

Quantum[®]

User's Guide

Scalar Key Manager 2.7



Quantum Scalar Key Manager 2.7 User's Guide, 6-66531-12 Rev B, February 2020, Product of 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.

COPYRIGHT STATEMENT

© 2020 Quantum Corporation. All rights reserved.

Quantum, the Quantum logo, DLT, DLTape, the DLTape logo, SuperLoader, Scalar, DXi, StorageCare, StorNext, GoProtect, and Vision are registered trademarks of Quantum Corporation and its affiliates in the United States and/or other countries. All other trademarks are the property of their respective owners. Quantum specifications are subject to change.



Contents

Preface

xiii

Chapter 1

Overview

1

Library Managed Encryption 2

How SKM Key Management Works 3

Encryption Keys 4

Encryption Certificates. 5

Keystore 6

Mirrored Hard Disk Drives 6

Why You Need to Back Up Your SKM Servers 7

Chapter 2

Planning Your SKM Environment

9

SKM Server Requirements 9

Multiple Libraries Accessing One SKM Server Pair 11

Disaster Recovery Planning 12

<hr/>		
Chapter 3	Using the SKM Appliance Server	15
	Safety	15
	SKM 2.7 Appliance Server (and later versions).	17
	SKM 2.6 Appliance (and Earlier Versions)	19
	Powering On the SKM Appliance Server	26
	Powering Off the SKM Appliance Server	26
<hr/>		
Chapter 4	Initial Configuration and Setup	27
	Installing and Configuring the SKM Appliance Servers	28
	Installing and Configuring the SKM VM Servers	39
	Installing and Configuring the SKM KVM Servers	49
	Installing TLS Certificates on the SKM Server for Pre-SKM 2.4 (240Q) .	59
	Installing TLS Certificates on the SKM Server for SKM 2.4 (240Q) or Later	70
	Configuring Your Library For SKM	83
	Configuring Multiple Libraries	90
	Backing Up the Servers	90
<hr/>		
Chapter 5	Logging On and Changing the Configuration	91
	Logging on to the Command Line Interface	92
	Accessing SKM Admin Commands	93
	Quitting SKM Admin Commands.	95
	Logging Off of the SKM Server Command Line Interface.	95
	Running the Setup Wizard.	96
	Changing the Password.	97
	Changing the IP Address	98
	Changing the Time Zone	99
	Changing the Date and Time.	100

	Changing the Hostname	100
	Displaying and Installing TLS Communication Certificates on the SKM Server	101
Chapter 6	Backing Up and Restoring the SKM Server	103
	Backing Up the SKM Server	103
	Restoring the SKM Server	107
Chapter 7	Retrieving SKM Reports, Logs, and Information	111
	Command Line Operations	112
	Displaying the Command Line Help Menu.	112
	Viewing the SKM Server Software Version.	113
	Capturing SKM Server Logs and Snapshots	114
	Displaying the End User License Agreement	116
	Turning Trace Level Logging On and Off	117
	Displaying SKM Server Reports	117
	Viewing the SKM Encryption Key Import Warning Log	127
	Running the Specified Reports Option Only (O 1-6).	127
Chapter 8	Using the Library to Initiate SKM Functions	135
	Generating Data Encryption Keys	136
	Importing TLS Communication Certificates on the Library.	139
	Exporting and Importing Data Encryption Keys.	140
	Exporting and Importing Encryption Certificates.	140
	Sharing Encrypted Tapes Offsite	141
	Running EKM Path Diagnostics	142
Chapter 9	Using the SKM Server to Initiate SKM Functions	143

Sharing Encrypted Tapes Offsite	144
Exporting and Importing Encryption Certificates.	146
Exporting and Importing Encryption Keys	149

Chapter 10	Troubleshooting	159
	Frequently Asked Questions	159
	LED Error Indicators.	161
	Library RAS/Diagnostic Tickets	165
	POST Error Codes.	166
	Troubleshooting Guide	166
	Locating the SKM Server Serial Number	170

Chapter 11	Replacing the SKM Server and its Components	173
	Replacing a Hard Disk Drive.	174
	Replacing an SKM Appliance Server and Both Hard Disk Drives.	181
	Reinstalling an SKM VM Server	183

Chapter 12	Upgrading and Rolling Back SKM Server Software	187
	Upgrading to Version 2.6 or 2.7 and Later Versions	188
	Upgrading to Version 2.5	196
	Upgrading to Version 2.4	208
	Upgrading to Version 2.3	209
	Upgrading to Version 2.2	209
	Upgrading to Version 2.0	211
	Upgrading from Version 1.0 to Version 1.1.	211
	Installing the Import/Export Utility	213
	Rolling Back SKM Server Software.	216

Chapter 13 Module	Updating the SKM Keystore After Replacing a Library Control 221	
	Running the Library Serial Number Replacement Script on SKM 1.0 and 1.1 Servers (Version 100G or 110G)	222
	Running the Library Serial Number Replacement Script on SKM 2.x Servers (Version 200G)	226
	Locating the Serial Number of the Control Module/Chassis.	229
<hr/>		
Appendix A	Specifications	239
<hr/>		
Glossary		245
<hr/>		
Index		249



Figures

Figure 1	SKM 2.7 Appliance Server Front Panel	18
Figure 2	SKM 2.7 Appliance Server Rear Panel.	18
Figure 3	LED Location on Front of SKM 2.7 Appliance Server	19
Figure 4	Front Panel Buttons, LEDs, and Connectors	20
Figure 5	Rear Panel Connectors	22
Figure 6	Rear Panel LEDs	25
Figure 7	SKM 2.7 Appliance Server Rear Panel.	30
Figure 8	SKM 2.6 Appliance Server Rear Panel.	31
Figure 9	SKM 2.7 Appliance Server Front Panel	32
Figure 10	SKM 2.6 Appliance Server Front Panel	33
Figure 11	Changing the Password	36
Figure 12	SKM Admin Commands	37
Figure 13	Configuring the MAC Address (Example).	43
Figure 14	Video Card Settings	44
Figure 15	Changing the Password	47
Figure 16	SKM Admin Commands	48
Figure 17	Changing the Password	56
Figure 18	SKM Admin Commands	58

Figure 19	Example of Quantum Certificate Bundle Displayed on Screen	69
Figure 20	EKM Path Diagnostics PASSED Window	85
Figure 21	SKM Admin Commands (Example)	94
Figure 22	Help Menu	113
Figure 23	Software Version	114
Figure 24	SKM Server Reports Menu	118
Figure 25	SKM Server Keys	119
Figure 26	Keys and Aliases	120
Figure 27	Template Information With Next Increment Identified	121
Figure 28	Quantum Reserved Key Information	122
Figure 29	Keys Used Today Information	123
Figure 30	System Status Information	124
Figure 31	System Status "End" Display	125
Figure 32	Used Key Information Selection	126
Figure 33	Used Key Information Selection "a"	126
Figure 34	Help Menu	128
Figure 35	Library and SKM server physical layout	144
Figure 36	SKM 2.7 Appliance Server Front Panel	162
Figure 37	SKM 2.7 Appliance Server Rear Panel	162
Figure 38	LED Location on Front of SKM 2.7 Appliance Server	163
Figure 39	LED Locations on Front of SKM Appliance Server	164
Figure 40	SKM 2.7 Appliance Server Front Panel	175
Figure 41	SKM 2.7 Appliance Server Rear Panel	175
Figure 42	LED Location on Front of SKM 2.7 Appliance Server	176
Figure 43	LED Locations on Front of SKM 2.6 Appliance Server	177
Figure 44	Replacing a Hard Disk Drive in SKM 2.7 Appliance Server	178
Figure 45	Replacing a Hard Disk Drive in SKM 2.6 Appliance Server	179
Figure 46	Sample libreplace.py Script Output, SKM 1.x	225

Figure 47 Sample libreplace.py Script Output, SKM 2.0. 228

Figure 48 Scalar i3 Serial Number Label Location CM 230

Figure 49 Scalar i3 Serial Number Label Location Side. 230

Figure 50 Scalar i3 Serial Number Label Location WebGUI 231

Figure 51 Scalar i3 Serial Number Label Location CM 232

Figure 52 Scalar i3 Serial Number Label Location Side. 232

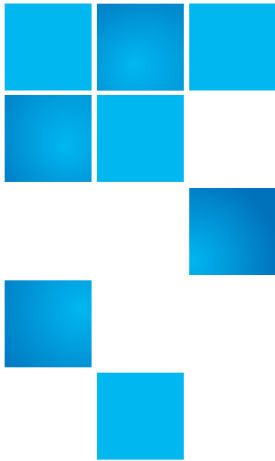
Figure 53 Scalar i6 Serial Number Label Location WebGUI 233

Figure 54 Scalar i40/i80 Serial Number Label and Location 234

Figure 55 Scalar i500 Serial Number Label Location 235

Figure 56 Scalar i500 Serial Number/WWN Label. 235

Figure 57 Scalar i2000/i6000 Serial Number Label and Location . . . 236



Preface

Audience

This book is intended for storage and security administrators responsible for security and backup of vital data, and anyone assisting in the setup and maintenance of Scalar® Key Manager (SKM) servers and software in the operating environment. It assumes the reader has a working knowledge of storage devices and networks.

Purpose

This book contains information to help you install, configure, and run your SKM system.

Document Organization

This document is organized as follows:

- [Chapter 1, Overview](#), provides an overview of tape encryption and the Scalar Key Manager (SKM) components.
- [Chapter 2, Planning Your SKM Environment](#), provides considerations for how to set up your SKM server environment.
- [Chapter 3, Using the SKM Appliance Server](#), discusses safety, hardware, and general operating instructions for the SKM appliance server.
- [Chapter 4, Initial Configuration and Setup](#), provides instructions on how to initially set up and configure the SKM server.

- [Chapter 5, Logging On and Changing the Configuration](#), provides instructions on how to log on, log off, and change the existing SKM server configuration.
- [Chapter 6, Backing Up and Restoring the SKM Server](#), describes how to back up and restore the SKM server.
- [Chapter 7, Retrieving SKM Reports, Logs, and Information](#), describes the various SKM reports and logs and how to access them.
- [Chapter 8, Using the Library to Initiate SKM Functions](#), describes how to use the library to perform vital SKM functions, such as importing and exporting keys and certificates and sharing encrypted tapes offsite.
- [Chapter 10, Troubleshooting](#), provides a list of frequently asked questions and describes how to detect and resolve problems.
- [Chapter 11, Replacing the SKM Server and its Components](#), describes how and under what circumstances to replace an SKM appliance server, a defective hard disk drive, and SKM VM server.
- [Chapter 12, Upgrading and Rolling Back SKM Server Software](#), explains how to update and roll back SKM server software.
- [Chapter 13, Updating the SKM Keystore After Replacing a Library Control Module](#), explains the additional steps you must take when replacing a library control module.
- [Appendix A, Specifications](#), provides hardware, software, and operational specifications for the SKM server.

This document concludes with a [glossary](#) and an [index](#).

Definition of Terms

Scalar Key Manager can be deployed in one of two ways:

- a physical pair of appliances (servers) purchased from Quantum, or
- a pair of virtual machines (VMs) installed in a VMware® or KVM environment.

This guide uses the following terms to differentiate between the two types of deployment:

- **SKM appliance server** — Physical key server purchased from Quantum.

- **SKM VM server** — Virtual machine key server purchased from Quantum and installed in a VMware or KVM environment.
- **SKM server** — Generic term applying to either an SKM appliance server or an SKM VM server.

Notational Conventions

This manual uses the following conventions:

The graphics in this document are representative only and may not reflect your exact installation.

Note: Notes emphasize important information related to the main topic.

Caution: Cautions indicate potential hazards to equipment and are included to prevent damage to equipment.

WARNING: Warnings indicate potential hazards to personal safety and are included to prevent injury.

Product Safety Statements

Quantum will not be held liable for damage arising from unauthorized use of the SKM appliance server hardware. The user assumes all risk in this aspect.

The SKM appliance server is engineered and manufactured to meet all safety and regulatory requirements. Be aware that improper use may result in bodily injury, damage to the equipment, or interference with other equipment.

WARNING: Before operating the SKM appliance servers, read all instructions and warnings in this document and in the Scalar Key Manager Safety Information by Lenovo document located at (Reference Guides)

<https://www.quantum.com/serviceandsupport/softwareanddocumentationdownloads/skm/index.aspx?whattab=Fifth>

Documentation and Software

The following publications provide information related to Scalar Key Manager. For the latest versions of library documents, visit (click on applicable library):

https://qsupport.quantum.com/kb/flare/Content/doc_portal/Content/docs-portal/docs_portal.html

For the latest SKM documentation and firmware updates, see:

<https://www.quantum.com/serviceandsupport/softwareanddocumentationdownloads/skm/index.aspx?whattab=Fifth>

Document No.	Document Title
6-68775-01	Scalar Key Manager Quick Start
6-66572-06	Scalar Key Manager Safety Information by Lenovo
6-66535-03	Scalar Key Manager Open Source License Agreement
6-66545-xx	Scalar i40 and Scalar i80 User's Guide
6-01210-xx	Scalar i500 User's Guide
6-00421-xx	Scalar i2000 User's Guide
6-66879-xx	Scalar i6000 User's Guide
6-68528-xx	Scalar i3 Documentation Center
6-68529-xx	Scalar i6 Documentation Center

Contacts

Quantum company contacts are listed below.

Quantum Corporate Headquarters

For information about contacting Quantum, including Quantum office locations, go to:

<http://www.quantum.com/aboutus/contactus/index.aspx>

Quantum Home Page

Visit the Quantum home page at:

<http://www.quantum.com>

Getting More Information or Help

Quantum. Global Services

StorageCare™, Quantum's comprehensive service approach, leverages advanced data access and diagnostics technologies with cross-environment, multi-vendor expertise to resolve backup issues faster and at lower cost.

Accelerate service issue resolution with these exclusive Quantum StorageCare services:

- **Service and Support Web site** - Register products, license software, browse Quantum Learning courses, check backup software and operating system support, and locate manuals, FAQs, firmware downloads, product updates and more in one convenient location. Benefit today at:

www.quantum.com/support

- **Online Service Center** - Submit online service requests, update contact information, add attachments, and receive status updates via email. Online Service accounts are free from Quantum. That account can also be used to access Quantum's Knowledge Base, a comprehensive repository of product support information. Sign up today at StorageCARE Customer Center:

https://quantumserviceandsupport.custhelp.com/app/utills/login_form/redirect/MyOrg

- To find contact information for your location: Visit Quantum's Support Contact page to find contact information for locations worldwide at:

www.quantum.com/ServiceandSupport/Contacts/ProductSelect/Index.aspx



Chapter 1

Overview

Data is one of the most highly valued resources in a competitive business environment. Protecting that data, controlling access to it, and verifying its authenticity while maintaining its availability are priorities in our security-conscious world. Data encryption is a tool that answers many of these needs.

The LTO-4, LTO-5, LTO-6, LTO-7, and LTO-8 Fibre Channel and SAS tape drives are capable of encrypting data as it is written to any LTO-4, LTO-5, LTO-6, LTO-7, and LTO-8 data cartridge. Encryption is performed at full line speed in the tape drive after compression. (Compression is more effectively done before encryption.) This new capability adds a strong measure of security to stored data without the processing overhead and performance degradation associated with encryption performed on the server or the expense of a dedicated data encryption appliance.

This chapter covers:

- [Library Managed Encryption](#)
- [How SKM Key Management Works](#)
- [Encryption Keys](#)
- [Encryption Certificates](#)
- [Keystore](#)
- [Mirrored Hard Disk Drives](#)
- [Why You Need to Back Up Your SKM Servers](#)

Library Managed Encryption

The library managed tape drive encryption solution is composed of four major elements:

- [Encryption-Enabled Tape Drive](#)
- [Encryption-Capable Media](#)
- [Scalar Key Manager \(SKM\)](#)
- [Encryption-Enabled Tape Library](#)

Encryption-Enabled Tape Drive

LTO-4, LTO-5, LTO-6, LTO-7, and LTO-8 Fibre Channel and SAS tape drives are encryption capable. This means that they are functionally capable of performing hardware encryption, but this capability has not yet been activated. In order to perform hardware encryption, the tape drives must be encryption enabled. They can be encryption enabled via the tape library.

See [Supported Libraries and Tape Drives](#) on page 241 for a list of which tape drives are supported by SKM on your library.

Encryption-Capable Media

LTO-4 and higher tape cartridges are encryption capable. Data written to encryption-supported and encryption-capable media in SKM-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 erased (re-labeled), or have been written to using library managed encryption at the first write operation at the beginning of tape (BOT).

- You cannot append encrypted data to a non-encrypted tape.
- You cannot append non-encrypted data to an encrypted tape.
- You cannot encrypt data to an unlabeled tape.

Scalar Key Manager (SKM)

Encryption involves the use of several kinds of keys. How these keys are generated, maintained, controlled, and transmitted depends upon the

operating environment where the encrypting tape drive is installed. Some host applications are capable of performing key management. For environments without such applications or those where application agnostic encryption is desired, Quantum provides the Scalar Key Manager (SKM) solution to perform all necessary key management tasks. [How SKM Key Management Works](#) on page 3 describes these tasks in more detail.

Encryption-Enabled Tape Library

On an encryption-enabled library, tape encryption occurs automatically and transparently. The library communicates with the SKM server to obtain data encryption keys for the drives to read from or write to tapes.

Library managed encryption is provided for LTO-4, LTO-5, LTO-6, LTO-7, and LTO-8 tape drives in a Quantum Scalar tape library. Key generation and management are performed by SKM. Data encryption keys pass from SKM to the drives via the library, making encryption transparent to applications.

How SKM Key Management Works

Scalar Key Manager (SKM) generates, protects, stores, and maintains data encryption keys that are used to encrypt information being written to, and decrypt information being read from, tape media (tape and cartridge formats).

SKM acts as a process awaiting key generation or key retrieval requests sent to it through a secure TCP/IP communication path between SKM and the tape library.

When a new data encryption key is needed, the tape drive requests a key, which the library forwards to the primary SKM server. The library requests a data encryption key from the primary SKM server first, unless the primary SKM server is down and failover to the secondary SKM server has occurred. If failover to the secondary SKM server occurred, then the library continues to request data encryption keys from the secondary SKM server until either the library is rebooted or the secondary server goes down and failover back to the primary occurs.

After a library reboot, the library goes back to forwarding requests to the primary server.

Upon receipt of the request, SKM retrieves an existing data encryption key from the keystore and securely transfers it to the library, which then provides it to the tape drive where it is used to encrypt the data being written to tape. Once a data encryption key is assigned to a tape, it is never reused on another tape.

When an encrypted tape is read by a tape drive, the tape drive requests, via the library, the required data encryption key from the SKM server. SKM retrieves the required data encryption key from the keystore and securely transfers it to the library, which provides it to the tape drive. The tape drive uses the data encryption key to perform encryption or decryption.

No data encryption key is stored anywhere on the cartridge memory or the tape. Only the name of the data encryption key is stored on the tape, so that in the future the key can be requested for further read or write purposes. The first read/write operation on an encrypted tape requires the tape drive to request the data encryption key.

Encryption Keys

An encryption key is typically a random string of bits generated specifically to encrypt and decrypt data. Encryption keys are created using algorithms designed to ensure that each key is unique and unpredictable. The longer the length of key used, the harder it is to break the encryption code.

The LTO-4, LTO-5, LTO-6, LTO-7, and LTO-8 method of encryption uses 256-bit AES algorithm to encrypt data. 256-bit AES is the encryption standard currently recognized and recommended by the U.S. government, which allows three different key lengths. 256-bit keys are the longest allowed by AES.

SKM uses two types of encryption algorithms:

- Symmetric
- Asymmetric

Symmetric, or secret key encryption, uses a single key for both encryption and decryption. Symmetric key encryption is generally used for encrypting large amounts of data in an efficient manner. 256-bit AES encryption uses symmetric keys.

Asymmetric, or public/private encryption, uses a pair of keys. Data that is encrypted using one key can only be decrypted using the other key in the public/private key pair. When an asymmetric key pair is generated, the public key is typically used to encrypt, and the private key is typically used to decrypt.

SKM uses both symmetric and asymmetric keys—symmetric encryption for high-speed encryption of user or host data stored on tape, and asymmetric encryption (which is necessarily slower) for secure communication and protecting the symmetric keys while in transit.

Encryption Certificates

Each SKM server pair uses one unique encryption certificate. The encryption certificate contains the public key of the public/private key pair that protects data encryption keys during transit to another site. The destination SKM server provides its public key to the source SKM server as part of its encryption certificate, which the source SKM server uses to wrap (encrypt) exported data encryption keys for transport. Upon arrival, the file containing the wrapped data encryption keys can only be unwrapped by the corresponding private key, which resides on the destination SKM server and is never shared.

For more information, see the following:

- [Encryption Keys](#) on page 4
- [Sharing Encrypted Tapes Offsite](#) on page 141
- [Sharing Encrypted Tapes Offsite](#) on page 144

Keystore

The keystore contains:

- All of the data encryption keys generated by the SKM server on which it resides. These keys are used for encrypting and decrypting tapes.
- A copy of the data encryption keys generated by the other SKM server in the pair.
- Data encryption keys that you imported (for example, keys that other companies or individuals sent to you). These keys can be used to decrypt tapes provided by the other companies or individuals.
- Your SKM server pair's encryption certificate.
- Encryption certificates that you imported (for example, that other companies or individuals sent to you). These are used to wrap your data encryption keys for transit to another party to use in decrypting tapes you may have provided to them.
- Public and private keys used for secure communication.
- Metadata (for example, which data encryption keys were used on which tapes).

Mirrored Hard Disk Drives

This section applies only to the SKM appliance server hardware. If you are running SKM in a VM environment, this section does not apply.

Caution: Do not remove any hard drive from the appliance server unless it is failed or you are instructed to do so by Quantum service. Removing any hard drive may render it unusable.

Each SKM appliance server contains two hard disk drives in a RAID 1 (mirrored) configuration. The two hard disk drives are constantly being synchronized, so that each is an exact duplicate of the other. If one hard disk drive fails, the other one contains all the required information to

allow the server to continue to work as normal. As soon as the failed hard disk drive is replaced, all the data on the working hard disk drive is duplicated onto the new hard disk drive.

Why You Need to Back Up Your SKM Servers

Every time new data encryption keys are generated, you must back up both SKM servers before you begin using the keys to encrypt data. You need to back up BOTH servers because every time keys are generated on one server, the library copies them to the other server. If a server fails and you have not backed it up, the restored server will not contain all the keys and would fail any requests for keys that were not backed up. You should also back up both SKM servers any time you import keys from another source.

Although SKM contains features designed to protect your keystore in case of hard disk drive or server failure, these features do not cover every situation.

In the following cases, if you have no backup, there is no way to recover your keystores:

- If both SKM servers (and all four hard disk drives, if using the SKM appliance servers) were to suffer environmental damage causing them to become inoperable, the only way to recover your keystore is via the backup.
- If you forget your password, the only way to recover your data is to completely replace your server and its hard disk drives, and perform a restore from your backup.

Also, each SKM server generates its own unique data encryption keys, meaning that the keystore on each SKM server is different. This is why you need to back up each SKM server separately, every time a server generates or imports data encryption keys.

For instructions on how to perform a backup, see [Backing Up the SKM Server](#) on page 103.

Chapter 1: Overview
Why You Need to Back Up Your SKM Servers



Chapter 2

Planning Your SKM Environment

Use the information in this chapter to determine the operating environment for your SKM system. This chapter includes:

- [SKM Server Requirements](#)
- [Multiple Libraries Accessing One SKM Server Pair](#)
- [Disaster Recovery Planning](#)

SKM Server Requirements

Caution: Quantum requires that you do not install any software, file, or operating system on the SKM appliance server or SKM VM server unless it is an upgrade or patch supplied by Quantum. Doing so may make your server inoperable and will void the warranty.

- The SKM server must have IP connectivity through any firewalls to all Quantum libraries using the SKM appliance server to obtain encryption keys.
- SKM uses TCP ports 80, 6000 and 6001 for SKM server communication. These ports must all be open on your network in a

bi-directional mode in order for SKM communication between the SKM servers and libraries to work.

- For equipment and resources needed, refer to:
 - [Items Required for Setup](#) on page 28
 - [Equipment and Software Needed for VMware](#) on page 39
- For temperature and humidity requirements on the SKM appliance server, see [SKM Appliance Server Environmental Specifications](#) on page 240.

SKM Appliance Server Cooling and Airflow Requirements

To maintain proper airflow and system cooling, observe the following:

- Ensure there is adequate space around the server to allow the server cooling system to work properly. Leave approximately 2 inches (50 mm) of open space around the front and rear of the server.
- Do not place objects in front of the fans.
- Do not leave open space above or below an installed server in your rack cabinet. To help prevent damage to server components, always install a filler panel to cover the open space and to help ensure proper air circulation.

Caution: Do not operate the server for more than 10 minutes without a drive installed in each bay.

Caution: Do not open the server cover to adjust or fix internal components. If the server has a problem, contact Quantum Support for a replacement.

SKM Appliance Server Rack Considerations

If the SKM appliance server is installed in a rack, consider the following:

WARNING: Do not place any object weighing more than 110 lb. (50 kg) on top of rack-mounted devices.

- Install the server only in a rack cabinet that has perforated doors.
- Do not block any air vents. Usually 6 in. (15 cm) of air space provides proper airflow.
- Plan the device installation starting from the bottom of the rack cabinet.
- Install the heaviest device in the bottom of the rack cabinet.
- Do not leave open space above or below an installed server in your rack cabinet. To help prevent damage to server components, always install a filler panel to cover the open space and to help ensure proper air circulation.
- Do not extend more than one device out of the rack cabinet at the same time.
- Connect all power cords to properly wired and grounded electrical outlets.
- Do not overload the power outlet when installing multiple devices in the rack.

Multiple Libraries Accessing One SKM Server Pair

Multiple libraries may access and use the same SKM server pair. The only requirement is that they be available to the SKM servers through TCP/IP connectivity. If you want to connect more than one library to an SKM server pair, keep the following in mind:

- All tape libraries using the same SKM Pair need to also use the same library based TLS Certificates.
- Each library must be licensed to use SKM. See your library user's guide or online help for instructions.

- Each library can only be configured to use one SKM server pair at a time.
- Each library triggers the SKM servers to create a unique set of data encryption keys. When more libraries are connected to an SKM server, more initial data encryption keys will reside in the SKM server's keystore.
- Each library's set of unique data encryption keys is maintained separately on the SKM server. When you generate more keys for a particular library, this does not affect any of the other libraries and their sets of encryption keys. Each library only triggers creation of its own set of keys.

Disaster Recovery Planning

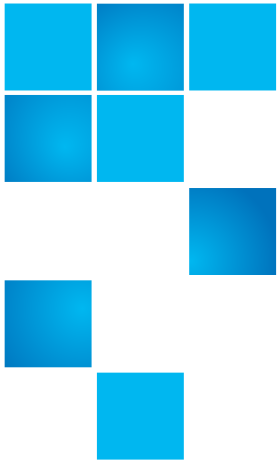
Quantum recommends that you plan for disaster recovery in the following ways:

- Maintain each of the two SKM servers in different geographical locations, preferably in different cities, states, or countries, to mitigate the possibility of both servers being compromised in the event of natural disaster or theft.
- Back up the SKM server each time new keys are generated or keys are imported and store the backups in a safe location (see [Backing Up the SKM Server](#) on page 103).

Caution: Do not use SKM to encrypt the sole copy of your SKM server 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.

- Remember your password. If you lose your password, you lose login access to the SKM server, including backup and restore capability. If you lose your password, Quantum will not be able to recover it for you.

- Replace a failed appliance or VM server immediately. Even though the other SKM server allows you to continue to operate, you do not want to risk the second server failing as well.
- **SKM appliance servers only:** Replace a failed hard disk drive immediately. Even though the second hard disk drive allows you to continue to operate, redundancy is removed and a second hard disk drive failure would cause the server to fail.



Chapter 3

Using the SKM Appliance Server

This chapter discusses the SKM appliance server safety, hardware, and general operating instructions. Topics include:

- [Safety](#)
- [SKM 2.7 Appliance Server \(and later versions\)](#)
- [SKM 2.6 Appliance \(and Earlier Versions\)](#)
- [Powering On the SKM Appliance Server](#)
- [Powering Off the SKM Appliance Server](#)

Caution: Never install any software or operating system onto an SKM appliance server unless it is an upgrade or patch supplied by Quantum. Doing so may make your server inoperable and will void your warranty.

Safety

This section provides some important information for handling the SKM appliance server safely. Please also review the safety information in Safety Information by Lenovo located at (Reference Guides):

<https://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SKM/Index.aspx?whattab=Fifth>

This section covers:

- [Electrical Safety](#)
- [Handling Static-Sensitive Devices](#)

Electrical Safety

WARNING: DANGER: Electrical current from power, telephone, and communication cables is hazardous. To avoid a shock hazard, follow all the warnings that follow:

WARNING: Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.

WARNING: Connect all power cords to a properly wired and grounded electrical outlet.

WARNING: Connect to properly wired outlets any equipment that will be attached to this product.

WARNING: Never turn on any equipment when there is evidence of fire, water, or structural damage.

WARNING: Disconnect all cables before moving the SKM appliance.

Handling Static-Sensitive Devices

Caution: Static electricity can damage the server and other electronic devices. To avoid damage, keep static-sensitive devices in their static-protective packages until you are ready to install them. To reduce the possibility of damage from electrostatic discharge, observe the following precautions:

Caution: Limit your movement. Movement can cause static electricity to build up around you.

Caution: Handle the device carefully, holding it by its edges or its frame.

Caution: Do not leave the device where others can handle and damage it.

Caution: While the device is still in its static-protective package, touch it to an unpainted metal surface on the outside of the server for at least 2 seconds. This drains static electricity from the package and from your body.

Caution: Remove the device from its package and install it directly into the server without setting down the device. If it is necessary to set down the device, put it back into its static-protective package. Do not place the device on the server cover or on a metal surface.

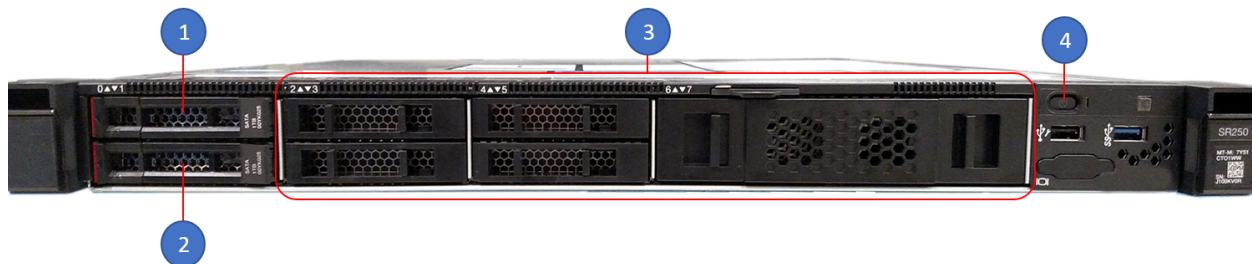
Caution: Take additional care when you handle devices during cold weather. Heating reduces indoor humidity and increases static electricity.

SKM 2.7 Appliance Server (and later versions)

The SKM 2.7 Appliance Server is a compact, cost-effective, single-processor 1U rack server.

- [Figure 1](#) provides a front view of the server.
- [Figure 2](#) provides a rear view of the server.
- [Figure 3](#) provides a location of the drive LEDs.

Figure 1 SKM 2.7 Appliance Server Front Panel



1	Drive 0 (2.5 inch)	3	Drive Slots (empty)
2	Drive 1 (2.5 inch)	4	Power Button/LED

Figure 2 SKM 2.7 Appliance Server Rear Panel

The Ethernet ports on the rear of the server are as follows:

- Unmarked port (far left: port) 10/100/1000 Mb Ethernet port
- Port 1 (middle port): 1GbE port
- Port 2 (far right: port): 1GbE port

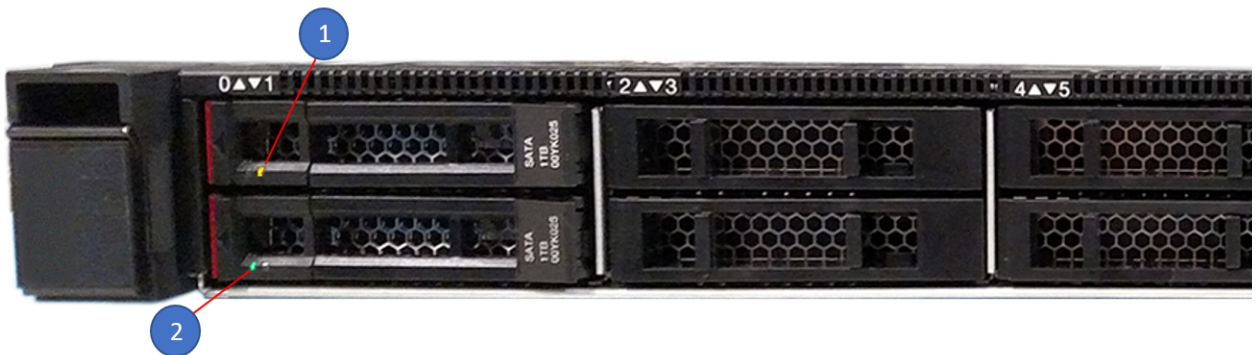


1	Serial Port (DB-9)	5	Power Supply Unit (PSU)
2	Configuration/Management Port	6	Power Cord Connection
3	1 GbE Port (RJ-45)	7	VGA Port
4	1 GbE Port (RJ-45)		

The amber hard disk drive status LED will be solidly illuminated on a failed hard disk drive.

- See [Figure 3](#) for location of amber LED illuminated on the failed drive (Slot 0, Callout 1).
- Notice that the drive in Slot 1 (Callout 2) has a green LED (meaning the drive is operational).

Figure 3 LED Location on Front of SKM 2.7 Appliance Server



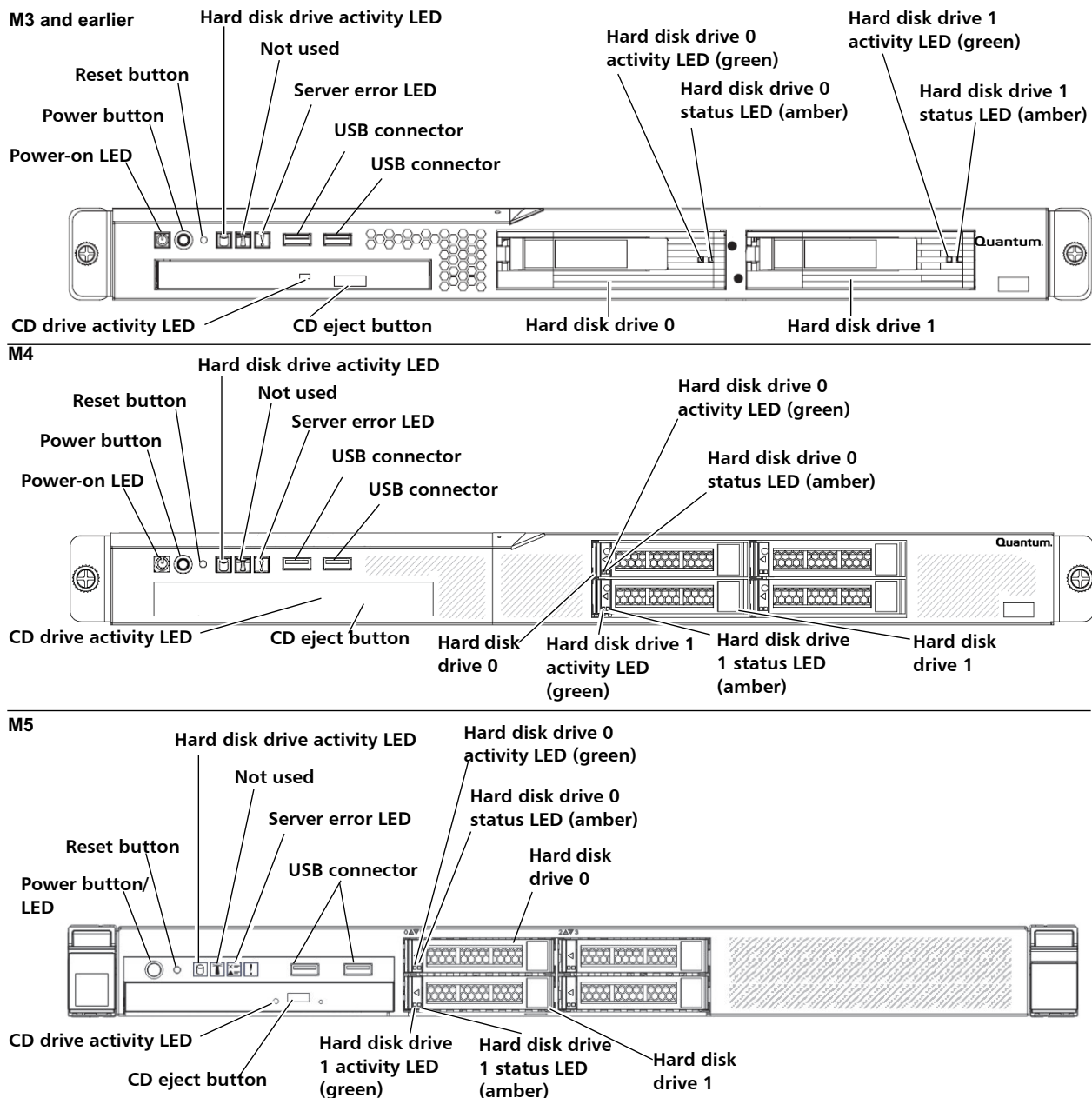
SKM 2.6 Appliance (and Earlier Versions)

This section describes the buttons, light-emitting diodes (LEDs), and connectors on the front and rear of the SKM appliance server.

