Setting Up Quantum Encryption Key Manager on Your Scalar i500 Library

Quantum Encryption Key Manager (Q-EKM) is a Java software program that generates, protects, stores, and manages encryption keys. These keys are used by IBM LTO-4 and IBM LTO-5 tape drives to encrypt information being written to, and decrypt information being read from, tape media. The encryption keys pass through the library; therefore encryption is transparent to the applications.

Scalar i500 library support for Q-EKM is an optional, licensed feature that must be enabled from the library in order to begin encrypting data using the IBM LTO tape drive encryption capabilities.

For more information about the Q-EKM server and Q-EKM best practices, please refer to the *Quantum Encryption Key Manager User's Guide*.

Q-EKM Supported Tape Drives and Media

Q-EKM on the Scalar i500 supports encryption on LTO-4 and LTO-5 data cartridges using IBM LTO-4 Fibre Channel tape drives, IBM LTO-4 SAS tape drives, and IBM LTO-5 Fibre Channel tape drives. Q-EKM does not support encryption on other tape drive types or manufacturer brands.

Caution: You must be running Q-EKM version 2.0 (or higher) to support IBM LTO-5 tape drives.

Setting Up Q-EKM On the Library

Step 1: Upgrade Firmware

Upgrade your library and tape drive firmware to the latest released versions.

Step 2: Install the License Key on the Library

1. Obtain a license key for encryption, following the instructions on the *License Key Certificate* you received.
2. Do one of the following:
   - From the operator panel, select **Setup > Licenses**.
   - From the web client, select **Setup > License**.
3. Enter the new Q-EKM license key.
4. Click **Apply**.

   A progress window displays, showing time elapsed. When complete, a green **Success** message appears, and the status changes to “Operation Succeeded.” Encryption Key Management (EKM) is now listed as a feature on the screen. (If a **Failure** message appears, you may have entered an incorrect license key—try again.)
5. Click **Close**.

Step 3: Install Q-EKM on a Server or Servers

You must supply a server or servers on which to install Q-EKM. Quantum Field Services will schedule an appointment to install the software and configure your servers.

> **Note:** Since the i500 library needs to communicate with the Q-EKM server in real time when reading from or writing to an encryption-enabled drive, it is strongly recommended that you use both a primary and secondary Q-EKM server. This way, if the primary server is unavailable at the time the library needs encryption information, the secondary server can handle the request. The Scalar i500 library allows you to configure up to two Q-EKM servers for redundancy/failover purposes.

Step 4: Configure Encryption Settings and Key Server Addresses

Make sure you complete all steps above before proceeding.

1. Unload tape cartridges from all encryption-capable tape drives in the library.
2. From the web client, select **Setup > Encryption > System Configuration**.
3. **Key Server Type:** If this field is visible, select **Q-EKM** from the drop-down list.
4. **Automatic EKM Path Diagnostics**: Enable or disable this feature and set the test interval as desired. You may also specify the number of consecutive missed test intervals required to generate a RAS ticket. For more information, see Automatic EKM Path Diagnostics on page 7.

5 **Secure Sockets Layer (SSL)**: To enable SSL for communication between the library and the key servers, select the **SSL Connection** checkbox. The default is Disabled. If you enable SSL, you must make sure that the **Primary** and **Secondary Key Server Port Numbers** (see below) match the SSL port numbers set on the Q-EKM servers. The default SSL port number is 443.

> **Note:** Keys are always encrypted before being sent from the Q-EKM key server to a tape drive, whether SSL is enabled or not. Enabling SSL provides additional security.

6 In the **Primary Key Server IP Address or Host** text box, enter either:

- The IP address of the primary key server (if DNS is not enabled), or
- The host name of the primary key server (if DNS is enabled).

7 Enter the port number for the primary key server into the **Primary Key Server Port Number** text box. The default port number is 3801 unless SSL is enabled. If SSL is enabled, the default port number is 443.

> **Note:** If you change the port number setting on the library, you must also change the port number on the Q-EKM key server to match or Q-EKM will not work properly. See the *Quantum Encryption Key Manager User's Guide* for information on setting the port number on the Q-EKM key server.

8 If you are using a secondary key server for failover purposes, enter the IP address or host name of the secondary key server into the **Secondary Key Server IP Address or Host** text box.

> **Note:** If you do not plan to use a secondary key server, you may type a zero IP address, 0.0.0.0, into the **Secondary Key Server IP Address or Host** text box, or you may leave this text box blank.

9 If you configured a secondary key server (previous step), enter the port number for the secondary key server into the **Secondary Key Server Port Number** text box. The default port number is 3801, unless SSL is enabled. If SSL is enabled, the default port number is 443.

