X console. Refer the EKM 2.X user's guide.
7. From the location where EKM 2.X is installed, copy the following files to the folder you created on the EKM 3.0 server in the previous step. If EKM 2.X is installed on a different physical system, use a removable drive or a server share of the same operating system.
   - In Windows, from **<*root*>:\ekm\gui**, copy **EKMKeys.jck**. In Linux, this is located in **/var/ekm/gui**.
   - In Windows, from **<*root*>:\ekm\gui**, copy **KeyManagerConfig.properties** (this is the EKM configuration file). In Linux, this is located in **/var/ekm/gui**.
   - In Windows, from **<*root*>:\ekm\gui\keygroups**, copy **keygroup.xml**. In Linux, this is located in **/var/ekm/gui/keygroups**.
   - In Windows, from **<*root*>:\ekm\gui\drivetable**, copy **ekm_drivetable.dt**. In Linux, this is located in **/var/ekm/gui/drivetable**.

   CAUTION: In Windows, use Notepad to create or edit text files. If you use Wordpad, this procedure will fail.

8. Edit the **KeyManagerConfig.properties** file so that it contains only the following properties:

   - **config.keygroup.xml.file**
   - **config.keystore.password.obfuscated**
   - **config.keystore.file**
   - **config.drivetable.file.url**

   Delete the other lines. For an example, refer to Code Example in this procedure.

9. Add the following DB2 options to the new **KeyManagerConfig.properties** file:

   - jdbcURL = jdbc:db2://localhost:<*EKM 3.0 DB2 database port*>/<*EKM 3.0 DB2 database name*>

     or

     jdbcURL = jdbc:db2://<*EKM 3.0 server IP address*>:<*EKM 3.0 DB2 database port*>/<*EKM 3.0 DB2 database name*>
   - jdbcUID = <*DB2 administrator user name*>
   - jdbcPW = <*DB2 administrator password*>
   - dbType = DB2

   For an example, refer to Code Example in this procedure.

   NOTE: The variables are parameters that you set when you installed EKM 3.0. Do not enter the less than and greater than symbols (< >) around variables. The variables, user names, and passwords are case-sensitive.

10. Add the password entry for the EKM 3.0 default keystore to the **KeyManagerConfig.properties** file. The password entry is:

    tklm.encryption.password = <*ekm 3.0 keystore password*>.

    The updated **KeyManagerConfig.properties** file should look similar to the following example:

Code Example for Windows

```
config.keygroup.xml.file = File:c:\\<EKM_Files>\
\KeyGroups.xml
config.keystore.password.obfuscated = 38087C9DA4A4696A6B6C
config.keystore.file = c:\\<EKM_Files>\\EKMKeys.jck
config.drivetable.file.url = File:c:\\<EKM_Files>\
\ekm_drivetable.dt
jdbcURL = jdbc:db2://localhost:50010/ekm_dell
jdbcUID = ekmdell1
jdbcPW = Dell1234
dbType = DB2
tklm.encryption.password = Dell1234
```

Where *EKM_Files* is the folder you created previously.

Code Example for Linux

```
config.keygroup.xml.file = File:/opt/<EKM_Files>/
KeyGroups.xml
config.keystore.password.obfuscated = 38087C9DA4A4696A6B6C
config.keystore.file = /opt/<EKM_Files>/EKMKeys.jck
config.drivetable.file.url = File:/opt/<EKM_Files>/
ekm_drivetable.dt
jdbcURL = jdbc:db2://localhost:50010/ekm_dell
jdbcUID = ekmdell1
jdbcPW = Dell1234
dbType = DB2
tklm.encryption.password = Dell1234
```

Where *EKM_Files* is the folder you created previously.

11. Navigate to the **EKM2DKMMerge** folder on the EKM 3.0 installation media. From the **EKM2DKMMerge** folder, copy the **EKM2DKMMerge.jar** file to the folder you created earlier in this procedure (for example C:\EKM_Files in Windows, or /opt/EKM_Files in Linux).

    NOTE: You must use the same command prompt or terminal session for all of the following steps. If you change command prompts or terminal sessions, the CLASSPATH that you set will not automatically apply to other command prompts or terminal sessions.

12. On the EKM 3.0 server, configure the paths for WAS and TIP that are needed by the merge tool.

    In Windows:

    a. In a command prompt, navigate to **<*root*>:\Dell\EKM\bin**.

    b. Enter the following command to run the command line script:

    ```
    setupCmdLine.bat
    ```

    Example:

    ```
    C:\Dell\EKM\bin\setupCmdLine.bat
    ```

    c. Press **Enter**. The command runs and the system displays the following text displays on the last line:

    ```
    goto :EOF
    ```

    In Linux:

    a. In a terminal session, navigate to **/opt/dell/ekm/bin**.

    b. Enter the following command:

    ```
    . setupCmdLine.sh
    ```

    c. The command runs. Upon successful completion of the command in Linux, a blank prompt displays. There is no indicator that the command completed.

    NOTE: The **setupCmdLine.sh** script must have execute permission.

13. Create a command line batch (.bat) file (in Linux, .sh) to source in the needed .jar files required by the merge tool and to set additional parameters for the CLASSPATH:

    a) Copy the following temporary CLASSPATH setup into a text file and name it <*filename*>.bat or in Linux, <*filename*>.sh (for example, **setupclasspath.bat** in Windows, or **setupclasspath.sh** in Linux).

    b) Save the .bat/.sh file in the folder that you created earlier in this procedure, for example C:\EKM_Files or /opt/EKM_Files.

    CAUTION: In Windows, use Notepad to create or edit text files. If you use Wordpad, this procedure will fail.

    c) Edit the batch file:

    In Windows, edit the batch file to replace ***c:\EKM\Needed*** with the path where you placed the **EKM2DKMMerge.jar** file, for example **c:\EKM_Files**.

    In Linux, edit the shell script to replace **/opt/EKM_Files** with the path where you placed the **EKM2DKMMerge.jar** file.

    Temporary CLASSPATH setup for Windows

    ```
    set JAVA_HOME=%WAS_HOME%\java
    set PATH=%JAVA_HOME%\bin;%JAVA_HOME%\jre\bin;%PATH%
    set CLASSPATH=c:\EKM\Needed\EKM2DKMMerge.jar;%CLASSPATH%
    set CLASSPATH=.;%WAS_HOME%\plugins\com.ibm.icu_3.4.5.jar;%WAS_HOME%
    \products\tklm\migration\j2ee.jar;%WAS_HOME%\plugins
    \com.ibm.tklm.commands.jar;%WAS_HOME%\products\tklm\migration
    \com.ibm.tklm.kmip.adapter.jar;%WAS_HOME%\profiles\TIPProfile
    \installedApps\TIPCell\tklm_kms.ear\com.ibm.tklm.kmip.jar;"C:\Program
    Files\Dell\db2dkm\java\db2jcc.jar";"C:\Program Files\Dell\db2dkm\java
    \db2jcc_license_cu.jar";%WAS_HOME%\profiles\TIPProfile\installedApps
    \TIPCell\tklm_kms.ear\com.ibm.tklm.keyserver.jar;%WAS_HOME%\profiles
    ```

```
\TIPProfile\installedApps\TIPCell\tklm_kms.ear
\com.ibm.tklm.server.api.jar;%WAS_HOME%\profiles\TIPProfile\installedApps
\TIPCell\tklm_kms.ear\com.ibm.tklm.server.db.ejb.jar;%CLASSPATH%
```

NOTE: Replace the drive letters as necessary.