SKM Appliance servers use different IBM-branded servers. Quantum has deployed M3, M4, and M5 IBM servers for SKM appliances.

[Figure 4](#) on page 20 shows the buttons, light-emitting diodes (LEDs), and connectors on the front of the server.

Figure 4 Front Panel Buttons, LEDs, and Connectors



Button, LED, or Connector	Function
Power-on LED	<ul style="list-style-type: none"> • Off: Indicates AC power is not present, or the power supply or the LED itself has failed. Note: If this LED is off, it does not mean that there is no electrical power in the server. The LED might be burned out. To remove all electrical power from the server, you must disconnect the power cord from the electrical outlet. • On solid: Indicates the server is powered on. • Blinking slowly (once per second): Indicates the server is powered off and is ready to be powered on. You can press the power button to power on the server. • Blinking rapidly (4 times per second): Not present in all models. Indicates the server is powered off and is not ready to be powered on. The power button is disabled. This will last approximately 1 to 3 minutes after connecting to AC power.
Power button	<p>Press this button to power on the server. To power off the server you need to press and hold the button for more than four seconds. You may need to use a pen to press the button.</p> <p>Some servers come with a disc-shaped shield installed around the button to prevent the server from being powered off accidentally. You may remove the shield if you prefer.</p>
Reset button	<p>Press this button to reset the server hardware and run the power-on self-test (POST). You might need to use a pen or the end of a straightened paper clip to press the button. Resetting takes 2 to 3 minutes.</p>
Hard disk drive activity LED (Green)	<p>When this LED is blinking, it indicates that a hard disk drive is in use.</p>
Server error LED	<p>This amber LED has an exclamation point in it. When this LED is illuminated, it indicates that a server error has occurred (including when a hard disk drive is not in a slot; for example, when you replace a damaged hard disk drive).</p>
USB connectors	<p>You may connect a USB device such as a mouse or keyboard to either of these connectors. The only reason you might use a USB device is to connect directly to the command line interface without using an SSH connection.</p>

Button, LED, or Connector	Function
CD/DVD eject button	Press this button to release a CD or DVD from the CD/DVD drive. Note: Some server models have a CD drive; others have a DVD drive.
CD/DVD drive activity LED	When this LED is lit, it indicates that the CD/DVD drive is in use.
Hard disk drive 0 and 1 activity LEDs	These green LEDs blink either once every 16 seconds or several times rapidly every 16 seconds (depending on server model) during normal activity. When the hard disk drive is being accessed, the LED blinks at a faster rate. During RAID rebuild (which occurs when a hard disk drive is replaced), the LED flickers very fast so that it may appear to be on solid.
Hard disk drive 0 and 1 status LEDs	These amber LEDs will be on solid to indicate a the hard disk drive is faulty and needs to be replaced. During a RAID rebuild (which occurs when a hard disk drive is replaced), the LED of the hard disk drive that is updating will blink slowly (once per second).

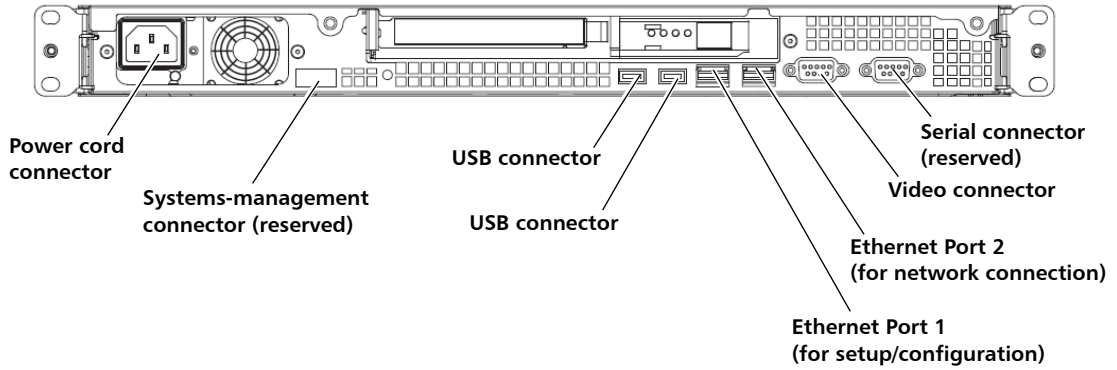
Rear Panel Connectors and LEDs

The following two figures show the connectors and LEDs on the rear of the server.

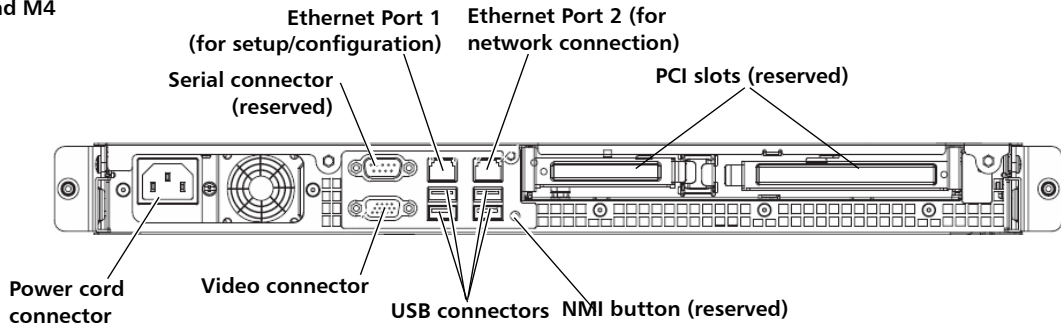
Figure 5 Rear Panel Connectors

[Figure 5](#) shows the connectors on the rear of the server. Your server will look like one of the two drawings below.

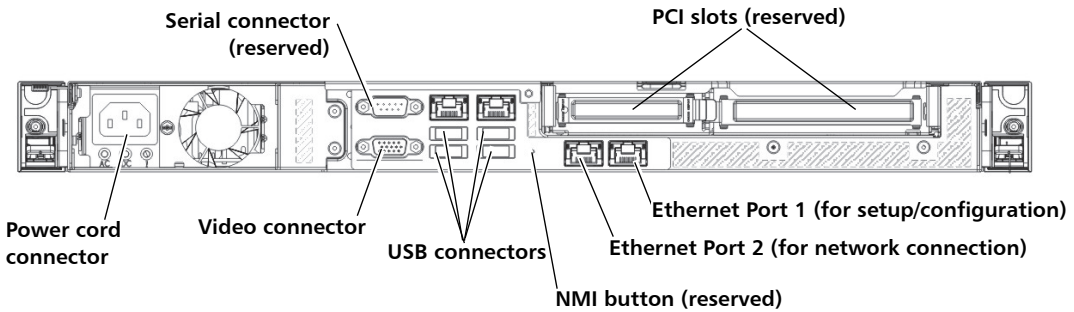
M2 and earlier



M3 and M4



M5

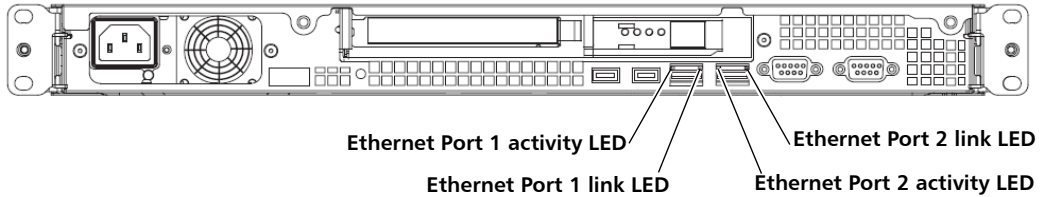


Connector	Function
Power-cord connector	Connect the power cord to this connector.
Serial connector	Reserved.
Video connector	You may connect a monitor to this connector. The only reason you might connect a monitor is to connect directly to the command line interface without using an SSH connection.
Ethernet Port 1	Use this port for setup and initial configuration with a local SSH connection only. You might also use this port if you forget the IP address of Port 2 need reconfigure the SKM server to reset Port 2. Do not connect this port to your network. The IP address of Port 1 is static and cannot be changed. The IP address is 192.168.18.3 . This port is referred to as eth0 in the command line interface.
Ethernet Port 2	Use this port to connect the SKM server to your network. The default IP address for this port is 192.168.18.4 . You will change the IP address during initial setup. This port is referred to as eth1 in the command line interface.
USB connectors	You may connect a USB device such as a mouse or keyboard to any of these connectors. The only reason you might use a USB device is to connect directly to the command line interface without using an SSH connection.
Systems-management connector	Reserved.
NMI button	Reserved.
PCI slots	Reserved.

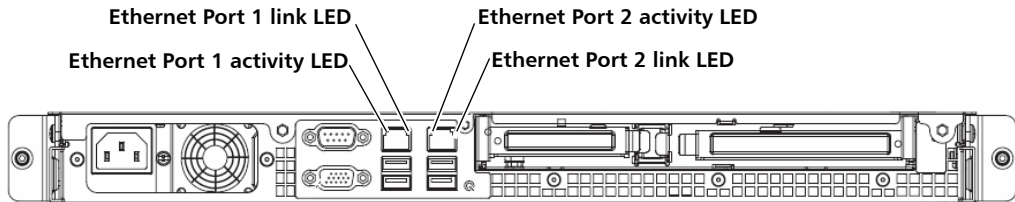
Figure 6 Rear Panel LEDs

Figure 6 shows the LEDs on the rear of the server. Your server will look like one of the two drawings below.

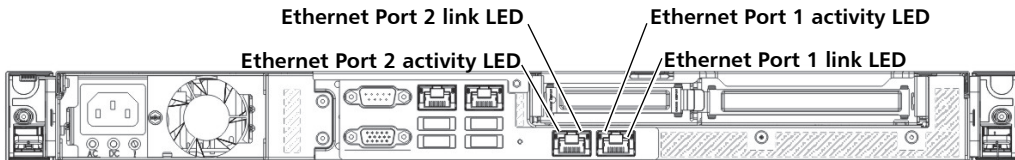
M2 and earlier



M3 and M4



M5



LED	Function
Ethernet activity LED	When this LED is on, it indicates that there is activity between the server and the network.
Ethernet link LED	When this LED is on, it indicates that the Ethernet controller is connected to the network.

Powering On the SKM Appliance Server

To power on the SKM appliance server, press the power button.

Depending on the model of server you have, it will take 20 seconds to 3 minutes after the server is connected to AC power for the power button to become active. When the power button is active, the power-on LED blinks slowly (once per second).

Note: If a power failure occurs while the server is powered on, the server will restart automatically when power is restored.

Powering Off the SKM Appliance Server

To power off the server, press the power button and hold it in for four seconds.

While the server remains connected to AC power, one or more fans might continue to run. To remove all power from the server, you must disconnect it from the power source.

Caution: The power button on the server does not turn off the electrical current supplied to the device. To remove all electrical current from the device, ensure that the power cord is disconnected from the power source.



Chapter 4

Initial Configuration and Setup

SKM can be deployed in one of two ways:

- A pair of physical appliances (servers) purchased from Quantum, or
- A pair of virtual machines (VMs) installed in a VMware® or KVM environment.

These instructions guide you through installing and configuring both options.

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

This chapter covers:

- [Installing and Configuring the SKM Appliance Servers](#)
- [Installing and Configuring the SKM VM Servers](#)
- [Installing TLS Certificates on the SKM Server for Pre-SKM 2.4 \(240Q\)](#)
- [Installing TLS Certificates on the SKM Server for SKM 2.4 \(240Q\) or Later](#)
- [Configuring Your Library For SKM](#)
- [Configuring Multiple Libraries](#)
- [Backing Up the Servers](#)

Installing and Configuring the SKM Appliance Servers

Follow the instructions in this section if you are deploying a pair of physical SKM appliance servers.

Caution: The SKM appliance servers are designed for one purpose only—to store and manage your encryption keys. Do not install additional hardware on the servers. Never install any software, file, or operating system on the servers unless it is an upgrade or patch supplied by Quantum. Doing so can make your server inoperable and will void your warranty.

Items Required for Setup

You need the following to install and configure each SKM appliance server:

- (2) SKM appliance servers (each comes with two hard disk drives installed).
- Power cord (supplied).
- Rackmount kit with installation instructions (supplied).
- CAT5e Ethernet cable, crossover (for initial configuration, not supplied).
- CAT5e Ethernet cable, standard (for standard operation, not supplied).
- Laptop or PC, to connect to each server to perform initial configuration.
- To access all the features of SKM, the most recent library firmware is recommended. See the Release Notes for your library for information on the minimum firmware required to run SKM, and most recent firmware versions available for your library.
- For Microsoft® Windows®, you may need to install utilities 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>.

- The SKM server must have IP connectivity through any firewalls to all Quantum libraries using the SKM appliance server to obtain encryption keys.
- SKM uses TCP ports 80, 6000 and 6001 for SKM server communication. These ports must all be open on your network in a bi-directional mode in order for SKM communication between the SKM servers and libraries to work.

Installing the SKM Appliance Servers

Follow the instructions below for **both SKM appliance servers**.

Caution: Do not remove any hard drive from the appliance server unless it is failed or you are instructed to do so by Quantum service. Removing any hard drive may render it unusable.

- 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).

Note: The Scalar Key Manager rack box ships in each appliance/server box. The “Rack Installation Guide” ship within the rack box.

- 2 Install the SKM appliance server in a rack. Follow the Scalar Key Manager Rack Installation instruction sheet (included with the rail kit and located at (Product Use Guides):

<https://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SKM/Index.aspx?whattab=Fifth>

- 3 Connect the power cord into the rear of the SKM appliance server (see [Figure 7](#) or [Figure 8](#)) and plug it into a grounded power outlet. Depending on the server model you have, it may take up to 20 seconds or more for power button to become active. During this time, one or more fans might run loudly and then quiet down. On some models, the power-on LED on the front panel (see [Figure 9](#) or [Figure 10](#)) blinks rapidly (4 times per second), indicating the power button is not active yet.

[Figure 7](#) provides an illustration of the SKM 2.7 Appliance Server (rear view).

- The power cord connector is located on the power supply unit (PSU), at the right-rear of the server.
- The Ethernet ports on the rear of the server are as follows:
 - Configuration/Management Port: Unmarked port (far left: port) 10/100/1000 Mb Ethernet port (Callout 2)
 - Port 1 (middle port): 1GbE network port (Callout 3)
 - Port 2 (far right: port): 1GbE network port (Callout 4)

Figure 7 SKM 2.7 Appliance Server Rear Panel

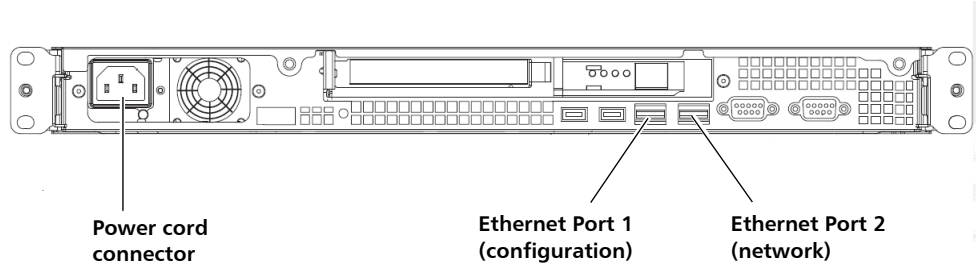


1	Serial Port (DB-9)	5	Power Supply Unit (PSU)
2	Configuration/Management Port	6	Power Cord Connection
3	1 GbE Port (RJ-45)	7	VGA Port
4	1 GbE Port (RJ-45)		

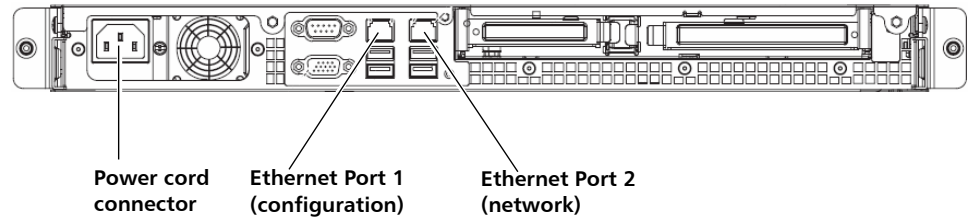
Figure 8 SKM 2.6 Appliance Server Rear Panel

Figure 8 shows the rear of the SKM 2.6 Appliance Server (and earlier versions).

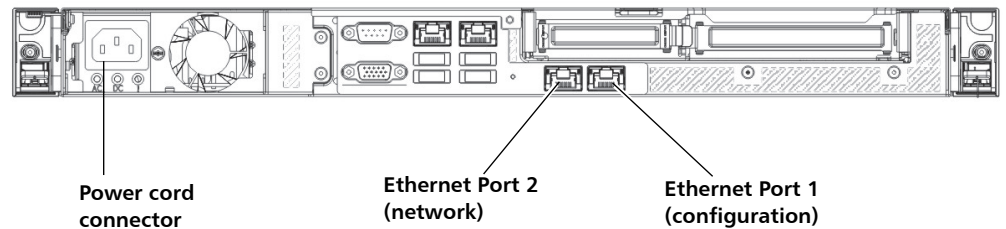
M2 and earlier



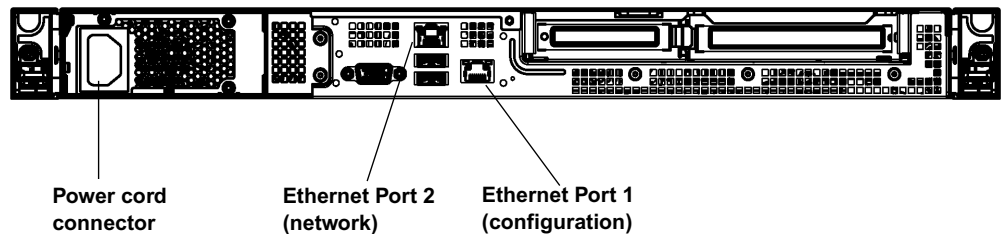
M3 and M4



M5



M6



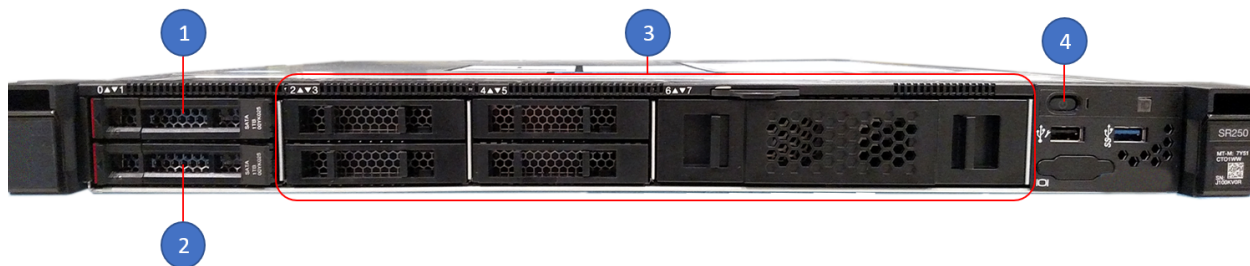
- 4 Observe the power-on LED on the front panel (see [Figure 9](#) or [Figure 10](#)). Wait until the power-on LED blinks slowly (once per second) to indicate that the power button is active.

If the power-on LED is not blinking, there could be a problem with the power supply or the LED. Check the power connection. If this LED still does not blink, contact Quantum Support.

- 5 Power ON the SKM appliance server by pressing the power button on the front of the server (see [Figure 9](#) or [Figure 10](#)).

Figure 9 SKM 2.7 Appliance Server Front Panel

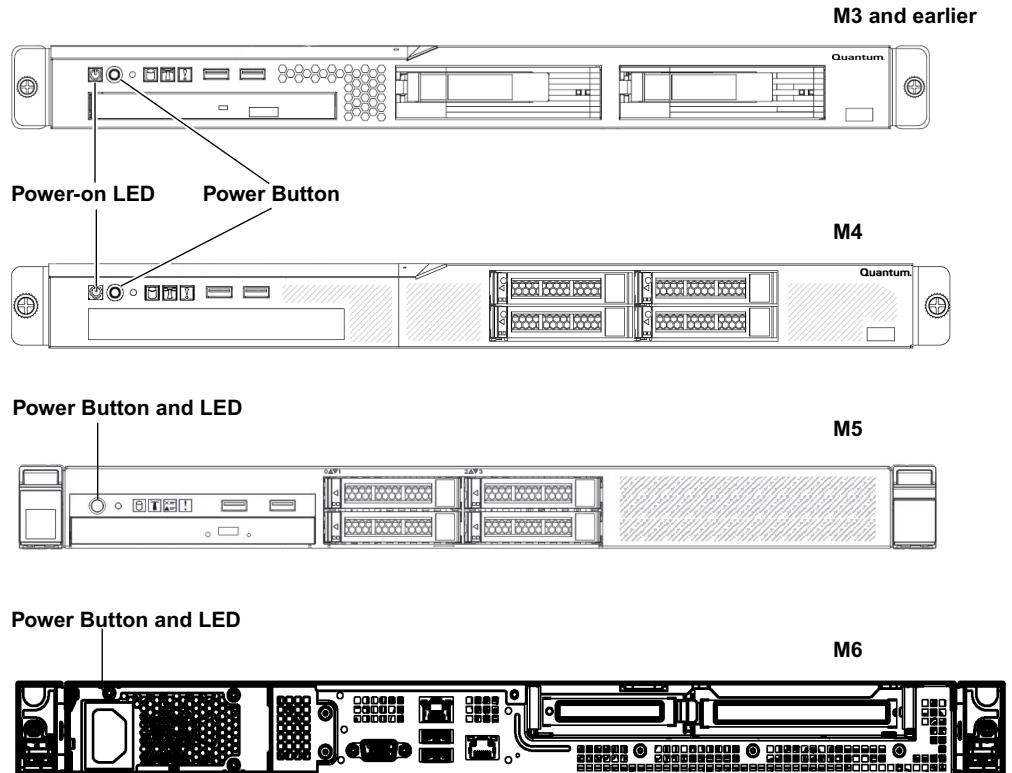
[Figure 9](#) shows the front of the SKM 2.7 Appliance Server (and later versions). It provides the location of the “power-on button and the installed drives.



1	Drive 0 (2.5 inch)	3	Drive Slots (empty)
2	Drive 1 (2.5 inch)	4	Power Button/LED

Figure 10 SKM 2.6 Appliance Server Front Panel

Figure 10 shows the rear of the SKM 2.6 Appliance Server (and earlier versions). It provides the location of the “power-on LED and the power button).



- 6 Again observe the power-on LED on the front panel. Wait until it is illuminated but not blinking, indicating the server is powered on.
- 7 Allow up to 3 minutes for the server to complete startup before you connect via SSH in the next step.

Configuring the SKM Appliance Servers

Follow the instructions below for **both SKM appliance servers**.

Note: Both SKM appliance servers must be configured, operational, and connected to the network before any libraries can be set up to use 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 the following values. Before beginning, decide what you want each of these values to be. You can also change these values in the future.

- Password
- Time zone, date, and time
- IP address, netmask, and gateway

Allow 30 minutes per server to complete the configuration.

- 1 Set the IP address of the laptop or PC you will use to connect to the SKM appliance server to **192.168.18.100**.
- 2 Connect a crossover CAT5e Ethernet cable from the laptop or PC to:
 - SKM 2.7 Appliance Server (and later versions) Configuration/Management Port on the rear of the SKM server (see [Figure 7](#) on page 30).
 - SKM 2.6 Appliance Server (and earlier versions) **Ethernet Port 1** on the rear of the SKM server (see [Figure 8](#) on page 31).

Note: The SKM 2.7 Appliance Server Configuration/Management Port and/or the SKM 2.6 Appliance Server Ethernet Port 1 are only used for configuration.

Once you perform the initial configuration, you will use Ethernet Port for SKM appliance server communication via your network.

- 3 Using SSH, connect to the server using the IP address for Ethernet Port 1: **192.168.18.3**.

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

- 4 At the **login** prompt, type the following (this is the user login ID which will never change):

akmadmin

- 5 At the **Password** prompt, type the default password:

password

- 6 At the `akmadmin@skmserver` prompt, type the following:
`./skmcmds`
- 7 At the **Password** prompt, type the default password again:
`password`
The End User License Agreement displays.
- 8 Read the license agreement. Press **<Enter>** to scroll through the agreement. At the end, type `y` to accept and continue or `n` to decline and stop the installation process.
- 9 Press **<Enter>** to begin the setup wizard.
- 10 The first setup wizard task prompts you to change the `akmadmin` password (see [Figure 11](#)). There is only one password for SKM. It is called the `akmadmin` password, and is required for all logins and access to SKM Admin Commands, including backup and restore.

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

If you change the password from the default and forget it, there is no way to retrieve it!

Each SKM 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 SKM server, including backup and restore capability. Quantum will NOT be able to restore the password.

Charges may apply for replacement of an SKM appliance server required due to changing and then forgetting the password.

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

- If you do not wish to change the password at this time, type `n` and press **<Enter>** at the “change password” prompts and the

default password (password) remains. You can change the password at any time later using SKM Admin Commands.

- If you wish to change the password:
 - a At the “change password” prompt, type **y** and press **<Enter>**.
 - a At the **(current) UNIX password** prompt, type the default password (password) and press **<Enter>**.
 - b Type a new password and press **<Enter>**.
 - c Type the new password again and press **<Enter>**.
 - d Press **<Enter>**.

Figure 11 Changing the Password

```
Changing akadmin password.  
-----  
Changing password for akadmin.  
(current) UNIX password:  
Enter new UNIX password:  
Retype new UNIX password:
```

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

Note: To ensure proper TLS certificate generation, Quantum recommends setting both the Primary and Secondary SKM servers to the same date, time and time zone even if they are in different time zones. (On both servers, use the date, time and time zone values applicable to the Primary SKM server.)

Then, 24 hours after TLS certificate generation, you can correctly set the date, time and time zone for the secondary server.

The IP address you are configuring is for Ethernet Port 2, the port you will be using for network connection to SKM.

Ethernet Port 1 IP Address (never changes): 192.168.18.3

Ethernet Port 2 Default IP Address: 192.168.20.4 or 192.168.18.4 depending on the server version.

Note: Ports are identified on the back of the server as Port 1 and Port 2, but when configuring SKM through the console the ports are referred to onscreen as Ports 0 and 1 respectively. (That is, labeled Port 1 = Port 0 in the console, and labeled Port 2 = Port 1 in the console.)

Note: The netmask must match the netmask and gateway of the connected libraries.

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

The list of SKM Admin Commands displays (see [Figure 12](#)). If you made any mistakes during the setup wizard, you can go back and change them by entering the number corresponding to the item.

Figure 12 SKM Admin
Commands

```
SKM Admin Commands (Version 260Q.GC00600)
SKM
Server Cert's Validity:
/etc/akm/Certs/QKMServerSignedCert.pem
Not Before: May 1 19:01:37 2009 GMT and Not After : May 1 19:01:37 2019 GMT
Admin Cert's Validity:
/home/akmadmin/.akmadmin/Certs/QKMAdminSignedCert.pem
Not Before: May 1 19:01:38 2009 GMT and Not After : May 1 19:01:38 2019 GMT

Current Date/Time: Fri Feb 15 13:19:24 CST 2019

-----
1) Launch SKM server setup wizard.
2) Change user account password.
3) Capture SKM server snapshot.
4) Set SKM server IP address.
5) Set SKM server time zone.
6) Set SKM server date and time.
7) Back up SKM server.
8) Restore SKM server.
9) Set SKM server hostname.
d) Display/update TLS communication certificates.
u) Update SKM server software.
r) Roll back SKM server software.
v) View SKM server reports.
k) Key/Certificate import and export.
t) Set Minimum TLS Communication Support (1.0, 1.1 or 1.2).
```

- 13 Type `q` and press **<Enter>** at the **Command** prompt to quit, save your changes, and restart the SKM server. This process takes a few seconds. Wait until the `akmadmin@skmserver` prompt appears.

Note: You MUST quit at this point. Otherwise your changes will not be saved and you will not be able to continue the installation process.

- 14 Disconnect the crossover CAT5e Ethernet cable from the SKM 2.7 Appliance Server Configuration/Management Port and/or the SKM 2.6 Appliance Server **Ethernet Port 1** (see [Figure 7](#) on page 30 or [Figure 8](#) on page 31).
- 15 On the laptop you are using to configure SKM, change the hard-coded IP address back to DHCP.
- 16 Connect a standard CAT5e Ethernet cable from **Ethernet Port 2** on the back of the SKM appliance server to your network (see [Figure 8](#) on page 31). You will connect to this port using the IP address assigned in [Step 11](#) above.
- 17 Complete steps 1-16 on the secondary SKM server before proceeding.
- 18 When you are finished, do one of the following:
 - For pre-SKM 2.4 (240Q) systems, proceed to [Installing TLS Certificates on the SKM Server for Pre-SKM 2.4 \(240Q\)](#) on page 59.
 - For SKM 2.4 (240Q) and later systems, proceed to [Installing TLS Certificates on the SKM Server for SKM 2.4 \(240Q\) or Later](#) on page 70.

Note: You can see the version of software you are running at the top of the SKM **Admin Commands** menu. To view the software version without accessing SKM Admin Commands, refer to “Viewing the SKM Server Software Version” in the SKM User’s Guide.

Installing and Configuring the SKM VM Servers

Follow the instructions in this section if you are deploying a pair of SKM VM servers for installation in a VMware environment.

Perform all the instructions in this section **for each SKM VM server**. Use a different installation CD for each VM.

Caution: It is recommended that the two SKM VM servers be installed in different physical locations to provide better protection in case of disaster.

Caution: Quantum requires that you do not install any software, file, or operating system on the SKM appliance server or SKM VM server unless it is an upgrade or patch supplied by Quantum. Doing so may make your server inoperable and will void the warranty.

Note: Quantum provides support for SKM, however Quantum does not support the virtual environment hardware or software (VMware or KVM).

Equipment and Software Needed for VMware

You need the following to set up and configure the SKM VM servers:

- Scalar Key Manager VM Installation packages.
 - SKM VM server software (.ova image)
 - SKM server Quantum-provided TLS communication certificate bundle (.tgz file)
- VMware® vSphere™ Client installed on a computer. The computer may be the same as the server that hosts the VM but it does not have to be. The vSphere Client is required for initial setup; after that, you can use vSphere Client or another method to access the SKM VM server.

Note: These instructions in this section use vSphere Client version 4.1.0. If you use a different version of vSphere, the instructions may differ.

- SKM VM CD (if applicable)
- Resources required for each SKM VM server:
 - (1) Ethernet interface
 - 1 GB RAM
 - 8 GB of disk space
 - VM host software must be one of the following:
 - VMware ESX 4.x (64 bit)
 - VMware ESXi 4.x (64 bit)
 - VMWare ESXi 5.x (64 bit)
 - VMWare ESXi 6.x (64 bit) requires 252Q or greater software
- Video memory must be set to 3 MB.
- To access all the features of SKM 2.2, the most recent library firmware is recommended. See the Release Notes for your library for information on the minimum firmware required to run SKM, and most recent firmware versions available for your library.
- If you plan to connect to the SKM VM server (now or in the future) via a Microsoft Windows machine, you may need to install utilities 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>.
- The SKM server must have IP connectivity through any firewalls to all Quantum libraries using the SKM appliance server to obtain encryption keys.
- SKM uses TCP ports 80, 6000 and 6001 for SKM server communication. These ports must all be open on your network in a bi-directional mode in order for SKM communication between the SKM servers and libraries to work.

Deploying the .ova Image for VMware

Follow the instructions below for **both SKM VM servers**. The .ova installation process is performed via VMware's vSphere Client.

- 1 Access the Scalar Key Manager 2.x VM Installation software that you will load on each server.
- 2 You may copy the .ova image to a shared network drive for faster deployment if you wish.
- 3 Launch vSphere Client.
- 4 Log on to the VM host.
- 5 Highlight the IP address of the VM host.
- 6 Select **File > Deploy OVF Template**.

The **Deploy OVF Template** wizard opens.

- 7 Complete the wizard screens and click **Finish** when done.

A progress bar displays on the screen. When complete, the SKM VM server name appears in the list of VMs on the screen. Deployment takes a few minutes to several hours depending on network speed and location of the .ova image in relation to the VM host. Wait until the file deploys before continuing.

Caution: Do NOT power on the VM instance yet. Wait until you configure the MAC address per the instructions below. Otherwise, you will have problems with the MAC address later.

Configuring the SKM VM Servers for VMware

Follow the instructions below for **both SKM VM servers**.

Note: Both SKM VM servers must be configured, operational, and connected to the network before any libraries can be set up to use them.

Caution: You must use a different SKM software package for each VM server. Keep track of which SKM software package you use for which SKM server. The TLS certificates and serial number/MAC address/license key are unique and you must use the correct ones if you ever need to reinstall the SKM server. Also, if you accidentally use the same SKM software package for both VM servers, you will not be able to complete the configuration.

