Quantum Key Manager

# Quantum Key Manager Quick Start Guide

## Server Setup, Library Configuration, and TLS Certificate Installation

This quick start guide provides basic installation and configuration instructions for the Quantum Key Manager (QKM). QKM requires the use of two servers. Each server comes with two hard disk drives that are configured as RAID 1 (mirrored) to protect your keystore and metadata in case one hard disk drive fails. For more information, see the *Quantum Key Manager User's Guide* (PN 6-66531-xx) on the *Quantum Key Manager Documentation CD*.

> **Caution:** The server appliances are designed for one purpose only — to store and manage your encryption keys. Do not install additional hardware, software, files, or operating systems on the server. Doing so can make the server unusable and will void your warranty.

Perform all of the following steps, **in order,** before you begin encrypting tapes.

## Items Required for Setup

You need the following to install and configure each QKM server:

- QKM server (each comes with two hard disk drives installed).
- Power cord (supplied).
- Rackmount kit (supplied).
- Ethernet cable, crossover (for initial configuration, not supplied).
- Ethernet cable, standard (for standard operation, not supplied).
- Laptop or PC, to connect to each server to perform initial configuration.
- The most recent library firmware installed on your library. (Minimum versions required: **Scalar i500: 570G**; **Scalar i2000: 595A**.)
- For Microsoft ® Windows®, you may need to install a utility to use secure shell (SSH) and secure file transfer protocol (SFTP). Two such utilities are PuTTY, available at http://www.chiark.greenend.org.uk/~sgtatham/putty/ and WinSCP, available at http://winscp.net.

## Contents

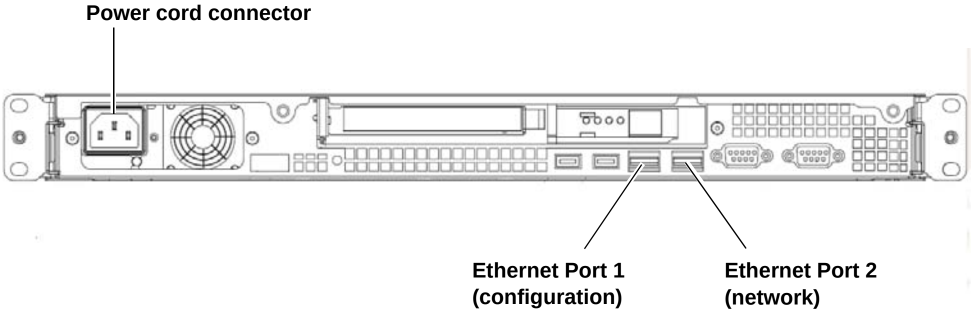
www.quantum.com

# Step 1: Installing the QKM Servers

Follow the instructions below for **both QKM servers**.

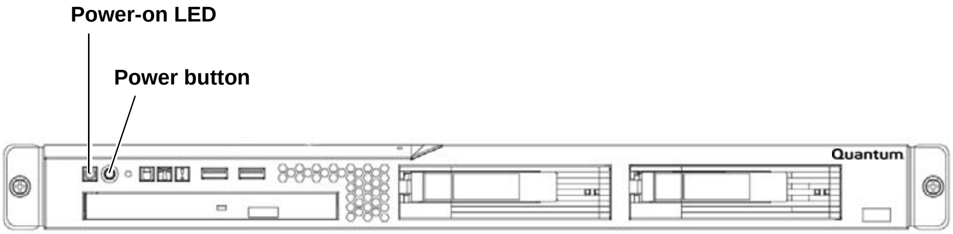
1. Determine the location for the servers. It is recommended that the two servers be in different geographical locations for disaster recovery purposes. Ensure the air temperature is below 95 °F (35 °C).
2. Install the QKM server in a rack. Follow the *Rack Installation Instructions* (included with the rail kit and located on the *Quantum Key Manager Documentation CD*).
3. Connect the power cord into the rear of the QKM server (see Figure 1) and plug it into a grounded power outlet.

