Dell™ PowerVault™ Encryption Key Manager

Quick Start Guide for LTO Ultrium 4 and LTO Ultrium 5

This guide gets you started with a ***basic configuration*** for encryption on LTO Gen 4 and LTO Gen 5 tape drives. Visit **http://support.dell.com** to download the latest library and drive firmware prior to installing and configuring the Dell PowerVault Encryption Key Manager to ensure that there are no issues.

The Dell PowerVault Encryption Key Manager (referred to as the Encryption Key Manager from this point forward) is a Java™ software program that assists encryption-enabled tape drives in generating, protecting, storing, and maintaining encryption keys. These keys are used to encrypt information being written to, and decrypt information being read from, LTO tape media. The Encryption Key Manager operates on Linux® and Windows®, and is designed to be a shared resource deployed in several locations within an enterprise.

This document shows how quickly you can install and set up the Encryption Key Manager using the graphical user interface (GUI) or using commands. This document shows how to use the JCEKS keystore type because the JCEKS keystore type is the easiest and most transportable of the keystores supported. If you want more information about a particular step or another supported keystore type, see the *Dell Encryption Key Manager User's Guide*, which can be found at: **http://support.dell.com** or on the Dell Encryption Key Manager media provided with your product.

Note: IMPORTANT Encryption Key Manager HOST SERVER CONFIGURATION INFORMATION: It is recommended that machines hosting the Dell Encryption Key Manager program use ECC memory in order to minimize the risk of data loss. The Encryption Key Manager performs the function of requesting the generation of encryption keys and passing those keys to the LTO-4 and LTO-5 tape drives. The key material, in wrapped (encrypted form) resides in system memory during processing by the Encryption Key Manager. Note that the key material must be transferred without error to the appropriate tape drive so that data written on a cartridge may be recovered (decrypted). If for some reason key material is corrupted due to a bit error in system memory, and that key material is used to write data to a cartridge, then the data written to that cartridge will not be recoverable (i.e. decrypted at a later date). There are safeguards in place to make sure that such data errors do not occur. However, if the machine hosting the Encryption Key Manager is not using Error Correction Code (ECC) memory there remains a possibility that the key material may become corrupted while in system memory and the corruption could then cause data loss. The chance of this occurrence is small, but it is always recommended that machines hosting critical applications (like the Encryption Key Manager) use ECC memory.

Do This First: Install Encryption Key Manager Software

1. Insert your Dell Encryption Key Manager CD. If installation does not start automatically in Windows, navigate to the CD and double click on Install_Windows.bat.

   For Linux, installation does not start automatically. Go to the CD root directory and enter `Install_Linux.sh`.

   An end user license agreement is displayed. You must acknowledge this license agreement in order for installation to continue.

   The installation copies all contents (documentation, GUI files, and configuration property files) appropriate to your operating system from the CD to your hard drive. During installation, your system is checked for the correct IBM Java Runtime Environment. If not found, it is automatically installed.

   When installation is complete, the Graphical User Interface (GUI) is started.

Method 1: Set up Encryption Key Manager Using the GUI

This procedure creates a basic configuration. At successful completion the Encryption Key Manager server is started.

1. If the GUI is not started, open it as follows:

   On Windows
   Navigate to c:\ekm\gui and click `LaunchEKMGui.bat`

   On Linux platforms
   Navigate to /var/ekm/gui and enter `. ./LaunchEKMGui.sh`
   Note: Specify . ./ (period space period forward slash) before the Linux shell command to ensure that the shell will be able to find the script.

2. On the EKM Server Configuration page (Figure 1) enter the data in all required fields (indicated by an asterisk *). Click on the question mark to the right of any data field for a description. Click **Next** to go to the EKM Server Certificate Configuration page.