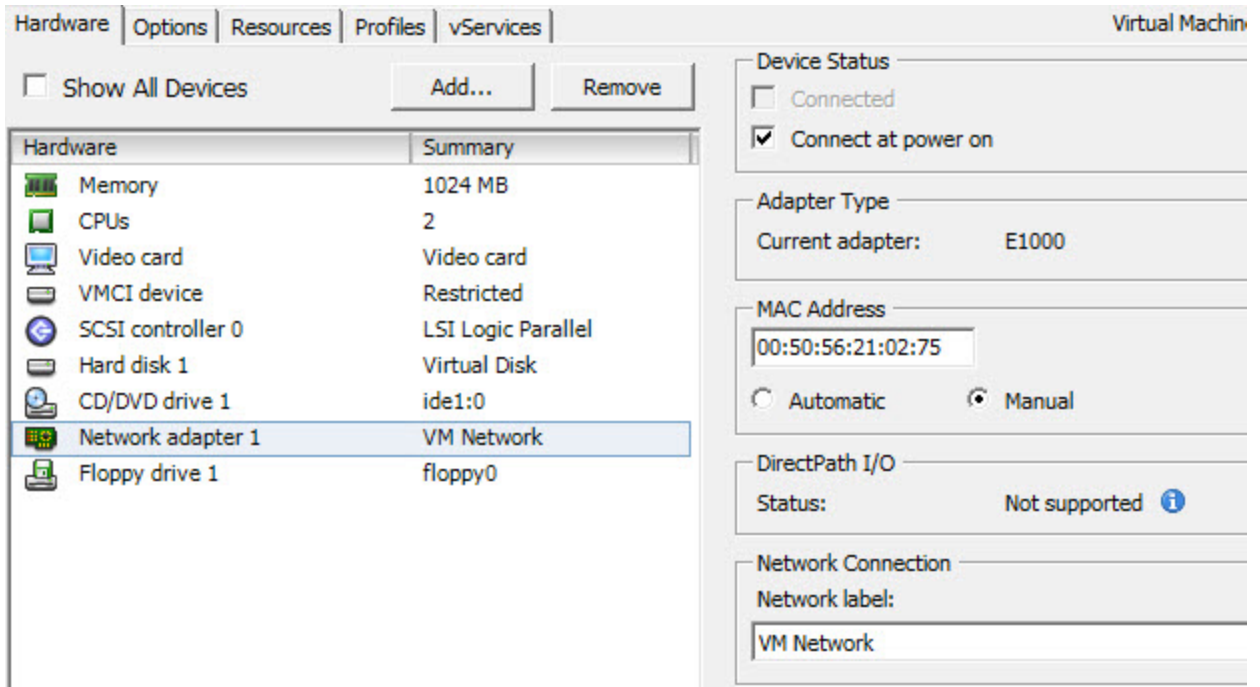
The configuration process requires you to read and accept the end user license agreement, and then complete a setup wizard. The setup wizard helps you configure the following values. Before beginning, decide what you want each of these values to be. You can also change these values in the future.

- Password
- Time zone, date, and time
- IP address, netmask, and gateway

Allow 30 minutes per server to complete the configuration.

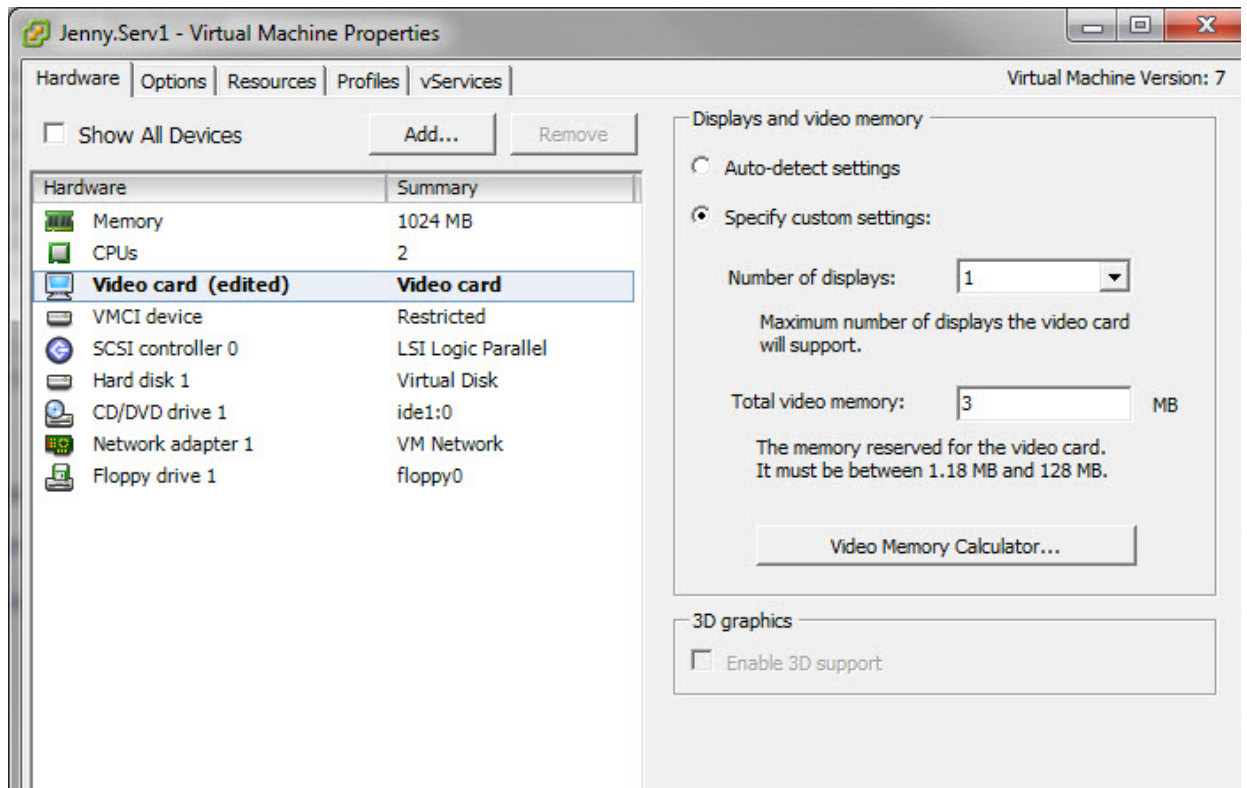
- 1 Using vSphere Client, make sure the SKM VM server you just created is powered OFF (right-click the VM server, select **Power**, then select **Power Off**).
- 2 Right-click the SKM VM server and select **Edit Settings**.
- 3 Configure the MAC address as follows (see [Figure 13](#)):
 - a Under the **Hardware** tab, select **Network adapter 1**.
 - b Under **MAC Address**, select **Manual**.
 - c In the **MAC Address** field, type the **MAC ID** from the label of the SKM software package from which you deployed the .ova image.
 - d Click **OK**.

Figure 13 Configuring the
MAC Address (Example)



- 4 Configure the video memory as follows:
 - a Right-click the SKM VM server and select **Edit Settings**.
 - b Under the **Hardware** tab, select **Video card** (see [Figure 14](#)).
 - c On the right side of the screen, under **Enter total video RAM**, change the setting to **3 MB**.
 - d Click **OK**.

Figure 14 Video Card Settings



- 5 Power ON the SKM VM server (right-click the SKM VM server in the left panel, select **Power**, then select **Power On**).
- 6 Highlight the SKM VM server in the left panel.
- 7 In the right panel, click the **Console** tab. Wait a few moments for the software to load.

Note: When using the console, you will lose the ability to use your mouse/cursor. To regain the use of the mouse/cursor, press **<Ctrl+Alt>**.

Note: If you receive the following error message when trying to use the console, follow the workaround steps listed below.
Error message: This kernel requires an x86-64 CPU, but only detected an xxx CPU. Unable to boot - please use a kernel appropriate for your CPU.
Workaround: First be sure that you are indeed using a 64-bit host server. If so, change the host BIOS processor settings as follows, then follow the onscreen instructions:
- 64-bit: Yes
- Virtual Technology: Enable
- Execute Disable: Disable

- 8 At the **skmserver login** prompt, type the following (this is the user login ID which will never change):
akmadmin
- 9 At the **Password** prompt, type the default password:
password
- 10 At the **akmadmin@skmserver** prompt, type:
./skmcmds
- 11 At the **Password** prompt, type the default password:
password
- 12 When prompted for the license, type the 29-digit **License Key** (including hyphens) from the label on the CD case of the CD from which you deployed the .ova image, and press **<Enter>**. The license is not case sensitive.
The license file is created.
- 13 When prompted, press **<Enter>**.
The End User License Agreement displays.
- 14 Read the license agreement. Press **<Enter>** to scroll through the agreement. At the end, type y to accept and continue or n to decline and stop the installation process.
- 15 When prompted, press **<Enter>** to set up the server.
- 16 The first setup wizard task prompts you to change the akmadmin password (see [Figure 15](#)). There is only one password for SKM. It is

called the akadmin password, and is required for all logins and access to commands, including backup and restore.

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

If you change the password from the default and forget it, there is no way to retrieve it!

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

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

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

- If you do not wish to change the password at this time, type **n** and press **<Enter>** at the “change password” prompts and the default password (password) remains. You can change the password at any time later using SKM Admin Commands.
- If you wish to change the password:
 - a** At the **(current) UNIX password** prompt, type the default password (password) and press **<Enter>**.
 - b** Type the new password and press **<Enter>**.
 - c** Type the new password again and press **<Enter>**.
 - d** Press **<Enter>**.

Figure 15 Changing the Password

```
Changing akadmin password.  
-----  
Changing password for akadmin.  
(current) UNIX password:  
Enter new UNIX password:  
Retype new UNIX password:
```

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

Note: To ensure proper TLS certificate generation, Quantum recommends setting both the Primary and Secondary SKM servers to the same date, time and time zone even if they are in different time zones. (On both servers, use the date, time and time zone values applicable to the Primary SKM server.)

Then, 24 hours after TLS certificate generation, you can correctly set the date, time and time zone for the secondary server.

Note: The default SKM VM server IP address is: **192.168.20.4**.

- 18 When finished, press **<Enter>**.

A message lets you know there are no certificates loaded on the SKM server.

- 19 Press **<Enter>**.

The list of SKM Admin Commands displays (see [Figure 16](#)). If you made any mistakes during the setup wizard, you can go back and change them by typing the number corresponding to the item you want to change at the **Command** prompt.

Figure 16 SKM Admin
Commands

```
SKM Admin Commands (Version 260Q.GC00600)
SKM
Server Cert's Validity:
/etc/akm/Certs/QKMServerSignedCert.pem
Not Before: May 1 19:01:37 2009 GMT and Not After : May 1 19:01:37 2019 GMT
Admin Cert's Validity:
/home/akmadmin/.akmadmin/Certs/QKMAAdminSignedCert.pem
Not Before: May 1 19:01:38 2009 GMT and Not After : May 1 19:01:38 2019 GMT

Current Date/Time: Fri Feb 15 13:19:24 CST 2019

-----
1) Launch SKM server setup wizard.
2) Change user account password.
3) Capture SKM server snapshot.
4) Set SKM server IP address.
5) Set SKM server time zone.
6) Set SKM server date and time.
7) Back up SKM server.
8) Restore SKM server.
9) Set SKM server hostname.
d) Display/update TLS communication certificates.
u) Update SKM server software.
r) Roll back SKM server software.
v) View SKM server reports.
```

20 At the **Command** prompt, type **q** and press **<Enter>** to quit, save your changes, and restart the SKM key server. This process takes a few seconds.

Note: You **MUST** quit at this point. Otherwise your changes will not be saved and you will not be able to continue the installation process.

21 Complete steps 1-20 on the secondary SKM server before proceeding.

22 When you are finished, do one of the following:

- For pre-SKM 2.4 (240Q) systems, proceed to [Installing TLS Certificates on the SKM Server for Pre-SKM 2.4 \(240Q\)](#) on page 59.
- For SKM 2.4 (240Q) and later systems, proceed to [Installing TLS Certificates on the SKM Server for SKM 2.4 \(240Q\) or Later](#) on page 70.

Installing and Configuring the SKM KVM Servers

Follow the instructions in this section if you are deploying a pair of SKM VM servers for installation in a KVM environment.

Perform all the instructions in this section **for each SKM VM server**. Use a different installation CD for each VM.

Caution: It is recommended that the two SKM VM servers be installed in different physical locations to provide better protection in case of disaster.

Caution: Quantum requires that you do not install any software, file, or operating system on the SKM appliance server or SKM VM server unless it is an upgrade or patch supplied by Quantum. Doing so may make your server inoperable and will void the warranty.

Equipment and Software Needed for KVM

You need the following to set up and configure the SKM VM servers:

- Two (2) Scalar Key Manager VM Installation CD packages. You must use a different CD package for each SKM server. Each CD package contains:
 - SKM VM server software (.raw.bz2 image)
 - SKM server Quantum-provided TLS communication certificate bundle (.tgz file)
 - Printed label on the CD case containing a unique serial number, MAC ID, and license key (required for installation)
- QEMU-KVM installed on a computer. The computer may be the same as the server that hosts the VM but it does not have to be. Access to QEMU-KVM is required for initial setup.
- Resources required for each SKM VM server:
 - (1) Ethernet interface
 - (1) CD ROM drive

- 1 GB RAM
- 8 GB of disk space
- KVM host software must Virtual Machine Manager 0.9.0 or higher
- Library firmware must be at the following minimum versions to run SKM. To access all the features of SKM 2.2 or later version, the most recent library firmware is recommended.

Library	Minimum Firmware Required
Scalar i3/i6	All firmware versions
Scalar i40/i80	120G
Scalar i500	570G
Scalar i6000	600A

- The SKM server must have IP connectivity through any firewalls to all Quantum libraries using the SKM appliance server to obtain encryption keys.
- SKM uses TCP ports 80, 6000 and 6001 for SKM server communication. These ports must all be open on your network in a bi-directional mode in order for SKM communication between the SKM servers and libraries to work.

Deploying the .raw Image on KVM

Follow the instructions below for **both SKM VM servers**. The .raw installation process is performed via QEMU-KVM.

- 1 Insert the Scalar Key Manager VM Installation CD into the your computer's CD ROM drive.
- 2 Decompress the .raw.bz2 image file to a known location. You may copy the image to a shared network drive for faster deployment if you wish.

For example: `bunzip2 5-01071-01_220Q.GC00300.raw.bz2`

- 3 Launch QEMU-KVM.
- 4 Log on to the VM host.
- 5 Under the local host, right-click and select **New**.

The **New VM** wizard opens.

Create a new virtual machine
Step 1 of 5

Enter your virtual machine details

Name:

Connection: localhost (QEMU/KVM)

Choose how you would like to install the operating system

- Local install media (ISO image or CDROM)
- Network Install (HTTP, FTP, or NFS)
- Network Boot (PXE)
- Import existing disk image

Cancel Back Forward

6 In the **Name** field, type the name of the new virtual machine.

7 Select **Import existing disk image** and click **Forward**.

Create a new virtual machine
Step 2 of 4

Provide the existing storage path:

Browse...

Choose an operating system type and version

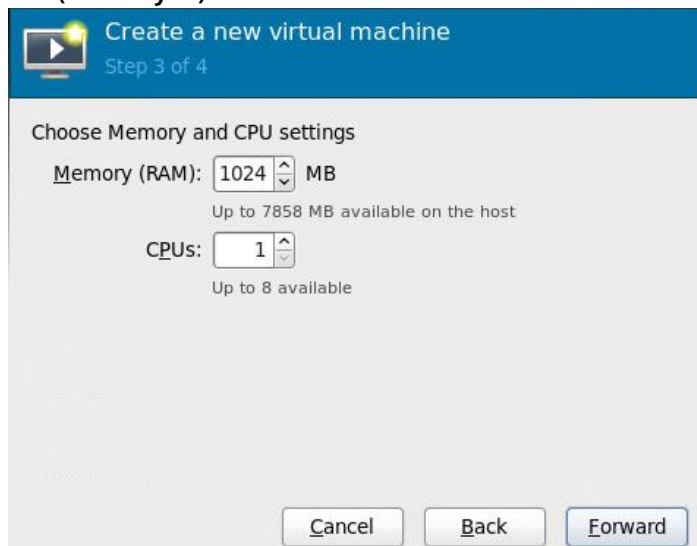
OS type: Generic

Version: Generic

Cancel Back Forward

8 Click **Browse** and navigate to the **.raw** file.

9 For OS type select **Linux** and for Version select **Ubuntu [version] (Lucid Lynx)**. Click **Forward**.



- 10 For **Memory (RAM)** select **1024** and for **CPUs** select **2**. Click **Forward**.

Create a new virtual machine
Step 4 of 4

Ready to begin installation of **SKMPRI**

OS: Ubuntu 10.04 (Lucid Lynx)
Install: Import existing OS image
Memory: 1024 MB
CPUs: 2
Storage: 8.0 Gb /SKM Raw /SKMPRI/220Q.GC00100.raw

Customize configuration before install

▼ Advanced options

Host device em4 (Bridge 'bridge0') ▾

Set a fixed MAC address

52:54:00:f5:f5:28

Virt Type: kvm ▾

Architecture: x86_64 ▾

Cancel Back Finish

- 11 For **Advanced Options** select the host device which corresponds with your virtual network interface.
- 12 Select Set a fixed MAC address and enter the MAC address provided on the installation CD. Ensure **Virt Type** is set to **kvm** and the **Architecture** is set to the default value.
- 13 Click **Finish** when done.

A progress bar displays on the screen. When complete, the SKM VM server name appears in the list of VMs on the screen. Deployment takes a few minutes to several hours depending on network speed and location of the .ova image in relation to the VM host. Wait until the file deploys before continuing.

Configuring the SKM VM Servers for KVM

Follow the instructions below for **both SKM VM servers**.

Note: Both SKM VM servers must be configured, operational, and connected to the network before any libraries can be set up to use them.

Caution: You must use a different CD package for each VM server. Keep track of which CD you use for which SKM server. It is recommended that you keep each CD in its respective CD case and write on the case which server it applies to. The TLS certificates and serial number/MAC address/license key are unique and you must use the correct ones if you ever need to reinstall the SKM server. Also, if you accidentally use the same CD package for both VM servers, you will not be able to complete the configuration.

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 the following values. Before beginning, decide what you want each of these values to be. You can also change these values in the future.

- Password
- Time zone, date, and time
- IP address, netmask, and gateway

Allow 30 minutes per server to complete the configuration.

- 1 Power ON the SKM VM server (right-click the SKM VM server in the left panel, select **Power**, then select **Power On**).
- 2 Highlight the SKM VM server in the left panel.
- 3 In the right panel, click the **Console** tab. Wait a few moments for the software to load.

Note: When using the console, you will lose the ability to use your mouse/cursor. To regain the use of the mouse/cursor, press **<Ctrl+Alt>**.

Note: If you receive the following error message when trying to use the console, follow the workaround steps listed below.
Error message: This kernel requires an x86-64 CPU, but only detected an xxx CPU. Unable to boot - please use a kernel appropriate for your CPU.
Workaround: First be sure that you are indeed using a 64-bit host server. If so, change the host BIOS processor settings as follows, then follow the onscreen instructions:
- 64-bit: Yes
- Virtual Technology: Enable
- Execute Disable: Disable

- 4 At the **skmserver login** prompt, type the following (this is the user login ID which will never change):
akmadmin
- 5 At the **Password** prompt, type the default password:
password
- 6 At the **akmadmin@skmserver** prompt, type:
./skmcmds
- 7 At the **Password** prompt, type the default password:
password
- 8 When prompted for the license, type the 29-digit **License Key** (including hyphens) from the label on the CD case of the CD from which you deployed the .ova image, and press **<Enter>**. The license is not case sensitive.
The license file is created.
- 9 When prompted, press **<Enter>**.
The End User License Agreement displays.
- 10 Read the license agreement. Press **<Enter>** to scroll through the agreement. At the end, type **y** to accept and continue or **n** to decline and stop the installation process.
- 11 When prompted, press **<Enter>** to set up the server.
- 12 The first setup wizard task prompts you to change the akmadmin password (see [Figure 15](#)). There is only one password for SKM. It is

called the akadmin password, and is required for all logins and access to commands, including backup and restore.

Figure 17 Changing the Password

```
Changing akadmin password.  
-----  
Changing password for akadmin.  
(current) UNIX password:  
Enter new UNIX password:  
Retype new UNIX password:
```

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

If you change the password from the default and forget it, there is no way to retrieve it!

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

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

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

- If you do not wish to change the password at this time, type **n** and press **<Enter>** at the “change password” prompts and the default password (password) remains. You can change the password at any time later using SKM Admin Commands.
- If you wish to change the password:
 - a At the **(current) UNIX password** prompt, type the default password (password) and press **<Enter>**.
 - b Type the new password and press **<Enter>**.
 - c Type the new password again and press **<Enter>**.

d Press <Enter>.

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

Note: To ensure proper TLS certificate generation, Quantum recommends setting both the Primary and Secondary SKM servers to the same date, time and time zone even if they are in different time zones. (On both servers, use the date, time and time zone values applicable to the Primary SKM server.)

Then, 24 hours after TLS certificate generation, you can correctly set the date, time and time zone for the secondary server.

Note: The default SKM VM server IP address is: **192.168.20.4**.

- 14 When finished, press <Enter>.

A message lets you know there are no certificates loaded on the SKM server.

- 15 Press <Enter>.

The list of SKM Admin Commands displays (see [Figure 16](#)). If you made any mistakes during the setup wizard, you can go back and change them by typing the number corresponding to the item you want to change at the **Command** prompt.

Figure 18 SKM Admin
Commands

```
SKM Admin Commands (Version 260Q.GC00600)
SKM
Server Cert's Validity:
/etc/akm/Certs/QKMServerSignedCert.pem
  Not Before: May  1 19:01:37 2009 GMT and Not After : May  1 19:01:37 2019 GMT
Admin Cert's Validity:
/home/akmadmin/.akmadmin/Certs/QKMAAdminSignedCert.pem
  Not Before: May  1 19:01:38 2009 GMT and Not After : May  1 19:01:38 2019 GMT

Current Date/Time: Fri Feb 15 13:19:24 CST 2019

-----
1) Launch SKM server setup wizard.
2) Change user account password.
3) Capture SKM server snapshot.
4) Set SKM server IP address.
5) Set SKM server time zone.
6) Set SKM server date and time.
7) Back up SKM server.
8) Restore SKM server.
9) Set SKM server hostname.
d) Display/update TLS communication certificates.
u) Update SKM server software.
r) Roll back SKM server software.
```

16 At the **Command** prompt, type `q` and press **<Enter>** to quit, save your changes, and restart the SKM key server. This process takes a few seconds.

Note: You **MUST** quit at this point. Otherwise your changes will not be saved and you will not be able to continue the installation process.

17 Complete steps 1-16 on the secondary SKM server before proceeding.

18 When you are finished, do one of the following:

- For pre-SKM 2.4 (240Q) systems, proceed to [Installing TLS Certificates on the SKM Server for Pre-SKM 2.4 \(240Q\)](#) on page 59.
- For SKM 2.4 (240Q) and later systems, proceed to [Installing TLS Certificates on the SKM Server for SKM 2.4 \(240Q\) or Later](#) on page 70.

Installing TLS Certificates on the SKM Server for Pre-SKM 2.4 (240Q)

Note: All TLS Certificates that were provided on the initial CDs are likely already expired. New TLS Certificates must be generated by the customer or obtained from Quantum.

TLS certificates are required on the SKM server. You can choose to use the Quantum-provided TLS certificates or install your own, as follows:

- **SKM appliance server:** The SKM appliance server comes with Quantum-provided TLS certificates already installed. You can install your own TLS certificates (to overwrite the installed certificates) if you wish.

Note: This applies only to earlier SKM releases. Beginning with SKM 2.5, TLS certificates are no longer pre-installed, and must be installed on both the SKM server and tape library.

- **SKM VM server:** The Scalar Key Manager 2.2 VM Installation CD contains Quantum-provided TLS certificates that you can install on the SKM VM server. Alternatively, you can install your own TLS certificates on the SKM VM server.

If you install your own TLS certificates, you must make sure that your certificates meet all of the requirements in [Configuring Your Library For SKM](#) on page 83.

Note: Any time you install TLS certificates, they will overwrite any TLS certificates currently installed on the SKM server.

Note: Beginning with SKM 2.4 (240Q), a different procedure is used to install TLS certificates. Refer to [Installing TLS Certificates on the SKM Server for SKM 2.4 \(240Q\) or Later](#) on page 70.

Requirements for Installing User-provided TLS Certificates

When providing your own certificates, it is assumed you understand the concepts of PKI and can access the tools or third-party resources needed to generate or obtain certificates. See [Importing TLS Communication Certificates on the Library](#) on page 139 and [Exporting and Importing Encryption Certificates](#) on page 146 for more information.

Note: You must be running SKM 1.1 or higher on your SKM servers in order to install your own TLS certificates.

Note: If you install your own TLS certificates on the SKM server, you must also install your own certificates on the library. Similarly, if you use the Quantum-provided TLS certificates on the SKM server, you must also use the Quantum provided TLS certificates on the library. Some newer libraries come with Quantum-provided TLS certificates pre-installed, and other newer libraries require certificate installation. See your library user's guide for instructions on how to verify whether TLS certificates are installed on the library and how to install them.

You need to provide the following certificates:

- Root Certificate (also called the CA certificate, or Certificate Authority Certificate)
- Server Certificate
- Admin Certificate

These files must be in the proper format, as follows. If any of the following requirements is not met, none of the certificates will be imported.

- The Root Certificate must be 2048 bits.
- The Root Certificate must be in PEM format.
- The Admin and Server certificates must be in pkcs12 (.p12) format, with a separate certificate and private key contained in each.
- The Admin and Server certificates must be at least 1024 bits.

Note: SKM-attached Scalar libraries support communication certificate key lengths of 1024 bits. Communication certificates larger than 1024 bits, such as 2048 and 4096 bit key lengths, are not currently supported by all library models, but will be supported with a future prerequisite library firmware release. (Refer to the Scalar library release notes or contact Quantum/support for additional information and availability of required library firmware). However, using communication certificates with key bit lengths larger 1024 bits will affect library performance with respect to encryption key retrieval times and encryption key generation, import and export operations. While certificate key lengths of 2048 bits slightly slow operations in single and multi-library attached SKM server environments, the use of communication certificates with a key length of 4096 bits should be avoided in SKM configuration environments where multiple Scalar tape libraries are attached to a single SKM server pair.

- The Admin and Server certificates must be signed by the Root Certificate.
- Certificates must have the Organization name (O) set in their Issuer and Subject info.
- The Admin certificate must have its Organizational Unit name (OU) set as "akm_admin" in its Subject Info.
- The same Root Certificate must be installed on the SKM servers and the library.
- All the certificates must have a valid validity period according to the date and time settings on the SKM server.

OpenSSL Parameter Descriptions

Descriptions of the OpenSSL Parameters are listed below.

Note: These parameters must be defined: C, ST, L, O, OU, and CN.

- **Version** — the version of the X.509 specification that the certificate follows.
- **Serial** — the certificate's serial number.

- **signatureAlg** — the algorithm used by the Certificate Authority to sign the certificate.
- **BeginDate** — the date at which the certificate became valid.
- **EndDate** — the certificate's expiry date.
- **PublicKey** — the certificate's public key.
- **FriendlyName** — the certificate's friendly name.
- **Subject: CN** — the certificate owner's common name.
- **Subject: E** — the certificate owner's e-mail address.
- **Subject: T** — the certificate owner's title.
- **Subject: L** — the certificate owner's locality.
- **Subject: ST** — the certificate owner's state of residence.
- **Subject: O** — the organization to which the certificate owner belongs.
- **Subject: OU** — the name of the organizational unit to which the certificate owner belongs.
- **Subject: C** — the certificate owner's country of residence.
- **Subject: STREET** — the certificate owner's street address.
- **Subject: ALL** — the certificate owner's complete distinguished name.
- **Issuer: CN** — the certificate issuer's common name.
- **Issuer: E** — the certificate issuer's e-mail address.
- **Issuer: T** — the certificate issuer's title.
- **Issuer: L** — the certificate issuer's locality.
- **Issuer: ST** — the certificate issuer's state of residence.
- **Issuer: O** — the organization to which the certificate issuer belongs.
- **Issuer: OU** — the organizational unit to which the certificate issuer belongs.
- **Issuer: C** — the certificate issuer's country of residence.
- **Issuer: STREET** — the certificate issuer's street address.
- **Issuer: ALL** — the certificate issuer's complete distinguished name.

Creation Process

The process of creating TLS Certificates is outlined in the basic procedure below. Be sure to follow these steps in the order shown.

Create Root Certificate in 2048 PEM Format

- 1 Create a 2048 bit RSA key file (file CA_rsa_key.pem).

Example: `$ openssl genrsa -out CA_rsa_key.pem 2048`

- 2 Create a root certificate request file which will be signed in the next step (file CA_request.pem).

Example: `$ openssl req -new -key CA_rsa_key.pem -out CA_request.pem -days 3653`

- 3 Create a self signed root certificate (file CA_signed.pem).

Example: `$ openssl x509 -req -days 3653 -in CA_request.pem -signkey CA_rsa_key.pem -out CA_signed.pem`

- 4 Create a readable file CA_signed_info.pem which can be opened in an editor.

Example: `$ openssl x509 -noout -fingerprint -text <CA_signed.pem> CA_signed_info.pem`

Create Admin Certificate for the Library

- 1 Create a 1024 bit RSA key (file Admin_lib_rsa_key.pem).

Example: `$ openssl genrsa -out Admin_lib_rsa_key.pem 1024`

- 2 Create an admin certificate request file which will be signed in the next step (file Admin_lib_request.pem) – OU=akm_admin must be used.

Example: `$ openssl req -new -key Admin_lib_rsa_key.pem -out Admin_lib_request.pem -days 3653`

- 3 Create a signed Admin certificate (file Admin_lib_signed.pem) - CA certificate must be used for creation.

Example: `$ openssl x509 -req -days 3653 -in Admin_lib_request.pem -CA CA_signed.pem -Cakey`

```
CA_rsa_key.pem -set_serial 1 -out  
Admin_lib_signed.pem
```

- 4 Create a readable file Admin_lib_signed_info.pem which can be opened in an editor.

```
Example: $ openssl x509 -noout -fingerprint -text  
<Admin_lib_signed.pem> Admin_lib_signed_info.pem
```

- 5 Convert the RSA and the signed Admin files into the p12 format (password protected).

```
Example: $ openssl pkcs12 -export -in  
Admin_lib_signed.pem -inkey Admin_lib_rsa_key.pem -  
out Admin_lib.p12 -passin pass:password
```

Create Client Certificate for the Library

- 1 Create a 1024 bit RSA key (file Client_lib_rsa_key.pem).

```
Example: $ openssl genrsa -out Client_lib_rsa_key.pem  
1024
```

- 2 Create a client certificate request file which will be signed in the next step (file Client_lib_request.pem).

```
Example: $ openssl req -new -key  
Client_lib_rsa_key.pem -out Client_lib_request.pem -  
days 3653
```

- 3 Create a signed Client certificate (file Client_lib_signed.pem) - CA certificate must be used for creation.

```
Example: $ openssl x509 -req -days 3653 -in  
Client_lib_request.pem -CA CA_signed.pem -CAkey  
CA_rsa_key.pem -set_serial 2 -out  
Client_lib_signed.pem
```

- 4 Create a readable file Client_lib_signed_info.pem which can be opened in an editor.

```
Example: $ openssl x509 -noout -fingerprint -text  
<Client_lib_signed.pem> Client_lib_signed_info.pem
```

- 5 Convert the RSA and the signed Client files into the p12 format (password protected).

Example: \$ openssl pkcs12 -export -in Client_lib_signed.pem -inkey Client_lib_rsa_key.pem -out Client.p12 -passin pass:password

Create Admin Certificate for the Primary SKM Server

- 1 Create a 1024 bit RSA key (file Admin_serv1_rsa_key.pem).

Example: \$ openssl genrsa -out Admin_serv1_rsa_key.pem 1024

- 2 Create an Admin certificate request file which will be signed in the next step (file Admin_serv1_request.pem) – OU=akm_admin must be used.

Example: \$ openssl req -new -key Admin_serv1_rsa_key.pem -out Admin_serv1_request.pem -days 3653

- 3 Create a signed Admin certificate (file Admin_serv1_signed.pem) - CA certificate must be used for creation.

Example: \$ openssl x509 -req -days 3653 -in Admin_serv1_request.pem -CA CA_signed.pem -CAkey CA_rsa_key.pem -set_serial 3 -out Admin_serv1_signed.pem

- 4 Create a readable file Admin_serv1_signed_info.pem which can be opened in an editor.

Example: \$ openssl x509 -noout -fingerprint -text <Admin_serv1_signed.pem> Admin_serv1_signed_info.pem

- 5 Convert the RSA and the signed Admin files into the p12 format (password protected).

Example: \$ openssl pkcs12 -export -in Admin_serv1_signed.pem -inkey Admin_serv1_rsa_key.pem -out Admin_serv1.p12 -passin pass:password

Create Server Certificate for the Primary SKM Server

- 1 Create a 1024 bit RSA key (file Server1_rsa_key.pem).

Example: \$ openssl genrsa -out Server1_rsa_key.pem 1024

- 2 Create a Server certificate request file which will be signed in the next step (file Server1_request.pem).
Example: `$ openssl req -new -key Server1_rsa_key.pem -out Server1_request.pem -days 3653`
- 3 Create a signed Server certificate (file Server1_signed.pem) - CA certificate must be used for creation.
Example: `$ openssl x509 -req -days 3653 -in Server1_request.pem -CA CA_signed.pem -CAkey CA_rsa_key.pem -set_serial 4 -out Server1_signed.pem`
- 4 Create a readable file Server1_signed_info.pem which can be opened in an editor.
Example: `$ openssl x509 -noout -fingerprint -text <Server1_signed.pem> Server1_signed_info.pem`
- 5 Convert the RSA and the signed Server files into the p12 format (password protected).
Example: `$ openssl pkcs12 -export -in Server1_signed.pem -inkey Server1_rsa_key.pem -out Server1.p12 -passin pass:password`

Create Admin Certificate for the Secondary SKM Server

- 1 Create a 1024 bit RSA key (file Admin_serv2_rsa_key.pem).
Example: `$ openssl genrsa -out Admin_serv2_rsa_key.pem 1024`
- 2 Create an Admin certificate request file which will be signed in the next step (file Admin_serv2_request.pem) – OU=akm_admin must be used.
Example: `$ openssl req -new -key Admin_serv2_rsa_key.pem -out Admin_serv2_request.pem -days 3653`
- 3 Create a signed Admin certificate (file Admin_serv2_signed.pem) - CA certificate must be used for creation.
Example: `$ openssl x509 -req -days 3653 -in Admin_serv2_request.pem -CA CA_signed.pem -CAkey CA_rsa_key.pem -set_serial 5 -out Admin_serv2_signed.pem`

- 4 Create a readable file `Admin_serv2_signed_info.pem` which can be opened in an editor.

Example: `$ openssl x509 -noout -fingerprint -text <Admin_serv2_signed.pem> Admin_serv2_signed_info.pem`

- 5 Convert the RSA and the signed Admin files into the p12 format (password protected).

Example: `$ openssl pkcs12 -export -in Admin_serv2_signed.pem -inkey Admin_serv2_rsa_key.pem -out Admin_serv2.p12 -passin pass:password`

Create Server Certificate for the Secondary SKM Server

- 1 Create a 1024 bit RSA key (file `Server2_rsa_key.pem`).

Example: `$ openssl genrsa -out Server2_rsa_key.pem 1024`

- 2 Create a Server certificate request file which will be signed in the next step (file `Server2_request.pem`)

Example: `$ openssl req -new -key Server2_rsa_key.pem -out Server2_request.pem -days 3653`

- 3 Create a signed Server certificate (file `Server2_signed.pem`) - CA certificate must be used for creation.

Example: `$ openssl x509 -req -days 3653 -in Server2_request.pem -CA CA_signed.pem -CAkey CA_rsa_key.pem -set_serial 6 -out Server2_signed.pem`

- 4 Create a readable file `Server2_signed_info.pem` which can be opened in an editor.

Example: `$ openssl x509 -noout -fingerprint -text <Server2_signed.pem> Server2_signed_info.pem`

- 5 Convert the RSA and the signed Server files into the p12 format (password protected).

Example: `$ openssl pkcs12 -export -in Server2_signed.pem -inkey Server2_rsa_key.pem -out Server2.p12 -passin pass:password`

Installation Process

This procedure must be performed on both SKM servers.