Figure 1 Rear Panel



4. Approximately 20 seconds after you connect the server to AC power, the power button becomes active, and one or more fans might start running loudly for about 20 seconds. Observe the Power-on LED on the front panel of the QKM server (see Figure 2). It should be flashing, indicating the server is turned off and connected to an AC power source. If the LED is not flashing, there could be a problem with the power supply or the LED. Check the power connection. If this LED still does not flash, contact Service.
5. Turn on the QKM server by pressing the power button on the front of the server (see Figure 2).

Figure 2 Front Panel



6. Again observe the Power-on LED on the front panel of the QKM server. Wait until it is on but not flashing, indicating the server is turned on.
7. Wait about 3 minutes to allow the server to complete startup before you connect via SSH in the next step.

# Step 2: Configuring the QKM Servers

Follow the instructions below for **both QKM servers**.

> **Note:** Both servers must be configured and connected to the network before you can configure any libraries that will be using them.

The configuration process requires you to read and accept the end user license agreement, and then complete a setup wizard. The setup wizard helps you configure your password, IP address, netmask, gateway, time zone, date, and time. Before beginning, decide what you want each of these values to be. You can also change these values in the future.

Allow 30 minutes per server to complete the configuration.

1 Connect a crossover Ethernet cable from a laptop or PC to **Ethernet Port 1** on the rear of the QKM server (see Figure 1).

> **Note:** Ethernet Port 1 is used only for configuration. Once you perform the initial configuration, you will use Ethernet Port 2 for QKM server communication via your network.

2 Using SSH, connect to the server using the IP address **192.168.18.3**.

> **Note:** The IP address of Ethernet Port 1 is a static IP address that cannot be changed.

3 At the login prompt, enter the user login ID (which will never change):

**akmadmin**

4 At the password prompt, enter the default password:

**password**

5 At the command prompt, enter:

**./qkmcmds**

The End User License Agreement displays.

6 Read and accept the license agreement. Press **<Enter>** to scroll through the agreement, and at the end, enter **y** to accept.

7 Press **<Enter>** to begin the setup wizard.

8 At the password prompt, enter the default password again:

**password**

9 The first setup wizard task prompts you to change your password. There is only one password for QKM, which is required for all login and access to Admin commands, including backup and restore. **If you lose the password, there is no way to retrieve it.**

If you do not wish to change the password at this time, just press **<Enter>** and the default password (**password**) remains. You can change the password at any time later using the Admin commands menu.

**EXTREMELY IMPORTANT:**
**Remember Your Password!**

**If you forget your password, there is no way to retrieve it!**

**Each QKM server has its own password.**
**If you set them differently, you must remember both.**

**If you forget your password, you will lose login access to the QKM server, including backup and restore capability. Quantum will NOT be able to restore the password.**

**CAUTION! CAUTION! CAUTION! CAUTION! CAUTION!**

10 Continue through the setup wizard to configure the rest of the settings: time zone, date and time, QKM server IP address, netmask, and gateway. If you press **<Enter>** without entering a value, the existing value remains.

**Note:** The IP address you are configuring is for Ethernet Port 2, the port you will be using for QKM operations.
**Ethernet Port 1 IP Address** (never changes): 192.168.18.3
**Ethernet Port 2 Default IP Address**: 192.168.18.4

11 When the setup wizard is complete, press **<Enter>**.

The list of QKM Admin commands displays. If you made any mistakes during the setup wizard, you can go back and change them by entering the number corresponding to the item. To view the list at any time, enter **./qkmcmds** at the command prompt.

12 Enter **q** at the command prompt to save your changes and restart the QKM key server process. This process takes a few seconds.

13 Disconnect the crossover Ethernet cable from **Ethernet Port 1**.

14 Connect a standard Ethernet cable from **Ethernet Port 2** on the back of the QKM server to your network (see Figure 1). You will connect to this port using the IP address assigned in step 10 above.

15 Repeat the above steps on the other server in the QKM server pair.

## Step 3: Installing the EKM License on the Library

Make sure that you purchased enough license capacity to cover all the tape drives that you will be using for library-managed encryption. If you want more than one library to use QKM, you must install a separate license on each library.