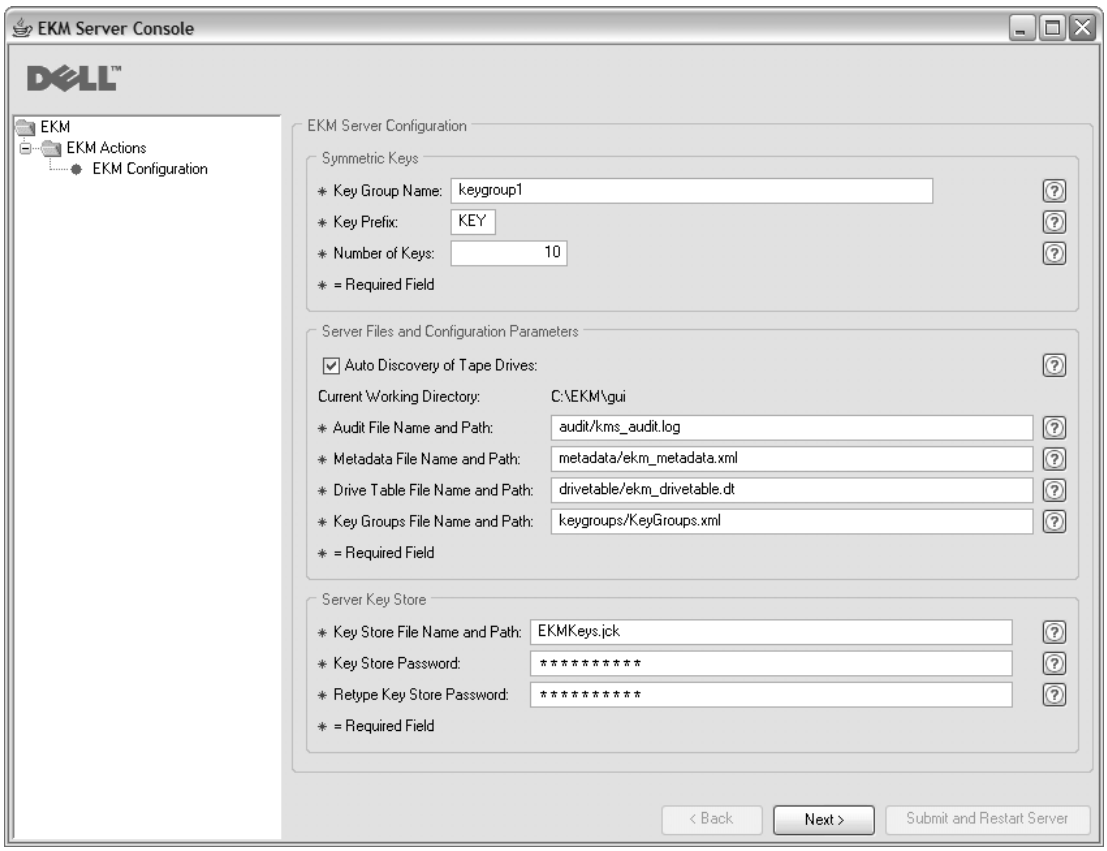

Figure 1. EKM Server Configuration Page

Notes:

a. The Encryption Key Manager server should be refreshed using the GUI after drives are added through auto discovery to ensure that they are stored in the drive table.

b. Once you have set the keystore password, **do not change** it unless it's security has been breached. The passwords are obfuscated to eliminate any security exposure. Changing the keystore password requires that the password on every key in that keystore be changed individually using the **keytool** command. See "Changing Keystore Passwords" in the *Dell Encryption Key Manager User's Guide*.

3. On the EKM Server Certificate Configuration page (Figure 2) enter the key store alias and fill in any additional fields that may serve to identify the certificate and its purpose. Click **Submit and Start Server**.