- 1 SSH in to the SKM server. (If you have an SKM VM server, you can SSH in or continue to use the vSphere console and proceed to [Step 4](#) below.)
- 2 At the login prompt, type the login ID:
akmadmin
- 3 At the **Password** prompt, type your password.
- 4 At the akmadmin@skmserver prompt, type:
./skmcmds
- 5 At the **Password** prompt, type your password.
A message displays alerting you that the SKM key server will be stopped.
- 6 Type y to agree to stop the SKM key server and continue.
A message appears stating the SKM key server is being stopped.
- 7 Press <Enter> to continue.
The list of SKM Admin Commands displays.
- 8 At the **Command** prompt, type d to **Display/update TLS communication certificates**.
The **Display/update TLS communication certificates** menu displays.
- 9 Using SFTP, transfer the Quantum certificate bundle file or your own certificates to the **/home/akmadmin/certs** directory on the SKM server. Be sure to move the appropriate bundle; there is a primary bundle and a secondary bundle.
- 10 At the **Command** prompt, enter one of the following:
 - If you used the -d or no -d option: i (to Install user provided communication certificates)OR
 - If you used the -q option: a (to Apply Quantum-provided communication certificate bundle).
- 11 Once you have transferred the files, press <Enter>.

A list of the certificate/bundle files currently in the /home/akmadmin/certs directory displays ([Figure 19](#) shows an example).

Figure 19 Example of Quantum Certificate Bundle Displayed on Screen

```
Email address []

Generating the SKM primary server, secondary server and library communication certificates.

Creating certificates for tapelibrary.

Creating certificates for primary.

Creating certificates for secondary.

Quantum bundle generation is complete. All the generated files are located in /home/akmadmin/generatedcerts/qbundles.

The following bundles need to be loaded onto the library and SKM servers using the user interface:
  1) TapeLibraryQKMCert_121220191026.tgz
  2) QKMPrimaryServerCert_121220191026.tgz
  3) QKMSecondaryServerCert_121220191026.tgz

akmadmin@skmserver:~$
```

12 Type the file name of the appropriate certificate/bundle and press **<Enter>**. If you are installing your own certificates, follow the onscreen instructions to load all three certificates.

The certificates are installed.

13 Press **<Enter>**.

14 At the **Command** prompt, type **q** and press **<Enter>** to exit to the Display/update TLS communication certificates menu.

15 At the **Command** prompt, type **q** and press **<Enter>** to quit, save your changes, and restart the SKM key server. This process takes a few seconds.

Note: You MUST quit at this point. Otherwise the server will remain stopped and you will not be able to continue the configuration process on the library.

- 16 Repeat all preceding steps (1-15) on the secondary SKM server.
- 17 Back up the SKM server (changing the TLS Certificates needs to be captured for a restore to work).
- 18 Proceed to [Configuring Your Library For SKM](#) on page 83.

Installing TLS Certificates on the SKM Server for SKM 2.4 (240Q) or Later

Note: Use the SKM server that has the earliest Date/Time/Time zone configured for generating the TLS Certificates.

- If the TLS Certificates are generated on an SKM server that has a Date/Time/Time zone that is later than the other server, then the TLS Certs will now work on the other server until that Date/Time has been reached.
- This has caused a lot of confusion and wasted a lot of time on escalations in the past.
- This same requirement also applies to the Date/Time/Time Zone configured on the tape libraries.

Beginning with SKM 2.4 (240Q), it is now possible to self-generate library/SKM TLS communication certificates using SKM server with version 2.4 (240Q) or greater loaded.

This certificate-generation process generates sets of TLS certificates that can be loaded onto the primary and secondary SKM servers and all libraries attached to the servers.

Note: The TLS certificate generation process must be run on only one of the SKM servers, so there is no need to generate TLS Certificates on both SKM servers. Either the Primary or Secondary SKM server can be used to generate the certificates.

Specifically, the genSKMcerts script is loaded onto the SKM servers using one of three ways to generate certificates:

- By executing the script using the “-d” option. Certificates are generated using a set of default values similar to the certificates currently provided by Quantum.
- By executing the script without using the “-d” option. If the “-d” option is not used, information used to generate the certificates must be provided.
- By executing the script with the “-Q” option. A Quantum certificate bundle is generated using a default set of values.

Begin the Installation

- 1 SSH in to the SKM server. (If you have an SKM VM server, you can SSH in or continue to use the vSphere console and proceed to Step 4 below.)
- 2 At the **skmserver login** prompt, type the login ID:
akmadmin
- 3 At the **Password** prompt, type your password.

Executing the Script Using the -d Option

Use the following procedure to generate certificates using the -d option, which uses default values. The generated certificates are valid for ten years from the date on which they were generated.

- 1 Once logged into an SKM server running 240Q or greater, execute **genSKMcerts -d** to generate certificates using the defaults.

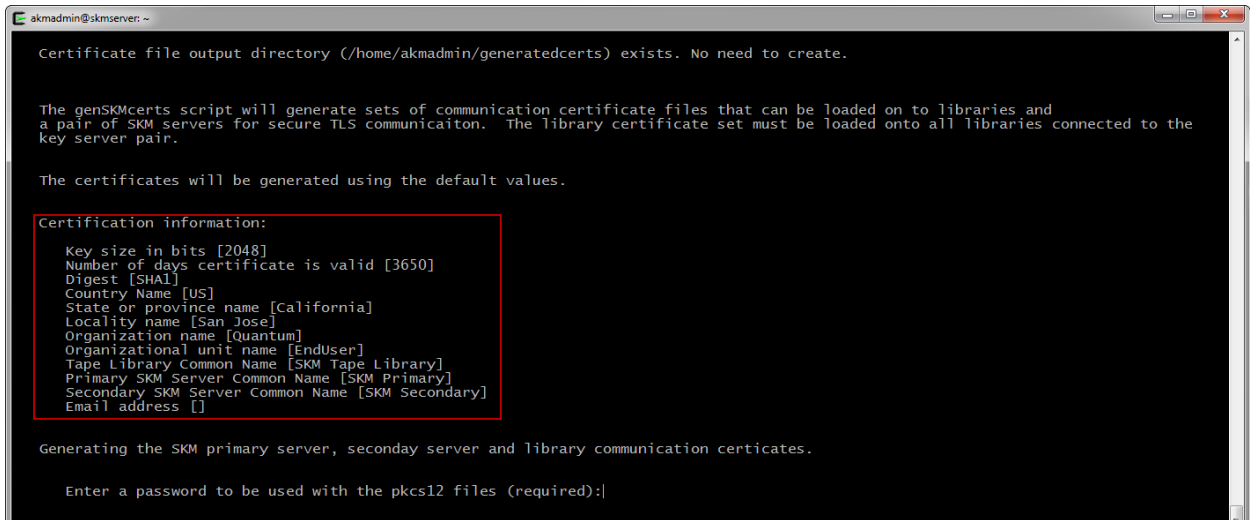


```
akmadmin@skmserver: ~  
akmadmin@skmserver:~$ genSKMcerts -d
```

Chapter 4: Initial Configuration and Setup

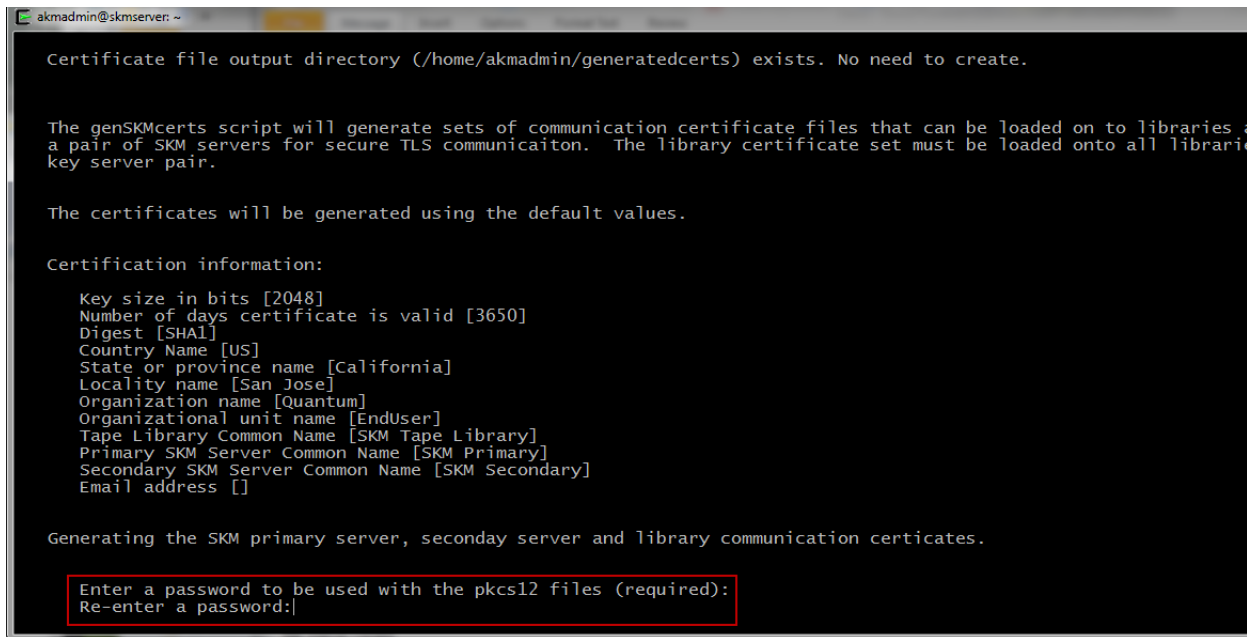
Installing TLS Certificates on the SKM Server for SKM 2.4 (240Q) or Later

The following illustration shows the default values (in brackets) used:



```
akmadmin@skmserver: ~  
Certificate file output directory (/home/akmadmin/generatedcerts) exists. No need to create.  
  
The genSKMcerts script will generate sets of communication certificate files that can be loaded on to libraries and  
a pair of SKM servers for secure TLS communication. The library certificate set must be loaded onto all libraries connected to the  
key server pair.  
  
The certificates will be generated using the default values.  
  
Certification information:  
Key size in bits [2048]  
Number of days certificate is valid [3650]  
Digest [SHA1]  
Country Name [US]  
State or province name [California]  
Locality name [San Jose]  
Organization name [Quantum]  
Organizational unit name [EndUser]  
Tape Library Common Name [SKM Tape Library]  
Primary SKM Server Common Name [SKM Primary]  
Secondary SKM Server Common Name [SKM Secondary]  
Email address []  
  
Generating the SKM primary server, secondary server and library communication certificates.  
  
Enter a password to be used with the pkcs12 files (required):|
```

- 2 When prompted, enter and re-enter a password that will be used during the pk12 file generation.



```
akmadmin@skmserver: ~  
Certificate file output directory (/home/akmadmin/generatedcerts) exists. No need to create.  
  
The genSKMcerts script will generate sets of communication certificate files that can be loaded on to libraries and  
a pair of SKM servers for secure TLS communication. The library certificate set must be loaded onto all libraries  
key server pair.  
  
The certificates will be generated using the default values.  
  
Certification information:  
Key size in bits [2048]  
Number of days certificate is valid [3650]  
Digest [SHA1]  
Country Name [US]  
State or province name [California]  
Locality name [San Jose]  
Organization name [Quantum]  
Organizational unit name [EndUser]  
Tape Library Common Name [SKM Tape Library]  
Primary SKM Server Common Name [SKM Primary]  
Secondary SKM Server Common Name [SKM Secondary]  
Email address []  
  
Generating the SKM primary server, secondary server and library communication certificates.  
  
Enter a password to be used with the pkcs12 files (required):  
Re-enter a password:|
```

TLS certificate generation is completed using the default values. A message informs you when certificate generation is complete. The location of the certificates (/home/akmadmin/generatedcerts) is also provided.

- 3 Complete the process by loading the certificates onto the SKM servers and tape libraries using the procedures described in the user's guide for the applicable libraries.
 - For the Scalar i40/i80, refer to "Importing Encryption Certificates" in the Scalar i40 and Scalar i80 User's Guide.
 - For the Scalar i6000, refer to "Step 3 — Installing TLS Communication Certificates on the Library" in the Quantum Scalar i6000 User's Guide.
 - For the Scalar i3, refer to the topic "Load Certificate - Encryption" in the Scalar i3 Documentation Center:
https://qsupport.quantum.com/kb/flare/content/Scalar_i3/docCenter/Encryption_Overview.htm?Highlight=load%20certificates
 - For the Scalar i6, refer to the topic in the Scalar i6 Documentation Center:
https://qsupport.quantum.com/kb/flare/content/Scalar_i6/docCenter/Encryption_Overview.htm?Highlight=load%20certificates

Names of the files to copy are listed on the final screen that informs you that certificate generation is complete.

```

akmadmin@skmsserver: ~
Tape Library Common Name [Backup Libraries]
Primary SKM Server Common Name [SKM Primary]
Secondary SKM Server Common Name [SKM Secondary]
Email address [john.doe@widgets.com]

Is the certificate information displayed correct (y=yes, n=no): y
Generating the SKM primary server, secondary server and library communication certificates.

Enter a password to be used with the pkcs12 files (required):
Re-enter a password to be used with the pkcs12 files:

Creating certificates for tapelibrary.
Creating certificates for primary.
Creating certificates for secondary.

Certificate generation is complete. All the generated certificate files are located in /home/akmadmin/generatedcerts/ sub directory (tapelibrarycerts, skmprimarycerts or skmsecondarycerts.)

The following files need to be loaded onto the library using the remote GUI interface:
1) SKM_CA_signed_093020161411.pem
2) SKM_tapelibrary_admin_093020161411.pk12
3) SKM_tapelibrary_client_093020161411.pk12
The following files need to be loaded onto the primary SKM server using ./skmcmds:
1) SKM_CA_signed_093020161411.pem
2) SKM_primary_admin_093020161411.pk12
3) SKM_primary_server_093020161411.pk12
The following files need to be loaded onto the secondary SKM server using ./skmcmds:
1) SKM_CA_signed_093020161411.pem
2) SKM_secondary_admin_093020161411.pk12
3) SKM_secondary_server_093020161411.pk12

akmadmin@skmsserver:~$

```

- 4 If desired, you can verify the certificate details by running the `ls -R generatedcerts/` command.

```

akmadmin@skmsserver: ~
akmadmin@skmsserver:~$ ls -R generatedcerts/
generatedcerts/:
skmprimarycerts  skmsecondarycerts  tapelibrarycerts

generatedcerts/skmprimarycerts:
SKM_CA_signed_093020161455.pem  SKM_primary_admin_093020161455.pk12  SKM_primary_server_093020161455.pk12

generatedcerts/skmsecondarycerts:
SKM_CA_signed_093020161455.pem  SKM_secondary_admin_093020161455.pk12  SKM_secondary_server_093020161455.pk12

generatedcerts/tapelibrarycerts:
SKM_CA_signed_093020161455.pem  SKM_tapelibrary_admin_093020161455.pk12  SKM_tapelibrary_client_093020161455.pk12
akmadmin@skmsserver:~$

```

Executing the Script Without Using the -d Option

Use the following procedure to generate certificates without using the -d option. This method requires you to enter certificate values. If desired, you can press **Enter** to accept the default value (displayed in brackets) for any item.

- 1 Once logged into an SKM server running version 2.4 (240Q) or greater, execute `genSKMcerts` to begin entering the values used to generate certificates.

```
akmadmin@skmserver: ~  
akmadmin@skmserver:~$ genSKMcerts
```

- 2 Enter the size of the key in bits. Valid key sizes are 1024, 2048 or 4096 bits. The default size is 2048 bits.

```
akmadmin@skmserver: ~  
Certificate file output directory (/home/akmadmin/generatedcerts) exists. No need to create.  
  
The genSKMcerts script will generate sets of communication certificate files that can be loaded on to libraries a  
a pair of SKM servers for secure TLS communicaiton. The library certificate set must be loaded onto all librari  
key server pair.  
  
Please provide the certicate information requested (or hit enter to use the default value shown in brackets [ ].)  
Enter key size in bits (1024, 2048, 4096) [2048]:
```

- 3 Enter the duration in days for which the TLS certificates will be valid. The default duration is 10 years (3650 days).

```
akmadmin@skmserver: ~  
Certificate file output directory (/home/akmadmin/generatedcerts) exists. No need to create.  
  
The genSKMcerts script will generate sets of communication certificate files that can be loaded on to libraries a  
a pair of SKM servers for secure TLS communicaiton. The library certificate set must be loaded onto all librari  
key server pair.  
  
Please provide the certicate information requested (or hit enter to use the default value shown in brackets [ ].)  
Enter key size in bits (1024, 2048, 4096) [2048]: 2048  
Enter number of days the certificate will be valid [3650]: 365
```

Chapter 4: Initial Configuration and Setup

Installing TLS Certificates on the SKM Server for SKM 2.4 (240Q) or Later

- 4 At this time the only valid certificate digest is “SHA1”, so press **Enter** to accept the default value and continue.
- 5 Enter your two-character country identifier.

```
akmadmin@skmsserver: ~  
Certificate file output directory (/home/akmadmin/generatedcerts) exists. No need to create.  
  
The genSKMcerts script will generate sets of communication certificate files that can be loaded on to libraries a  
a pair of SKM servers for secure TLS communicaiton. The library certificate set must be loaded onto all libraries  
key server pair.  
  
Please provide the certicate information requested (or hit enter to use the default value shown in brackets[ .])  
Enter key size in bits (1024, 2048, 4096) [2048]: 2048  
Enter number of days the certificate will be valid [3650]: 365  
Enter certificate digest (currently only SHA1 supported) [SHA1]:  
Enter two character country name [US]:
```

- 6 Enter your state or province name.

```
akmadmin@skmsserver: ~  
Certificate file output directory (/home/akmadmin/generatedcerts) exists. No need to create.  
  
The genSKMcerts script will generate sets of communication certificate files that can be loaded on to libraries a  
a pair of SKM servers for secure TLS communicaiton. The library certificate set must be loaded onto all libraries  
key server pair.  
  
Please provide the certicate information requested (or hit enter to use the default value shown in brackets[ .])  
Enter key size in bits (1024, 2048, 4096) [2048]: 2048  
Enter number of days the certificate will be valid [3650]: 365  
Enter certificate digest (currently only SHA1 supported) [SHA1]:  
Enter two character country name [US]: US  
Enter state or province name [California]:
```

- 7 Enter your locality or city name.

```
akmadmin@skmsserver: ~  
Certificate file output directory (/home/akmadmin/generatedcerts) exists. No need to create.  
  
The genSKMcerts script will generate sets of communication certificate files that can be loaded on to libraries and  
a pair of SKM servers for secure TLS communicaiton. The library certificate set must be loaded onto all libraries con  
by server pair.  
  
Please provide the certicate information requested (or hit enter to use the default value shown in brackets[ .])  
Enter key size in bits (1024, 2048, 4096) [2048]: 2048  
Enter number of days the certificate will be valid [3650]: 365  
Enter certificate digest (currently only SHA1 supported) [SHA1]:  
Enter two character country name [US]: US  
Enter state or province name [California]: Texas  
Enter locality name (city) [San Jose]:
```

8 Enter your company or organization name.

```
akmadmin@skmserver: ~  
Certificate file output directory (/home/akmadmin/generatedcerts) exists. No need to create.  
  
The genSKMcerts script will generate sets of communication certificate files that can be loaded on to libraries and  
a pair of SKM servers for secure TLS communication. The library certificate set must be loaded onto all libraries and  
key server pair.  
  
Please provide the certificate information requested (or hit enter to use the default value shown in brackets[ ].)  
Enter key size in bits (1024, 2048, 4096) [2048]: 2048  
Enter number of days the certificate will be valid [3650]: 365  
Enter certificate digest (currently only SHA1 supported) [SHA1]:  
Enter two character country name [US]: US  
Enter state or province name [California]: Texas  
Enter locality name (city) [San Jose]: Richardson  
Enter organization name (company) [Quantum]:
```

9 Enter your organizational unit or section name.

```
admin@skmserver: ~  
Certificate file output directory (/home/akmadmin/generatedcerts) exists. No need to create.  
  
The genSKMcerts script will generate sets of communication certificate files that can be loaded on to libraries and  
a pair of SKM servers for secure TLS communication. The library certificate set must be loaded onto all libraries and  
key server pair.  
  
Please provide the certificate information requested (or hit enter to use the default value shown in brackets[ ].)  
Enter key size in bits (1024, 2048, 4096) [2048]: 2048  
Enter number of days the certificate will be valid [3650]: 365  
Enter certificate digest (currently only SHA1 supported) [SHA1]:  
Enter two character country name [US]: US  
Enter state or province name [California]: Texas  
Enter locality name (city) [San Jose]: Richardson  
Enter organization name (company) [Quantum]: Widgets Inc.  
Enter organizational unit name (section) [EndUser]:
```

- 10 The next three entries are common names for the Tape libraries, SKM primary server and SKM secondary server. The names must be unique because these names will be used for the different sets of certificates.

Chapter 4: Initial Configuration and Setup

Installing TLS Certificates on the SKM Server for SKM 2.4 (240Q) or Later

```
akmadmin@skmsserver: ~  
Certificate file output directory (/home/akmadmin/generatedcerts) exists. No need to create.  
  
The genSKMcerts script will generate sets of communication certificate files that can be loaded on to libraries and  
a pair of SKM servers for secure TLS communication. The library certificate set must be loaded onto all libraries and  
key server pair.  
  
Please provide the certificate information requested (or hit enter to use the default value shown in brackets[ .])  
  
Enter key size in bits (1024, 2048, 4096) [2048]: 2048  
Enter number of days the certificate will be valid [3650]: 365  
Enter certificate digest (currently only SHA1 supported) [SHA1]:  
Enter two character country name [US]: US  
Enter state or province name [California]: Texas  
Enter locality name (city) [San Jose]: Richardson  
Enter organization name (company) [Quantum]: Widgets Inc.  
Enter organizational unit name (section) [EndUser]: Manufacturing  
Enter tape library common name (must be unique)[SKM Tape Library]:  
Enter primary SKM server common name (must be unique)[SKM Primary]:  
Enter secondary SKM server common name (must be unique)[SKM Secondary]:
```

11 The last entry is optional: an email address that will be included with the certificate information.

```
ertificate file output directory (/home/akmadmin/generatedcerts) exists. No need to create.  
  
he genSKMcerts script will generate sets of communication certificate files that can be loaded on to libraries and  
pair of SKM servers for secure TLS communication. The library certificate set must be loaded onto all libraries and  
ey server pair.  
  
lease provide the certificate information requested (or hit enter to use the default value shown in brackets[ .])  
  
Enter key size in bits (1024, 2048, 4096) [2048]: 2048  
Enter number of days the certificate will be valid [3650]: 365  
Enter certificate digest (currently only SHA1 supported) [SHA1]:  
Enter two character country name [US]: US  
Enter state or province name [California]: Texas  
Enter locality name (city) [San Jose]: Richardson  
Enter organization name (company) [Quantum]: widgets Inc.  
Enter organizational unit name (section) [EndUser]: Manufacturing  
Enter tape library common name (must be unique)[SKM Tape Library]: Backup Libraries  
Enter primary SKM server common name (must be unique)[SKM Primary]: Primary  
Enter secondary SKM server common name (must be unique)[SKM Secondary]: Secondary  
Enter email address (optional) : john.doe@widgets.com
```


12 When prompted, confirm that the displayed information is correct.

```
akmadmin@skmserver: ~  
Enter organizational unit name (section) [EndUser]: Manufacturing  
Enter tape library common name (must be unique)[SKM Tape Library]: Backup Libraries  
Enter primary SKM server common name (must be unique)[SKM Primary]:  
Enter secondary SKM server common name (must be unique)[SKM Secondary]:  
Enter email address (optional) : john.doe@widgets.com  
  
Certification information:  
Key size in bits [2048]  
Number of days certificate is valid [365]  
Digest [SHA1]  
Country Name [US]  
State or province name [Texas]  
Locality name [Richardson]  
Organization name [Widgets Inc.]  
Organizational unit name [Manufacturing]  
Tape Library Common Name [Backup Libraries]  
Primary SKM Server Common Name [SKM Primary]  
Secondary SKM Server Common Name [SKM Secondary]  
Email address [john.doe@widgets.com]  
  
Is the certificate information displayed correct (y=yes, n=no):
```

- Enter **y** to confirm and begin the certificate-generation process.
- Enter **n** if you want to change any of the values you entered. Note that the defaults are now the values you previously entered, so you can easily bypass any correct values and change only the incorrect values.

After you confirm that the displayed values are correct, certificate generation begins.

13 When prompted, enter and re-enter a password that will be used during the pk12 file generation.

```
akmadmin@skmserver: ~  
Organizational unit name [EndUser]  
Tape Library Common Name [SKM Tape Library]  
Primary SKM Server Common Name [SKM Primary]  
Secondary SKM Server Common Name [SKM Secondary]  
Email address []  
  
Is the certificate information displayed correct (y=yes, n=no): y  
Generating the SKM primary server, secondary server and library communication certificates.  
  
Enter a password to be used with the pkcs12 files (required):  
Re-enter a password:
```

A message informs you when certificate generation is complete. The location of the certificates (/home/akmadmin/generatedcerts) is also provided.

- 14 Complete the process by loading the certificates onto the SKM servers and tape libraries using the procedures described in the user's guide for the applicable libraries.
 - For the Scalar i40/i80, refer to "Importing Encryption Certificates" in the Scalar i40 and Scalar i80 User's Guide.
 - For the Scalar i6000, refer to "Step 3 — Installing TLS Communication Certificates on the Library" in the Quantum Scalar i6000 User's Guide.
 - For the Scalar i3, refer to the topic "Load Certificate - Encryption" in the Scalar i3 Documentation Center: https://qsupport.quantum.com/kb/flare/content/Scalar_i3/docCenter/Encryption_Overview.htm?Highlight=load%20certificates
 - For the Scalar i6, refer to the topic in the Scalar i6 Documentation Center: https://qsupport.quantum.com/kb/flare/content/Scalar_i6/docCenter/Encryption_Overview.htm?Highlight=load%20certificates

Names of the files to copy are listed on the final screen that informs you that certificate generation is complete.

```

akmadmin@skmserver: ~
Tape Library Common Name [SKM Tape Library]
Primary SKM Server Common Name [SKM Primary]
Secondary SKM Server Common Name [SKM Secondary]
Email address []

Generating the SKM primary server, secondary server and library communication certificates.

Enter a password to be used with the pkcs12 files (required):
Re-enter a password to be used with the pkcs12 files:

Creating certificates for tapelibrary.
Creating certificates for primary.
Creating certificates for secondary.

Certificate generation is complete. All the generated certificate files are located in /home/akmadmin/generatedcerts
sub directory (tapelibrarycerts, skmprimarycerts or skmsecondarycerts.)

The following files need to be loaded onto the library using the remote GUI interface:
1) SKM_CA_signed_093020161346.pem
2) SKM_tapelibrary_admin_093020161346.pk12
3) SKM_tapelibrary_client_093020161346.pk12
The following files need to be loaded onto the primary SKM server using ./skmcmds:
1) SKM_CA_signed_093020161346.pem
2) SKM_primary_admin_093020161346.pk12
3) SKM_primary_server_093020161346.pk12
The following files need to be loaded onto the secondary SKM server using ./skmcmds:
1) SKM_CA_signed_093020161346.pem
2) SKM_secondary_admin_093020161346.pk12
3) SKM_secondary_server_093020161346.pk12

```

- 15 If desired, you can verify the certificate details by running the `ls -R generatedcerts/` command.

```
akmadmin@skmsserver: ~  
akmadmin@skmsserver:~$ ls -R generatedcerts/  
generatedcerts/  
skmprimarycerts skmsecondarycerts tapelibrarycerts  
generatedcerts/skmprimarycerts:  
SKM_CA_signed_093020161455.pem SKM_primary_admin_093020161455.pk12 SKM_primary_server_093020161455.pk12  
generatedcerts/skmsecondarycerts:  
SKM_CA_signed_093020161455.pem SKM_secondary_admin_093020161455.pk12 SKM_secondary_server_093020161455.pk12  
generatedcerts/tapelibrarycerts:  
SKM_CA_signed_093020161455.pem SKM_tapelibrary_admin_093020161455.pk12 SKM_tapelibrary_client_093020161455.pk12  
akmadmin@skmsserver:~$
```

Executing the Script with the -Q Option

After certificates are generated, follow this procedure to generate a set of Quantum bundles that can be loaded onto the library and SKM servers using the user interface.

- 1 Enter the command `genSKMcerts -Q`.
- 2 On screen messages provide status as the Quantum certificate bundles are generated using the default values, so no user input is required. (The generated bundle files are saved at `/home/akmadmin/generatedcerts/qbundles`.)

Chapter 4: Initial Configuration and Setup

Installing TLS Certificates on the SKM Server for SKM 2.4 (240Q) or Later

```
akmadmin@skmserver: ~  
akmadmin@skmserver:~$  
akmadmin@skmserver:~$  
akmadmin@skmserver:~$ genSKMcerts -Q  
Certificate file output directory (/home/akmadmin/generatedcerts) exists. No need to create.  
  
The genSKMcerts script will generate Quantum bundles for the SKM servers and tape libraries.  
Enter Quantum service user password:  
Generating Quantum certificate bundles.  
The certificates will be generated using the default values.  
  
Certification information:  
Key size in bits [2048]  
Number of days certificate is valid [3650]  
Digest [SHA1]  
Country Name [US]  
State or province name [California]  
Locality name [San Jose]  
Organization name [Quantum]  
Organizational unit name [EndUser]  
Tape Library Common Name [SKM Tape Library]  
Primary SKM Server Common Name [SKM Primary]  
Secondary SKM Server Common Name [SKM Secondary]  
Email address []  
  
Generating the SKM primary server, secondary server and library communication certificates.  
  
Creating certificates for tapelibrary.  
Creating certificates for primary.  
Creating certificates for secondary.  
Quantum bundles output directory exists. No need to create.  
Quantum bundle generation is complete. All the generated files are located in /home/akmadmin/generatedcerts/qbundles.  
The following bundles need to be loaded onto the library and SKM servers using the user interface:  
1) TapeLibraryQKMCert_101720161819.tgz  
2) QKMPrimaryServerCert_101720161819.tgz  
3) QKMSecondaryServerCert_101720161819.tgz  
akmadmin@skmserver:~$
```

After bundle generation is complete, load the bundles listed on the screen onto the library and SKM servers using the user interface.

- The **TapeLibraryQKMCert_XXXXXXXXX.tgz** bundle may be loaded onto any library attached to the SKM server pair.
- The **QKMPrimaryServerCert_XXXXXX.tgz** bundle must be loaded onto the primary SKM server.
- The **QKMSecondaryServerCert_XXXXXX.tgz** bundle must be loaded onto the secondary SKM server.

Configuring Your Library For SKM

All of the steps that follow deal with configuring your library for SKM and generating data encryption keys. Depending on the size of your library, it may take up to 2.5 hours to complete all of the following steps.

Also, please note that you cannot perform the following configuration steps **until you have completed all previous steps**. Both SKM servers must be fully configured and up and running.

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

Follow the instructions for your library:

- [Configuring the Scalar i40/i80 and Scalar i500 Tape Libraries](#) on page 83
- [Configuring the Scalar i6000 Tape Library](#) on page 86
- [Configuring the Scalar i3/i6 Tape Library](#) on page 88

Configuring the Scalar i40/i80 and Scalar i500 Tape Libraries

Perform these steps, in order, on the **Scalar i40/i80 and Scalar i500 libraries only**.

See the library user's guide or online help for detailed instructions on how to complete each of these steps.

- 1 Install the Encryption Key Management (EKM) license on your library.
- 2 Prepare partitions for library-managed encryption:
 - a Install LTO-4, LTO-5, LTO-6, LTO-7, and/or LTO-8 tape drives in the library, if not already installed. Unload all tape cartridges from these tape drives.
 - b Ensure that the partitions you want to configure for SKM contain only LTO-4, LTO-5, LTO-6, LTO-7, and/or LTO-8 tape drives.

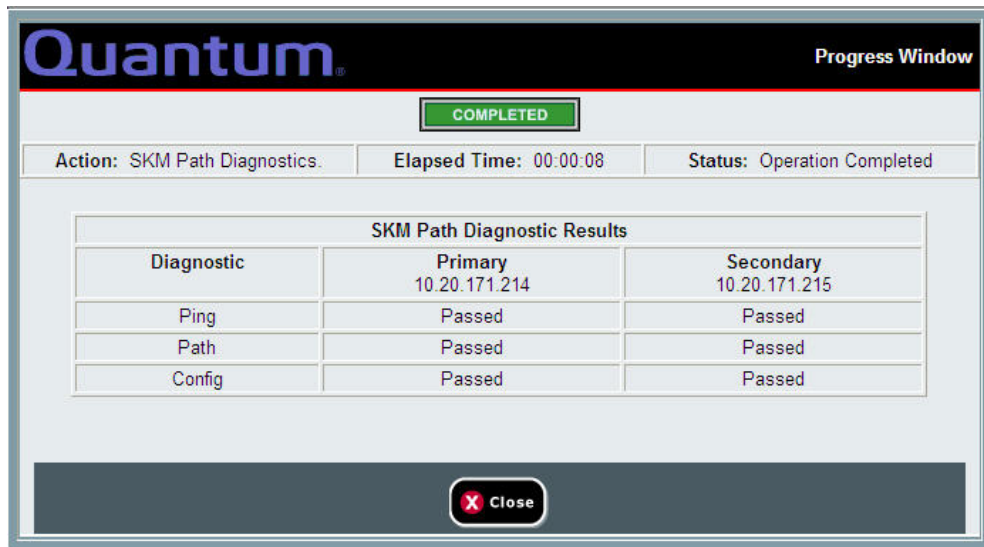
- c On the tape drives, install the latest version of firmware that is qualified for the library firmware installed on your library. Refer to the library release notes for the correct version of tape drive firmware.
- 3 TLS certificates must be installed on the library as well as on the SKM server. Verify the appropriate TLS communication certificates are installed on the library. If you installed your own TLS certificates on the SKM servers, you must install your own TLS certificates on the library. If you used Quantum-supplied TLS certificates on the SKM servers, you must use Quantum-supplied certificates on the library.

Some newer libraries ship with TLS certificates already installed, and other newer libraries require certificate installation. See your library user's guide for instructions on how to check whether TLS certificates are installed, where to download, and how to install them.

Note these general guidelines:

- For pre-2.4 SKM servers, preloaded TLS certificates on the library will work
 - For 2.4 (240Q) and later SKM servers, preloaded TLS certificates on the library will not work, and you must download the generated library TLS certificate onto the library
- 4 Configure the SKM server IP addresses on the library.
 - a From the library's Web client, navigate to the encryption system configuration screen.
 - b Enter the primary and secondary SKM server IP addresses or host names in the fields provided.
 - c Click **Apply**.
 - 5 Run EKM Path Diagnostics and make sure all the tests pass. Pass/fail status is displayed in a progress window after the diagnostics completes (see [Figure 20](#)). This is required to make sure the library is connected properly to both SKM servers. If any of the tests fail, follow the instructions in the online help or library user's guide to troubleshoot and then run EKM Path Diagnostics again.

Figure 20 EKM Path
Diagnostics PASSED Window



- 6 Configure SKM partitions and generate data encryption keys:
 - a On the library's Web client, navigate to the encryption partition configuration screen.
 - b For each partition in which you will use SKM, in the **Encryption Method** drop-down list, select **Enable Library Managed**.
 - c Click **Apply**.

Data encryption keys are generated. When you enable library managed encryption on a partition in the library for the first time, the library automatically triggers each SKM server to generate a set of unique data encryption keys. The key generation process should take 30 minutes or less to complete, depending on network performance. The library notifies you when the process is complete.
 - d Wait for the process to complete before continuing to the next step.
- 7 Save the library configuration.
- 8 Proceed to [Backing Up the SKM Server](#) on page 103.

Configuring the Scalar i6000 Tape Library

Perform these steps, in order, on the **Scalar i6000 library only**.

See the library user's guide or online help for detailed instructions on how to complete each of these steps.