NOTE: If you are using 64–bit Windows, edit the batch file to replace **Program Files** in the CLASSPATH above with **Program Files (x86)**.

Temporary CLASSPATH setup for Linux

```
export JAVA_HOME=$WAS_HOME/java
export PATH=${JAVA_HOME}/bin:${JAVA_HOME}$/jre/bin:$PATH
export CLASSPATH=/opt/EKM_Files/EKM2DKMMerge.jar:$CLASSPATH
export CLASSPATH=.:$WAS_HOME/plugins/com.ibm.icu_3.4.5.jar:$WAS_HOME/
products/tklm/migration/j2ee.jar:$WAS_HOME/plugins/
com.ibm.tklm.commands.jar:$WAS_HOME/products/tklm/migration/
com.ibm.tklm.kmip.adapter.jar:$WAS_HOME/profiles/TIPProfile/installedApps/
TIPCell/tklm_kms.ear/com.ibm.tklm.kmip.jar:/opt/dell/db2ekm/java/
db2jcc.jar:/opt/dell/db2ekm/java/db2jcc_license_cu.jar:$WAS_HOME/profiles/
TIPProfile/installedApps/TIPCell/tklm_kms.ear/com.ibm.tklm.keyserver.jar:
$WAS_HOME/profiles/TIPProfile/installedApps/TIPCell/tklm_kms.ear/
com.ibm.tklm.server.api.jar:$WAS_HOME/profiles/TIPProfile/installedApps/
TIPCell/tklm_kms.ear/com.ibm.tklm.server.db.ejb.jar:$CLASSPATH
```

14. Run the batch file you just created. Within the same command prompt or terminal session on the EKM 3.0 server, navigate to the folder you created earlier in this procedure (for example, C:\EKM_Files in Windows, or /opt/EKM_Files in Linux), and run the batch file you created in the previous step. In Linux, source the file that you created previously, for example, . setupclasspath.sh.
15. Within the same command prompt or terminal session on the EKM 3.0 server, run the following Java command:

```
java<space>com.ibm.tklm.ekm2tklm.MergeEKM2KLM<space>KeyManagerConfig.propert
ies
```

NOTE: The commands are case-sensitive. Do not enter the less than and greater than symbols (< >) around variables.

The **KeyManagerConfig.properties** file is the file that you updated earlier in this procedure.

This command merges EKM 2.X into EKM 3.0.

Upon successful completion, the following message displays:

```
TKLM version: 2.0.0.0 201007241325Starting EKM to KLM MergeKMSDebug.init,
debug output filename not specified: using defaultCTGKS0250I: Successfully
migrated the Encryption Key Manager keystores, certificates and
keys.CTGKS0251I: Successfully migrated the Encryption Key Manager key
groups.CTGKS0249I: Successfully migrated the Encryption Key Manager
devices.Migration Complete.
```

NOTE: If you receive errors, view the debug log to determine the cause. If desired, you can save the debug log to another location or rename it to make it become static, otherwise the EKM 2.X to EKM 3.0 merge tool will append data to it. In Windows, the debug log is located in the following directory on the EKM 3.0 server: **<*root*>:\Dell\EKM\bin\products\tklm\logs\debug.log**. In Linux, the debug log is located in the following directory on the EKM 3.0 server: **/opt/dell/ekm/bin/products/tklm/logs/debug.log**.

NOTE: If you receive the following error, you are attempting to migrate while a duplicate item is on the EKM 2.X server and the EKM 3.0 server. .

```
Duplicate <item> = <item>Migration failed. Please refer to the debug
file for more information.
```

Refer to Deleting the ekmcert Certificate, Keys, and Key Groups, and Renaming Devices

If you receive the following error and you want to delete the key instead of renaming it, do not close the command prompt or terminal session. You will need to copy the key alias from the command prompt or terminal session.

```
Duplicate Key Alias= <key alias>
```

Refer to Deleting the ekmcert Certificate, Keys, and Key Groups, and Renaming Devices.

CAUTION: Deleting a key is the equivalent of deleting any data protected by that key as the data will no longer be accessible. Deleted keys cannot be recovered by any means for security purposes.

16. Start the EKM 3.0 server using the **startserver** command. Refer to Starting and Stopping the EKM 3.0 Server in Windows or Starting and Stopping the EKM 3.0 Server in Linux.
17. Verify that the EKM 2.X key groups, keys, and devices migrated to EKM 3.0. Refer to Verifying the EKM 2.X to EKM 3.0 Merge or Migration. If the merge procedure was successful, the procedure is complete. If you want to merge additional EKM 2.X versions into EKM 3.0, refer to Merging Additional EKM 2.X Versions into EKM 3.0. If the merge procedure was not successful, refer to Merge Failure.

CAUTION: Do not run EKM 2.X after you have merged its keys into EKM 3.0. Dell strongly recommends that you back up the EKM 2.X files after you merge the keys into EKM 3.0.

Verifying the EKM 2.X to EKM 3.0 Merge or Migration

This chapter describes how to verify that the EKM 2.X to EKM 3.0 merge or migration procedures were successful and that the tape libraries are functional.

To verify that the EKM 2.X has been successfully merged or migrated into EKM 3.0, perform the following steps:

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.
   The **Welcome to Dell Encryption Key Manager** screen appears.
2. In the navigation pane, navigate to **Dell Encryption Key Manager → Key and Device Management**.
   The **Key and Device Management** screen appears.
3. In the **Manage keys and devices** drop-down menu, select **LTO** and click **Go**.
   The **Key and Device Management** screen displays the migrated EKM keygroup(s) and the number of keys in each group.
4. In the drop-down menu at the top of the table, select **View Keys, Key Group Membership and Drives**. If keys appear in the left side of the table, then the merge was successful.
5. The migration does not import the EKM 2.X configured devices. You must configure the EKM 2.X devices. Refer to Adding a Device to a Device Group.
6. In the EKM 3.0 portal, verify that EKM 3.0 is configured to accept device requests automatically. The setting on the **Key and Device Management** screen should be **Automatically accept all new device requests for communication**.
7. Verify the devices on your library:
   a) Verify that the SSL port and the TCP port are correctly configured in your tape library.
   b) Run key path diagnostics from your tape library to verify your tape library configuration.

   NOTE: Refer to the tape library's user's guide for full details. For information on locating the tape library's user's guide, see the Documentation and Reference Materials section of the **ReadThisFirst.txt** file on the EKM 3.0 installation media.