If you purchased QKM at the same time as your library, then your Encryption Key Management (EKM) license may already be installed on the library. If it is, you can skip this step. You can check the **Licenses** page on the library interface to see if the EKM license is installed.

If you purchased QKM separately from the library, you will receive, separately, instructions on how to obtain your license key and install it on the library. Follow the instructions to install your license key. If you have any questions, contact Service.

## Step 4: Scheduling Sufficient Time for Configuring the Library and Generating Keys

All of the steps that follow deal with configuring your library for QKM and generating encryption keys. Depending on the size of your library, it may take up to 2 hours to complete all of the following steps.

**Caution:** Do not perform any library or host-initiated operations on the partitions to be used for QKM until all of the following steps are complete.

Also, please note that you cannot perform the following configuration steps **until all previous steps have been completed.**

# Step 5: Preparing QKM Partitions on the Library

1. Install HP LTO-4 tape drives in the library, if not already installed.
2. Ensure that the partitions you want to configure for QKM contain **only** HP LTO-4 tape drives.
3. On the HP LTO-4 tape drives, install the latest version of firmware that is qualified for the library firmware installed on your library. Refer to the library release notes for the correct version of tape drive firmware.

# Step 6: Configuring the QKM Server IP Addresses on the Library

1. On the library's remote web client, navigate to the encryption server setup screen:
   - Scalar i500 menu path: **Setup > Encryption > System Configuration**
   - Scalar i2000 menu path: **Setup > Encryption > Server Configuration**
2. Select **QKM** from the **Key Server Type** drop-down list.
3. Enter the QKM primary and secondary server IP addresses or hostnames in the fields provided.

Refer to your library user's guide or online help for detailed instructions.

# Step 7: Installing the QKM TLS Certificates

The TLS certificates allow the library to communicate with the QKM servers.

### Items Required

- A computer with a CD ROM drive and Internet access.
- The *Quantum Key Manager TLS Certificates CD* (shipped separately from the QKM servers). The CD contains one .tgz file. This .tgz file contains all the certificates that need to be loaded onto your library.

> **Note:** You do not need to open or extract any of the files from the .tgz file.

**Procedure**

1 First check to see if the certificates are already installed on your library. From your library's remote web client, select **Tools > QKM Management > Encryption Certificate > Import.**

On this screen, next to the **Import TLS Certificates** checkbox, there is a line of text stating whether the certificates are currently installed on the library. If the certificates are installed, then you do not need to install them again, and you can skip the rest of this section. If certificates are **not** installed, continue to the next step.

2 Insert the *Quantum Key Manager TLS Certificates CD* into the computer's CD ROM drive.

3 From the library screen that you accessed in step 1 above, select the **Import TLS Certificates** checkbox.

4 Browse to the .tgz file located on the CD. (If desired, you can copy the .tgz file to another location on your computer and browse to it there.)

5 Select the .tgz file and click **Open**.

6 Click **Apply** or **OK**.

7 When the operation completes, make sure the certificates were installed on the library by reading the text next to the **Import TLS Certificates** checkbox. The text should state that the certificates are installed on the library.

# Step 8: Running QKM Path Diagnostics

This is an optional, but recommended, step.

QKM Path diagnostics checks to make sure the key servers are running and communicating with the library. If the library detects any communication issues, or if the TLS certificates are not installed, you receive an error message.

On the library's remote web client, access the diagnostics test as follows:

| | |
|---|---|
| Scalar i500 | **1.** From the menu, click **Setup > Encryption > System Configuration**.<br>**2.** Click the **Click here to run EKM Path Diagnostics** link. |
| Scalar i2000 | **1.** From the menu, click **Setup > Encryption > Server Configuration**.<br>**2.** Click the EKM Path Diagnostics **Test** button. |

Refer to your library documentation or online help for details about the diagnostics.

## Step 9: Configuring the Partitions and Generating Encryption Keys

QKM is enabled at the partition level.

- You must enable library managed encryption on each partition separately.
- Partitions you want to configure for QKM must contain **only** HP LTO-4 tape drives.
- Both QKM servers must be fully configured and up and running.