- 1 Install the Encryption Key Management (EKM) license on your library.
- 2 Prepare partitions for library-managed encryption by doing the following:
 - a Install the following tape drives in the library, if not already installed. Unload all tape cartridges from these tape drives.
For the Scalar i6000:
 - HP LTO-4 through LTO-6
 - IBM LTO-5 through LTO-8
 - b On the 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.
- 3 TLS certificates must be installed on the library as well as on the SKM server. Refer to the following links to the Scalar i6000 Documentation Centers for instructions on how to install certificates.

Note: Click on: Quantum Scalar Key Manager (Q_SKM) User's Guide

For Scalar i6000 documentation center:

https://qsupport.quantum.com/kb/flare/content/Scalar_i6000/docCenter/Index.htm

- 4 Configure the SKM server IP addresses and generate data encryption keys.
 - a On the library's remote Web client, navigate to the EKM server configuration screen.
 - b Enter the SKM primary and secondary server IP addresses or hostnames in the fields provided.
 - c Click **OK**.

Data encryption keys are generated. As soon as you apply the SKM server IP addresses, the library automatically triggers each SKM server to generate a set of unique data encryption keys. The key generation process should take 30 minutes or less to complete, depending on network performance. The library generates a RAS ticket when the process is complete. Wait until you receive this ticket before going to the next step.

Note: If the key generation fails, the library generates a RAS ticket. Follow the instructions in the ticket to resolve any errors, then initiate manual key generation by changing the encryption method on an SKM partition to **Enable Library Managed** (as described in [Step 5](#) below). If key generation continues to fail, run EKM Path Diagnostics to help determine where the problem lies.

- 5 Configure partitions for library-managed encryption.
 - a From the **Navigation** panel, select **Partitions**.
 - b In the **North Panel**, select the partition you want to set up.
 - c From the **Operations** panel, click **EKM**.
 - d At the **Enable Library-Managed Encryption (LME)** field, select the check box to enable LME.
 - e Click **Apply** to save your settings.
 - f Click **Close** to exit the window.

For additional information, refer to these links to the Quantum Documentation Center:

- For Scalar i6000 running firmware version i12.x or below:
For Scalar i6000 running firmware version i12.x or below:
<https://www.quantum.com/serviceandsupport/softwareanddocumentationdownloads/s2k/index.aspx?whattab= Fifth>
- For Scalar i6000 running firmware version i13.x or above :
http://qsupport.quantum.com/kb/flare/content/Scalar_i6000/docCenter/Index.htm

- 6 Proceed to [Backing Up the SKM Server](#) on page 103.

Configuring the Scalar i3/i6 Tape Library

Perform these steps, in order, on the **Scalar i3 or i6 library only**.

Refer to the i3 or i6 Documentation Center for detailed instructions on how to complete each of the following steps.

- Scalar i3 Documentation Center:
<http://www.quantum.com/scalari3docs>
- Scalar i6 Documentation Center:
<http://www.quantum.com/scalari6docs>

- 1 Install the Encryption Key Management (EKM) license on your library.
- 2 Prepare partitions for library-managed encryption by doing the following:
 - a Install the following tape drives in the library, if not already installed. Unload all tape cartridges from these tape drives.

For the Scalar i3:

 - IBM HH SAS LTO6
 - IBM HH SAS LTO7
 - IBM HH FC LTO6
 - IBM HH FC LTO7
 - IBM HH FC LTO8
 - IBM HH SAS LTO8

For the Scalar i6:

 - IBM FH FC LTO6
 - IBM FH FC LTO7
 - IBM FH FC LTO8
 - b On the 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.
- 3 TLS certificates must be installed on the library as well as on the SKM server. Refer to the following links to the Scalar i3/i6 Documentation Centers for instructions on how to install certificates.

- For the Scalar i3, refer to the topic “Load Certificate - Encryption” in the Scalar i3 Documentation Center:
https://qsupport.quantum.com/kb/flare/content/Scalar_i3/docCenter/Encryption_Overview.htm?Highlight=load%20certificates
 - For the Scalar i6, refer to the topic in the Scalar i6 Documentation Center:
https://qsupport.quantum.com/kb/flare/content/Scalar_i6/docCenter/Encryption_Overview.htm?Highlight=load%20certificates
- 4 Configure the SKM server IP addresses and generate data encryption keys.
- a On the library’s remote Web client, navigate to the EKM server configuration screen.
 - b Enter the SKM primary and secondary server IP addresses or hostnames in the fields provided.
 - c Click **OK**.

Data encryption keys are generated. As soon as you apply the SKM server IP addresses, the library automatically triggers each SKM server to generate a set of unique data encryption keys. The key generation process should take 30 minutes or less to complete, depending on network performance. The library generates a RAS ticket when the process is complete. Wait until you receive this ticket before going to the next step.

Note: If the key generation fails, the library generates a RAS ticket. Follow the instructions in the ticket to resolve any errors, then initiate manual key generation by changing the encryption method on an SKM partition to **Enable Library Managed** (as described in [Step 5](#) below). If key generation continues to fail, run EKM Path Diagnostics to help determine where the problem lies.

- 5 Configure partitions for library-managed encryption.
- a From the **Navigation** panel, select **Partitions**.
 - b In the **North Panel**, select the partition you want to set up.
 - c From the **Operations** panel, click **EKM**.

- d At the **Enable Library-Managed Encryption (LME)** field, select the check box to enable LME.
- e Click **Apply** to save your settings.
- f Click **Close** to exit the window.

For additional information, refer to these links to the Scalar i3 or Scalar i6 Documentation Center:

- For the Scalar i3, refer to the topic “Load Certificate - Encryption” in the Scalar i3 Documentation Center:
https://qsupport.quantum.com/kb/flare/content/Scalar_i3/docCenter/Encryption_Overview.htm?Highlight=load%20certificates
- For the Scalar i6, refer to the topic in the Scalar i6 Documentation Center:
https://qsupport.quantum.com/kb/flare/content/Scalar_i6/docCenter/Encryption_Overview.htm?Highlight=load%20certificates

- 6 Proceed to [Backing Up the SKM Server](#) on page 103.

Configuring Multiple Libraries

If you will have multiple libraries accessing the same SKM server pair, repeat [Configuring Your Library For SKM](#) on page 83 and [Backing Up the SKM Server](#) on page 103 for each additional library.

Backing Up the Servers

You must back up both SKM servers before you begin to encrypt data. See [Backing Up the SKM Server](#) on page 103 for instructions.



Chapter 5

Logging On and Changing the Configuration

While most encryption operations will occur automatically and transparently, you will need to access the SKM server on occasion to perform certain functions, which are described in this chapter.

This chapter discusses using the SKM server software and SKM Admin Commands. Topics include:

- [Logging on to the Command Line Interface](#)
- [Accessing SKM Admin Commands](#)
- [Quitting SKM Admin Commands](#)
- [Logging Off of the SKM Server Command Line Interface](#)
- [Running the Setup Wizard](#)
- [Changing the Password](#)
- [Changing the IP Address](#)
- [Changing the Time Zone](#)
- [Changing the Date and Time](#)
- [Changing the Hostname](#)
- [Displaying and Installing TLS Communication Certificates on the SKM Server](#)

Caution: Quantum requires that you do not install any software, file, or operating system on the SKM appliance server or SKM VM server unless it is an upgrade or patch supplied by Quantum. Doing so may make your server inoperable and will void the warranty.

Logging on to the Command Line Interface

The SKM server command line interface, provides access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93) and also allow you to perform some commands without stopping the SKM server (see [Command Line Operations](#) on page 112).

Note: There is only one SKM server login ID, `akmadmin`. This login ID cannot be changed.

To log on to the SKM server command line at any time after initial setup:

- 1 Connect to the SKM server.
 - **SKM appliance server:** Use SSH.
 - **SKM VM server:** You can connect using SSH or vSphere.

Note: If you are using Microsoft® Windows®, you may need to install a utility to use SSH. Two such utilities are PuTTY, available at <http://www.chiark.greenend.org.uk/~sgtatham/putty/> and WinSCP, available at <http://winscp.net>.

Caution: Remember that there are two SKM servers with different IP addresses. Make sure that you are accessing the correct server.

- 2 At the `skmserver login` prompt, type the login ID:

```
akmadmin
```

3 At the **Password** prompt, type your password.

The `akmadmin@<hostname>` prompt appears (where `<hostname>` is the SKM server hostname).

4 From here you can either:

- Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93). This stops the SKM server while you are accessing the commands.
- Issue certain commands directly from the command line (see [Command Line Operations](#) on page 112).

Accessing SKM Admin Commands

SKM Admin Commands allows you to configure your SKM server, update server software, and perform backup and restore operations.

Details about SKM Admin Commands include:

- When you access SKM Admin Commands, the SKM server process is stopped. This means the library can no longer communicate with the SKM server to request encryption keys. When you quit SKM Admin Commands, the server process restarts. See [Quitting SKM Admin Commands](#) on page 95 for more information.
- You can make as many configuration changes during a session as you wish, but in order to save your changes, you must type `q` at the **Command** prompt to quit SKM Admin Commands. See [Quitting SKM Admin Commands](#) on page 95 for more information.
- When changing configuration settings, you can press `<Enter>` to leave the current setting unchanged.
- Only one user can access SKM Admin Commands at a time. If you try to log on and another user is logged on, you will receive a message that the system is already running and you will not be able to log on.

To access SKM Admin Commands:

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 At the `akmadmin@<hostname>` prompt (where `<hostname>` is the SKM server hostname), type:
`./skmcmds`
- 3 At the **Password** prompt, type your password.
A message displays alerting you that the SKM server will be stopped.
- 4 Enter `y` to agree to stop the SKM server and continue.
A message appears stating the SKM server is being stopped.
- 5 Press `<Enter>` to continue.
The list of SKM Admin Commands displays, followed by the **Command** prompt (see [Figure 21](#) for an example).

Figure 21 SKM Admin
Commands (Example)

```
SKM Admin Commands (Version 270Q.GC00600)
SKM
Server Cert's Validity:
  /etc/akm/Certs/QKMServerSignedCert.pem
  Not Before: Dec 17 19:32:01 2019 GMT and Not After : Dec 14 19:32:01 2029 GMT
Admin Cert's Validity:
  /home/akmadmin/.akmadmin/Certs/QKMAAdminSignedCert.pem
  Not Before: Dec 17 19:32:01 2019 GMT and Not After : Dec 14 19:32:01 2029 GMT

Current Date/Time: Wed Jan 15 03:36:44 MST 2020

-----
1) Launch SKM server setup wizard.
2) Change user account password.
3) Capture SKM server snapshot.
4) Set SKM server IP address.
5) Set SKM server time zone.
6) Set SKM server date and time.
7) Back up SKM server.
8) Restore SKM server.
9) Set SKM server hostname.
d) Display/update TLS communication certificates.
u) Update SKM server software via DVD. (Disabled)
r) Roll back SKM server software. (Disabled)
v) View SKM server reports.
k) Key/Certificate import and export.
t) Set Minimum TLS Communication Support (1.0, 1.1 or 1.2).
q) Quit.
-----
Command: █
```


Quitting SKM Admin Commands

Quitting SKM Admin Commands saves any changes you made during the session, ends your SKM Admin Commands session, and restarts the SKM server. You must quit in order to save your changes.

If your session times out or terminates unexpectedly before you quit, any changes you made will not be saved.

Caution: As long as SKM Admin Commands remains open, the SKM server remains stopped and the library cannot communicate with it to perform encryption operations

Caution: If you are using SSH to access SKM Admin Commands, your session will automatically terminate after a period of inactivity. If your session terminates before you quit, any changes you made will not be saved.

Caution: If you are using the vSphere Client console to access SKM Admin Commands (SKM VM servers only), your session will never automatically terminate and the SKM server will remain stopped. It is important that you remember to quit your session so that encryption can continue.

To quit SKM Admin Commands and restart the server, type **q** and press **<Enter>** at the **Command** prompt.

Logging Off of the SKM Server Command Line Interface

Logging off, or exiting, refers to the final step in closing your session. After you quit SKM Admin Commands (see [Quitting SKM Admin Commands](#) on page 95), you are still logged on to the command line interface.

If you are using SSH, your session automatically logs off after a period of inactivity. If you are using vSphere (SKM VM servers only), the session never terminates and you remain logged on until you log off. In addition, when you quit SKM Admin Commands, if you do not log off of the command line interface, the system allows you to access SKM Admin Commands again for 60 minutes without requiring you to enter a password.

Caution: To prevent unauthorized users from moving, adding, or deleting files and directories and possibly rendering the SKM server unusable, it is recommended that you log off as soon as you complete your operations.

To log off, type **exit** or **logout** at the **akmadmin@<hostname>** prompt (where <hostname> is the SKM server hostname).

Running the Setup Wizard

The setup wizard leads you through a series of steps to change the SKM server password, time zone, date, time, IP address, netmask, and gateway. You should not need to run the entire setup wizard after initial setup, but you can if you wish to do so. The setup wizard is described in more detail in [Chapter 4, Initial Configuration and Setup](#).

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 At the **Command** prompt, type **1** and press **<Enter>** to **Launch SKM server setup wizard**.
- 4 Complete the setup wizard.
- 5 At the **Command** prompt, type **q** and press **<Enter>** to quit SKM Admin Commands, save your changes, and restart the SKM server.

Changing the Password

There is only one password for an SKM server, which is required for all logons and access to SKM Admin Commands. Each SKM server has a password, and the passwords can be different on the two SKM servers in the pair. You need to enter the password frequently to gain access to certain functions. You can change this password at any time, but be careful. It is critical that you do not lose your password, because if you do there is no way to recover it. Without the password, you cannot log on to the SKM server, or perform backups and restores. The default password is **password**. You can change the password using the setup wizard or by selecting the option from the SKM Admin Commands list.

If you lose the password, there is no way to retrieve it. The only way to recover from such a situation is:

- **SKM appliance server:** Completely replace the SKM server appliance and then restore the last saved backup (see [Replacing an SKM Appliance Server and Both Hard Disk Drives](#) on page 181).
- **SKM VM server:** Delete and then re-create the SKM VM server using the original .ova image and your latest saved backup (see [Reinstalling an SKM VM Server](#) on page 183 for instructions).

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

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

If you forget the password, you will lose logon access to the SKM server, including backup and restore capability. Quantum will NOT be able to restore the password.

Charges may apply for replacement of an SKM appliance server required due to changing and then forgetting the password.

CAUTION! CAUTION! CAUTION! CAUTION! CAUTION!

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 At the **Command** prompt, type **2** and press <Enter> to **Change user account password**.
Follow the prompts to change your password.
- 4 At the **Command** prompt, type **q** and press <Enter> to quit SKM Admin Commands, save your changes, and restart the SKM server.

Changing the IP Address

When you first install your SKM server and run the setup wizard, you set the IP address. At any time after that, you can change the IP address as follows.

Caution: Changing the IP address should not be taken lightly. Remember that if you change the IP address on your server, you must also change it in the library remote Web client of each library that is attached to the SKM server pair or the libraries will not be able to communicate with the SKM server. This requires a number of steps that are detailed below.

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 At the **Command** prompt, type **4** to **Set SKM server IP address**.
- 4 Follow the prompts to change your IP address.
- 5 At the **Command** prompt, type **q** and press <Enter> to quit SKM Admin Commands, save your changes, and restart the SKM server.

- 6 Update the IP address on each library that uses this SKM server, as follows (see your library user's guide or online help for details):
 - a Make sure that no tape cartridges are mounted in any of the tape drives in any of the SKM partitions in the library.
 - b Access the library's remote Web client.
 - c Navigate to the encryption partition configuration screen and change the encryption method on all SKM partitions from **Enable Library Managed** to **Allow Application Managed**.
 - d Navigate to the encryption system server configuration screen and update the IP address of the SKM server.

Caution: Be sure to update the correct server IP address (primary vs. secondary).

- e Navigate back to the encryption partition configuration screen and change the encryption method on all SKM partitions from **Allow Application Managed** to **Enable Library Managed**.

Changing the Time Zone

To change the time zone at any time after initial configuration:

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 At the **Command** prompt, type **5** and press **<Enter>** to **Set SKM server time zone**.
- 4 Follow the prompts to set the time zone.
- 5 At the **Command** prompt, type **q** and press **<Enter>** to quit SKM Admin Commands, save your changes, and restart the SKM server.

Changing the Date and Time

Caution: If the SKM servers Date/Time is set before or after the validity date/time of the TLS Certificate then the Certificates will be invalid and not work.

To change the date and time at any time after initial configuration:

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 At the **Command** prompt, type **6** and press **<Enter>** to **Set SKM server date and time**.
- 4 Follow the prompts to set the date and time.
- 5 At the **Command** prompt, type **q** and press **<Enter>** to quit SKM Admin Commands, save your changes, and restart the SKM server.

Changing the Hostname

The SKM server's default hostname is **skmserver**. You can change the hostname using SKM Admin Commands.

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 At the **Command** prompt, type **9** and press **<Enter>** to **Set SKM server hostname**.

The **Command** prompt displays the current hostname in brackets.

- 4 Type a new hostname and press **<Enter>**.

The new hostname displays.

- 5 Press <Enter>.
- 6 At the **Command** prompt, type **q** and press <Enter> to quit SKM Admin Commands, save your changes, and restart the SKM server.

Displaying and Installing TLS Communication Certificates on the SKM Server

This option allows you to see what certificates you have installed on your SKM servers and change them if you wish. This section covers:

- [Displaying the TLS Certificates](#)
- [Installing the TLS Certificates](#)

Displaying the TLS Certificates

To view the certificates currently installed on the SKM server:

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 At the **Command** prompt, type **d** and press <Enter> to **Display/update TLS communication certificates**.

The **Display/update TLS communication certificates** menu displays.

- 4 At the **Command** prompt, type **s** and press <Enter> to **Show current communication certificate information**.

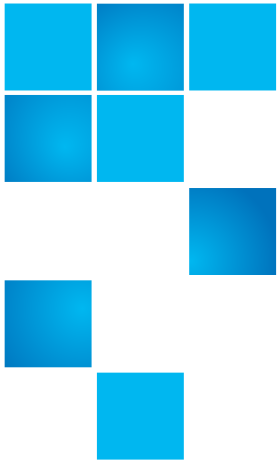
The names and locations of the currently installed certificates display.

- 5 To view certificate information, type the number of the certificate or type **a** for all, and press <Enter>. To quit, type **q** and press <Enter>.
- 6 At the **Command** prompt, type **q** to quit and return to SKM Admin Commands.

Installing the TLS Certificates

For detailed instructions on installing TLS certificates, see:

- [Installing TLS Certificates on the SKM Server for Pre-SKM 2.4 \(240Q\) on page 59.](#)
- [Installing TLS Certificates on the SKM Server for SKM 2.4 \(240Q\) or Later on page 70](#)



Chapter 6

Backing Up and Restoring the SKM Server

It is critical that you keep a current backup of each SKM server so that you can restore it if the server were to become inoperable. This chapter describes:

- [Backing Up the SKM Server](#)
- [Restoring the SKM Server](#)

Backing Up the SKM Server

Every time new data encryption keys are generated, you must back up both SKM servers before you begin using the keys to encrypt data. You should also back up both SKM servers any time you import keys from another source. You must back up each server separately because each contains different data. If a server fails and needs to be replaced, the backup is required to restore operation.

For more information on why you need to back up your SKM servers, see [Why You Need to Back Up Your SKM Servers](#) on page 7.

The backup contains your keystore and certain server configuration files. The backup does not contain your password or server IP address.

Caution: It is critical that you back up both servers before using new 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.

If both servers are lost, and no backup exists, Quantum will be unable to restore any data from your encrypted media.

The backup is required for server hardware replacement or for restoring a rebuilt SKM VM server.

CAUTION! CAUTION! CAUTION! CAUTION!

Note: For multiple libraries accessing the same SKM server pair: If you are configuring more than one library to use the same SKM servers, be aware that each library triggers the SKM servers to create a set of data 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.

There are two ways to back up the server. Both will stop the SKM server process prior to backup and restart the server process after the backup is complete. It is faster to use the command line interface unless you are already in SKM Admin Commands.

- [Backing Up Using SKM Admin Commands](#)
- [Backing Up Using the Command Line Interface](#)

Backing Up Using SKM Admin Commands

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

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 At the **Command** prompt, type **7** to **Back up SKM server**.
- 4 Press **<Enter>**.

Backup files are created and consolidated into a single file, whose name and location are displayed on the screen.

- 5 Note the name and location of the backup file:

```
/home/akmadmin/backups/SKM<version>KeyServer<serial number><date><time>.tgz
```

- 6 Use SFTP to copy the backup file to a desired location.

Caution: You must copy the backup file to another location and not just leave it on the SKM server. This is so that, if the SKM server fails, you can restore the backup from the remote location onto the new server.

Caution: Keep track of which backup file applies to which server so you know which one to restore in the event that you lose a server.

Caution: **Do not use SKM to encrypt the sole copy of your SKM server 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>**.
The SKM Admin Commands menu displays.
- 8 At the **Command** prompt, type **q** and press **<Enter>** to quit SKM Admin Commands and restart the SKM key server.
- 9 Repeat the above steps on the other server in the SKM server pair.

Backing Up Using the Command Line Interface

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

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 At the `akmadmin@<hostname>` prompt (where `<hostname>` is the SKM server hostname), issue the following command:

```
./skmcmds -B
```

Backup files are created and consolidated into a single file, whose name and location are displayed on the screen.

- 3 Note the name and location of the backup file:

```
/home/akmadmin/backups/SKM<version>KeyServer<serial number><date><time>.tgz
```

- 4 Use SFTP to copy the backup file to a desired location.

Caution: You must copy these backup files to another location and not just leave them on the SKM server. This is so that, if the SKM server fails, you can restore the backup from the remote location onto the new server.

Caution: Keep track of which backup file applies to which server so you know which one to restore in the event that you lose a server.

Caution: **Do not use SKM to encrypt the sole copy of your SKM server 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.

- 5 Repeat the above steps on the other server in the SKM server pair.

Restoring the SKM Server

The only time you should need to restore the server is when you replace an SKM appliance server or reinstall an SKM VM server. You will perform the restore procedure as part of the server replacement procedure (see [Chapter 11, Replacing the SKM Server and its Components](#)).

The restore procedure places all of the information contained in your backup onto the replacement SKM server. The backup contains your keystore database, which includes:

- the data encryption keys generated on the SKM server,
- the copies of the data encryption keys generated on the other server in the SKM server pair, and
- any metadata for data encryption keys used up until the time the backup was performed.

The backup does not include metadata for data encryption keys used after the backup was performed.

- 1 Get the backup files you wish to restore and place them in a location you can access via your network. The file name is the following:

```
SKM2_0KeyServer<serial number><date><time>.tgz
```

Caution: Make sure you use the backup for the failed server, not the working server. The backups are not the same. The filenames of the backup files contain the serial number of the server.

- 2 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 3 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 4 At the **Command** prompt, type **8** and press **<Enter>** to **Restore SKM server**.

5 Press <Enter>.

A message displays instructing you to copy a previous backup file to the `/home/akmadmin/backups` folder on the SKM server using SFTP.

Note: You cannot restore SKM 1.x backup files onto an SKM 2.0 or higher system.

6 Use SFTP to copy the file from your known location to the `/home/akmadmin/backups` folder on the SKM server.

Note: If you are using Microsoft Windows, you may need to install a program to use SFTP. Two such utilities are PuTTY, available at <http://www.chiark.greenend.org.uk/~sgtatham/putty/> and WinSCP, available at <http://winscp.net>.

7 When finished copying the file, press <Enter>.

8 A list of available SKM server backup files displays. Type the number of the file you want to use and press <Enter>.

The server is restored. A message appears telling you that after you exit SKM Admin Commands, you need to either reboot each connected library or toggle a partition encryption method from Enable Library Managed to Allow Application Managed, and then back to Enable Library Managed. You will do this when you get to [Step 11](#) below.

9 Press <Enter> again.

The list of SKM Admin Commands displays.

10 At the **Command** prompt, type `q` and press <Enter> to quit SKM Admin Commands and restart the SKM server.

The files are loaded onto the SKM server's hard disk drives and the SKM server restarts.

11 Complete the restore operation as soon as possible by performing the following steps on every library that accesses the SKM server:

Caution: The library cannot use the restored SKM server to serve new data encryption keys until you complete these steps. Each library keeps track of the last data encryption key served by the SKM server. These steps reset the restored SKM server so that it does not serve previously used data encryption keys.

- a Access the library's remote Web client.
- b Navigate to the encryption partition configuration screen and change one SKM partition from **Enable Library Managed** to **Allow Application Managed**. Make sure to apply the change. On some libraries, you click **Apply**. On others, you may need to go through several screens before finishing.
- c Wait 3 minutes to allow the changes to complete.
- d Change the SKM partition back to **Enable Library Managed**.
- e Check to see if any RAS/diagnostic tickets were generated. If not, the restore operation succeeded. If a ticket was generated, follow the resolution instructions and try again.
- f Repeat the above steps on each library that accesses the SKM server.



Chapter 7

Retrieving SKM Reports, Logs, and Information

The SKM server collects data about its activities that you may need to access, primarily for troubleshooting purposes. This chapter describes the various logs and reports you can access, in the following sections:

- [Command Line Operations](#)
- [Displaying the Command Line Help Menu](#)
- [Viewing the SKM Server Software Version](#)
- [Capturing SKM Server Logs and Snapshots](#)
- [Displaying the End User License Agreement](#)
- [Turning Trace Level Logging On and Off](#)
- [Displaying SKM Server Reports](#)
- [List of Key Aliases \(Option 2\)](#)
- [Display Key Template Information \(Option 3\)](#)
- [Viewing the SKM Encryption Key Import Warning Log](#)

Command Line Operations

There are several commands you can run directly from the command line without having to access SKM Admin Commands. These commands are listed in a help menu that you can access from the command line (see [Displaying the Command Line Help Menu](#) on page 112). Most of these commands provide information or logs, and are described in this chapter. Those that do not are covered in other chapters. The functions you can perform from the command line are:

- [Displaying the Command Line Help Menu](#) on page 112
- [Viewing the SKM Server Software Version](#) on page 113
- [Capturing the Snapshot From the Command Line Without Stopping the Server](#) on page 114
- [Displaying the End User License Agreement](#) on page 116
- [Backing Up Using the Command Line Interface](#) on page 106
- [Turning Trace Level Logging On and Off](#) on page 117

Displaying the Command Line Help Menu

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 At the `akmadmin@<hostname>` prompt (where `<hostname>` is the SKM server hostname), issue the following command to display the help menu (see [Figure 22](#)):

```
./skmcmds -h
```

Figure 22 Help Menu

```
akmadmin@skm228:~$ ./skmcmds -h
usage: ./skmcmds [-hvLEDBO]
-h:          View this help message.
-v:          View skmcmds version.
-L:          Capture SKM server snapshots without stopping key server.
-E:          Display End User License Agreement (EULA).
-B:          Back up SKM server.
-D on|off:   Turn trace level logging on or off.
-R:          Display only the reports menu. The reports do not require the key
server to be stopped so key fetches will still work from the libraries
-O 1-6       Run the specified reports option only.

example: ./skmcmds -D on

akmadmin@skm228:~$ █
```

Viewing the SKM Server Software Version

You can see the version of software you are running at the top of the SKM Admin Commands menu (see [Accessing SKM Admin Commands](#) on page 93). Alternatively, to view the software version without accessing SKM Admin Commands, do the following:

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 At the `akmadmin@<hostname>` prompt (where `<hostname>` is the SKM server hostname), issue the following command:

```
./skmcmds -v
```

The software version is displayed and the `akmadmin@<hostname>` prompt reappears.

Figure 23 Software Version

```
akmadmin@skm227:~$ ./skmcmds -v
[sudo] password for akmadmin:

./skmcmds : SKM Admin Commands (Version 270Q.GC00600)
./skmcmds : SKM Server Version <akmd Version 4.6.1.1850.1>
./skmcmds : SKM Server Admin Version <akmadmin Version 3.0.9>
./skmcmds : SKM Server Minimum TLS Communication Version: 1.2

akmadmin@skm227:~$
```

Capturing SKM Server Logs and Snapshots

The SKM server logs contain information about all activities performed by the SKM server.

Quantum Support may request that you retrieve the logs using one or more of the methods described below. You should not need to retrieve these logs unless directed to do so by Quantum Support.

The SKM server snapshot is a complete collection of all of the logs generated by the SKM server, including error, audit, systems, and configuration logs. There are two ways to capture the snapshot. Both methods pull the same information.

- [Capturing the Snapshot From the Command Line Without Stopping the Server](#) — This is the preferred method because it does not stop the SKM server.
- [Capturing the Snapshot Using SKM Admin Commands](#) — This method is less preferable since it stops the SKM server.

Capturing the Snapshot From the Command Line Without Stopping the Server

The most efficient way to collect the logs from the SKM server is to do so from the command line. This method is quicker and does not stop the SKM server.

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).

- 2 At the `akmadmin@<hostname>` prompt (where `<hostname>` is the SKM server hostname), issue the following command:

```
./skmcmds -L
```

The logs are gathered and placed into a single .tgz file:

```
/home/akmadmin/  
skm_logcapture_<serial number><date>_<time>.tgz
```

- 3 Use secure file transfer protocol (SFTP) to copy the file to a desired location.

Note: If you are using Microsoft Windows, you may need to install a utility to use SFTP. Two such utilities are PuTTY, available at <https://www.chiark.greenend.org.uk/~sgtatham/putty/> and WinSCP, available at <https://winscp.net/eng/index.php>.

- 4 Press `<Enter>` to return to the `akmadmin@<hostname>` prompt.

Capturing the Snapshot Using SKM Admin Commands

An alternative method of collecting the SKM server logs is via SKM Admin Commands. This method stops the SKM server. Normally you would not choose this method, but if the SKM server is stopped anyway and you want to capture the logs at the same time, you can do so.

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 Enter **3** to **Capture SKM server snapshot**.

The logs are gathered and placed into a single .tgz file:

```
/home/akmadmin/  
skm_logcapture_<serial number><date>_<time>.tgz
```

- 4 Use secure file transfer protocol (SFTP) to copy the file to a desired location.

Note: If you are using Microsoft Windows, you may need to install a utility to use SFTP. Two such utilities are PuTTY, available at <https://www.chiark.greenend.org.uk/~sgtatham/putty/> and WinSCP, available at <https://winscp.net/eng/index.php>.

- 5 At the **Command** prompt, type **q** and press **<Enter>** to quit SKM Admin Commands and restart the SKM server.

Displaying the End User License Agreement

The End User License Agreement (EULA) is displayed during initial configuration of the SKM server. You were required to accept the agreement before configuring the server. If you want to read the license agreement at any time after initial setup, do the following:

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 At the **akmadmin@<hostname>** prompt (where **<hostname>** is the SKM server hostname), issue the following command:

```
./skmcmds -E
```

The first few paragraphs of the license display.

- 3 Press **<Enter>** to scroll through the license agreement one line at a time. Type **end** to advance one paragraph (or several lines) at a time.

At the end of the license agreement, the date of acceptance displays.

- 4 Press **<Enter>** to return to the **akmadmin@<hostname>** prompt.

Turning Trace Level Logging On and Off

SKM server software logging can get very verbose, so this option is turned off by default. If you turn it on, the SKM server software generates more logging, which may be useful for troubleshooting purposes. You should keep this turned **OFF** unless Quantum Support directs otherwise. The “-D” option is only available on firmware versions **252Q** and lower.

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 At the `akmadmin@<hostname>` prompt (where `<hostname>` is the SKM server hostname), issue one of the following commands:

```
./skmcmds -D on  
./skmcmds -D off
```

Displaying SKM Server Reports

This section provides the following information:

- [Accessing SKM Server Reports](#)
- [Number of SKM Server Keys \(Option 1\)](#)
- [List of Key Aliases \(Option 2\)](#)
- [Display Key Template Information \(Option 3\)](#)
- [Display Quantum Reserved Key \(Option 4\)](#)
- [Display Keys Used Today \(Option 5\)](#)
- [Display System Status \(Option 6\)](#)
- [Display Used Key Information \(Option 7\)](#)

Accessing SKM Server Reports

To access the SKM server reports complete the following:

SKM 1.x

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Issue the following command:

```
akmadmin 1037 | grep '^EK' | wc -l
```

The number of keys in the keystore displays.

SKM 2.x

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 At the **Command** prompt, type **v** for **View SKM server reports** and press **<Enter>**.
- 4 The SKM Server Reports menu displays (see [Figure 24](#)).

Figure 24 SKM Server Reports Menu

```
SKM Server Reports.
-----
1) Number of SKM server keys.
2) List of key aliases.
3) Display key template information.
4) Display Quantum Reserved key.
5) Display keys used today.
6) Display system status.
7) Display used key information.
q) Quit.
-----
Command: █
```

Number of SKM Server Keys (Option 1)

To list the number of SKM server keys complete the following:

- 1 Type **1** at the SKM Server Reports menu and press **<Enter>** to display the number of data encryption keys that are in the SKM server's keystore.

[Figure 25](#) provides an example of the display.

Figure 25 SKM Server Keys

```
SKM Server Reports.
-----
1) Number of SKM server keys.
2) List of key aliases.
3) Display key template information.
4) Display Quantum Reserved key.
5) Display keys used today.
6) Display system status.
7) Display used key information.
q) Quit.
-----
Command: 1

Number of SKM Server keys: 4096

Press <Enter>
```

- 2 Press **<Enter>** to return to the SKM server reports menu.
- 3 At the **Command** prompt, type **q** and press **<Enter>** to quit the SKM server reports menu.
- 4 Press **<Enter>** to return to SKM Admin Commands.

- 5 At the **Command** prompt, type **q** and press **<Enter>** to quit SKM Admin Commands and restart the SKM server.

List of Key Aliases (Option 2)

This option displays a list all of the keys in the keystore. You should only need to bring up this list if directed to do so by Quantum Support.

Looking at the key names can help verify whether the keys are being copied from one server to the other. Keys generated on the primary server begin with EKA and keys generated by the secondary server begin with EKB. The server should contain keys that begin with both "EKA" and "EKB".

To view a list of all of the data encryption key aliases:

- 1 Type **2** at the SKM Server Reports menu and press **<Enter>** to display the list of keys and their aliases.

The list displays (see [Figure 26](#)). The keys are all displayed in order, with the "EKA" keys displayed first.

Figure 26 Keys and Aliases



```
EKA00E09E0014FD000035
EKA00E09E0014FD000036
EKA00E09E0014FD000037
EKA00E09E0014FD000038
EKA00E09E0014FD000039
EKA00E09E0014FD00003A
EKA00E09E0014FD00003B
EKA00E09E0014FD00003C
EKA00E09E0014FD00003D
EKA00E09E0014FD00003E
EKA00E09E0014FD00003F
EKA00E09E0014FD000040
EKA00E09E0014FD000041
EKA00E09E0014FD000042
EKA00E09E0014FD000043
EKA00E09E0014FD000044
EKA00E09E0014FD000045
--More-- (1/2)
```

- 2 Do any of the following:

- To quickly skip to the keys beginning with “EKB”, type /EKB.
 - Press <Enter> to scroll through the list one key at a time
 - Type q to exit the list.
- 3 Press <Enter> to return to the SKM server reports menu.
 - 4 At the **Command** prompt, type q and press <Enter> to quit the SKM server reports menu.
 - 5 Press <Enter> to return to SKM Admin Commands.
 - 6 At the **Command** prompt, type q and press <Enter> to quit SKM Admin Commands and restart the SKM server.

Display Key Template Information (Option 3)

You should not need to run this report unless directed by Quantum Support for troubleshooting. This report displays one template for each library that is attached to the SKM server and is useful for seeing how many libraries are attached. You can also look at the **Next increment** value to see whether any keys have been used. If it is at “000000”, no keys from that template have been used yet.

To view template information:

- 1 Type 3 at the SKM Server Reports menu and press <Enter> for template information.

The template information displays (see [Figure 27](#)).