Merge Failure

If the merge procedure fails, perform the following steps:

1. Verify that the EKM 3.0 server is started. If it is not, start the EKM 3.0 server using the **startserver** command. Refer to Starting and Stopping the EKM 3.0 Server in Windows or Starting and Stopping the EKM 3.0 Server in Linux.
2. Close the command prompt.
3. Capture the debug log by saving it to another location or renaming it.

   The debug log is located in the following directory: **<*root*>:\Dell\EKM\bin\products\tklm\logs\debug.log** in Windows, or **/opt/dell/ekm/bin/products/tklm/logs/debug.log** in Linux.
4. Restore EKM 3.0 through the EKM 3.0 portal from the backup that you created in the first step of EKM 2.X to EKM 3.0 Merge Procedure. For instructions on restoring from a backup, refer to Restoring from a Backup.
5. Perform the merge procedure again. Refer to EKM 2.X to EKM 3.0 Merge Procedure.

Merging Additional EKM 2.X Versions into EKM 3.0

Perform this procedure if you have migrated or merged EKM 2.X into EKM 3.0 and you want to merge additional EKM 2.X versions into EKM 3.0.

1. Remove the **ekmcert** certificate from EKM 3.0. Refer to Deleting the ekmcert Certificate, Keys, and Key Groups, and Renaming Devices.
2. Perform the merge procedure for each additional EKM 2.X version you want to merge. Refer to EKM 2.X to EKM 3.0 Merge Procedure.

Deleting the ekmcert Certificate, Keys, and Key Groups, and Renaming Devices

When performing an EKM 2.X to EKM 3.0 merge, there cannot be duplicate **ekmcert** certificates, key aliases, key group aliases, or devices in EKM 2.X and on the EKM 3.0 server.

NOTE: If there are duplicate keys or key groups, Dell recommends that you rename the duplicate keys and key groups in EKM 2.X before merging them into EKM 3.0. Refer to the EKM 2.X user's guide for more information. If the duplicate keys or key groups are obsolete, you can delete them in EKM 2.X. However, deleting a key is the equivalent of deleting any data protected by that key as the data will no longer be accessible. Deleted keys cannot be recovered by any means for security purposes.

If you have duplicate devices, you must delete a device in EKM 2.X.

If you receive the following error when performing the merge procedure, delete the appropriate item based on the error message.

```
Duplicate <item> = <item> Migration failed. Please refer to the debug file for
more information.
```

Refer to the appropriate section:

- ekmcert Certificate Deletion
- Deleting a Specific Key
- Deleting a Device

ekmcert Certificate Deletion

Each EKM 2.X installation has one **ekmcert** certificate. If you are merging or migrating more than one EKM 2.X into EKM 3.0, you must delete the **ekmcert** certificate in EKM 3.0 before attempting to merge a new EKM 2.X.

Because **ekmcert** is a certificate and not a key, it is not part of any key groups on the EKM 3.0 server. Therefore, if you merged an EKM 2.X version into EKM 3.0 and then removed EKM 2.X key groups from EKM 3.0, the **ekmcert** certificate from the merge will still exist on the EKM 3.0 server, and may exist even if you restore from a previous backup. Because the merge tool attempts to add the **ekmcert** certificate again, the merge will fail.

You must remove the **ekmcert** certificate from the EKM 3.0 server if any of the following situations exist:

- You migrated an EKM 2.X into EKM 3.0 during the EKM 3.0 installation procedure
- This is not the first time you have merged EKM 2.X into EKM 3.0
- You need to delete a previously-merged or migrated EKM 2.X version
- You receive the following error when you attempt a merge. This error indicates the **ekmcert** certificate is already in EKM 3.0:

  ```
  Duplicate Key Alias = ekmcert Migration failed. Please refer to the debug file for more information.
  ```

To delete the **ekmcert** certificate, refer to Deleting the ekmcert Certificate.

Deleting the ekmcert Certificate

To verify that the **ekmcert** certificate is on EKM 3.0 and delete it, perform the following steps:

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.
   The **Welcome to Dell Encryption Key Manager** screen appears.
2. In the navigation pane, navigate to **Dell Encryption Key Manager** → **Advanced Configuration** → **Server Certificates**.
   The **Administer Server Certificates** screen appears.
3. On the **Administer Server Certificates** screen, verify that the **ekmcert** certificate is listed and not currently in use.
   If the **ekmcert** certificate is not currently in use, go to the next step. If the **ekmcert** certificate is currently in use, perform the following steps:
   a) Select the **ekmcert** certificate.
   b) Click **Modify**.
   c) Uncheck the **Current Certificate In Use** check box.
   d) Click **Modify Certificate**.
   The **Administer Server Certificates** screen appears. The certificate displays as not in use.
4. Select the **ekmcert** certificate again.
5. Click **Delete** at the top of the table.
   A confirmation window appears.
6. Click **OK** to delete the certificate.
   The certificate is removed from the list.

Deleting a Specific Key

This chapter describes how to delete a single key. You cannot delete a key that is associated with a device.

CAUTION: Deleting a key is the equivalent of deleting any data protected by that key as the data will no longer be accessible. Deleted keys cannot be recovered by any means for security purposes.

NOTE: If you received an error message that you have a duplicate key when you performed a merge from EKM 2.X to EKM 3.0, Dell recommends that you rename the duplicate key in EKM 2.X. Refer to the EKM 2.X user's guide for more information.

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.
   The **Welcome to Dell Encryption Key Manager** screen appears.
2. In the navigation pane, navigate to **Dell Encryption Key Manager → Key and Device Management**.
   They **Key and Device Management** screen appears.
3. In the **Manage keys and devices** drop-down menu, select **LTO** and click **Go**.
   The **Key and Device Management** screen appears.
4. In the drop-down menu at the top of the table, select **View Keys, Key Group Membership and Drives**.
   The keys display in the table.
5. Click the key you want to delete to highlight it.
6. Click **Delete** at the top of the table.
   A confirmation pop-up window appears.
7. If you are sure you want to delete the selected key, click **OK**.
   The key is deleted.

Deleting a Device

This chapter describes how to delete a device. A device is an individual drive installed in the tape library. The serial number is displayed on the right-hand side of the tape drive.

NOTE: If you received an error message that you have a duplicate device when you performed a merge from EKM 2.X into EKM 3.0, Dell recommends that you delete the device in EKM 2.X. Refer to the EKM 2.X user's guide for more information.

To delete the device from EKM 3.0, perform the following steps:

1. Log into the EKM 3.0 portal. Refer to Logging into the Encryption Key Manager 3.0 Portal.
   The **Welcome to Dell Encryption Key Manager** screen appears.
2. In the navigation pane, navigate to **Dell Encryption Key Manager → Key and Device Management**.
   The **Key and Device Management** screen appears.
3. In the **Manage keys and devices** drop-down menu, select the device group that contains the device you want to delete.
4. Click **Go**.
   The devices that belong to the device group are listed.
5. Click the device you want to delete to highlight it.
6. Click **Delete** at the top of the table.
   A confirmation pop-up window appears.
7. Click **OK** in the pop-up window.
   The device is deleted.