**1** On the library’s remote web client, navigate to the encryption partition configuration screen. From the menu bar, click **Setup > Encryption > Partition Configuration.**

**2** Select **Enable Library Managed** for each partition on which you will use QKM.

**Note:** When you change the encryption method on a partition, the partition is taken offline. When the change completes, the partition comes back online automatically.

**Note:** If the library encounters any problems accessing the QKM servers, or if the TLS certificates are not installed, the library generates an error message. Correct the error and try again.

**3** **Key generation begins.** When you enable library managed encryption on a partition in the library for the first time, the library automatically triggers each QKM server to generate a set of unique encryption keys. This may take 15 minutes to an hour, depending on the size of your library. The library notifies you when the process is complete.

**4** Wait for the process to complete before continuing to the next step.

## Step 10: Saving the Library Configuration

Save the library configuration. See your library documentation for more details about saving the configuration.

- Scalar i500 menu path: **Tools > Save/Restore Configuration**
- Scalar i2000 menu path: **Tools > Save/Restore**

# Step 11: Backing Up the Keystores

**EXTREMELY IMPORTANT:**
**Back Up Your Keystores!**

**It is critical that you back up both keystores before using the keys to encrypt data.**

**The only way to read encrypted tapes is via the keys in the keystore. If your servers fail without a backup, you will permanently lose access to all your encrypted data.**

**The backup is required for server hardware replacement.**

**CAUTION! CAUTION! CAUTION! CAUTION! CAUTION!**

Once the encryption keys are generated on the primary and secondary key servers, you must back up each keystore separately because they contain different data. If a server fails and needs to be replaced, the backup is required to restore operation.

**Note:** **For multiple libraries accessing the same QKM server pair:** If you are configuring more than one library to use the same QKM servers, be aware that each library triggers the QKM servers to create a set of encryption keys which are added to the keystore. You need to make sure all the keys are included in your backup before you start using those keys. If you are configuring several libraries at the same time, you can wait until all the keys are generated and then perform a single backup of each server, provided that you do not use the keys before you back them up. However, if there is a time delay between the key generation during which you intend to begin serving keys for encryption, you will need to perform multiple backups — one after each key generation session.

Perform the following steps for **each QKM server** separately.

1. Connect to the QKM server using SSH.
2. Log in using the password you created earlier.
3. At the command prompt, enter:

   ```
   ./qkmcmds
   ```

   A message displays alerting you that performing QKM Admin commands will stop the QKM key server process until you quit and exit Admin Commands.

**4** Enter **y** to agree to stop the QKM key server process.

A list of commands displays.

**5** At the command prompt, enter the number or letter corresponding to **Back up keystore**.

All the relevant files that you need to restore your keystore are gathered and placed into two .tgz files.

- /home/akmadmin/QKMApp<SN><date><time>.tgz
- /home/akmadmin/QKMData<SN><date><time>.tgz

**6** Use SFTP to copy the backup files to a desired location.

**Caution:** You must copy these backup files to another location and not just leave them on the QKM server. If the QKM server fails, you can restore the backup from the remote location onto the new server.

**Caution:** **Do not use QKM to encrypt the sole copy of your QKM server keystore backup.** If both servers were to fail, you would not be able to recover the encrypted backup and would lose all data you had stored on all your encrypted tapes.

**7** Press **<Enter>**.

**8** Enter **q** to quit the Admin commands and restart the QKM key server process.

**9** Repeat the above steps on the other server in the QKM server pair.

For assistance contact Quantum Technical Assistance center:

| | |
|---|---|
| North America | +1-800-284-5101 |
| UK, France, and Germany | 00800 4 QUANTUM |
| EMEA | +44 1256 848 766 |

For worldwide support: www.quantum.com/contactsupport

Quantum®

Backup. Recovery. Archive. It's What We Do.

Quantum Corp. (NYSE: QTM) is the leading global storage company specializing in backup, recovery and archive. Combining focused expertise, customer-driven innovation, and platform independence, Quantum provides a comprehensive range of disk, tape, media, and software solutions supported by a world-class sales and service organization. As a long-standing and trusted partner, the company works closely with a broad network of resellers, OEMs, and other suppliers to meet customer's evolving data protection needs.