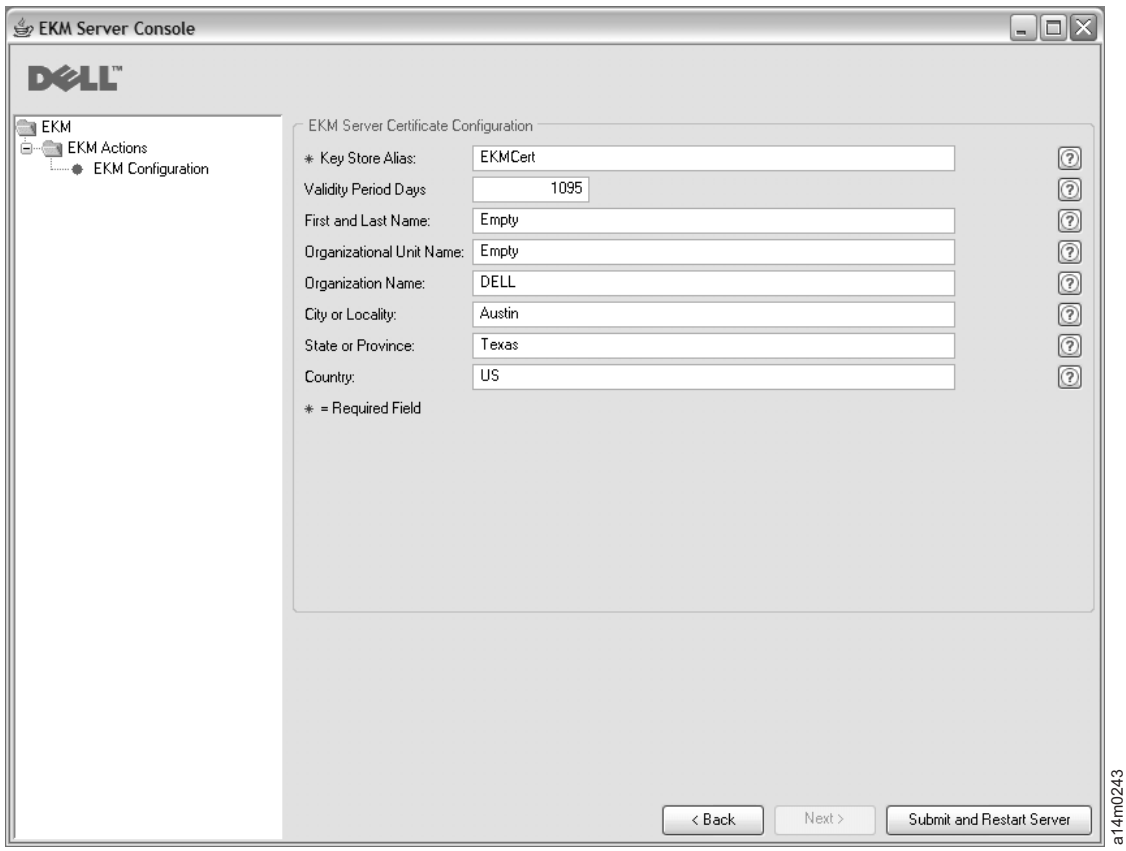

Figure 2. EKM Server Certificate Configuration Page

Note: Interrupting the Encryption Key Manager GUI during key generation requires an Encryption Key Manager re-install.

Keystore file corruption will occur if your stop the Encryption Key Manager key generation process before it is complete. To recover from this event, follow these steps:

- If the Encryption Key Manager was interrupted during the initial install, navigate to the directory where the directory is located (example x:\ekm). Delete the directory and restart the install.
- If the Encryption Key Manager was interrupted while adding a new keygroup, stop your Encryption Key Manager server, restore your keystore file with the latest backup keystore (this file is located in your x:\ekm\gui\backupfiles folder). Note that the backup file contains the date and time stamp as part of the file name (for example, 2007_11_19_16_38_31_EKMKeys.jck). The date and time stamp must be removed once the file is copied into the x:\ekm\gui directory. Restart the Encryption Key Manager server and add the key group that was previously interrupted.

4. A backup window (Figure 3) displays reminding you to back up your Encryption Key Manager data files. Enter the path where backup data is to be saved. Click **Backup**.

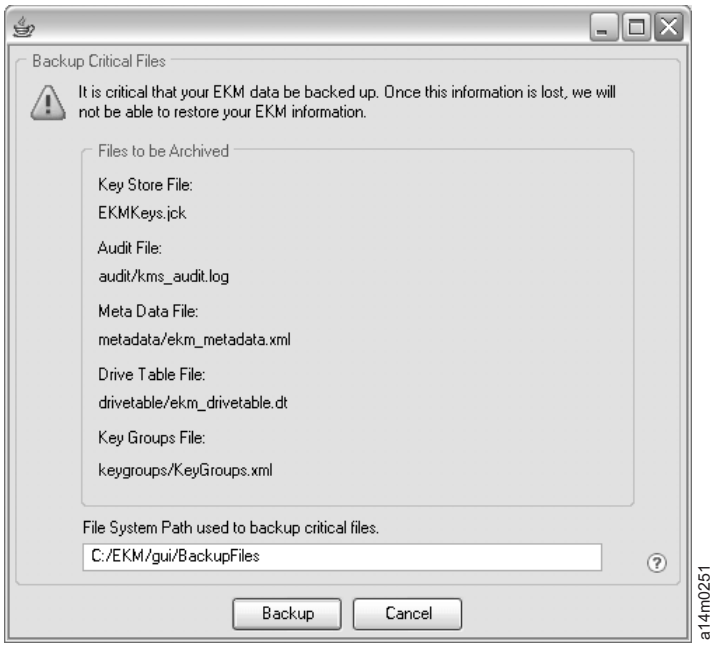

Figure 3. Backup Critical Files Window

5. The User Login page displays. Enter the default user name EKMAdmin and the default password changeME. Click **Login**.