Verifying the EKM 2.X Keystore Library is Removed from EKM 3.0

This procedure is optional. This chapter describes how to verify that all of the EKM 2.X keystore entries (the **ekmcert** certificate, and the keys in the EKM 2.X keystore) are removed from the EKM 3.0 server. To do this, perform the following steps:

1. At a command prompt or terminal session on the EKM 3.0 server, navigate to the folder you created during the EKM 2.X to EKM 3.0 Merge Procedure (for example, **C:\EKM_Files** in Windows, or **/opt/EKM_Files** in Linux).
2. Ensure that the Java SDK tool **keytool** is available in the command-line path.
3. List the contents of the EKM 2.X keystore by issuing the following command:
   ```
   keytool -list -keystore <EKM_2.X_keystore_name> -storetype JCEKS
   ```

where <*EKM_ 2.X_ keystore_name*> is the name of the EKM 2.X keystore you are importing.

For example:

keytool -list -keystore *EKMKeys.jck* -storetype JCEKS

The system prompts you for a password.

4. Enter the EKM 2.X keystore password and press **Enter**.

   The EKM 2.X keystore type, the **ekmcert** certificate, the keystore provider, and the keys in the EKM 2.X keystore are displayed. You will use the list of keys to compare against the EKM 3.0 keystore to verify that these keys are not in the EKM 3.0 keystore.

   NOTE: Keep the command prompt open. In a later step, you will search for these keys and/or the **ekmcert** certificate in the EKM 3.0 keystore to verify that they have been removed from EKM 3.0.

5. Start the EKM 3.0 server using the **startserver** command. Refer to Starting and Stopping the EKM 3.0 Server in Windows or Starting and Stopping the EKM 3.0 Server in Linux.
6. *In a Windows command prompt*, navigate to **<*root*>:\Dell\EKM\bin**. *In Linux*, navigate to **/opt/dell/ekm/bin**.
7. Log onto the WebSphere server using the **wsadmin** command. Refer to Logging onto the WebSphere Server.
8. At the **wsadmin** prompt, using the key alias obtained earlier, issue one of the following commands to list a specific key or certificate on the EKM 3.0 server:

   For keys:

   ```
   print AdminTask.tklmKeyList('[-alias <key alias>]')
   ```

   For the **ekmcert** certificate:

   ```
   print AdminTask.tklmKeyList('[-alias ekmcert]')
   ```

   NOTE: You obtained the key aliases in a previous step. In Windows, you can copy the aliases using the toolbar on the command prompt window.

   NOTE: If you want to visually compare the key aliases, you can list all of the keys on the EKM 3.0 server by issuing the following command:

   ```
   print AdminTask.tklmKeyList('[-alias]')
   ```

9. Press **Enter**.

   The command runs.

   If the duplicate key is not on EKM 3.0, the following text displays:

   ```
   Found 0 keys.
   ```

   If the key or certificate is on EKM 3.0, the UUID and the key or certificate alias display.

   If the key or certificate is on EKM 3.0, delete the key or certificate from EKM 3.0. Refer to Deleting a Specific Key.

   Repeat this step for each duplicate key that was listed previously.

7

Uninstalling EKM 3.0

This chapter describes how to uninstall EKM 3.0 from Windows and Linux.

CAUTION: Uninstalling EKM 3.0 will render all encrypted data written to the Dell PowerVault Tape Library via library-managed encryption (LME) unreadable. Ensure all critical data is restored before uninstalling EKM 3.0. If there is a possibility that you may reinstall EKM 3.0 in the future, create a backup before uninstalling EKM 3.0. Copy the EKM 3.0 backup and installation profile (if you saved an installation profile) to an external drive before uninstalling EKM 3.0. When you reinstall EKM 3.0, use this backup file to perform the restore operation. Refer to Performing Backups and Restoring from a Backup.

NOTE: The uninstall process takes approximately 35 minutes. Do not turn off the system until the uninstall process completes.

NOTE: Uninstalling EKM 3.0 also uninstalls WebSphere and DB2. If you are using the DB2 for other applications, Dell recommends that you not uninstall EKM 3.0. It is recommended that you stop the EKM 3.0 service instead. For information on stopping the EKM 3.0 service, refer to Starting and Stopping the EKM 3.0 Server in Windows or Starting and Stopping the EKM 3.0 Server in Linux.

NOTE: If you have a primary/secondary server setup, you must also perform the uninstall procedure on the secondary EKM 3.0 server.

NOTE: If you want to reinstall EKM 3.0, refer to Reinstalling EKM 3.0.

Uninstalling EKM 3.0 in Windows

This procedure uses the EKM 3.0 uninstall program for Windows.

NOTE: The uninstall process takes approximately 35 minutes. Do not turn off the system until the installation completes.

1. In Windows 2008 versions, open the **Control Panel** and navigate to **Programs and Features**.
   In Windows Server 2003 R2 with Service Pack 2, open the **Control Panel** and navigate to **Add or Remove Programs**.
2. Right-click **EKM 3.0** and select **Uninstall**.
3. Follow the on-screen instructions.
   When the uninstall is complete, the **Uninstall Complete** window appears.
4. In the **Uninstall Complete** window, click **Done**.
   A dialog box appears, stating that the system will reboot.
5. In the dialog box, click **Done**. (If you do not click **Done**, Windows will still reboot after about a minute.)

   NOTE: If Windows does not reboot, restart the machine manually.

   NOTE: If you encounter errors during the uninstall process, you can view the main install log in the user's home directory at **<*root*>:\Users\Administrator**. The main install log file is **IA-TIPxxx**. Scroll to the bottom of the main install log file to determine where the process stopped or the last error occurred. You can also view the log files in **<*root*>:\tklmv2properties** for more details.

   NOTE: If you are reinstalling EKM 3.0 and the installation fails due to an incomplete uninstall, perform the uninstall manually. Refer to Manually Uninstalling EKM 3.0 in Windows.

Uninstalling EKM 3.0 in Linux

This procedure uses the EKM 3.0 uninstall program for Linux.

NOTE: The uninstall process take approximately 35 minutes. Do not turn off the system until the installation completes.

1. Open a terminal session and navigate to **/opt/dell/ekm/Uninstall_EKM**.
2. Run **Uninstall EKM** by issuing the following command:

   ```
   ./Uninstall EKM
   ```

   A pop-up window appears.
3. Click **Run** in the pop-up window.

   The **Uninstall EKM** window appears.
4. Click **Uninstall**.

   The uninstall process runs.
5. When the uninstall is complete, the **Uninstall Complete** window appears. Click **Done**.

   The system reboots.

NOTE: If you are reinstalling EKM 3.0 and the installation fails due to an incomplete uninstall, perform the uninstall manually. Refer to Manually Uninstalling EKM 3.0 in Linux.