> **Note:** If you are using a secondary key server, then the port numbers for both the primary and secondary key servers must be set to the same value. If they are not, synchronization and failover will not occur.

10 Click **Apply**.

Step 5: Configure Partition Encryption

Encryption on the Scalar i500 tape library is enabled by partition only. You cannot select individual tape drives for encryption; you must select an entire partition to be encrypted.

Q-EKM partitions can only contain IBM LTO-4 and IBM LTO-5 tape drives.

Caution: You must be running Q-EKM version 2.0 (or higher) to support IBM LTO-5 tape drives.

Data written to encryption-supported and encryption-capable media in Q-EKM-supported tape drives will be encrypted *unless* data was previously written to the media in a non-encrypted format. In order for data to be encrypted, the media must be blank or have been written to using library managed encryption at the first write operation at the beginning of tape (BOT).

Configure the partition(s) as follows:

1 From the web client, select **Setup > Encryption > Partition Configuration**.

A list of all your partitions displays, along with a drop-down menu displaying the encryption method for each partition.

2 If you want to change the encryption method for a partition, make sure that no tape drives in that partition have cartridges loaded in them. If tape drives have cartridges loaded, you cannot change the encryption method.

3 Select an encryption method from the drop-down menu for each partition. (For tape drives that support encryption, the default is **Allow Application Managed.**) The Encryption Method applies to all encryption-capable tape drives and media in that partition.

Encryption Method	Description
Enable Library Managed	**For use with Q-EKM.** Enables encryption support via a connected Q-EKM server for all encryption-capable tape drives and media assigned to the partition.
Allow Application Managed	**Not for use with Q-EKM.** Allows an external backup application to provide encryption support to all encryption-capable tape drives and media within the partition. The library will NOT communicate with the Q-EKM key server on this partition. This is the default setting if you have encryption-capable tape drives in the partition. This option should remain selected ***unless*** you are connecting the library to an external Q-EKM server. **Note:** If you want an external application to manage encryption, you must specifically configure the application to do so. The library will not participate in performing this type of encryption.
Unsupported	Means that no tape drives in that partition support encryption. If **Unsupported** is shown, it will be greyed out and you will not be able to change the setting.

4 Click **Apply**.

5 Save the library configuration (for instructions, see the *Scalar i500 User's Guide*).

Run EKM Path Diagnostics

Perform EKM Path Diagnostics as described in Using EKM Path Diagnostics on page 5.

Using EKM Path Diagnostics

The EKM Path Diagnostics consists of a series of short tests to validate whether the key servers are running, connected, and able to serve keys as required.

Run the Manual EKM path diagnostics any time you change the key server settings or library encryption settings, and when you replace a tape drive. It is recommended that you test each drive that communicates with key manager servers.

The diagnostics consists of the following tests:

> **Note:** The tape drive used for the test must be unloaded and online in order to run any of the tests.

- **Ping** — Verifies the Ethernet communication link between the library and the key servers.
- **Drive** — Verifies the tape drive's path in the library (communication from library to tape drive sled and from tape drive sled to tape drive). The tape drive must be unloaded, ready, and online in order to run this test. If this test fails, the Path and Config tests are not performed.
- **Path** — Verifies that EKM services are running on the key servers. This test cannot run if the Drive test fails.
- **Config** — Verifies that the key servers are capable of serving encryption keys. This test cannot run if the Drive test fails.

If any of the tests fail, try the following resolutions and run the test again to make sure it passes:

- **Ping Test Failure** — Verify that the Q-EKM server host is running and accessible from the network to which the library is connected.
- **Drive Test Failure** — Look for any tape drive RAS tickets and follow the resolution instructions in the ticket.
- **Path Test Failure** — Verify that the Q-EKM server is actually running and that the port/SSL settings match the library configuration settings.
- **Config Test Failure** — Verify that the Q-EKM server is set up to accept the tape drive you are testing.