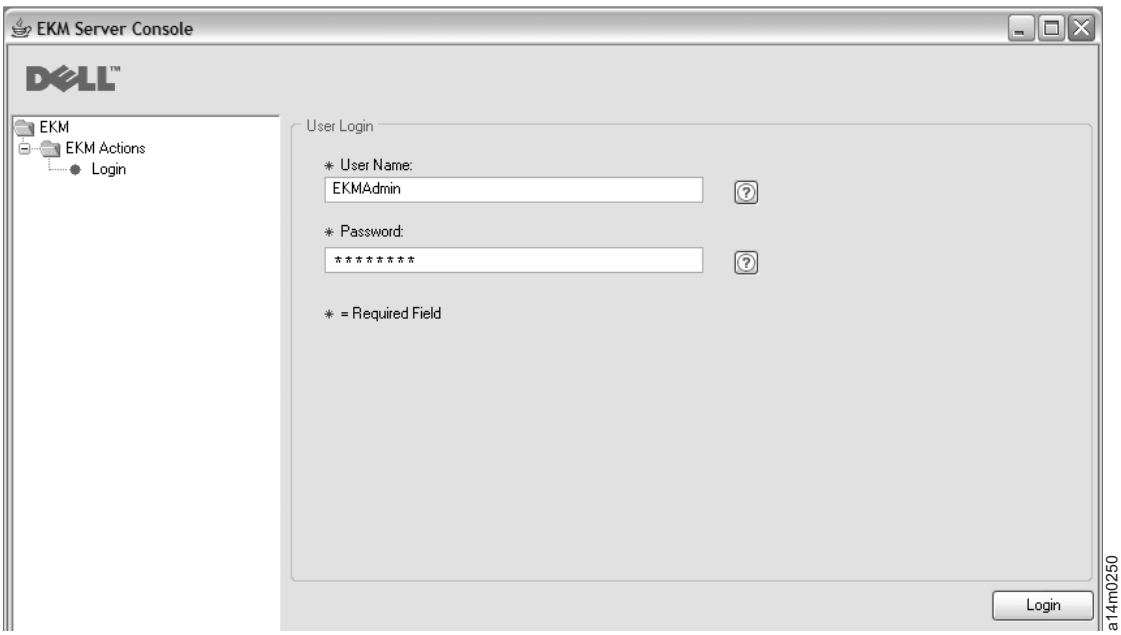

Figure 4. User Login Page

The Dell Encryption Key Manager server is launched in the background.

6. Select **Server Health Monitor** in the GUI navigator to verify that the Encryption Key Manager server is up.

How to Locate the Correct Host IP Address

Limitations in the current Encryption Key Manager GUI may prevent it from displaying the Encryption Key Manager host IP address in the Server Health Monitor:

- If the host is configured with an IPv6 address, the Encryption Key Manager application will not be able to display the IP address.
- If the Encryption Key Manager application is installed in a Linux system, the Encryption Key Manager application displays the localhost address and not the actual active IP port.

a. To retrieve the actual IP address of the host system, locate the IP port address by accessing the network configuration.
   - In a Windows system, open a command window and enter `ipconfig`.
   - For Linux enter `isconfig`.

How to Identify the EKM SSL Port

a. Start the Encryption Key Manager server using the command line.
   - On Windows, navigate to cd `c:\ekm` and click **startServer.bat**
   - On Linux platforms, navigate to `/var/ekm` and enter `startServer.sh`
   - See "Starting, Refreshing, and Stopping the Key Manager Server" in the *Dell Encryption Key Manager User's Guide* for more information.

b. Start the CLI client using the command line.
   - On Windows, navigate to cd `c:\ekm` and click **startClient.bat**
   - On Linux platforms, navigate to `/var/ekm` and enter `startClient.sh`
   - See "Starting the Command Line Interface Client" in the *Dell Encryption Key Manager User's Guide* for more information.

c. Login to a CLI client on the Encryption Key Manager server using the following command:

   ```
   login –ekmuser userID –ekmpassword password
   ```

   where *userID* = EKMAdmin and *password* = changeME (This is the default Password. If you previously changed the default password use your new password.)

   Once login is successful `User successfully logged in` is displayed.

d. Identify the SSL port by entering the following command:

   ```
   status
   ```

   The displayed response should be similar to this: `server is running. TCP port: 3801, SSL port: 443`.

   Make a note of the SSL configured port and ensure it is the port used to configure your library-managed encryption settings.

e. Logout from the command line. Enter the following command:

   ```
   exit
   ```

   Close the command window.

Method 2: Set up Encryption Key Manager Using Commands

Step 1. Create a JCEKS Keystore

CAUTION: It is highly recommended that a copy of the Encryption Key Manager and all associated files be made on a regular basis. If Encryption Key Manager encryption keys are lost or corrupted, there is no method of recovering the encrypted data.