8

Troubleshooting

This chapter provides troubleshooting information, frequently asked questions, common errors messages, and support contact information.

NOTE: If your issue is not covered in this chapter, refer to the TKLM troubleshooting guide. For information on how to access the TKLM documentation, see the Documentation and Reference Materials section of the **ReadThisFirst.txt** file on the EKM 3.0 installation media.

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Visit **www.dell.com/support**.
2. Select your support category.
3. Verify your country or region in the Choose a Country/Region drop-down menu at the top of page.
4. Select the appropriate service or support link based on your need.

System Prerequisite Checks

EKM 3.0 performs system prerequisite checks before the installation. If you receive an error message after the **License Agreement** screen, follow the instructions in the error message. For the most common errors, refer to the items below for instructions.

Minimum System Requirements Failed

If you receive a **Minimum System Requirements Failed** error, click **Cancel and Exit** and confirm that your system meets the requirements. Refer to Hardware and Software Requirements for the system requirements.

User not an Administrator on this System

You must be a root user on Linux or an administrator in Windows in order to install EKM 3.0.

SELinux Must be Disabled

If SELinux is installed and enabled, disable SELinux before starting the installation.

To disable SELinux in RHEL5, perform the following steps:

1. From the top toolbar on the desktop, navigate to **System** → **Administration** → **Security Level and Firewall**.
   The **Security Level Configuration** window appears.
2. Click the **SELinux** tab. In the **SELinux Setting** box, click the arrows and select **Disabled**.
3. Click **Apply**.
4. Click **OK**.
5. Reboot the system for the changes to take effect.

To disable SELinux in RHEL4, perform the following steps:

1. Navigate to **Applications** → **System Settings** → **Security Level** .
   A pop-up window appears.
2. In the pop-up window, select the **SELinux** tab.
3. In the drop-down menu, select **Disable**.
4. Reboot the system.

compat-libstdc++ Not Installed

If a "compat-libstdc++ Not Installed" error message displays, refer to Installing the compat-libstdc++ Library.

Minimum Shared Memory Limits Requirements Failed

When installing EKM 3.0 on Linux, the following error displays:

```
The system did not meet the minimum shared memory requirements needed for the
installation.
Make sure your system meets the minimum requirements before attempting this
installation.
```

To resolve this issue, perform the following steps:

1. To increase the shared memory to the required size and make it persistent, open a terminal session and issue the following command:

```
echo "kernel.msgmni = 1024" >> /etc/sysctl.conf
echo "kernel.msgmax = 65536" >> /etc/sysctl.conf
echo "kernel.msgmnb = 65536" >> /etc/sysctl.conf
echo "kernel.sem = 250 256000 32 1024" >> /etc/sysctl.conf
echo "kernel.shmmax = 1268435456" >> /etc/sysctl.conf
```

NOTE: These are the minimum values required to install EKM 3.0 on Linux. EKM 3.0 may need more shared memory (kernel.shmmax) in order to install successfully. If the install fails, then uninstall EKM 3.0, increase kernel.shmmax by approximately 25%, and reinstall EKM 3.0. To uninstall EKM 3.0, refer to Uninstalling EKM 3.0.

2. Issue the following command so that the system uses the new shared memory size immediately (otherwise, you must reboot):

```
sysctl -p
```

DB2 User Already Exists as Regular User

The user name provided for the **DB2 User Name** field already exists as a user on the system. Choose a different user name.

Existing TKLM or EKM 3.0 on the Same System

TKLM or EKM 3.0 is already installed. Uninstall the existing instance or install EKM 3.0 on another system.

Existing DB2 on the Same System

DB2 is already installed. Uninstall DB2 or install EKM 3.0 on another system.

ksh Not Installed

The EKM 3.0 installer needs **ksh**. Install **ksh** and then install EKM 3.0. Refer to your operating system's documentation.

Hostname has Special Characters

The hostname of the computer system on which you are installing EKM 3.0 must not contain any spaces or special characters such as hyphens (-) or underscores (_). EKM 3.0 supports only alphanumeric characters in the hostname.

Domain Name

The domain name of the computer system on which you are installing EKM 3.0 must not contain any spaces or special characters such as hyphens (-) or underscores (_). EKM 3.0 supports only alphanumeric characters in the domain name.

Invalid /etc/hosts file

The file **/etc/hosts** must contain a valid entry for the loopback IPv4 address. The entry must be in the following format:

<Loopback IPv4 address><space><fully-qualified hostname><space><short hostname>

Where <*space*> indicates a blank space.

Error Codes

To access a list of error codes and their descriptions, refer to the Documentation and Reference Materials section of the **ReadThisFirst.txt** file on the EKM 3.0 installation media.

Windows Reference Files

You can use the following log files and error files to troubleshoot issues with the EKM 3.0 Windows installation:

- **C:\tklm_install.stderr** (standard error log file)
- **C:\tklmV2properties*.log** (DB2 install log files)
- **C:\Users\Administrator\IA-TIPInstall-00.txt** (EKM 3.0 install log file)

  NOTE: This path applies to Windows Server 2008 versions. For Windows Server 2003 R2 with Service Pack 2, the EKM 3.0 install log file is located at **C:\Documents and Settings\Administrator\IA-TIPInstall-00.txt**.
- **C:\Dell\EKM\products\tklm\logs\audit\tklm_audit.txt** (audit file). (This file can also be used to troubleshoot usage issues in addition to installation issues.)

NOTE: The paths above assume C: as the root drive. Substitute your root drive letter for **C:**.

Linux Reference Files

You can use the following log files and error files to troubleshoot issues with the EKM 3.0 Linux installation:

- **/root/IA-TipInstall_*.log**
- **/tklm_install.stderr** (standard error log file)
- **/tklmV2properties/*.log**
- **/opt/dell/ekm/products/tklm/logs/audit/tklm_audit.log**

Manually Uninstalling EKM 3.0

When uninstalling EKM 3.0, first use the automated uninstall procedure. Refer to Uninstalling EKM 3.0. If the automated uninstall process fails, manually uninstall EKM 3.0.

Manually Uninstalling EKM 3.0 in Windows

If you are reinstalling EKM 3.0 and the installation fails due to an incomplete uninstall, perform the uninstall manually. If any item is already uninstalled, skip that step.

NOTE: If you have the option to reinstall the operating system on your server, Dell recommends that you re-install the operating system and then install EKM 3.0.

NOTE: The paths in this procedure are for Windows Server 2008 versions. Where applicable in this procedure, for Windows Server 2003 R2 with Service Pack 2, navigate to **Start** → **Control Panel** → **Add or Remove Programs** .