Figure 27 Template Information With Next Increment Identified

```
Template information:
-----
Template information for EKA00E09E0014FD
Version <akmadmin Version 2.0.3>
Tran Len <00093>
Tran Id <1122>
Return Code <0000>
Increment length <06>
Next increment <000000>
Last increment <0003FF>
Key served <N>
Template full <N>
Increment code <H>
```

- 2 Press <Enter> to return to the SKM server reports menu.
- 3 At the **Command** prompt, type **q** and press <Enter> to quit the SKM server reports menu.
- 4 Press <Enter> to return to SKM Admin Commands.
- 5 At the **Command** prompt, type **q** and press <Enter> to quit SKM Admin Commands and restart the SKM server.

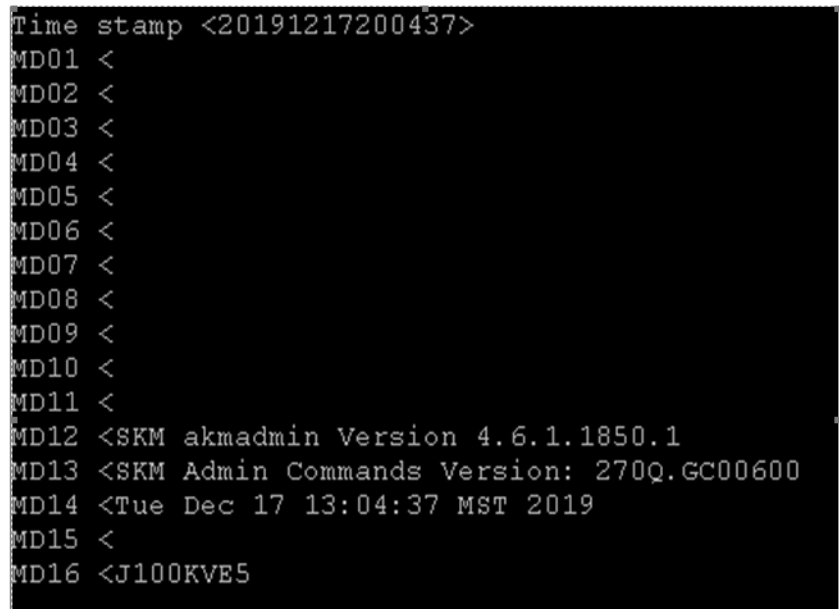
Display Quantum Reserved Key (Option 4)

To view Quantum reserved key information:

- 1 Type **4** at the SKM Server Reports menu and press <Enter> for reserved key information.

The reserved key information displays (see [Figure 28](#)).

Figure 28 Quantum Reserved Key Information



```
Time stamp <20191217200437>
MD01 <
MD02 <
MD03 <
MD04 <
MD05 <
MD06 <
MD07 <
MD08 <
MD09 <
MD10 <
MD11 <
MD12 <SKM akadmin Version 4.6.1.1850.1
MD13 <SKM Admin Commands Version: 270Q.GC00600
MD14 <Tue Dec 17 13:04:37 MST 2019
MD15 <
MD16 <J100KVB5
```

- 2 Press <Enter> to return to the SKM server reports menu.
- 3 At the **Command** prompt, type **q** and press <Enter> to quit the SKM server reports menu.
- 4 Press <Enter> to return to SKM Admin Commands.

- 5 At the **Command** prompt, type **q** and press **<Enter>** to quit SKM Admin Commands and restart the SKM server.

Display Keys Used Today (Option 5)

To display keys used today:

- 1 Type **5** at the SKM Server Reports menu and press **<Enter>** for keys used today information.

The keys used today information displays (see [Figure 29](#)).

Note: This report may take several minutes to generate.

Figure 29 Keys Used Today Information

```
SKM Server Reports.
-----
1) Number of SKM server keys.
2) List of key aliases.
3) Display key template information.
4) Display Quantum Reserved key.
5) Display keys used today.
6) Display system status.
7) Display used key information.
q) Quit.
-----
Command: 5

Display keys used since 00:00:01 01-30-2020 (utc)

This could take a few minutes to complete.

Used keys report for 01-30-2020

Current utc time 18:25:56

Volume Label           Key Alias                Timestamp(utc)
=====
000544L7                EKA00E09E3EC131000021    20200124172345
000604L8                EKB00E09E3EC131000000    20200124172823
=====

Press <Enter>
```

- 2 Press <Enter> to return to the SKM server reports menu.
- 3 At the **Command** prompt, type **q** and press <Enter> to quit the SKM server reports menu.
- 4 Press <Enter> to return to SKM Admin Commands.
- 5 At the **Command** prompt, type **q** and press <Enter> to quit SKM Admin Commands and restart the SKM server.

Display System Status (Option 6)

To display system status:

- 1 Type **6** at the SKM Server Reports menu and press <Enter> for keys used today information.

The system status information displays (see [Figure 30](#)).

Figure 30 System Status
Information

```
SKM server status
Text length <02824>
More Flag <N9999>
Application status <0000>
Disk status <00999999>
Core status <99999999>
Voltage status <99999999>
Battery status <99>
Fan status <9999>
Temperature status <99999999>
Text length <02824>
Status text <-----BEGIN SENSORS-----
sh: 1: sensors: not found
-----END SENSORS-----
-----BEGIN DISK 0 /dev/sg0-----
^M
Enclosure Device ID: 69
Slot Number: 0
Drive's position: DiskGroup: 0, Span: 0, Arm: 0
Enclosure position: N/A
Device Id: 0
WWN: 5000c500c337aff6
Sequence Number: 2
Media Error Count: 0
```

- 2 Press <Enter>, the down arrow key, or <Page Down> to scroll down through the report.

- 3 When "End" displays ([Figure 31](#)), type **q** and press <Enter> to quit the SKM server reports menu.

Figure 31 System Status "End" Display

```
FDE Enable: Disable
Secured: Unsecured
Locked: Unlocked
Needs EKM Attention: No
Foreign State: None
Device Speed: 6.0Gb/s
Link Speed: 6.0Gb/s
Media Type: Hard Disk Device
Drive Temperature :38C (100.40 F)
PI Eligibility: No
Drive is formatted for PI information: No
PI: No PI
Drive's NCQ setting : Enabled
Port-0 :
Port status: Active
Port's Linkspeed: 6.0Gb/s
Drive has flagged a S.M.A.R.T alert : No

Exit Code: 0x00
-----END DISK 1 /dev/sg2-----
>
(END)
```

- 4 Press <Enter> to return to SKM Admin Commands.
- 5 At the **Command** prompt, type **q** and press <Enter> to quit SKM Admin Commands and restart the SKM server.

Display Used Key Information (Option 7)

To display used key information:

- 1 Type **7** at the SKM Server Reports menu and press <Enter> for used key information.

The used key information displays (see [Figure 32](#)).

Figure 32 Used Key Information Selection

```
Used Key Information (Select a template or all)

Template information:
TemplateName (used keys)
-----
1) EKB00E09E3EC131 (1)
a) All Templates
q) Quit
-----
Selection: █
```

- 2 Use a number key followed by <Enter> to select a template, or press <a> followed by <Enter> to select all templates.

[Figure 33](#) provides an example of the “a” option, All Templates.

Figure 33 Used Key Information Selection “a”

```
Used Key Information (Select a template or all)

Template information:
TemplateName (used keys)
-----
1) EKB00E09E3EC131 (1)
a) All Templates
q) Quit
-----
Selection: a

Generating used key report for all templates.
***Checking keys for template: EKB00E09E3EC131

Used key report /home/akmadmin/allusedkeyreport.csv has been generated.

Press <Enter>
```

- 3 Press <Enter> to return to the SKM server reports menu.
- 4 At the **Command** prompt, type **q** and press <Enter> to quit the SKM server reports menu.
- 5 Press <Enter> to return to SKM Admin Commands.

- 6 At the **Command** prompt, type **q** and press **<Enter>** to quit SKM Admin Commands and restart the SKM server.

Viewing the SKM Encryption Key Import Warning Log

During a key import operation, if at least one data encryption key in the file of exported keys is successfully imported but at least one data encryption key is not successfully imported, the library generates an “import warning” message as well as a RAS/diagnostic ticket. The ticket directs you to view the Import Warning Log, which contains a list of the data encryption keys that were not imported.

When this error occurs, it may mean that the file containing the data encryption keys is corrupted. Obtain a new copy of the file and try the key import operation again.

See your library user’s guide or online help for instructions on how to view the SKM Encryption Key Import Warning Log.

Running the Specified Reports Option Only (O 1-6)

This section provides the following information:

- [./skmcmds -O 1 Command](#)
- [./skmcmds -O 2 Command](#)
- [./skmcmds -O 3 Command](#)
- [./skmcmds -O 4 Command](#)
- [./skmcmds -O 5 Command](#)
- [./skmcmds -O 6 Command](#)

You can run specified reports by using the `./skmcmds -O 1-6` command. See [Figure 34](#) below.

Figure 34 Help Menu

```
akmadmin@skm228:~$ ./skmcmds -h
usage: ./skmcmds [-hvLEDBO]
-h:          View this help message.
-v:          View skmcmds version.
-L:          Capture SKM server snapshots without stopping key server.
-E:          Display End User License Agreement (EULA).
-B:          Back up SKM server.
-D on|off:   Turn trace level logging on or off.
-R           Display only the reports menu. The reports do not require the key
server to be stopped so key fetches will still work from the libraries
-O 1-6      Run the specified reports option only.

example: ./skmcmds -D on

akmadmin@skm228:~$ █
```

./skmcmds -O 1 **Command**

To run the `./skmcmds -O 1` command, complete the following:

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 At the `akmadmin@<hostname>` prompt (where `<hostname>` is the SKM server hostname), issue the following command:

```
./skmcmds -O 1
```

The “Number of SKM Server keys” displays and the `akmadmin@<hostname>` prompt reappears.

```
./skmcmds -O 1

Number of SKM Server keys: 6195

akmadmin@skm228:~$ █
```

./skmcmds -O 2 **Command**

To run the `./skmcmds -O 2` command, complete the following:

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 At the `akmadmin@<hostname>` prompt (where `<hostname>` is the SKM server hostname), issue the following command:

```
./skmcmds -O 2
```

The “SKM server key list” displays and the `akmadmin@<hostname>` prompt reappears.

```
akmadmin@skm228:~$ ./skmcmds -O 2

SKM server key list (Press Enter to continue or 'q' to quit):

EKA00E09E097DEE000000
EKA00E09E097DEE000001
EKA00E09E097DEE000002
EKA00E09E097DEE000003
EKA00E09E097DEE000004
EKA00E09E097DEE000005
EKA00E09E097DEE000006
EKA00E09E097DEE000007
EKA00E09E097DEE000008
EKA00E09E097DEE000009
EKA00E09E097DEE00000A
EKA00E09E097DEE00000B
EKA00E09E097DEE00000C
EKA00E09E097DEE00000D
```

`./skmcmds -O 3` Command

To run the `./skmcmds -O 3` command, complete the following:

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 At the `akmadmin@<hostname>` prompt (where `<hostname>` is the SKM server hostname), issue the following command:

```
./skmcmds -O 3
```

The “template information” displays and the `akmadmin@<hostname>` prompt reappears.

```
./skmcmds -O 3

Template information:
-----
Template information for EKB00E09E3EC5FC (library WWN label: 3EC5FC):
arg Constant <EKB00E09E3EC5FC>
arg IncrementLen <6>
arg Constant len <15>
Padded Constant <EKB00E09E3EC5FC                >
Tran len <00093>
Tran Id <1122>
Return code <0000>
Increment len <06>
Next increment <000010                >
Last increment <0003FF                >
Key served flag <Y>
Template full flag <N>
Increment code <H>

-----
akmadmin@skm228:~$ █
```

./skmcmds -O 4 Command

To run the `./skmcmds -O 4` command, complete the following:

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 At the `akmadmin@<hostname>` prompt (where `<hostname>` is the SKM server hostname), issue the following command:

```
./skmcmds -O 4
```

The “key name and characteristics information” display and the `akmadmin@<hostname>` prompt reappears.

```
./skmcmds -O 4
*****
arg Key name <QTM_RESERVED>
arg Instance < >
Padded key name <QTM_RESERVED >
Padded Instance < >
Tran len <01258>
Tran Id <1004>
Return code <0000>
Key name <QTM_RESERVED >
Instance <39ojYnvTIIolBGXNMxJxCCQ==>
Current flag <Y>
Key size bits <0256>
Creation date <20191217>
Activation date <00000000>
Expiration date <00000000>
Rollover code <M>
Rollover days <0000>
Last rollover date <00000000>
Deletable flag <Y>
Revoked date <00000000>
Mirror flag <N>
Time stamp <20191217200437>
MD01 < >
MD02 < >
MD03 < >
MD04 < >
MD05 < >
MD06 < >
MD07 < >
MD08 < >
MD09 < >
MD10 < >
MD11 < >
MD12 <SKM akmadmin Version 4.6.1.1850.1 >
MD13 <SKM Admin Commands Version: 270Q.GC00600 >
MD14 <Tue Dec 17 13:04:37 MST 2019 >
MD15 < >
MD16 <J100KVE5 >
```

./skmcmds -O 5 Command

To run the `./skmcmds -O 5` command, complete the following:

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 At the `akmadmin@<hostname>` prompt (where `<hostname>` is the SKM server hostname), issue the following command:

```
./skmcmds -O 5
```

The “used key information” displays and the `akmadmin@<hostname>` prompt reappears.

Note: This command may take several minutes to complete.

```
./skmcmds -O 5

Display keys used since 00:00:01 01-17-2020 (utc)

This could take a few minutes to complete.

Used keys report for 01-17-2020

Current utc time 15:22:55

Volume Label                Key Alias                Timestamp(utc)
=====
=====
akmadmin@skm228:~$ █
```

./skmcmds -O 6 Command

To run the `./skmcmds -O 6` command, complete the following:

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 At the `akmadmin@<hostname>` prompt (where `<hostname>` is the SKM server hostname), issue the following command:

```
./skmcmds -O 6
```

The “SKM server status” displays and the `akmadmin@<hostname>` prompt reappears.

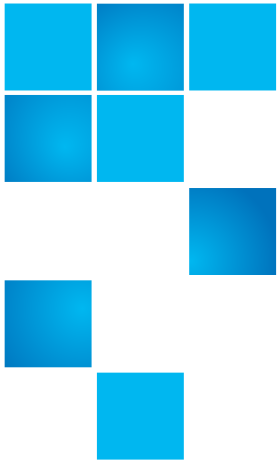
Note: Use the **Enter** key, **Page Up/Down** keys, or **Up/Down** arrows to access additional information.

```
akmadmin@skm228:~$ ./skmcmds -O 6

SKM server status
Text length <02822>
More Flag <N9999>
Application status <0000>
Disk status <00999999>
Core status <99999999>
Voltage status <99999999>
Battery status <99>
Fan status <9999>
Temperature status <99999999>
Text length <02822>
Status text <-----BEGIN SENSORS-----
sh: 1: sensors: not found
-----END SENSORS-----
-----BEGIN DISK 0 /dev/sg0-----
^M
Enclosure Device ID: 69
Slot Number: 0
Drive's position: DiskGroup: 0, Span: 0, Arm: 0
Enclosure position: N/A
Device Id: 0
WWN: 5000c500c337aff6
Sequence Number: 2
Media Error Count: 0
Other Error Count: 0
Predictive Failure Count: 0
Last Predictive Failure Event Seq Number: 0
PD Type: SATA

Raw Size: 931.512 GB [0x74706db0 Sectors]
Non Coerced Size: 931.012 GB [0x74606db0 Sectors]
Coerced Size: 930.390 GB [0x744c8000 Sectors]
Sector Size: 512
Logical Sector Size: 512
Physical Sector Size: 512
Firmware state: Online, Spun Up
Commissioned Spare : No
Emergency Spare : No
Device Firmware Level: LEK8
Shield Counter: 0
```

Chapter 7: Retrieving SKM Reports, Logs, and Information
Running the Specified Reports Option Only (O 1-6)



Chapter 8

Using the Library to Initiate SKM Functions

There are certain SKM operations and functions you need to perform using your library remote Web client. These operations include:

- [Generating Data Encryption Keys](#)
- [Importing TLS Communication Certificates on the Library](#)
- [Exporting and Importing Data Encryption Keys](#)
- [Exporting and Importing Encryption Certificates](#)
- [Sharing Encrypted Tapes Offsite](#)
- [Running EKM Path Diagnostics](#)

In addition, you must initially configure your library to work with the SKM servers. This is described in [Configuring Your Library For SKM](#) on page 83.

This document provides an overview of SKM library functions. For more detail and specifics, see your library user's guide.

Generating Data Encryption Keys

Data encryption keys are generated in sets of a specified quantity (see [Number of Data Encryption Keys Generated](#) on page 243). You can generate data encryption keys at the following times:

- [Generating Data Encryption Keys at Initial Setup](#)
- [Automatically Generating Data Encryption Keys When 80% Depleted](#)
- [Generating Data Encryption Keys When 100% Depleted](#)
- [Manually Generating Data Encryption Keys](#)

The library tracks data encryption key usage and reminds you to generate more keys when needed. If you try to generate data encryption keys on an SKM server that already has sufficient unused data encryption keys, then it will not create more. You will receive a message to that effect on the library remote Web client.

Note: Each library that you connect to an SKM server requires its own set of data encryption keys. Each library only pulls data encryption keys from the set that “belongs” to it. This means that an SKM server may contain several distinct sets of data encryption keys. When the data encryption keys for one library have all been used, then more keys must be generated.

Generating Data Encryption Keys at Initial Setup

At initial setup, the library triggers each SKM server to generate a set of data encryption keys. The process is described in the following sections:

Scalar i40 Scalar i80 Scalar i500	Step 6 on page 85, in section Configuring the Scalar i40/i80 and Scalar i500 Tape Libraries
Scalar i6000	Step 4 on page 86, in section Configuring the Scalar i6000 Tape Library
Scalar i3 Scalar i6	Step 4 on page 89, in section Configuring the Scalar i3/i6 Tape Library

Automatically Generating Data Encryption Keys When 80% Depleted

When an SKM server has used 80 percent of the data encryption keys assigned to a particular library, that library attempts to automatically generate data encryption keys on the SKM server. Both SKM servers must be running and operational in order for key generation to succeed.

Note: The data encryption key generation process takes 15 minutes on the Scalar i40, i80, and i500, and up to an hour on the Scalar i3, i6, and i6000.

- **If automatic key generation succeeds,** a RAS/diagnostic ticket informs you the keys were generated and instructs you to back up both SKM servers as soon as possible.
- **If automatic key generation fails:**
 - **Scalar i40/i80 and Scalar i500:** The library tries again every time a new key is requested, until the keys are 90 percent depleted. At that point, the library stops trying to auto-generate keys and issues a ticket stating that you must manually generate keys (see [Manually Generating Data Encryption Keys](#) on page 137).
 - **Scalar i6000:** The library tries again every time a new key is requested until all the keys are depleted.

Generating Data Encryption Keys When 100% Depleted

If an SKM server completely runs out of data encryption keys for a particular library, that library generates a RAS/diagnostic ticket, which states that you have run out of data encryption keys and that the library attempted to fail over to the other SKM server. If this happens, it is imperative that you manually generate a new set of data encryption keys on the depleted server immediately and then back up both SKM servers. See [Manually Generating Data Encryption Keys](#) on page 137.

Manually Generating Data Encryption Keys

To manually generate data encryption keys, you need to temporarily disable library managed encryption on a partition, and then enable it again. Enabling library managed encryption on a partition triggers the library to check both SKM servers to see if new data encryption keys are needed. If so, it creates the keys.

Note: The data encryption key generation process takes 15 minutes to an hour, depending on the library type. You should not run any library or host-initiated operations on SKM partitions during key generation and backup.

Caution: Avoid manually generating keys on more than five libraries simultaneously as the key generation process is resource-intensive on the server. Generating keys manually on more than five libraries at once could result in a failure to complete the key generation operation, or interfere with key retrieval operations. If a failure does occur during key generation, wait 10 minutes, then try to start it again. The key generation process will resume from where the error was encountered.

To manually generate data encryption keys:

- 1 Make sure that both SKM servers are running and operational.
- 2 From the library's Web client, access the encryption partition configuration screen.
- 3 Refer to the specific product documentation (i500, i6000, i3, or i6 libraries) if you need further details on how to Disable/Enable library managed encryption.

Caution: When you change the partition's encryption method to **Allow Application Managed**, the data that was written to the tapes while the partition was configured for **Enable Library Managed** can no longer be read, until you change the partition back to **Enable Library Managed**. You will only be disabling for a short time, and then changing back to **Enable Library Managed** (just to trigger the key generation process) so this should have little effect, unless you forget to turn it back to **Enable Library Managed**.

- 4 Wait 3 minutes to allow the changes to complete.
- 5 Go back to the encryption partition configuration screen and change the partition back to **Enable Library Managed**. Again, make sure to apply the changes.

- 6 Wait for the process to complete before resuming library operations.
- 7 Back up both SKM servers. You must back up both SKM servers every time you generate new data encryption keys to protect your data in case of catastrophic server failure. See [Backing Up the SKM Server](#) on page 103.

Importing TLS Communication Certificates on the Library

TLS communication certificates will always need to be loaded on the libraries that access the SKM servers.

You may use Quantum-provided certificates or your own certificates. If you install your own TLS certificates on the SKM server, you must also install your own certificates on the library. Similarly, if you use the Quantum-provided TLS certificates on the SKM server, you must also use the Quantum provided TLS certificates on the library.

Newer libraries come with Quantum-provided TLS certificates pre-installed. Quantum also ships out a set of library TLS certificates (separately from the SKM server) in case you need to install them. See your library user's guide for instructions on how to verify whether TLS certificates are installed on the library and how to install them.

Note: Beginning with SKM 2.5, TLS certificates are no longer pre-installed, and must be install on both the SKM server and tape library.

Exporting and Importing Data Encryption Keys

When you want to share encrypted tape cartridges with another site, or to read tapes encrypted by another site, you need to import and export data encryption keys via the library remote Web client. See [Sharing Encrypted Tapes Offsite](#) on page 141 for information and instructions on this process.

Both SKM servers must be connected and operational in order to import or export data encryption keys.

If errors occur during a data encryption key import operation, you receive an error message and a RAS/diagnostic ticket. See [Capturing SKM Server Logs and Snapshots](#) on page 114 for more information.

See your library user's guide or online help for instructions on exporting and importing data encryption keys.

After importing keys, make sure to back up both SKM servers.

Exporting and Importing Encryption Certificates

Note: You must use the SKM Admin menu to export and import encryption certificates.

You need to import and export encryption certificates as part of sharing encrypted tapes with other organizations. See [Encryption Certificates](#) on page 5 and [Sharing Encrypted Tapes Offsite](#) on page 141 for information and instructions on this process.

Both SKM servers must be connected and operational in order to import encryption certificates. You may export an SKM server's native encryption certificate when only one SKM server is connected/operational, because the two SKM servers in a pair share the same native encryption certificate.

See your library user's guide or online help for instructions on exporting and importing encryption certificates.

Sharing Encrypted Tapes Offsite

Note: You must use the SKM Admin menu to share encrypted tapes offsite.

It is common practice to share tapes with other organizations for data transfer, joint development, contracting services, or other purposes. If you are using SKM, you can share encrypted tapes with other organizations and individuals who also use SKM.

SKM creates unique key aliases across all SKM installations worldwide. This ensures that you can safely share SKM-encrypted tapes with other sites or companies.

In order to share encrypted data on a tape, a copy of the symmetric key used to encrypt the data on the tape must be made available to the other organization to enable them to read the tape.

In order for the symmetric key to be shared, the other organization must share their public key with you. This public key will be used to wrap the symmetric key when it is exported from the SKM keystore.

When the other organization imports the symmetric key into their SKM keystore, it will be unwrapped using their corresponding private key. This ensures that the symmetric key will be safe in transit since only the holder of the private key will be able to unwrap the symmetric key.

With the symmetric key that was used to encrypt the data in their SKM keystore, the other organization will then be able to read the data on the tape.

The general process for sharing a tape from an originating (i.e., source) organization to a receiving (i.e., destination) organization is as follows.

Note: See your library user's guide for a description including menu paths to the appropriate screens.

- 1 The destination administrator navigates to the encryption certificate export screen on the library remote Web client, exports the native encryption certificate that belongs to the destination SKM server, and saves the file to a known location on a computer.

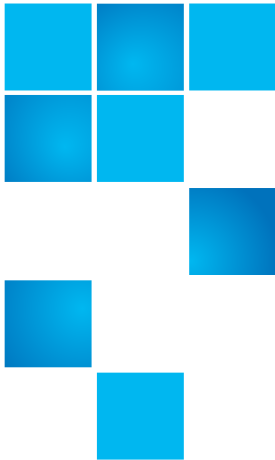
- 2 The destination administrator sends the native encryption certificate file to the source administrator.
- 3 The source administrator saves the encryption certificate file to a known location on a computer.
- 4 The source administrator navigates to the encryption certificate import screen on the library remote Web client and imports the encryption certificate onto the source SKM server.
- 5 The source administrator navigates to the encryption key export screen on the library remote Web client and exports the data encryption key(s) used to encrypt the shared tape(s), assigning the same encryption certificate noted above to wrap the data encryption keys. The source administrator saves the file containing the wrapped data encryption keys to a known location on a computer.
- 6 The source administrator sends the file containing the wrapped data encryption keys to the destination administrator.
- 7 The destination administrator saves the file containing the wrapped data encryption keys to a known location on a computer.
- 8 The destination administrator navigates to the encryption key import screen on the library remote Web client and imports the data encryption keys onto the destination SKM server.
- 9 The destination library can now read the encrypted tapes.

Running EKM Path Diagnostics

EKM path diagnostics consists of a series of short tests to validate whether the SKM servers are running, communicating with the library, and able to serve keys as required.

You should run the EKM path diagnostics any time you change the SKM server settings or library encryption settings.

For complete information about the EKM path diagnostic tests, how to run them, and how to troubleshoot them, see your library user's guide or online help.



Chapter 9

Using the SKM Server to Initiate SKM Functions

In SKM, functions that were once only available on the library can now be executed from the SKM command line interface. These operations include:

- [Exporting Encryption Certificates](#)
- [Importing Encryption Certificates](#)
- [Exporting All Encryption Keys](#)
- [Importing All Encryption Keys](#)
- [Exporting All Used Encryption Keys](#)
- [Importing All Used Encryption Keys](#)
- [Exporting Used Keys Based on Media Barcode](#)
- [Importing Used Keys Based on Media Barcode](#)

Administrators using SKM 2.0 or older can download a utility script which will add the new import and export functionality to their existing SKM server installation. See [Installing the Import/Export Utility](#) on page 213.

You must initially configure your library to work with the SKM servers. This is described in [Configuring Your Library For SKM](#) on page 83.

This document provides an overview of SKM server functions.

Sharing Encrypted Tapes Offsite

It is common practice to share tapes with other organizations for data transfer, joint development, contracting services, or other purposes. If you are using SKM, you can share encrypted tapes with other organizations and individuals who also use SKM.

SKM creates unique key aliases across all SKM installations worldwide. This ensures that you can safely share SKM-encrypted tapes with other sites or companies.

In order to share encrypted data on a tape, a copy of the symmetric key used to encrypt the data on the tape must be made available to the other organization to enable them to read the tape.

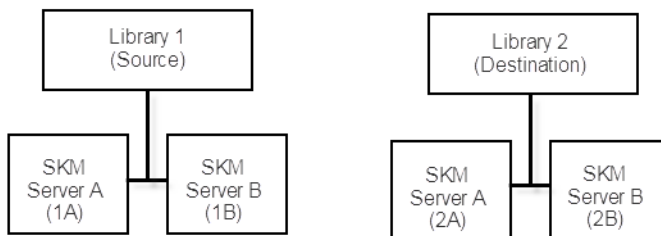
In order for the symmetric key to be shared, the other organization must share their public key with you. This public key will be used to wrap the symmetric key when it is exported from the SKM keystore.

When the other organization imports the symmetric key into their SKM keystore, it will be unwrapped using their corresponding private key. This ensures that the symmetric key will be safe in transit since only the holder of the private key will be able to unwrap the symmetric key.

With the symmetric key that was used to encrypt the data in their SKM keystore, the other organization will then be able to read the data on the tape.

The general process for sharing a tape from an originating (i.e., source) organization to a receiving (i.e., destination) organization is as follows.

Figure 35 Library and SKM server physical layout



Step	Perform on Source Server/SKM Pair	Perform on Destination Server/SKM Pair
1 Export/Import the native encryption certificate that belongs to destination SKM pair.	1. Export the native encryption certificate from the source server to a file in a known location.	
	2. Send the native encryption certificate file to the destination server administrator.	
		3. Import the encryption certificate received from the source server.
2 Export/Import the encryption keys used to encrypt the shared tapes.	1. Export the data keys used to encrypt the shared tape(s), assigning (wrapping with) the same encryption certificate as used above. Save the file to a known location	
	2. Send exported data key file to the destination server administrator.	
		3. Import the data key file to the destination server.

- 1 The source (library 1 in [Figure 35](#) on page 144) administrator navigates to the encryption certificate export screen, exports the native encryption certificate that will be sent to the destination SKM server (SKM server 2a), and saves the file to a known location on a computer.
- 2 The source administrator sends the native encryption certificate file to the destination (library 2 in [Figure 35](#) on page 144) administrator.
- 3 The destination administrator saves the encryption certificate file to a known location on a computer.
- 4 The destination administrator navigates to the encryption certificate import screen and imports the encryption certificate onto the source SKM server.

- 5 The source administrator navigates to the encryption key export screen and exports the data encryption key(s) used to encrypt the shared tape(s), assigning the same encryption certificate noted above to wrap the data encryption keys. The source administrator saves the file containing the wrapped data encryption keys to a known location on a computer.
- 6 The source administrator sends the file containing the wrapped data encryption keys to the destination administrator.
- 7 The destination administrator saves the file containing the wrapped data encryption keys to a known location on a computer.
- 8 The destination administrator navigates to the encryption key import screen and imports the data encryption keys onto the destination SKM server.
- 9 The destination library can now read the encrypted tapes.

Exporting and Importing Encryption Certificates

You need to import and export encryption certificates as part of sharing encrypted tapes with other organizations. See [Encryption Certificates](#) on page 5 and [Exporting and Importing Encryption Certificates](#) on page 146 for information and instructions on this process.

Both SKM servers must be connected and operational in order to import and export encryption certificates.

Note: Native certificates will not be available if keys have not yet been generated on the server.

See your library user's guide or online help for instructions on exporting and importing encryption certificates using your library.

Please see to [Figure 35](#) on page 144 as a visual aid to completing this procedure. The libraries and servers shown in [Figure 35](#) on page 144 are referenced in this procedure.

Exporting Encryption Certificates

To export a TLS communication certificate:

- 1 Log on to the SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92). Note which server you are logging on to (SKM server 1a in [Figure 35](#) on page 144).
- 2 Access SKM Admin Commands (see [Logging on to the Command Line Interface](#) on page 92).
- 3 Type **k** and press **<Enter>**.
The **IP Address** prompt displays.
- 4 Type the IP address of the other SKM server associated with the one you are running commands from (SKM server 1b in [Figure 35](#) on page 144). Press **<Enter>**.

The **Key/Certificate import and export** displays.

```
Key/Certificate import and export.  
  
Local SKM server IP address: 10.20.87.110  
  
Remote SKM server IP address: 10.20.87.111  
  
-----  
1) Encryption Certificate.  
2) Encryption Key.  
q) Quit.  
-----  
Command:
```

- 5 Type **1** and press **<Enter>**.
The **Certificate import and export** displays.
- 6 Type **e** and press **<Enter>** to Export the Certificate to the other server (SKM server 1b in [Figure 35](#) on page 144).
The **Public certificate list available for export** displays.
- 7 Type the number associated with the certificate you want to export and press **<Enter>**.
The certificate is exported to the file location shown in the interface. Note the location of the file.

```
Public certificate list available for export.
-----
1) QKMIECertUM210275UM210276 (NATIVE)
q) Quit
-----

Please select a certificate to export or (q) to quit: 1

Exporting certificate: QKMIECertUM210275UM210276 as QKMIECertUM210275UM210276.pem

Certificate: QKMIECertUM210275UM210276 was successfully exported to file /home/aknadmin/certs/QKMIECertUM210275UM210276.pem

Press <Enter>
```

8 Press **<Enter>**. If you wish to export another certificate, repeat [Step 7](#) on page 147. Otherwise type **q** and press **<Enter>** twice.

The **Certificate import and export** displays.

9 Type **q** and press **<Enter>** twice.

The **Key/Certificate import and export** displays.

10 Type **q** and press **<Enter>** twice.

The Command line interface main menu displays.

Importing Encryption Certificates

To import an encryption communication certificate:

Note: Ensure the TLS Communication Certificate has been exported by following the procedure [Exporting Encryption Certificates](#) on page 147.

1 Secure copy the certificate file to the server you want to import the certificate to.

2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).

3 Type **k** and press **<Enter>**.

The **IP Address** prompt displays.

4 Type the IP address of the secondary SKM server associated with the one you are running commands from (SKM server 2b in [Figure 35](#) on page 144). Press **<Enter>**.

The **Key/Certificate import and export** displays.

5 Type **1** and press **<Enter>**.

The **Certificate import and export** displays.

6 Type **i**, select the file to import, and press **<Enter>**.

7 Press **<Enter>** to import the certificate.

When complete, a success message displays.

8 Type **q** and press **<Enter>** twice.

The **Certificate import and export** displays.

9 Type **q** and press **<Enter>** twice.

The **Key/Certificate import and export** displays.

10 Type **q** and press **<Enter>** twice.

The Command line interface main menu displays.

Exporting and Importing Encryption Keys

When you want to share encrypted tape cartridges with another site, or to read tapes encrypted by another site, you need to import and export encryption keys.

Both SKM servers must be connected and operational in order to import or export encryption keys.

All files exported by the SKM application can be imported by libraries that use SKM, and all files exported by libraries using SKM can be imported by the SKM application. See your library user's guide or online help for instructions on exporting and importing encryption keys using your library.

After importing keys, make sure to back up both SKM servers.

Exporting All Encryption Keys

You can export all encryption keys associated with a library.

- 1 Log on to the first server pair's primary server (1a) SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).

- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 Type **k** and press **<Enter>**.
The **IP address of the SKM server** command line displays.
- 4 Type the IP address of the remote SKM server (SKM server 1b in [Figure 35](#) on page 144) and press **<Enter>** to show the Import/Export submenu.
- 5 Type **2** and press **<Enter>** to export the Encryption Key.
The Key import and export menu displays.

```
Key import and export.
-----
i) Import key(s).
e) Export key(s).
q) Quit.
-----
Command: _
```

- 6 Type **e** and press **<Enter>**.
The **Exporting keys** menu displays.

```
Exporting key(s).
-----
1) QKMIECertUM210275UM210276 (NATIVE)
q) Quit
-----
Please select a certificate to export or (q) to quit: _
```

- 7 Choose the menu item number corresponding to the Certificate file that the keys you want to export are associated with. Type the menu item number and press **<Enter>**.
The **Exporting keys** menu displays.


```
Exporting key(s).  
Using certificate: QKMIECertUM210275UM210276  
  
Available library templates for key export.  
-----  
1) EKA00E09E0978F6 (library WWN label: 0978F6)  
q) Quit  
-----  
Please select the library template or (q) to quit:
```

- 8 Choose the menu item number corresponding to the library template file that the keys you want to export are associated with. Type the menu item number and press <Enter>.

The **Key Export Options** menu displays.

```
Exporting key(s).  
Using certificate: QKMIECertUM210275UM210276  
  
Using library template: EKA00E09E0978F6  
  
Key export options.  
-----  
1) Used keys associated with the library.  
2) All keys associated with the library.  
3) Used keys based on media barcode.  
q) Quit  
-----  
Please select key export option or (q) to quit:
```

- 9 Type 2 and press <Enter>.

