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 tape drives to encrypt information being written to, and decrypt information being read from, tape media. The encryption keys pass through the library-to-drive interface; 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-4 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 data cartridges using IBM LTO-4 Fibre Channel and SAS tape drives. Q-EKM does not support encryption on other tape drive types or manufacturer brands, even if they are assigned to a partition selected for encryption.

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 Q-*EKM 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." Q-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 Q-EKM Server TCP/IP Addresses

Make sure you complete Steps 1 through 3 above before proceeding.

1. From the web client, select **Setup > Encryption > System Configuration**.
2. If you want to enable Secure Sockets Layer (SSL) for communication between the library and the Q-EKM servers, select the **SSL for Q-EKM Servers** "Enable" checkbox. The default is Disabled. If you enable SSL, you must make sure that the primary and secondary Q-EKM 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 server to a tape drive, whether SSL is enabled or not. Enabling SSL provides additional security.

3 In the **Primary Q-EKM IP Address or Host** text box, enter either:

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

4 Enter the port number for the primary Q-EKM server into the **Primary Q-EKM 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 for the Q-EKM server from the default setting on the library, you must also change the port number on the Q-EKM 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 server.

5 Optionally, enter the IP address or host name of the secondary Q-EKM server into the **Secondary Q-EKM IP Address or Host** text box.

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

6 If you configured a secondary Q-EKM server (previous step), enter the port number for the secondary Q-EKM server into the **Secondary Q-EKM 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 Q-EKM server, then the port numbers for both the primary and secondary Q-EKM servers must be set to the same value. If they are not, synchronization and failover will not occur.

7 Click **Apply**.

The Progress Window opens. The Progress Window contains information on the action, elapsed time, and status of the operation. Do one of the following:

- If **Success** appears in the Progress Window, the Q-EKM system settings were successfully configured. Click **Close** to close the Progress Window.
- If **Failure** appears in the Progress Window, the Q-EKM system settings were not successfully configured. Follow the instructions in the Progress Window to resolve any issues that occurred during the operation.

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.

If you encrypt a partition, all Q-EKM-supported tape drives in that partition are enabled for encryption. Any non-Q-EKM-supported tape drives in that partition are not enabled for encryption, and data written to non-supported media is not encrypted.

Data written to encryption-supported 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 on a partition, make sure that no tape drives in that partition have cartridges in them. If they do, 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 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**.

The Progress Window appears. The Progress Window contains information on the action, elapsed time, and status of the requested operation. Do one of the following:

- If **Success** appears in the Progress Window, the encryption system settings were successfully configured. Click **Close** to close the Progress Window.
- If **Failure** appears in the Progress Window, the encryption system settings were not successfully configured. Follow the instructions listed in the Progress Window to resolve any issues that occurred during the operation.

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

Using Q-EKM Path Diagnostics

The Q-EKM Path Diagnostics consists of a series of tests between a selected tape drive and the primary and secondary Q-EKM servers. It is a good idea to test each tape drive that communicates with Q-EKM servers.

Run this test any time you change the Q-EKM server settings or library encryption settings.

The diagnostics consists of the following tests:

- Ping — Verifies the Ethernet communication between the library and the Q-EKM 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).
- Path — Verifies that Q-EKM services are running on the Q-EKM servers.
- Config — Verifies that the Q-EKM servers are capable of serving encryption keys to the selected tape drive.

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 **Q-EKM > Q-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** and click the link that says "Click here to run Q-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**.

   A dialog box appears telling you that the selected partition will be taken offline.
3. Click **OK** to start the diagnostics.

   The Progress Window appears. The Progress Window contains information on the action, elapsed time, and status of the requested operation.
4. 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.

5. 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 the library is on.
   - **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.

6 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.

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 certificates associated with that tape drive or library.

Viewing Tape Drive Encryption Status

You can view the encryption status in the following ways:

- System Information Report
- Library Configuration Report
- Partition Encryption
- Licenses

System Information Report

To view the encryption status of partitions and tape drives, select **Reports > System Information** from the web client.

- The **Library Partitions** section shows the encryption method of each partition.
- The **Drives** section shows the type of encryption enabled on each tape drive.

Library Configuration Report

To view the encryption status of a tape drive or tape cartridge:

1. From the web client, select **Reports > Library Configuration**.
2. Click on a tape drive or slot.

   The encryption status is displayed in a pop-up status window.
3. Click **Close** to close the pop-up status window.

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 3 for more details.

Licenses

You can see if Q-EKM is enabled by viewing the licenses screen as follows:

- From the operator panel, select **Setup > Licenses**.
- From the web client, select **Setup > License**.