1. Navigate to **Start** → **Control Panel** → **Programs (or Programs and Features)** → **Uninstall a Program** . Uninstall IBM DB2 (**DB2 Workgroup Server Edition - DB2TKLMV2**).
2. Navigate to **Start** → **Control Panel** → **Programs (or Programs and Features)** → **Uninstall a Program** .
3. Click **EKM**.
4. Click **Uninstall/Change**.
   The EKM 3.0 uninstall wizard appears.
5. Follow the prompts in the uninstall wizard.
   After EKM 3.0 uninstalls, the system automatically restarts.
6. Navigate to **Start** → **Control Panel** → **Programs** → **Uninstall a Program**. Uninstall **IBM Update Installer for WebSphere software V7.0**.
7. Run the Windows Registry Editor program (Regedit). Navigate to **HKEY_CURRENT_USER** → **Software** → **IBM** → **DB2** → **InstalledCopies**. Delete the **DB2TLKMV2** folder.

   CAUTION: Use caution when editing the registry. If you make an improper change, the system could become unstable.
8. In Windows Explorer, navigate to **<*root*>:\Dell**, if it is present (for example, **C:\Dell**). Delete the **EKM** folder (if it is present) and all of its subfolders (**<*root*>:\Dell\EKM**).
9. On the root drive (for example, **C:**), delete the **tklmV2properties** folder (**<*root*>:\tklmV2properties**).
10. On the root drive, delete the **tklmdbarchive** folder. (**<*root*>:\tklmdbarchive**).
11. On the root drive, delete the folder with the same name as the DB2 user name.
12. On the root drive, delete the **tklm_install.stderr file** (**<*root*>:\tklm_install.stderr**).
13. In Windows Explorer, navigate to **<*root*>:\Program Files (x86)\dell**. Delete the DB2 install directory (**<*root*>:\Program Files (x86)\dell\db2dkm**).

    NOTE: In this step and in the following three steps, if your operating system is a 32-bit operating system, then replace "Program Files (x86)" with "Program Files."
14. In Windows Explorer, navigate to **<*root*>:\Program Files (x86)\ibm**. Delete the **Common** folder (**<*root*>:\Program Files (x86)\ibm\Common**).
15. In Windows Explorer, navigate to **<*root*>:\Program Files (x86)\ibm**. Delete the **gsk8** folder (**<*root*>:\Program Files (x86)\ibm\gsk8**).
16. Navigate to **Start** → **Administrative Tools** → **Computer Management** . In the left pane, navigate to **Local Users and Groups** → **Users** . In the right pane, delete the DB2 administrator account(s).

17. Navigate to **Start** → **Administrative Tools** → **Computer Management** . In the left pane, navigate to **Local Users and Groups** → **Groups** . In the right pane, delete the DB2 administrator groups (**DB2ADMINS** and **DB2USERS**).

18. In Windows Explorer, navigate to **<*root*>:\Users**. Delete the folder that has the same name as the DB2 user name.

19. In Windows Explorer, navigate to **<*root*>:\Users\Administrator**. Delete the **IA-TIPInstall-xx log** text file.

20. Stop and delete any of the following EKM 3.0 Windows services that are installed. To do this, issue the following commands at a command prompt at the root (for example, **C:**) drive. If the service is already stopped, you can skip the "stop" step.

    NOTE: If desired, you can stop and delete the services from the Windows Services utility

    ```
    sc stop "DBTKLM20"
    sc delete "DBTKLM20"
    sc stop "<DB2 user name>"
    sc delete "<DB2 user name>"
    sc stop "DB2GOVERNOR_DB2TKLMV2"
    sc delete "DB2GOVERNOR_DB2TKLMV2"
    sc stop "DB2LICD_DB2TKLMV2"
    sc delete "DB2LICD_DB2TKLMV2"
    sc stop "DB2MGMTSVC_DB2TKLMV2"
    sc delete "DB2MGMTSVC_DB2TKLMV2"
    sc stop "DB2REMOTECMD_DB2TKLMV2"
    sc delete "DB2REMOTECMD_DB2TKLMV2"
    sc stop "DB2DAS00"
    sc delete "DB2DAS00"
    ```

    NOTE: The following service is displayed as **Tivoli Integrated Portal - TIPProfile_Port_<*DB2 port number*>** in the Windows Services utility.

    ```
    sc stop "IBMWAS61Service - TIPProfile_Port_<DB2 port number>"
    sc delete "IBMWAS61Service - TIPProfile_Port_<DB2 port number>"
    ```

    NOTE: The DB2 port number defaults to 16310.

21. Issue the following commands at a command prompt at the root (for example, **C:**) drive:

    ```
    reg delete HKEY_LOCAL_MACHINE\software\classes\installer\Products
    \907E425044C581845A83FCBED0CD5771 /f
    reg delete HKEY_LOCAL_MACHINE\software\classes\installer\Features
    \907E425044C581845A83FCBED0CD5771 /f
    ```

22. Reboot the system.

23. If you want to reinstall EKM 3.0, refer to Performing the EKM 3.0 Installation Procedure.

Manually Uninstalling EKM 3.0 in Linux

If you are reinstalling EKM 3.0 and the installation fails due to an incomplete uninstall, perform the uninstall manually. If any item is already uninstalled, skip that step.

NOTE: If you have the option to reinstall the operating system on your server, Dell recommends that you re-install the operating system and then install EKM 3.0.

In the following procedure, replace the following variables (<*variable*>) with your installation paths or variable names.

- <*DB2_INSTALL_DIR*>: This is the directory you selected for the database installation.
- <*DB2_ADMIN*>: This is the DB2 administrator ID (for example, **ekm_dell1**).
- <*DB2_ADMIN_HOME*>: This is the home directory of the database (also called the database data location).
- <*DB2_DB_NAME*>: This is the database name.

1. Open a terminal session.
2. Remove the DB2 instance by issuing the following commands:

   ```
   cd /opt/dell/ekm/products/tklm/_uninst
   ./removeDB2Inst.sh <DB2_INSTALL_DIR>
   ./removeDB2Inst.sh <DB2_ADMIN>
   ./removeDB2Inst.sh <DB2_ADMIN_HOME>
   ./removeDB2Inst.sh <DB2_DB_NAME>
   ```

   For example:

   ```
   ./removeDB2Inst.sh /opt/dell/db2ekm
   ./removeDB2Inst.sh /ekm_dell1
   ./removeDB2Inst.sh /home/db2ekm
   ./removeDB2Inst.sh /db2ekm
   ```

3. Run TKLM Silent Uninstall with the response file by issuing the following commands:

   ```
   /opt/dell/ekm/_uninst/TIPInstall/uninstall -i silent -f
   /opt/dell/ekm/Uninstall_EKM/dkm_uninstall_response.txt
   ```

4. Remove the log files by issuing the following commands:

   ```
   rm -rf /tklmV2properties
   cd /opt/dell/ekm/
   rm tklm_install.stderr
   rm IA-TIPIn*.log
   rm EKM_Install*.log
   ```

5. Remove the DB2 user ID from the system by issuing the following command:

   ```
   userdel -r $DB2_ADMIN$
   ```

   For example:

   ```
   userdel -r ekm_dell1
   ```

6. Remove DB2 from the system by issuing the following commands:

   ```
   cd /opt/dell/ekm/install
   ./db2_deinstall -a
   ```

7. Remove the parent directory used for EKM 2.X merge/migration and the EKM 3.0 installation.

   ```
   rm -rf /opt/dell/ekm
   ```

8. Reboot the machine.
9. If you want to reinstall EKM 3.0, refer to Performing the EKM 3.0 Installation Procedure.

Reinstalling EKM 3.0

To reinstall EKM 3.0, perform the following steps:

1. Uninstall EKM 3.0 using the uninstall procedure. Refer to Uninstalling EKM 3.0.

   NOTE: If the machine did not reboot automatically when you uninstalled EKM 3.0, reboot the machine.