Create a keystore and populate it with a certificate and private key. The certificate is used to secure communications between Encryption Key Manager Servers and with the Encryption Key Manager CLI Client. This **keytool** command creates a new JCEKS keystore called EKMKeys.jck and populates it with a certificate and private key with the alias of ekmcert. This certificate is valid for 5 years. When this

certificate expires, communications between Encryption Key Manager Servers and between the Encryption Key Manager CLI Client and Encryption Key Manager Server may no longer work. Remove the old expired certificate and create a new one as specified in this step.

```
keytool -keystore EKMKeys.jck -storetype jceks -genkey -alias ekmcert -keyAlg RSA -keysize 2048 –validity 1825
```

The keytool command prompts you for information it uses to create a certificate that allows your Encryption Key Manager identification. The prompts, with sample responses, look similar to these:

```
What is your first and last name? [Unknown]:  ekmcert
What is the name of your organizational unit?   [Unknown]:  EKM
What is the name of your organization? [Unknown]:  Dell
What is the name of your City or Locality?   [Unknown]: Austin
What is the name of your State or Province?   [Unknown]:  TX
What is the two-letter country code for this unit? [Unknown]:  US
Is CN=ekmcert, OU=EKM, O=Dell, L=Austin, ST=TX, C=US correct?(type "yes" or "no"):
```

Type `yes` and press Enter.

Step 2. Generate Encryption Keys

Note: Before using the keytool command for the first time in any session, run the **updatePath** script to set the correct environment.

On Windows
Navigate to `cd c:\ekm` and click updatePath.bat

On Linux platforms
Navigate to /var/ekm and enter `. ./updatePath.sh`
Note: Specify . ./ (period space period forward slash) before the Linux shell command to ensure that the shell will be able to find the script.

For LTO encryption, the Encryption Key Manager needs a number of symmetric keys to be pre-generated and stored in a keystore. This **keytool** command generates 32 256-bit AES keys and stores them in the keystore created in step 3. Run this command from the Encryption Key Manager directory to have the keystore file created in that directory. The resulting keys will have the names key0000000000000000 through key000000000000001f.

```
keytool –keystore EKMKeys.jck –storetype jceks –genseckey –keyAlg aes –keysize 256 –aliasrange key00-1f
```

This command prompts you for a keystore password to access the keystore. Enter the desired password and press Enter. Press Enter again when prompted for a key password as that information is not needed. Do not type in a new or different password. This will cause the key password to be the same as the keystore password. Please note the keystore password entered here as it will be needed later when starting the Encryption Key Manager.

Note: Once you have set the keystore password, do not change it unless it's security has been breached. Changing the keystore password requires that all the password properties in the configuration file be changed as well. The passwords are obfuscated to eliminate any security exposure.

Step 3. Start the Encryption Key Manager Server

To start the Encryption Key Manager server without the GUI, launch the startServer script:

On Windows
Navigate to `cd c:\ekm\ekmserver` and click startServer.bat

On Linux platforms
Navigate to /var/ekm/ekmserver and enter `. ./startServer.sh`
Note: Specify . ./ (period space period forward slash) before the Linux shell command to ensure that the shell will be able to find the script.

CAUTION: It is highly recommended that a copy of the Encryption Key Manager and all associated files be made on a regular basis. If Encryption Key Manager encryption keys are lost or corrupted, there is no method of recovering the encrypted data.

Step 4. Start the Encryption Key Manager Command Line Interface Client

To start the Encryption Key Manager CLI client, launch the startClient script:

On Windows
Navigate to `cd c:\ekm\ekmclient` and click startClient.bat

On Linux platforms
Navigate to /var/ekm\ekmclient and enter `. ./startClient.sh`
Note: Specify . ./ (period space period forward slash) before the Linux shell command to ensure that the shell will be able to find the script.

Once the CLI client is successfully logged into the key manager server, you can execute any CLI commands. Use the quit command to shut down the CLI client when you are finished. The client will shut down automatically when unused for 10 minutes. See the *Dell Encryption Key Manager User's Guide*, which can be found at: **http://support.dell.com** or on the Dell Encryption Key Manager media provided with your product, for CLI command information.

For More Information

See the following publications for more information.

- *Dell Encryption Key Manager User's Guide* (included on your Dell Encryption Key Manager CD and available at **http://support.dell.com**).
- The *Library Managed Encryption for Tape* white paper suggesting best practices for LTO tape encryption (available at **http://www.dell.com**).