The system begins the export process. Depending on the number of keys associated with the Certificate and template, the export process may take up to 30 minutes. Do not press any keys during this time. A success message will display once the export process is complete. Note the name of the .tgz file.

```
Exporting all keys for template EKA00E09E0978F6 using certificate QKMIECertUM210275UM210276
Current time: Mon Apr 15 10:29:31 PDT 2013
Current time: Mon Apr 15 10:38:35 PDT 2013

A total of 2048 keys have been exported for template: EKA00E09E0978F6.
Key export filename: /home/akmadmin/keys/EXK00E09E0978F615042013.tgz
Press <Enter>
```

- 10 Press <Enter> to display the Key export options menu.
- 11 Type **q** and press <Enter> twice to display the **Exiting key export** message.
- 12 Press <Enter> to display the **Key import and export** menu.
- 13 Type **q** and press <Enter> twice to display the **Key/Certificate import and export** menu.
- 14 Type **q** and press <Enter> twice to quit and return to SKM Admin Commands.
- 15 Type **q** and press <Enter> to exit SKM.
- 16 Secure copy the key export file to the server you want to import the certificate to.

Importing All Encryption Keys

- 1 Log on to the first server pair's primary server (2a) SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 Type **k** and press <Enter>.
- 4 Type the IP address of the primary server in the second server pair (SKM server 2b in Figure 20 on page 98) you want to import the certificate to and press <Enter>. For example, type **10.20.80.110** and press <Enter>.
- 5 Type **2** and press <Enter>.

- 6 Type **i** and press **<Enter>**.
- 7 Select the file number you want to import and press **<Enter>**.
The import process begins.
- 8 Press **<Enter>** to display the Key export options menu.
- 9 Type **q** and press **<Enter>** twice to display the **Exiting key export** message.
- 10 Press **<Enter>** to display the **Key import and export** menu.
- 11 Type **q** and press **<Enter>** twice to display the **Key/Certificate import and export** menu.
- 12 Type **q** and press **<Enter>** twice to quit and return to SKM Admin Commands.
- 13 Type **q** and press **<Enter>** to exit SKM.

Exporting All Used Encryption Keys

You can export all used encryption keys associated with a library.

- 1 Log on to the first server pair's primary server (1a) SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 Type **k** and press **<Enter>**.
The **IP address of the SKM server** command line displays.
- 4 Type the IP address of the remote SKM server (SKM server 1b in [Figure 35](#) on page 144) and press **<Enter>** to show the Import/Export submenu.
- 5 Type **2** and press **<Enter>** to export the Encryption Key.
The Key import and export menu displays.
- 6 Type **e** and press **<Enter>**.
The **Exporting keys** menu displays.
- 7 Choose the menu item number corresponding to the Certificate file that the keys you want to export are associated with. Type the menu item number and press **<Enter>**.
The **Exporting keys** menu displays.

- 8 Choose the menu item number corresponding to the library template file that the keys you want to export are associated with. Type the menu item number and press **<Enter>**.

The **Key Export Options** menu displays.

- 9 Type **1** and press **<Enter>**.

The system begins the export process. Depending on the number of keys associated with the Certificate and template, the export process may take up to 30 minutes. Do not press any keys during this time. A success message will display once the export process is complete. Note the name of the file.

```
Please select key export option or (q) to quit: 1
Exporting used keys for template EKA00E09E0978F6 using certificate QKMIECertUM210275UM210276
Key export filename: /home/akmadmin/keys/EXK00E09E0978F615042013.tgz
Press <Enter>
```

- 10 Press **<Enter>** to display the Key export options menu.
- 11 Type **q** and press **<Enter>** twice to display the **Exiting key export** message.
- 12 Press **<Enter>** to display the **Key import and export** menu.
- 13 Type **q** and press **<Enter>** twice to display the **Key/Certificate import and export** menu.
- 14 Type **q** and press **<Enter>** twice to quit and return to SKM Admin Commands.
- 15 Type **q** and press **<Enter>** to exit SKM.
- 16 Secure copy the key export file to the server you want to import the certificate to.

Importing All Used Encryption Keys

- 1 Log on to the first server pair's primary server (2a) SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).

- 3 Type **y** and press **<Enter>** twice.
- 4 Type **k** and press **<Enter>**.
- 5 Type the IP address of the primary server in the second server pair (SKM server 2b in Figure 20 on page 98) you want to import the certificate to and press **<Enter>**. For example, type `sftp 10.20.80.110` and press **<Enter>**.
- 6 Type **2** and press **<Enter>**.
- 7 Type **i** and press **<Enter>**.
The import process begins. When the process is complete, the Key file list available for import menu displays.
- 8 Press **<Enter>** to display the Key export options menu.
- 9 Type **q** and press **<Enter>** twice to display the **Exiting key export** message.
- 10 Press **<Enter>** to display the **Key import and export** menu.
- 11 Type **q** and press **<Enter>** twice to display the **Key/Certificate import and export** menu.
- 12 Type **q** and press **<Enter>** twice to quit and return to SKM Admin Commands.

Exporting Used Keys Based on Media Barcode

You can export the last data key associated with a specific media barcode on the library.

- 1 Log on to the first server pair's primary server (1a) SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 Type **k** and press **<Enter>**.
The **IP address of the SKM server** command line displays.
- 4 Type the IP address of the remote SKM server (SKM server 1b in [Figure 35](#) on page 144) and press **<Enter>** to show the Import/Export submenu.
- 5 Type **2** and press **<Enter>** to export the Encryption Key.
The Key import and export menu displays.

- 6 Type **e** and press **<Enter>**.
The **Exporting keys** menu displays.
- 7 Choose the menu item number corresponding to the Certificate file that the keys you want to export are associated with. Type the menu item number and press **<Enter>**.
The **Exporting keys** menu displays.
- 8 Choose the menu item number corresponding to the library template file that the keys you want to export are associated with. Type the menu item number and press **<Enter>**.
The **Key Export Options** menu displays.
- 9 Type **3** and press **<Enter>**.
- 10 Type the full or partial barcode of the media you want to export the encryption keys for. Press **<Enter>**.
- 11 The system retrieves the barcode or barcodes that you entered and exports the keys in a compressed .tgz file.
The system retrieves the used key or keys associated with the barcode or barcodes that you entered and exports the keys in a compressed .tgz file. Note the name of the file.

```
Used keys filtered based on media barcode. A full
or partial barcode may be used (i.e. 0100, 010010L5).

Enter a value to search by (or q to quit): 000302

Exporting keys that match 000302.

Total number of keys matching criteria is 1

Exporting selective keys for template EKA00E09E0978F6 using certificate QKMIECertUM210275UM210276

Key export filename: /home/akmadmin/keys/EXK00E09E0978F615042013.tgz

Press <Enter>
```

- 12 Press **<Enter>** to display the Key export options menu.
- 13 Type **q** and press **<Enter>** twice to display the **Exiting key export** message.
- 14 Press **<Enter>** to display the **Key import and export** menu.

- 15 Type **q** and press **<Enter>** twice to display the **Key/Certificate import and export** menu.
- 16 Type **q** and press **<Enter>** twice to quit and return to SKM Admin Commands.
- 17 Type **q** and press **<Enter>** to exit SKM.
- 18 Secure copy the key export file to the server you want to import the certificate to.

Importing Used Keys Based on Media Barcode

- 1 Log on to the first server pair's primary server (2a) SKM server command line interface (see [Logging on to the Command Line Interface](#) on page 92).
- 2 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 3 Type **y** and press **<Enter>** twice
- 4 Type **k** and press **<Enter>**.
- 5 Type the IP address of the primary server in the second server pair (SKM server 2b in Figure 20 on page 98) you want to import the certificate to and press **<Enter>**. For example, type **sftp 10.20.80.110** and press **<Enter>**.
- 6 Type **2** and press **<Enter>**.
- 7 Type **i** and press **<Enter>**.
The import process begins. When the process is complete, the **Key file list available for import** menu displays.
- 8 Press **<Enter>** to display the Key export options menu.
- 9 Type **q** and press **<Enter>** twice to display the **Exiting key export** message.
- 10 Press **<Enter>** to display the **Key import and export** menu.
- 11 Type **q** and press **<Enter>** twice to display the **Key/Certificate import and export** menu.
- 12 Type **q** and press **<Enter>** twice to quit and return to **SKM Admin Commands**.

Chapter 9: Using the SKM Server to Initiate SKM Functions Exporting and Importing Encryption Keys



Chapter 10

Troubleshooting

This chapter discusses the following error scenarios and resolutions:

- [Frequently Asked Questions](#)
- [LED Error Indicators](#)
- [Library RAS/Diagnostic Tickets](#)
- [POST Error Codes](#)
- [Troubleshooting Guide](#)
- [Locating the SKM Server Serial Number](#)

Frequently Asked Questions

[Table 1](#) presents a list of common troubleshooting questions and answers.

Table 1 Frequently Asked
Questions

Question	Answer
How can I tell if the SKM server is running?	Run EKM Path Diagnostics test from the library. If all tests pass, the SKM server is running.
What is the difference between Application-Managed Encryption (AME) and Library-Managed Encryption (LME) and how do they work?	AME is not part of SKM. In AME, the ISV application manages the interaction with the encryption-capable drive. The ISV application may or may not encrypt data. With LME, the library (with the SKM server) manages the interaction with the encryption-capable tape drive. LME does not require any ISV support and is transparent to the application.
When is media encrypted?	Media (either new or re-labeled) is encrypted when it is initially written to at the beginning of the tape (BOT).
What state must the media be in to be encrypted using SKM?	The media must be either blank or erased. If any unencrypted data is on the media, appended data will not be encrypted. If the media contains anything other than LME-encrypted data, the data must be erased. Interleaving LME data with non-encrypted or AME-encrypted data is not supported.
How can I verify that tapes are being encrypted using SKM?	The library interface provides several reports that indicate which tapes are encrypted. See your library user's guide for details.
How can I tell which tapes are encrypted and which are not encrypted?	The library interface provides several reports that indicate which tapes are encrypted. See your library user's guide for details.
How will I be notified of write/read errors?	SKM does not report these types of errors. Errors are reported in the following ways: <ul style="list-style-type: none">• The host/ISV application reports read and write failures.• The library may issue a RAS/diagnostic ticket when a write or read operation fails.
How will I be notified of SKM server problems?	The library issues a RAS/diagnostic ticket.

Question	Answer
How will I know if one of the SKM servers in a pair goes down and fails over to the other one?	The library issues RAS/diagnostic tickets when a server failed and successfully failed over to the redundant server.
How will I know if both SKM servers go down?	<p>If both servers go down:</p> <ul style="list-style-type: none"> • The library issues RAS/diagnostic tickets when both servers are down. • The ISV application experiences read/write failures for encrypted data.
How will I know if just the secondary SKM server goes down (while the primary is still working fine)?	<p>When the library is power-cycled, it attempts to contact both SKM servers. If one or both servers cannot be contacted, the library generates a RAS/diagnostic ticket.</p> <p>During regular use, if Automatic EKM Path Diagnostics is enabled, the library will issue a RAS ticket if it cannot communicate with the secondary SKM server. If Automatic EKM Path Diagnostics is not enabled, then you will not be notified.</p> <p>Note: Automatic EKM Path Diagnostics is enabled by default and should be left enabled.</p>

LED Error Indicators

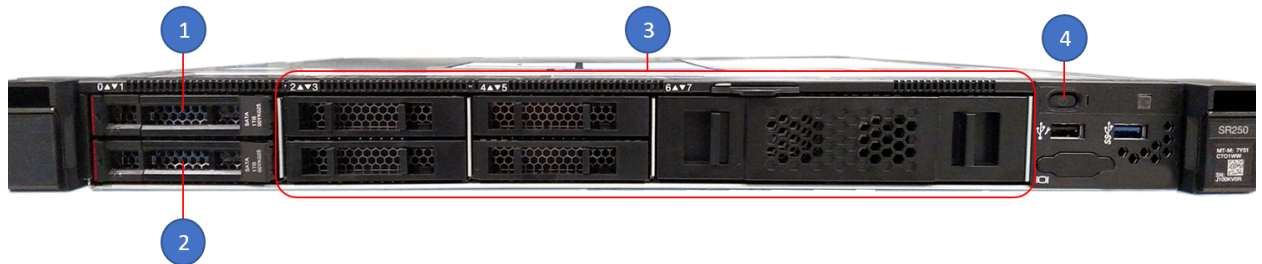
This section applies only to the SKM appliance server. This section includes:

- [SKM 2.7 Appliance Server \(and later versions\)](#)
- [SKM 2.6 Appliance Server \(and earlier versions\)](#)

SKM 2.7 Appliance Server (and later versions)

The two drives within the SKM 2.7 appliance server are located in Slot 0 and 1 (left front). Refer to [Figure 36](#) and [Figure 37](#).

Figure 36 SKM 2.7 Appliance
Server Front Panel



1	Drive 0 (2.5 inch)	3	Drive Slots (empty)
2	Drive 1 (2.5 inch)	4	Power Button/LED

Figure 37 SKM 2.7 Appliance
Server Rear Panel

The Ethernet ports on the rear of the server are as follows:

- Unmarked port (far left: port) 10/100/1000 Mb Ethernet port
- Port 1 (middle port): 1GbE port
- Port 2 (far right: port): 1GbE port



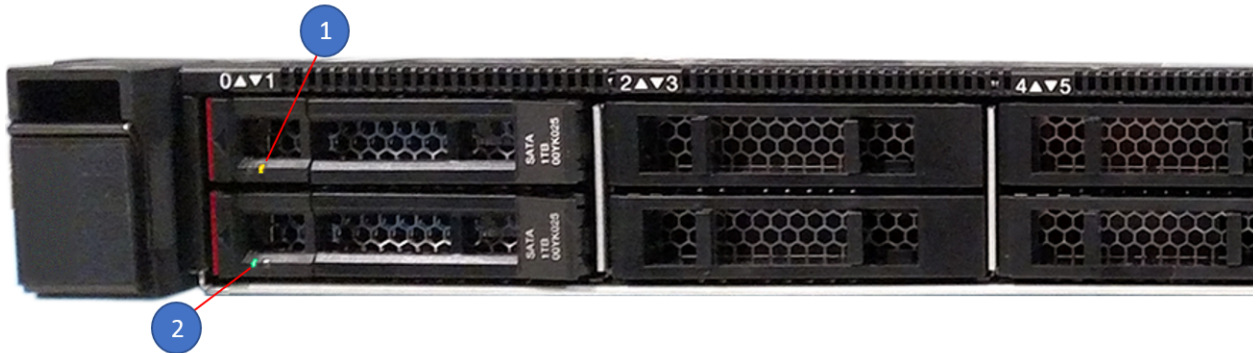
1	Serial Port (DB-9)	5	Power Supply Unit (PSU)
2	Configuration/Management Port	6	Power Cord Connection
3	1 GbE Port (RJ-45)	7	VGA Port
4	1 GbE Port (RJ-45)		

Drive Status LEDs

The amber hard disk drive status LED will be solidly illuminated on the failed hard disk drive.

- See [Figure 38](#) for location of amber LED illuminated on the failed drive (Slot 0, Callout 1).
- Notice that the drive in Slot 1 (Callout 2) has a green LED (meaning the drive is operational).

Figure 38 LED Location on Front of SKM 2.7 Appliance Server



SKM 2.6 Appliance Server (and earlier versions)

The LEDs on the front of the SKM appliance server can signal problems with the server. [Figure 39](#) shows the location of the LEDs, and [Table 2](#) on page 165 describes what the LED error codes mean. For additional explanation of all the LEDs and their functions, see [SKM 2.6 Appliance \(and Earlier Versions\)](#) on page 19.

Figure 39 LED Locations on
Front of SKM Appliance Server

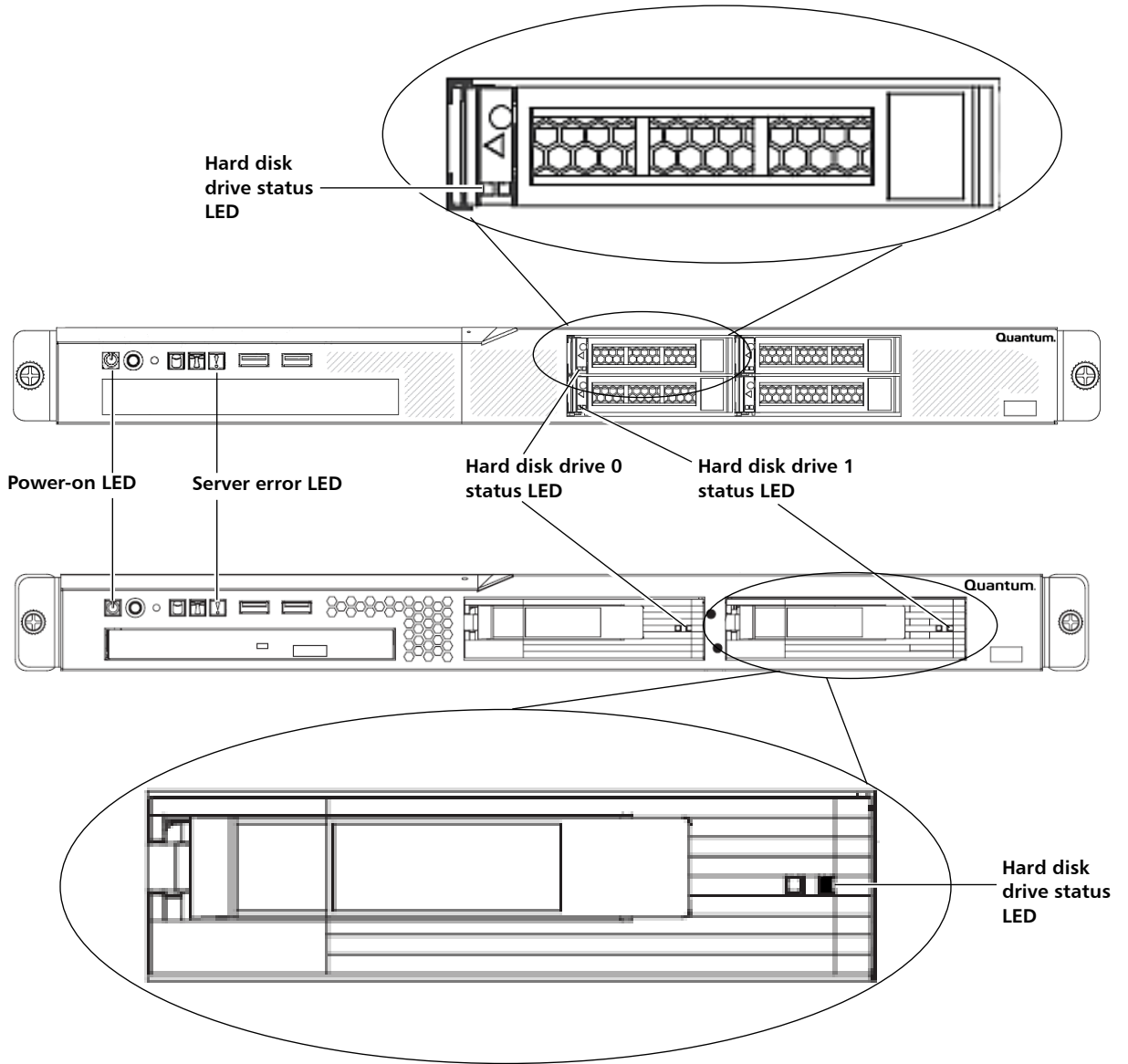


Table 2 SKM Server LED Error Codes

LED	Color	Error Code	What it means and what to do
Power-on LED	Green	Blinking	Server is powered off but is still connected to an AC power source. Power ON the server by pressing the power button.
		Off	AC power is not present, or LED is burned out. Check to see if the server is connected to a working AC power source. If it is, the LED may be burned out. Contact Quantum Support for a replacement server.
Server error LED	Amber (with exclamation point)	On solid	This LED illuminates during hard disk drive replacement when a hard disk drive is missing from its slot. It should go off again when the hard disk drive is replaced. If this LED is illuminated and both hard disk drives are properly installed, there is a problem with the server. Contact Quantum Support.
Hard disk drive status LED	Amber	On solid	The hard disk drive is faulty and must be replaced. Contact Quantum Support.
		Blinking	Indicates that a RAID rebuild is taking place.

Library RAS/Diagnostic Tickets

The library will generate Reliability, Availability, and Serviceability (RAS)/diagnostic tickets for certain SKM server conditions and library-initiated SKM operations. Some tickets are for information only. Others alert you to problems that need to be fixed. Follow the resolution instructions in the ticket to help clear or diagnose problems. Contact Quantum Support if you cannot resolve the problem yourself.

POST Error Codes

This section applies only to the SKM appliance server.

When you turn on the server, it performs a series of tests to check the operation of the server components. This series of tests is called the power-on self-test (POST).

Some server models have a “POST beep code,” described in the table below, to help identify whether the SKM appliance server is working or not. If your server does not have POST beep codes, use the LED indicators described in [LED Error Indicators](#) on page 161 to determine if a problem exists.

Beep Code	Indicates
One beep	Successful completion of POST with no errors.
More than one beep; any sequence of beeps.	POST detected a problem with the server. Contact Quantum Support.

Troubleshooting Guide

[Table 3](#) provides a list of problems and actions you can take to resolve them.

Table 3 Troubleshooting Guide

Symptom	Action
A problem occurs only occasionally and is difficult to diagnose.	Make sure that all cables and cords are connected securely to the rear of the server and attached devices.

Symptom	Action
<p>The SKM appliance server does not boot up. The power button does not work, and the reset button does work.</p> <p>Note: The power button will not function for 20 seconds to three minutes after the server has been connected to AC power.</p>	<p>Make sure that the power button is working correctly:</p> <ol style="list-style-type: none"> 1 Disconnect the server power cords. 2 Reconnect the power cords. 3 Press the power button. 4 If the server does not start, replace the server. Contact Quantum Support for assistance.
<p>The SKM appliance server unexpectedly shuts down, and the LEDs on the front panel are not on.</p>	<ol style="list-style-type: none"> 1 Make sure the power cord is connected to the server and plugged in to a working power source. 2 Turn the server back on and check the airflow from the fan. When the server is powered on, air is flowing from the fan grille. If there is no airflow, the fan is not working. This can cause the server to overheat and shut down. 3 Contact Quantum Support for SKM server replacement.
<p>The SKM appliance server fan is not working.</p>	<p>Contact Quantum Support.</p>
<p>The SKM appliance server fan is very noisy.</p>	<p>It is normal for the fan to be very noisy during initial startup for about 20 seconds, after which the fan should become quieter. If the fan does not quiet down after about 20 seconds, contact Quantum Support.</p>

Symptom	Action
The library cannot communicate with the SKM server.	<p>Check all of the following. If you have tried all of these items and the problem still exists, contact Quantum Support.</p> <ul style="list-style-type: none">• Check to see if there are any RAS/diagnostic tickets on the library relating to SKM. If so, follow any instructions listed in them.• Verify IP address on the SKM server and make sure it is configured correctly on the library.• Ensure the SKM server Ethernet cables and power cords are attached.• Ensure that the SKM server is powered on and is running. If you are currently accessing SKM Admin Commands, the server will be stopped. Make sure to quit SKM Admin Commands.• Check the LEDs on the SKM appliance server and hard disk drives to make sure that none indicate errors (see LED Error Indicators on page 161).• Make sure the date on both SKM servers and the library is set to the current date. Incorrect date settings may interfere with the TLS certificates and cause the library to stop communicating with the SKM servers.• Ensure that SKM TLS communication certificates are installed on the library. If they are not installed, install them. See your library user's guide or online help for instructions. <hr/> <p>Note: If you are using Quantum-provided TLS certificates on the library, you must use Quantum-provided TLS certificates on the SKM server. Similarly, if you are using your own TLS certificates on the library, you must use your own TLS certificates on the SKM server.</p> <hr/> <p>continued on next page</p>

Symptom	Action
<p>The library cannot communicate with the SKM server (continued).</p>	<ul style="list-style-type: none"> • Ensure the following ports are open in a bi-directional mode on all firewalls in your network: 80, 6000, and 6001. <p>To verify port 80 is open:</p> <ol style="list-style-type: none"> 1 Ping the SKM server’s IP address. 2 If the ping succeeds, then open a Web browser and type the IP address in the URL search bar (for example: http://12.34.56.78). If port 80 is open, a page containing the text “Quantum Scalar Key Manager (SKM)” will display. 3 If the page does not display, reboot the SKM server and try again. (On the SKM appliance, press the reset button or press and hold the power button for four seconds to power off the server, then press the button to power on the server.) If the page still does not display, the port is not open.
<p>You forgot the password.</p>	<p>There is no way to retrieve or reset a forgotten password. You will need to replace your SKM server following the instructions in the sections listed below. The replacement process includes restoring the latest backup.</p> <hr/> <p>Caution: If you do not have a saved backup, contact Quantum Support before proceeding.</p> <hr/> <p>Follow the instructions in the appropriate section below:</p> <ul style="list-style-type: none"> • SKM appliance server: Replace the server and both hard disk drives (see Replacing an SKM Appliance Server and Both Hard Disk Drives on page 181). • SKM VM server: Delete and then re-create the SKM VM server using the original .ova image and your latest saved server backup. See Reinstalling an SKM VM Server on page 183 for instructions.

Symptom	Action
You installed your own TLS communication certificates on the SKM server, which overwrote the Quantum TLS certificates. Now, you want to put the Quantum TLS certificates back on.	<p>SKM appliance server: Contact Quantum Support to obtain Quantum-provided TLS certificates, then install them following the instructions in Installing TLS Certificates on the SKM Server for Pre-SKM 2.4 (240Q) on page 59.</p> <p>SKM VM server: The Quantum-provided TLS certificates are located on the Scalar Key Manager 2.2 VM Installation CD. If you still have the CD, follow the instructions in Installing TLS Certificates on the SKM Server for Pre-SKM 2.4 (240Q) on page 59. If you no longer have the CD, contact Quantum Support to obtain TLS certificates.</p>
You receive the following error message when you power on the SKM VM server using vSphere: “This kernel requires an x86-64 CPU, but only detected an xxxx CPU. Unable to boot - please use a kernel appropriate for your CPU.”	<ol style="list-style-type: none"> 1 Make sure that you are indeed using a 64-bit host server. 2 If so, change the VM host BIOS processor settings as follows: <ul style="list-style-type: none"> - 64-bit: Yes - Virtual Technology: Enable - Execute Disable: Disable 3 Follow the onscreen instructions.
You receive an “Incorrect MAC address” message during setup and cannot run the <code>./skmcmds</code> command.	<ol style="list-style-type: none"> 1 Using vSphere Client, power OFF the VM server (right-click the VM server, select Power, then select Power Off). 2 Power ON the VM server (right-click the VM server, select Power, then select Power On). 3 Click the Console tab, log on to <code>akmadmin</code> again, and run <code>./skmcmds</code> again.

Locating the SKM Server Serial Number

If you need to contact Quantum Support for assistance, you will need to provide your SKM server serial number. You can find the serial number as follows:

- **On the SKM appliance server** — On a label located on the front panel or top cover of the appliance.

- **On the SKM VM server** — On a label located on the cover of the Scalar Key Manager VM CD case.
- **On the Library Web client** — On the library remote Web client in the following locations.
 - **Scalar i40/i80** — System Information Report in the Encryption section.
 - **Scalar i500** — System Information Report in the Encryption section.
 - **Scalar i6000** — EKM Server Status screen (found under the **Monitor** menu).



Chapter 11

Replacing the SKM Server and its Components

Under certain circumstances, you may need to replace an SKM appliance server hard disk drive or the entire SKM appliance server, or you may need to replace the SKM VM server. The following table describes replacement scenarios:

Procedure	When to perform
Replacing a Hard Disk Drive	When a single hard disk drive in an SKM appliance server fails.
Replacing an SKM Appliance Server and Both Hard Disk Drives	When any of the following occurs: <ul style="list-style-type: none">• The SKM appliance server fails but both hard disk drives remain intact.• Both hard disk drives fail.• When an SKM appliance server and both its hard disk drives are not operational.• Lost SKM user account password.
Reinstalling an SKM VM Server	When you forget the SKM user account password.

Replacing a Hard Disk Drive

This section applies only to SKM appliance servers.

Caution: Do not remove any hard drive from the appliance server unless it is failed or you are instructed to do so by Quantum service. Removing any hard drive may render it unusable.

The SKM server comes with two 3.5-inch or 2.5-inch, hot-swappable, hard disk drives. The hard disk drives are configured as RAID 1, in which the data on both hard disk drives is continuously being mirrored, so if you lose one, your data is preserved.

If a single hard disk drive fails, your SKM system will fail over to the remaining hard disk drive. The remaining hard disk drive will continue to handle operations on that SKM server, but without the security of a redundant hard disk drive. To restore redundancy and protect against server failure in case the other hard disk drive fails, you should replace the failed hard disk drive as soon as possible.

Since the hard disk drives are hot swappable, you do not need to power off the server in order to replace a single hard disk drive. During the replacement process, normal library and SKM server functions can continue.

Caution: Never remove more than one hard disk drive while the system is powered up.

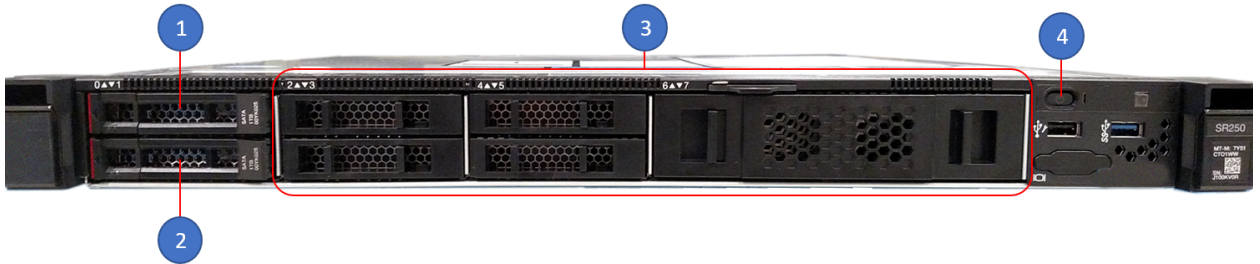
Caution: To maintain proper system cooling, do not operate the server for more than 10 minutes without a hard disk drive installed in each bay.

- 1 Read the safety information in [Safety](#) on page 15.
- 2 Locate the failed hard disk drive.

SKM 2.7 Appliance Server (and later versions)

The two drives within the SKM 2.7 appliance server are located in Slot 0 and 1 (left front). Refer to [Figure 40](#) and [Figure 41](#).

Figure 40 SKM 2.7 Appliance
 Server Front Panel



1	Drive 0 (2.5 inch)	3	Drive Slots (empty)
2	Drive 1 (2.5 inch)	4	Power Button/LED

Figure 41 SKM 2.7 Appliance
 Server Rear Panel

The Ethernet ports on the rear of the server are as follows:

- Unmarked port (far left: port) 10/100/1000 Mb Ethernet port
- Port 1 (middle port): 1GbE port
- Port 2 (far right: port): 1GbE port

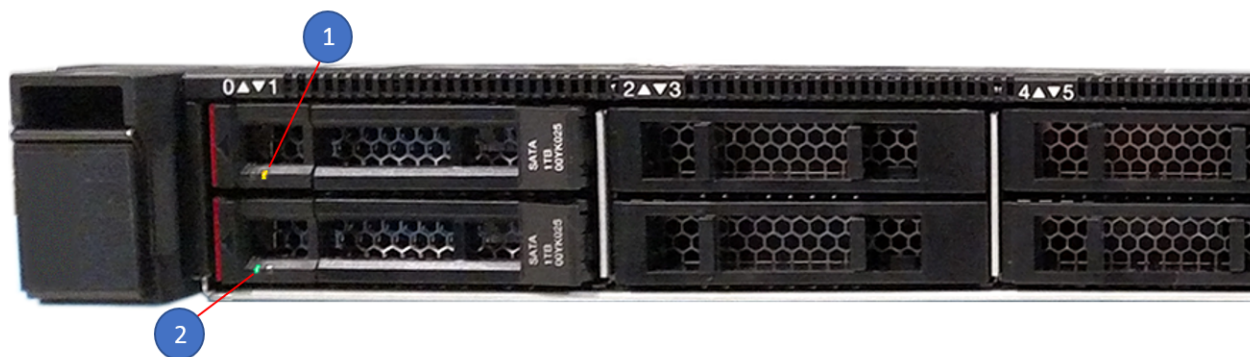


1	Serial Port (DB-9)	5	Power Supply Unit (PSU)
2	Configuration/Management Port	6	Power Cord Connection
3	1 GbE Port (RJ-45)	7	VGA Port
4	1 GbE Port (RJ-45)		

The amber hard disk drive status LED will be solidly illuminated on the failed hard disk drive.

- See [Figure 42](#) for location of amber LED illuminated on the failed drive (Slot 0, Callout 1).
- Notice that the drive in Slot 1 (Callout 2) has a green LED (meaning the drive is operational).

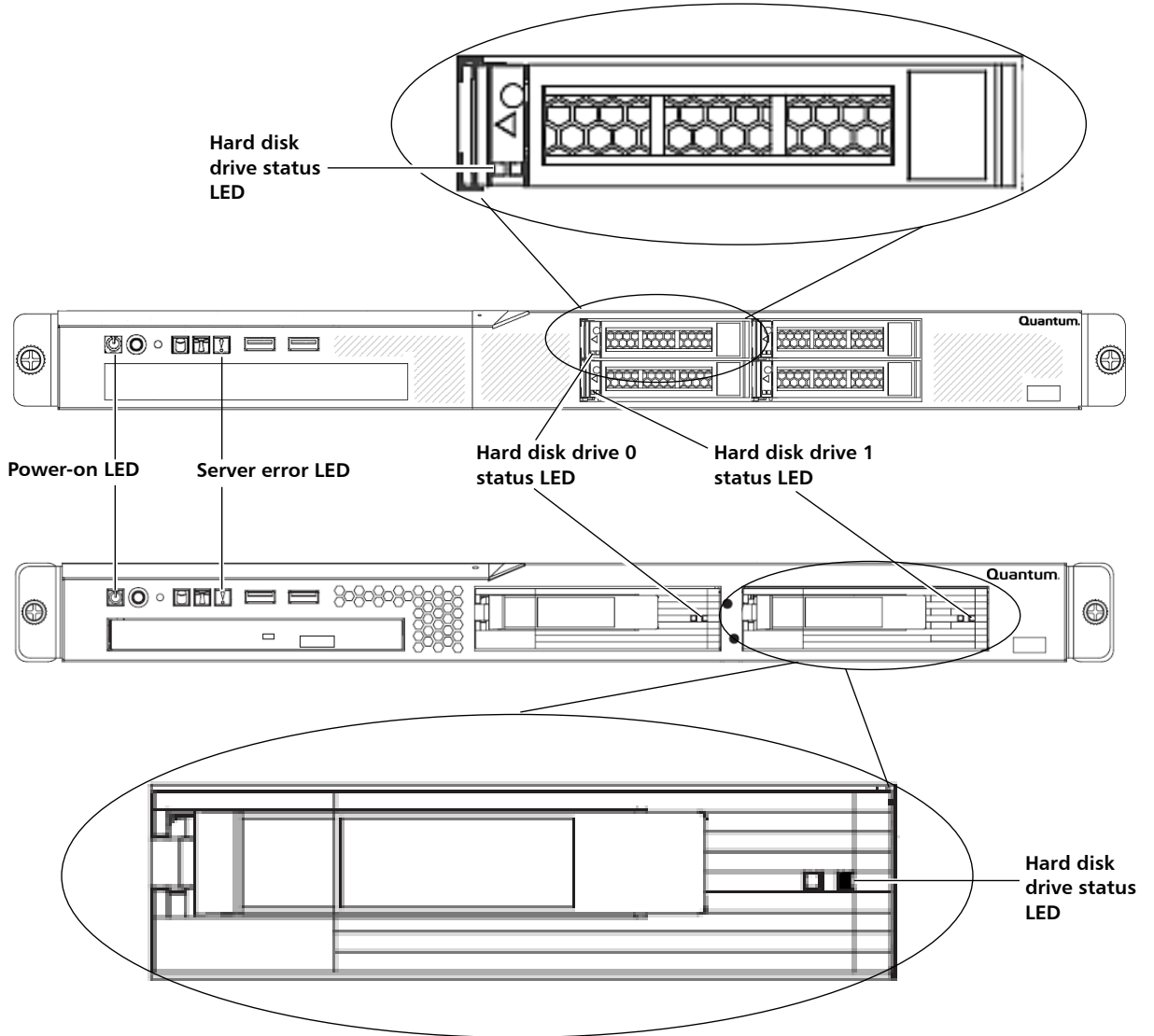
Figure 42 LED Location on Front of SKM 2.7 Appliance Server



SKM 2.6 Appliance Server (and earlier versions)

The amber hard disk drive status LED will be solidly illuminated on the failed hard disk drive. See [Figure 43](#) for location of LED.