2. Reinstall EKM 3.0 using the installation procedure. Refer to Performing the EKM 3.0 Installation Procedure.

   NOTE: If you saved an installation profile during the original EKM 3.0 installation, you can use it to reinstall EKM 3.0. However, if you are using a primary/secondary server configuration, and the installation profile belongs to the secondary EKM 3.0 server, do not use it to reinstall EKM 3.0 on the primary server.

Frequently Asked Questions

Can I install EKM 3.0 in an operating system that is not listed in the Hardware and Software Requirements chapter?

No. EKM 3.0 only supports the operating systems, their versions, editions, service pack levels, and bit levels listed in Hardware and Software Requirements.

Can I copy files from the EKM 3.0 installer onto the hard disk on my system and install from my local system?

No. EKM 3.0 only supports installation from the EKM 3.0 media. Refer to Installing EKM 3.0.

During the EKM 3.0 installation, what do I do when I receive an error message stating that the silent install failed?

Refer to the **tklm_install.stderr** file (standard error log file) for more information. *In Windows*, this file is located at **<*root*>:\tklm_install.stderr**. *In Linux*, it is located at **/tklm_install.stderr**. If an error code is listed in this file, refer to Error Codes.

After you have resolved the error situation described by the error code, perform a manual uninstall. Refer to Manually Uninstalling EKM 3.0. Reboot the system after you have manually uninstalled EKM 3.0, and then reinstall EKM 3.0.

When I reinstall EKM 3.0, what do I do when I receive an error message stating that the installation failed?

Perform a manual uninstall. Refer to Manually Uninstalling EKM 3.0. Reboot the system after you have manually uninstalled EKM 3.0, and then reinstall EKM 3.0.

During the EKM 3.0 installation, what do I do when I receive an error message stating that I do not have Windows Server 2003 R2 SP2 installed?

For a list of supported operating systems, refer to Hardware and Software Requirements. After you have installed the Windows Server 2003 R2 second CD, reboot the system before installing EKM 3.0.

CAUTION: This operation will overwrite the data on the tape media. Once overwritten, the data on the tape media will no longer be accessible.

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 3.0 configuration containing the keys for the tapes to be reused and a PowerVault TL2000 or TL4000.

You cannot overwrite tapes in this manner in the PowerVault ML6000. You can migrate tapes from an ML6000 to a TL2000 or TL4000 for this purpose. You must then point the TL2000 or TL4000 to the appropriate EKM 3.0 server.

To reuse previously-encrypted media, perform the following steps:

1. Ensure that the EKM 3.0 server is running and configured properly.
2. Log into the RMU GUI for the TL2000/TL4000 (administrator/service login is 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, or backup) to the media to be reused.

To verify that the encryption has been overwritten, perform the following steps:

1. Log into 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**.

You can remove or uninstall EKM 3.0 only after all desired media is overwritten. Dell recommends that you perform a backup of critical files in the EKM 3.0 GUI and back up the files to an external source such as a removable drive. This allows EKM 3.0 to be restored if additional tapes must be overwritten.

I am having issues with a new EKM 3.0 installation and need to reinstall. How can I determine if the EKM 3.0 ever provided keys?

1. Open a command prompt and navigate to the audit log file directory.

   In Windows, the audit log is located at **<*root*>:\Dell\EKM\products\tklm\logs\audit\tklm_audit.txt**.

   In Linux, the audit log is located at: **/opt/dell/ekm/products/tklm/logs/audit/tklm_audit.log**.
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 a text editor (for example, WordPad). Search for **Drive Serial Number**. If there is an entry, a key has been provided. If the **volser** entry is blank, this is the result of key path diagnostics, and you should search the file for additional entries associated with the drive serial number to be certain.

CAUTION: If keys have been provided, you must unencrypt the data on the affected media prior to uninstalling EKM 3.0 .

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

When you have enabled library-managed encryption on the tape library and have configured encryption-enabled partitions, changes to the drive settings are made to the drive(s) in those partitions. You must stop and restart the backup application services after the encryption-enabled partitions are configured to ensure the backup application recognizes the encryption setting in the drive(s).

NOTE: The tape backup application will not show encryption as **enabled** if library-managed encryption is used. The tape library will show the partitions as **encryption enabled**. Library-managed encryption is transparent to the tape backup application. The tape backup application only shows encryption as **enabled** if the application (for example, Symantec, CommVault, etc.) is providing the encryption keys to the drive(s).

How does EKM 3.0 handle the addition of new drives or the replacement of bad drive?

You can add new or replacement drives to the EKM 3.0 server through auto-discovery or manually. To add drives through auto-discovery, refer to Adding a Device to a Device Group.

Dell recommends that you use auto-discovery because 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, you can turn auto-discovery on and run test backups or key path diagnostics in the tape library to add the necessary drives to the drive table. Then you can turn off auto-discovery to prevent new drives from obtaining keys. As long as EKM 3.0 can authenticate the digital signature assigned to the drive at the factory, EKM 3.0 accepts the key request. The keys are grouped in the keystore in key groups and you can associate the key groups with the new/replacement drives after the drives are added.

NOTE: If you want to add a device manually, refer to the TKLM documentation. For information on how to access the TKLM documentation, see the Documentation and Reference Materials section of the **ReadThisFirst.txt** file on the EKM 3.0 installation media.

How does EKM 3.0 handle the addition of a new tape library or the replacement of a bad tape library?

In library-managed encryption, the tape library is only a proxy. You can add or replace tape libraries and provide keys as long as the EKM 3.0 can authenticate to the digital signature on the drive. The replacement tape library will need to be licensed for library-managed encryption and configured for use with the existing EKM 3.0.

How is compression affected by encryption and vice versa?

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

Is there a performance impact with encryption?

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

How do I request and use a third-party certificate?

Create a certificate request in EKM 3.0. Send this certificate request to a Certificate Authority. The certificate returned by the Certificate Authority can be imported into EKM 3.0 and used to protect data on an encryption-enabled device, or for SSL communication. Refer to TKLM documentation for more information on how to generate a certificate request,

import the certificate returned, and use it for encryption. For information on how to access the TKLM documentation, see the Documentation and Reference Materials section of the **ReadThisFirst.txt** file on the EKM 3.0 installation media.