Differences Between Manual and Automatic EKM Path Diagnostics

There are two ways to perform EKM Path Diagnostics:

- Manual EKM Path Diagnostics
- Automatic EKM Path Diagnostics

The Manual diagnostics differs from the Automatic diagnostics in the following ways:

- The Manual diagnostics takes affected partitions offline.
- The Automatic diagnostics does not take partitions offline, but it may delay moves to tape drives while they are being tested.
- The Manual diagnostics requires that you select one tape drive to use for the test. Since the test only validates the selected drive, if you want to test the path for each tape drive, you must run the test multiple times (once for each drive). In addition, if the tape drive is not available (it must be unloaded, ready, and online), the Drive, Path, and Config tests are not performed.
- The Automatic diagnostics tests every connected EKM server in turn, and the library selects the tape drive to use for each test. If the selected tape drive is not available (it must be unloaded, ready, and online), then the library tries another tape drive that is connected to the key server until it finds one that is available. If no tape drives connected to a particular key server are available, then that server is skipped and the tests are not performed. If a server is skipped for "X" number of consecutive test intervals (where "X" is configurable on the Web client), the library generates a RAS ticket. If a tape drive remains loaded for a long time, it is possible that it will never be tested. If you want to test a specific tape drive, then you should use the Manual EKM Path Diagnostics. In particular, if you replace a tape drive, run the Manual EKM Path Diagnostics.

Manual EKM Path Diagnostics

To perform the diagnostics:

1. Access the Q-EKM Path Diagnostics screen in one of two ways:

   - Enter library Diagnostics (select **Tools > Diagnostics**) and then select **EKM > EKM Path Diagnostics**. Note that entering Diagnostics will log off all other users of the same or lower privileges and take your partitions offline. When you exit Diagnostics, the partitions automatically come back online.
   - Select **Setup > Encryption > System Configuration** or **Setup > Encryption > Partition Configuration** and click the link that says "Click here to run EKM Path Diagnostics." Note that performing this action takes the partition in which the selected tape drive resides offline. When the test completes, the partition automatically comes back online.

   A list of all the tape drives enabled for library-managed encryption is displayed, along with the tape drive status and the partition in which each tape drive resides.

2. Select the tape drive on which you want to perform diagnostics and click **Apply**. Tape drives must be unloaded, ready, and online in order for the test to run.

   A dialog box appears telling you that the selected partition will be taken offline.

3. Click **OK** to start the diagnostics.

   The library performs the diagnostics and reports pass/fail results on each of the tests in the Progress Window.

   Note: The diagnostics tests may take several minutes to complete.

4. Do one of the following:

- If **Completed** appears in the Progress Window, the diagnostics were performed (this does not mean that the diagnostics passed, just that the diagnostics were performed). Click **Close** to close the Progress Window.
- If **Failure** appears in the Progress Window, the diagnostics were not able to be performed. Follow the instructions listed in the Progress Window to resolve any issues that occurred during the operation.

Automatic EKM Path Diagnostics

You can enable the library to automatically perform EKM Path Diagnostics at selected intervals. During each interval, the library tests every configured key server. The library generates a RAS ticket if there are problems. By default, this feature is disabled and the test interval is 10 minutes. It is recommended that you leave Automatic EKM Path Diagnostics disabled, unless network interruptions are a common cause of encryption failures at your site.

Caution: Running Automatic EKM Path Diagnostics may cause an increase in RAS tickets if tests are skipped due to tape drives being unavailable for a configurable number of consecutive test intervals. To reduce the occurrences of RAS tickets, you can specify the number of consecutive test intervals required to generate a RAS ticket to a higher number, or you can set the library to never generate a RAS ticket for missed test intervals.

For a list of tests performed, seeUsing EKM Path Diagnostics on page 5.

To enable Automatic EKM Path Diagnostics:

1. From the Web client, select **Setup > Encryption > System Configuration**.
2. Select the **Automatic EKM Path Diagnostics** check box.
3. Select a test interval from the drop-down list.
4. Specify the number of consecutive, missed test intervals required before the library generates a RAS ticket informing you that the test could not be performed within the specified intervals.

Backing Up Keystore Data

Due to the critical nature of the keys in your keystore, it is vital that you back up your keystore data on a non-encrypted device so that you can recover it as needed and be able to read the tapes that were encrypted using those encryption keys associated with that tape drive or library.

Viewing Tape Drive Encryption Settings

You can view the encryption settings in the following ways:

- **System Information Report** — To view encryption information on all key servers, partitions, and tape drives, select **Reports > System Information** from the web client. For more information, see the *Scalar i500 User's Guide*.
- **Library Configuration Report** — To view the encryption status of a selected tape drive or tape cartridge, select **Reports > Library Configuration** from the web client and click a tape drive or slot. The encryption status is displayed in a pop-up status window. For more information, see the *Scalar i500 User's Guide*.
- **Partition Encryption** — From the web client, select **Setup > Encryption > Partition Configuration** to view and change the encryption status of partitions. See Step 5: Configure Partition Encryption on page 4 for more details.

Made in the USA. Quantum Corporation provides this publication "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Quantum Corporation may revise this publication from time to time without notice.