Known Issues and Their Resolutions

Issue: I cannot create a backup.

Description:

Using Internet Explorer, you attempt to create a backup of the keystore. When you specify a backup location that does not exist, the backup is not created.

Resolution:

Do one of the following. If the action you try does not work, perform another listed action:

- Enable JavaScript in your browser. If you are using Internet Explorer V8, turn on Compatibility View mode.
- Use another supported browser. Refer to Hardware and Software Requirements for more information.
- Specify a folder that exists. If you want to specify a new folder, create the folder before creating the backup.

Issue: Multiple backups are created at once.

Description:

When you attempt to create a backup of the keystore, multiple backup files are created at the same time. This issue rarely occurs.

Resolution:

All of the backup files have the same contents. You can use any of the backup files for the restore operation.

Issue: I have to enter my login information twice.

Description:

After EKM 3.0 times out (after being idle for about 30 minutes), the first attempt to log back into EKM 3.0 is rejected and you are required to log in a second time.

Resolution:

Enter your EKM 3.0 login information both times.

Issue: The right pane is partially hidden by the navigation pane.

Description:

You are using Internet Explorer. You are accessing the EKM 3.0 **Key and Device Management** screen. You select either the key group or a tape drive. The right pane becomes partially hidden by the navigation pane.

Resolution:

Do one of the following:

- Refresh the screen.
- Maximize the browser.
- Use another supported browser. Refer to Hardware and Software Requirements for more information.

Issue: "Certificate Error" displays at the top of the browser.

Description:

You are using Internet Explorer 8 in Compatibility View mode. You import a certificate of authority successfully, but **Certificate Error** displays at the top of the screen next to the URL bar.

Resolution:

Do one of the following:

- Ignore the error. This error does not impact EKM 3.0 performance.
- Use a different supported browser (for example, Internet Explorer 6.X or Firefox). Refer to Hardware and Software Requirements.

Issue: I cannot sort information in tables.

Description:

Using the Filter fields at the top of the tables on the **Administer Server Certificates**, **Backup and Restore**, and **Credential Store** screens does not sort the items in the tables.

Resolution:

Click the header row of each column to sort the items.

Issue: I cannot enter a description of the backup I created.

Description:

When using Firefox on Windows, you generate a backup. You are not able to enter a description of the backup and a default description is used.

Resolution:

Use a supported version of Internet Explorer. Refer to Hardware and Software Requirements for more information.

Issue: Some actions within the EKM 3.0 GUI cause scripting errors to pop up within the browser.

Description

Scripting errors display within the browser and the requested action does not complete.

Resolution:

Do one of the following. If the action you try does not work, try a different one:

- Enable JavaScript in your browser. If you are using Internet Explorer V8, turn on Compatibility View mode.

  NOTE: You must enable Compatibility View mode after you log into EKM 3.0.
- Use another supported browser. Refer to Hardware and Software Requirements for more information.

Issue: During the uninstall, the progress bar does not show accurate progress.

Description

The uninstall progress bar does not show accurate progress. The bar jumps to approximately 30% at the beginning of the uninstall and remains there for the duration of the uninstall. It then moves to 100% at the end.

Resolution

This is a known issue that does not indicate a problem with the uninstall.

CAUTION: Do not reboot the system or exit from the uninstall.

Issue: The settings for the Key and Device Management screen do not take effect.

Description

On the Key and Device Management screen, when I change the settings for drive communication, the change does not take effect.

Resolution:

After you change the setting for drive communication, stop and start the EKM 3.0 server. The changes will take effect. Refer to Starting and Stopping the EKM 3.0 Server in Windows or Starting and Stopping the EKM 3.0 Server in Linux for more information.

Issue: On a Windows 2008 server, after completing the installation of EKM 3.0, the system tray displays a green icon associated with the installation procedure.

Description

The system tray displays a green icon.

Resolution

This is a known issue that does not affect the usability or reliability of EKM 3.0. When you log out of the system and log back in, the icon will not appear.

Issue: When configuring the installation of EKM 3.0, some fields display a "0".

Description

When configuring the installation of EKM 3.0, some fields display a "0". This happens when you use an installation profile when you install EKM 3.0 and the installation profile is either invalid or has missing fields.

Resolution

Confirm that you are using a valid installation profile.

NOTE: If you fill in the fields manually, you must ensure that the data matches exactly to the original installation, otherwise, the second server cannot be used as a backup server to the first server.

Issue: When creating a backup, a "software exception" error message displays.

Description

When you generate a backup, you receive an error message that there is a software exception.

Resolution

EKM 3.0 has a known limitation on servers that have 24 or more CPUs. You must install the latest universal fixpack for DB2 to resolve this issue.

NOTE: For more information, refer to the Release Notes at: **support.dell.com/manuals**. Navigate to **Software** → **Systems Management** → **Dell Encryption Key Manager** .

Issue: I cannot add roles to a newly-created user when using Internet Explorer V8.

Description

When you log in as an EKM 3.0 administrator, create a new user, and then attempt to add a role to the newly-created user, a JavaScript error displays and the role is not added.

Resolution

Create the user first, then add roles to the user using the **Administrative User Roles** screen. To access this screen, in the navigation pane, navigate to **Users and Groups** → **Administrative User Roles**. You can also resolve this issue by using a supported version of Firefox.

Issue: When I uninstall EKM 3.0, a Java "stack overflow exception" error displays.

Description

When you uninstall EKM 3.0, a Java error displays.

Resolution

Manually uninstall EKM 3.0. Refer to Manually Uninstalling EKM 3.0 for more information.

Issue: The EKM 3.0 uninstall process runs for several hours and does not complete.

Description

When you attempt to uninstall EKM 3.0, the uninstall does not complete.

Resolution

Manually uninstall EKM 3.0. Refer to Manually Uninstalling EKM 3.0 for more information.

Installing the compat-libstdc++ Library

The **compat-libstdc++-33-3.2.3-61** or later library must be installed before installing EKM 3.0 on Linux platforms.

If you receive the following error while installing EKM 3.0 on Linux, you must install **compat-libstdc++** :

```
Your operating system does not have the compat-libstdc++ packaged installed.
```

To install **compat-libstdc++**:

1. In a terminal session, navigate to the **compat-libstdc++** RPM file in the **EKMPREREQLIBS** folder on the EKM 3.0 installation media by issuing the following command:
   ```
   cd /<path_to_EKM_3.0_installation_dvd>/EKMPREREQLIBS
   ```
2. Install **compat-libstdc++** by issuing the following command:
   ```
   rpm -ivh compat-libstdc++*.rpm
   ```

   NOTE: If an error message displays, stating that the **compat-libstdc++** RPM you are attempting to install conflicts with **libstdc++-33** that is already installed, perform the following steps:

   a. Issue the following command:
      ```
      rpm –e libstdc++-33
      ```
   b. Issue the following command:
      ```
      rpm –ivh compat-libstdc++*.rpm
      ```