Figure 43 LED Locations on
Front of SKM 2.6 Appliance
Server



- 3 Pull open the drive handle on the failed hard disk drive and remove the hard disk drive from the bay (see [Figure 44](#) or [Figure 45](#)).

Note: The amber Server Error LED illuminates on the SKM 2.6 appliance server (and earlier versions), indicating a server fault due to a missing hard disk drive.

The SKM 2.7 appliance server (and later versions) does not have an LED.

- 4 Touch the static-protective package that contains the drive to any unpainted metal surface on the server; then, remove the drive from the package and place it on a static-protective surface.
- 5 Open the drive tray handle of the replacement hard disk drive so that the handle is perpendicular to the front of the drive in the open (unlocked) position (see [Figure 44](#) or [Figure 45](#)).
- 6 Align the drive assembly with the guide rails in the bay.
- 7 Gently push the drive assembly into the bay until the drive stops (see [Figure 44](#) or [Figure 45](#)).

Caution: To prevent damage to the drive tray, do not force the drive into the bay at an angle. Make sure that you carefully insert the hard disk drive straight into the drive bay as shown in [Figure 44](#) or [Figure 45](#).

Figure 44 Replacing a Hard Disk Drive in SKM 2.7 Appliance Server

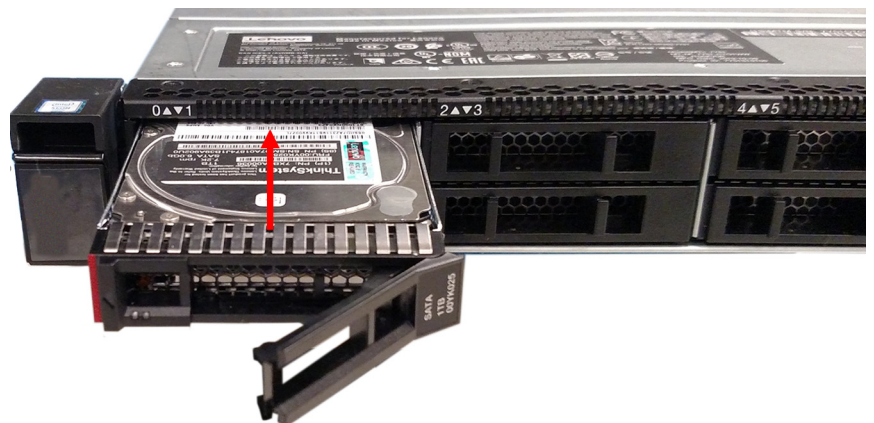
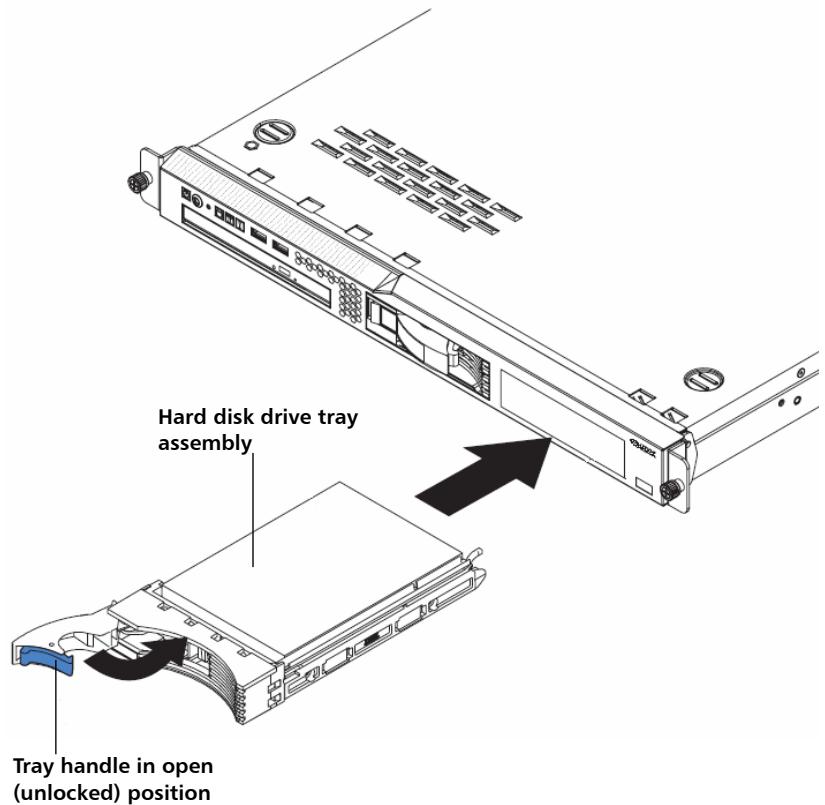


Figure 45 Replacing a Hard
Disk Drive in SKM 2.6
Appliance Server



- 8 Push the tray handle to the closed (locked) position.

The RAID rebuild process begins. The following sequence of LEDs indicates the stages of the rebuild:

Caution: Do not interfere with or remove a hard disk drive during the RAID rebuild.

- a The replacement hard disk drive's green activity LED blinks rapidly for 5 seconds as the hard disk drive registers with the system.

Note: The amber hard disk drive status LED illuminates. (This LED indicates the hard disk drive is “defective” because it is not mirrored yet, and it should turn off once the RAID rebuild is complete.)

- b The green activity LED on the existing good hard disk drive blinks, indicating it is being accessed.
 - c After about 5 seconds, the RAID rebuild begins, during which the green activity LEDs on both hard disk drives blink very fast so that they may appear to be on solid.
 - Rebuild process:
 - The replacement hard disk drive’s amber status LED blinks once per second.
 - The amber server error LED turns off as soon as the RAID rebuild process starts.
 - The RAID rebuild process may take up to 45 minutes.
 - d When the RAID rebuild is complete, the green activity LEDs on both hard disk drives blink in unison either once every 16 seconds or several times rapidly every 16 seconds (depending on server model).
- 9 When the RAID rebuild is complete, check the hard disk drive LEDs to make sure that the hard disk drive is operating correctly.
- The amber hard disk drive status LED should be **OFF**.
 - If it is still on, the drive is faulty, and you should contact Quantum Support.

Note: Properly dispose of the failed hard disk drive. Quantum requests that you do not return your hard disk drive because it may still contain your data encryption keys.

Caution: Do not use the failed hard disk drive in any other SKM server.

Replacing an SKM Appliance Server and Both Hard Disk Drives

This section applies only to SKM appliance servers.

You will replace the entire SKM appliance server and its two hard disk drives for a number of different reasons, including:

- The SKM appliance server fails but both hard disk drives remain intact.
- Both hard disk drives fail.
- The SKM appliance server and both its hard disk drives are not operational.
- You no longer have the SKM user account password.

The replacement procedure includes configuring the replacement SKM appliance server and restoring your last saved backup onto the replacement server. The entire process takes about one hour.

Caution: If you do not have a saved backup, contact Quantum Support before proceeding.

Caution: Do not remove the hard disk drives from the replacement server. You will replace the entire unit, including the hard disk drives.

Terminology

For ease of communication, we will use the following terminology:

- **Failed SKM appliance server** — The SKM appliance server, with its two hard disk drives installed, that you are removing and replacing. We will refer to it as “failed” even if it did not technically fail (for example, both hard disk drives failed but the server itself is still working).
- **Replacement SKM appliance server** — The replacement SKM appliance server, with its own two hard disk drives installed.

Required Items

- Replacement SKM appliance server with two installed hard disk drives.
- CAT5e crossover Ethernet cable for initial configuration (not supplied).
- Laptop or PC to connect to the replacement server for initial configuration.
- The latest saved backup taken from the failed SKM appliance server, placed in a retrievable location (see [Backing Up the SKM Server](#) on page 103).
- Remote access to a library that is connected to the SKM server.

Procedure

- 1 Contact Quantum Support for a replacement server.

Note: Charges may apply.

- 2 If not already powered off, power **OFF** the failed server by pressing the power button on the front panel and holding for four seconds.
- 3 Unplug the power cord and CAT5e Ethernet cable from the back of the server.
- 4 Remove the server from the rack.
- 5 Install and configure the replacement server following the instructions in [Installing and Configuring the SKM Appliance Servers](#) on page 28.

Note: Only install and configure the replacement server; leave the currently working SKM server as is.

Caution: It is highly recommended that you configure the replacement server with the same settings as the failed server, and that you do not change the IP address. Changing the IP address requires you to reconfigure the IP address on all libraries that communicate with that SKM server (see [Changing the IP Address](#) on page 98).

- 6 If you change the IP address of the replacement server from what it was on the failed server, update it on each library that is attached to the SKM server pair (for instructions, see [Step 6](#) in [Changing the IP Address](#) on page 98).
- 7 Restore your last saved backup of the failed server following the instructions in [Restoring the SKM Server](#) on page 107.
- 8 Remove the hard disk drives from the failed server and properly dispose of them. Quantum requests that you do not return your hard disk drives because they may still contain your data encryption keys.

Caution: Do not use the failed hard disk drives in any other SKM appliance server.

- 9 Return the failed server to Quantum.

Reinstalling an SKM VM Server

This section applies only to SKM VM servers.

You will reinstall the entire SKM VM server when you no longer have the SKM user account password.

The reinstall procedure includes configuring the replacement SKM VM server and restoring your last saved backup onto the replacement server. The entire process takes about one hour.

Caution: If you do not have a saved backup, contact Quantum Support before proceeding.

Terminology

For ease of communication, we will use the following terminology:

- **Failed SKM VM server** — The SKM VM server that you are removing and replacing. We will call it “failed server” even if it did not technically fail (for example, you lost the password).
- **Replacement SKM VM server** — The replacement SKM VM server.

Required Items

- The latest saved backup taken from the failed SKM VM server, placed in a retrievable location (see [Backing Up the SKM Server](#) on page 103).
- Remote access to your library.
- The original .ova image and TLS certificates that you used when you originally deployed and configured the failed SKM VM server. The .ova and Quantum-provided TLS certificates are located on the Scalar Key Manager 2.2 VM Installation CD. Make sure you use the correct CD for the SKM VM server you are replacing.
- All of the items required for installation as described in [Equipment and Software Needed for VMware](#) on page 39.

Procedure

Caution: If you do not have a saved backup, call Quantum Support before starting this procedure. This procedure deletes your failed SKM VM server.

- 1 Using vSphere Client, power **OFF** the failed server.
- 2 Using vSphere Client, delete the failed SKM VM server instance to which you lost the password.
- 3 Install and configure the replacement SKM VM server following the instructions in [Installing and Configuring the SKM VM Servers](#) on page 39. This includes deploying the original .ova image.

Note: Configure only the replacement server. Leave the currently working SKM VM server as is.

Caution: It is highly recommended that you configure the replacement server with the same settings as the failed server, and that you do not change the IP address. Changing the IP address requires you to reconfigure the IP address on all libraries that communicate with that SKM server (see [Changing the IP Address](#) on page 98).

- 4 If you change the IP address of the replacement SKM VM server from what it was on the failed SKM VM server, update it on each library that is attached to the SKM server pair (for instructions, see [Step 6](#) in [Changing the IP Address](#) on page 98).
- 5 Restore your last saved backup of the failed server following the instructions in [Restoring the SKM Server](#) on page 107.

Chapter 11: Replacing the SKM Server and its Components

Reinstalling an SKM VM Server



Chapter 12

Upgrading and Rolling Back SKM Server Software

Periodically, Quantum may issue updates or patches to the SKM software. These updates will include any needed operating system (Ubuntu) updates.

Caution: Quantum requires that you do not install any software, file, or operating system on the SKM appliance server or SKM VM server unless it is an upgrade or patch supplied by Quantum. Doing so may make your server inoperable and will void the warranty.

There is no automatic notification to alert you when new software is released. You must go to the following Quantum Web site to find out if there is an update (click Firmware):

<https://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SKM/Index.aspx>

Note: Also, refer to the Documentation tab, Product Updates, “Release Notes” for new software at: <https://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SKM/Index.aspx>

If there is an update, you can contact Quantum Support to request the installation ISO image, and then install it according to the procedures in this section.

Caution: If you upgrade or roll back the software on one server in an SKM server pair, remember to also upgrade/roll back the other one. The servers do not automatically sync or check to see whether they are both running the same version.

Chapter topics include:

- [Upgrading to Version 2.6 or 2.7 and Later Versions](#)
- [Upgrading to Version 2.5](#) on page 196
- [Upgrading to Version 2.4](#) on page 208
- [Upgrading to Version 2.3](#) on page 209
- [Upgrading to Version 2.2](#) on page 209
- [Upgrading to Version 2.0](#) on page 211
- [Upgrading from Version 1.0 to Version 1.1](#) on page 211
- [Installing the Import/Export Utility](#) on page 213
- [Rolling Back SKM Server Software](#) on page 216

Upgrading to Version 2.6 or 2.7 and Later Versions

This section provides steps to upgrade from SKM 2.6 to SKM 2.7. The process of upgrading from SKM 2.5 to SKM 2.6 is the same process (only the SKM numbering scheme in the displays will differ).

Caution: You must be at SKM 2.5 to upgrade to SKM 2.6.
You must be at SKM 2.6 to upgrade to SKM 2.7.

This section describes the steps to upgrade from SKM 2.6 to version 270Q.GC00600. You can upgrade by using a remote installation script.

Upgrading from SKM version 2.6 or a later version does not require Quantum Support.

Note: Before you begin the upgrade, backup your SKM server, disable LME on all partitions. Otherwise, the library will generate SKM Server Mismatch RAS tickets when upgrading one server at a time.

Upgrading from SKM 2.6 Using the Remote Script

Download the 270Q.GC00600remoteinstall-pkg.sh.gz file from Quantum.com:

<https://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SKM/Index.aspx>

- 6 Copy the script to one of the SKM servers in the pair to be upgraded, and then use scp, winscp or sftp to place it in /home/akmadmin.
- 7 Using putty or ssh, log into the SKM server using the **akmadmin** account.
- 8 Execute the command `gunzip 270Q.GC00600remoteinstall-pkg.sh.gz`.

Note: This command may take a few minutes to execute.

Chapter 12: Upgrading and Rolling Back SKM Server Software Upgrading to Version 2.6 or 2.7 and Later Versions

```
akmadmin@skmsserver: /home/akmadmin
login as: akmadmin
akmadmin@10.20.171.190's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-141-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Linux qkmserver 2.6.32-24-server #39-Ubuntu SMP Wed Jul 28 06:21:40 UTC 2010 x86_64 GNU/Linux

Scalar Key Management (SKM) Server
Version 260Q.GC00600

For SKM server setup and configuration, type
./skmcmds

Last login: Mon Jan 13 08:11:46 2020 from 10.20.172.46
akmadmin@skmsserver:~$ ls
270Q.GC00600remoteinstall-pkg.sh.gz  backups  certs  generatedcerts  keys  skmcmds
akmadmin@skmsserver:~$
```


- 9 Execute the command `chmod +x ./270Q.GC00600remoteinstall-pkg.sh`

```
akmadmin@skmsserver: /home/akmadmin
login as: akmadmin
akmadmin@10.20.171.190's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-141-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Linux qkmsserver 2.6.32-24-server #39-Ubuntu SMP Wed Jul 28 06:21:40 UTC 2010 x86_64 GNU/Linux

Scalar Key Management (SKM) Server
Version 260Q.GC00600

For SKM server setup and configuration, type
./skmcmds

Last login: Mon Jan 13 08:11:46 2020 from 10.20.172.46
akmadmin@skmsserver:~$ ls
270Q.GC00600remoteinstall-pkg.sh.gz backups certs generatedcerts keys skmcmds
akmadmin@skmsserver:~$ gunzip 270Q.GC00600remoteinstall-pkg.sh.gz
akmadmin@skmsserver:~$ ls
270Q.GC00600remoteinstall-pkg.sh backups certs generatedcerts keys skmcmds
akmadmin@skmsserver:~$ chmod +x ./270Q.GC00600remoteinstall-pkg.sh
akmadmin@skmsserver:~$
```

- 10 Execute the command `sudo ./270Q.GC00600remoteinstall-pkg.sh`. Use the same password you used to log in to the `akmadmin` account.

Note: This command may take 5-10 minutes to execute.

```
_64 GNU/Linux

Scalar Key Management (SKM) Server
Version 260Q.GC00600

For SKM server setup and configuration, type
./skmcmds

Last login: Mon Jan 13 08:11:46 2020 from 10.20.172.46
akmadmin@skmserver:~$ ls
270Q.GC00600remoteinstall-pkg.sh.gz backups certs generatedcerts keys skmcmds
akmadmin@skmserver:~$ gunzip 270Q.GC00600remoteinstall-pkg.sh.gz
akmadmin@skmserver:~$ ls
270Q.GC00600remoteinstall-pkg.sh backups certs generatedcerts keys skmcmds
akmadmin@skmserver:~$ chmod +x ./270Q.GC00600remoteinstall-pkg.sh
akmadmin@skmserver:~$ sudo ./
270Q.GC00600remoteinstall-pkg.sh      .create-lic-from-label/          .quantum
.akmadmin/                          .eulaconfirmation                .rnd
backups/                             generatedcerts/                  .setupwi
.bash_logout                        keys/                             skmcmds
.bashrc                              .profile                         .sudo_as
.cache/                              .qkmconfig                       _
certs/                              .Quantum EULA for_PTSS Software.txt
akmadmin@skmserver:~$ sudo ./270Q.GC00600remoteinstall-pkg.sh
[sudo] password for akmadmin:

Starting Remote SKM server upgrade without CD.

Mon Jan 13 09:24:07 MST 2020

    Checking disk space usage.

Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1       12G   2.2G  9.0G  20% /

SKM Version: 260Q.GC00600
SKM version greater than or equal to 250.
Enough space available for upgrade: 9334796
Enough space has been cleared or was available for upgrade .
Extracting installation components.
```

11 When the End User License Agreement (EULA) appears, read the agreement and then accept by entering y.

```
If the Software is held to infringe any intellectual property right and its use or sale enjoined, or if in the opinion of Quantum such Software is likely to become the subject of such a claim of infringement, Quantum may, in its sole discretion and at its own expense, either procure a license that will protect you against such claim without cost to you, replace such Software with non-infringing Software or require return of such Software and refund an equitable portion of the price paid by you to Quantum for such Software as your sole and exclusive remedy.

17. Miscellaneous. This Agreement sets forth all rights for the user of the Software and is the entire Agreement between the parties. This Agreement supersedes any other communications, representations or advertising relating to the Software and Documentation. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of Quantum. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by Quantum. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect.

18. Quantum Customer Contact. If you have any questions concerning these terms and conditions, or if you would like to contact Quantum for any other reason, you may contact your local Quantum entity at the number listed at http://www.quantum.com.

Do you agree to the EULA? (y=yes, n=no):
GetAns:Invalid Response:

Invalid Response:

Do you agree to the EULA? (y=yes, n=no): █
```

Note: After accepting the EULA, the upgrade begins. Refer to the next screen.

```
akmadmin@skmsserver: /home/akmadmin

Performing upgrade to 270Q.GC00600 from 260Q.GC00600

*****
* DO NOT STOP THE UPGRADE PROCESS!!!!!!! *
*****

Checking swap partition.

Total swap = 4192252.

*****
* Backuping up the key server *
*****
Generating a server backup.
```

- 12 When you are notified that the upgrade has completed successfully, press **Enter** to reboot the SKM server. (It will take a few minutes for the system to reboot.)

```
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
default          10.20.168.1    0.0.0.0         UG    0      0      0 eth0
10.20.168.0     *              255.255.248.0  U     0      0      0 eth0

Upgrade to version 270Q.GC00600 from version 260Q.GC00600 has completed successfully.

The SKM server will be rebooted to complete the SKM server upgrade.

Press <Enter>
█
```

- 13 After the system reboot completes, log into the SKM server as **akmadmin** using putty or ssh.
- 14 Once you log into the system, the new version should be displayed.

```
akmadmin@skmsserver: /home/akmadmin
login as: akmadmin
akmadmin@10.20.171.190's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Linux qkmsserver 2.6.32-24-server #39-Ubuntu SMP Wed Jul 28 06:21:40 UTC 2010 x86_64 GNU/Linux

Scalar Key Management (SKM) Server
Version 270Q.GC00600

For SKM server setup and configuration, type
./skmcmds

Last login: Mon Jan 13 03:28:14 2020 from 10.20.88.98
akmadmin@skmsserver:~$ █
```

- 15 Execute `akmadmin --admin-noop` to verify that the akmd process is working correctly. The return code should be all zeroes, <0000>.

```
akmadmin@skm227: /home/akmadmin
login as: akmadmin
akmadmin@10.20.171.227's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your I
ernet connection or proxy settings

Linux qkmserver 2.6.32-24-server #39-Ubuntu SMP Wed Jul 28 06:21:40 UTC 2010 x86_
GNU/Linux

Scalar Key Management (SKM) Server
Version 270Q.GC00600

For SKM server setup and configuration, type
./skmcmds

Last login: Mon Jan 13 05:50:59 2020 from 10.20.172.46
akmadmin@skm227:~$ akmadmin --admin-noop
Tran len <00008>
Tran Id <1044>
Return code <0000>
akmadmin@skm227:~$
```

- 16 Backup the SKM server per [Chapter 6](#), [Backing Up and Restoring the SKM Server](#).
- 17 Copy from the system the backup that was created after the upgrade. (Backups created after the upgrade are saved at `/home/akmadmin/backups`.)
Place this backup copy where you normally keep backups.
- 18 Repeat all steps for the second SKM server in the pair.

Upgrading to Version 2.5

This section describes the steps to upgrade SKM to version 250Q.GC00100, which includes an upgrade of the operating system to Ubuntu 14.04. You can upgrade either by using a remote installation script, or from an installation DVD.

Upgrading from SKM version 2.3 to version 2.5 does not require Quantum Support, but upgrading to SKM 2.5 from SKM versions earlier than 2.3 must be performed by Quantum Support. To upgrade from a pre 2.3 version, contact Quantum Support to schedule an upgrade.

Note: Before you begin the upgrade, disable LME on all partitions. Otherwise, the library will generate SKM Server Mismatch RAS tickets when upgrading one server at a time.

Upgrading from SKM 2.3 Using the Remote Script

- 1 Download the 250Q.GC00100remoteinstall-pkg.sh.gz file from Quantum.com: <https://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SKM/Index.aspx>
- 2 Copy the script to one of the SKM servers in the pair to be upgraded, and then use scp, winscp or sftp to place it in /home/akmadmin.
- 3 Using putty or ssh, log into the SKM server using the **akmadmin** account.
- 4 Execute the command `gunzip 250Q.GC00100remoteinstall-pkg.sh.gz`.

```
akmadmin@skmsserver: ~  
login as: akmadmin  
akmadmin@10.60.166.101's password:  
Linux qkmsserver 2.6.32-24-server #39-Ubuntu SMP Wed Jul 28 06:21:40 UTC 2010 x86_64 GNU/Linux  
  
Scalar Key Management (SKM) Server  
Version 230Q.GC00400  
  
For SKM server setup and configuration, type  
./skmcmds  
  
No mail.  
Last login: Thu Apr 13 09:20:43 2017 from 10.60.8.57  
akmadmin@skmsserver:~$ gunzip 250Q.QC00100remoteinstall-pkg.sh.gz  
akmadmin@skmsserver:~$ █
```

- 5 Execute the command `chmod +x ./250Q.GC00100remoteinstall-pkg.sh`

```
akmadmin@skmsserver: ~  
login as: akmadmin  
akmadmin@10.60.166.101's password:  
Linux qkmsserver 2.6.32-24-server #39-Ubuntu SMP Wed Jul 28 06:21:40 UTC 2010 x86_64 GNU/Linux  
  
Scalar Key Management (SKM) Server  
Version 230Q.GC00400  
  
For SKM server setup and configuration, type  
./skmcmds  
  
No mail.  
Last login: Thu Apr 13 09:20:43 2017 from 10.60.8.57  
akmadmin@skmsserver:~$ gunzip 250Q.QC00100remoteinstall-pkg.sh.gz  
akmadmin@skmsserver:~$ chmod +x 250Q.QC00100remoteinstall-pkg.sh  
akmadmin@skmsserver:~$ █
```

- 6 Execute the command `sudo ./250Q.GC00100remoteinstall-pkg.sh`. Use the same password you used to log in to the `akmadmin` account.

```
akmadmin@skmsserver: ~  
login as: akmadmin  
akmadmin@10.60.166.101's password:  
Linux skmsserver 2.6.32-24-server #39-Ubuntu SMP Wed Jul 28 06:21:40 UTC 2010 x86_64 GNU/Linux  
  
Scalar Key Management (SKM) Server  
Version 230Q.GC00400  
  
For SKM server setup and configuration, type  
./skmcmds  
  
No mail.  
Last login: Thu Apr 13 09:20:43 2017 from 10.60.8.57  
akmadmin@skmsserver:~$ gunzip 250Q.QC00100remoteinstall-pkg.sh.gz  
akmadmin@skmsserver:~$ chmod +x 250Q.QC00100remoteinstall-pkg.sh  
akmadmin@skmsserver:~$ sudo ./250Q.QC00100remoteinstall-pkg.sh  
[sudo] password for akmadmin:  
  
Starting Remote SKM server upgrade without CD.  
  
Extracting installation components.
```


7 When the End User License Agreement (EULA) appears, read the agreement and then accept by entering y.

```
akmadmin@skmserver:~$
NOTICE TO ALL USERS: PLEASE READ THIS CONTRACT CAREFULLY. BY INSTALLING OR USING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE SOFTWARE. This SKM End User License Agreement is available for further review and printing in the Scalar Key Manager Documentation CD.

1. Definitions.

a. "Software" means (a) all of the contents of the files, disk(s), CD-ROM(s) or other media (including electronic media) or such contents as are hosted by Quantum or its distributors, resellers, OEM/MSP partners, or other business partners (collectively "Authorized Partner(s)"), including but not limited to (i) Quantum or third party computer information or software; (ii) related explanatory materials in printed, electronic, or online form ("Documentation"); and (b) upgrades, modified or subsequent versions and updates of Software, if any, licensed to you by Quantum or an Authorized Partner as part of a maintenance contract or service subscription.

b. "Use" or "Using" means to access, install, download, copy or otherwise benefit from using the Software.

c. "Permitted Number" means one (1) unless otherwise indicated under a valid license (e.g., volume license) granted by Quantum.

d. "Computer" means a device that accepts information in digital or similar form and manipulates it for a specific result based upon a sequence of instructions.

e. "Quantum" means Quantum Corporation, a Delaware corporation, with headquarters located at 1650 Technology Drive, San Jose, CA 95110,

Do you agree to the EULA? (y=yes, n=no): y
```

After accepting the EULA, the upgrade begins.

```
akmadmin@skmserver:~$
Performing upgrade to 250Q.QC00100 from 230Q.GC00400

*****
*          DO NOT STOP THE UPGRADE PROCESS!!!!!!          *
*****

*****
*   Current version: 230Q.GC00400 , requires an O/S upgrade.   *
*****

Backing up /etc/apt/sources.list file.
Loading Ubuntu 14.04 sources.list file.
Backing up /etc/issue and /etc/modt.tail

Upgrading SKM server O/S to Ubuntu 14.04

The directory /media/apt exists. No need to create it.
Deleting /boot/grub/device.map file.
```

- 8 When you are notified that the upgrade has completed successfully, press **Enter** to reboot the SKM server. (It will take a few minutes for the system to reboot.)

```
akmadmin@skmsserver: ~
*****
Generating SKM server key database backup.
The file listed below maybe transferred from the SKM server after the reboot.

Backing up SKM key server.
SKM server backup is complete.

Please pull the following file off of the SKM server using sftp:
/home/akmadmin/backups/SKM2_2KeyServerVM_3FFFF104132017094055.tgz
Upgrade to version 250Q.QC00100 from version 230Q.GC00400 has completed successfully.

The SKM server will be rebooted to complete the SKM server upgrade.

Press <Enter>
```

- 9 After the system reboot completes, log into the SKM server as **akmadmin** using **putty** or **ssh**.

10 Once you log into the system, the new version should be displayed.

```
akmadmin@skmsserver: /home/akmadmin

Broadcast message from akmadmin@skmsserver
(/dev/pts/1) at 9:41 ...

The system is going down for reboot NOW!

Exiting remote SKM server upgrade.
login as: akmadmin
akmadmin@10.60.166.101's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-116-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
Linux gkmsserver 2.6.32-24-server #39-Ubuntu SMP Wed Jul 28 06:21:40 UTC 2010 x86_64 GNU/Linux

Scalar Key Management (SKM) Server
Version 250Q.QC00100

For SKM server setup and configuration, type
./skmcmds

No mail.
Last login: Thu Apr 13 09:24:00 2017 from 10.60.8.57
akmadmin@skmsserver:~$ █
```

- 11 Execute `akmadmin --admin-noop` to verify that the akmd process is working correctly. The return code should be all zeroes.

```
akmadmin@skmserver: ~  
login as: akmadmin  
akmadmin@10.60.166.243's password:  
Linux qkmserver 2.6.32-24-server #39-Ubuntu SMP Wed Jul 28 06:21:40 UTC 2010 x86_64 GNU/Linux  
  
Scalar Key Management (SKM) Server  
Version 250Q.GC00100  
  
For SKM server setup and configuration, type  
./skmcmds  
  
You have new mail.  
Last login: Tue May 11 12:46:47 2017 from 10.60.8.57  
akmadmin@skmserver:~$ akmadmin --admin-noop  
Version <akmadmin Version 2.1.1>  
Tran Len <00008>  
Tran Id <1044>  
Return Code <0000>  
akmadmin@skmserver:~$
```

- 12 Copy from the system the backup that was created after the upgrade. (Backups created after the upgrade are saved at `/home/akmadmin/backups`.)
Place this backup copy where you normally keep backups.
- 13 Repeat all steps for the second SKM server in the pair.

Upgrading Using an Installation DVD

Use this installation method to install from a DVD rather than from a script.

- 1 Create an installation DVD using the `SKM_2_5_250Q.GC00100_cdimage.iso` available on CSweb.
- 2 Insert the installation DVD into the SKM server you want to upgrade.
- 3 Use putty or ssh to log onto the SKM server using the `akmadmin` account.

- 4 Execute the command `./skmcmds` to access the menu. You might be prompted for the sudo password, which is the akmadmin account password.

When asked whether to stop the key server, you must answer **yes**.

```
akmadmin@skmserver: ~  
login as: akmadmin  
akmadmin@10.60.166.101's password:  
Linux qkmserver 2.6.32-24-server #39-Ubuntu SMP Wed Jul 28 06:21:40 UTC 2010 x86_64 GNU/Linux  
  
Scalar Key Management (SKM) Server  
Version 230Q.GC00400  
  
For SKM server setup and configuration, type  
./skmcmds  
  
No mail.  
Last login: Thu Apr 13 09:20:43 2017 from 10.60.8.57  
akmadmin@skmserver:~$ gunzip 250Q.QC00100remoteinstall-pkg.sh.gz  
akmadmin@skmserver:~$ chmod +x 250Q.QC00100remoteinstall-pkg.sh  
akmadmin@skmserver:~$ sudo ./250Q.QC00100remoteinstall-pkg.sh  
[sudo] password for akmadmin:  
  
Starting Remote SKM server upgrade without CD.  
  
Extracting installation components.
```

- 5 When the installation menu appears, choose option **u** to upgrade the server.

```
Server Cert's Validity:
/etc/akm/Certs/QKMServerSignedCert.pem
  Not Before: May  1 19:01:37 2009 GMT and Not After : May  1 19:01:37 2019 GMT
Admin Cert's Validity:
/home/akmadmin/.akmadmin/Certs/QKMAdminSignedCert.pem
  Not Before: May  1 19:01:38 2009 GMT and Not After : May  1 19:01:38 2019 GMT

Current Date/Time: Tue May 31 13:37:54 PDT 2016

-----
1) Launch SKM server setup wizard.
2) Change user account password.
3) Capture SKM server snapshot.
4) Set SKM server IP address.
5) Set SKM server time zone.
6) Set SKM server date and time.
7) Back up SKM server.
8) Restore SKM server.
9) Set SKM server hostname.
d) Display/update TLS communication certificates.
u) Update SKM server software.
r) Roll back SKM server software.
v) View SKM server reports.
q) Quit.
-----
Command: u
```

- 6 When prompted to insert the DVD into the server, press **Enter**. (You already inserted the DVD in step 2.)

```
-----
Command: u

Upgrading the SKM server via CD.
Please put the CD into the server and press enter or "q" to quit: 
```

- 7 When the End User License Agreement (EULA) appears, read the agreement and then accept by enter **y**. The upgrade begins after you accept the EULA and press **Enter**.

```
akmadmin@skmserver:~$
NOTICE TO ALL USERS: PLEASE READ THIS CONTRACT CAREFULLY. BY INSTALLING OR USING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE SOFTWARE. This SKM End User License Agreement is available for further review and printing in the Scalar Key Manager Documentation CD.

1. Definitions.

a. "Software" means (a) all of the contents of the files, disk(s), CD-ROM(s) or other media (including electronic media) or such contents as are hosted by Quantum or its distributors, resellers, OEM/MSP partners, or other business partners (collectively "Authorized Partner(s)"), including but not limited to (i) Quantum or third party computer information or software; (ii) related explanatory materials in printed, electronic, or online form ("Documentation"); and (b) upgrades, modified or subsequent versions and updates of Software, if any, licensed to you by Quantum or an Authorized Partner as part of a maintenance contract or service subscription.

b. "Use" or "Using" means to access, install, download, copy or otherwise benefit from using the Software.

c. "Permitted Number" means one (1) unless otherwise indicated under a valid license (e.g., volume license) granted by Quantum.

d. "Computer" means a device that accepts information in digital or similar form and manipulates it for a specific result based upon a sequence of instructions.

e. "Quantum" means Quantum Corporation, a Delaware corporation, with headquarters located at 1650 Technology Drive, San Jose, CA 95110,

Do you agree to the EULA? (y=yes, n=no): y
```

After accepting the EULA, the upgrade begins.

```
akmadmin@skmserver:~$
Performing upgrade to 250Q.QC00100 from 230Q.GC00400

*****
* DO NOT STOP THE UPGRADE PROCESS!!!!!! *
*****

*****
* Current version: 230Q.GC00400 , requires an O/S upgrade. *
*****
Backing up /etc/apt/sources.list file.
Loading Ubuntu 14.04 sources.list file.
Backing up /etc/issue and /etc/modt.tail

Upgrading SKM server O/S to Ubuntu 14.04

The directory /media/apt exists. No need to create it.
Deleting /boot/grub/device.map file.
```

The upgrade continues with package updates for security issues, and purging unnecessary packages. A system backup is also created.

```
akmadmin@skmserver: ~
python2.5-minimal | Purged |
libdrm-nouveau1 | Purged |
libept0 | Purged |
libxml-sax-perl | Purged |
wireless-tools | Purged |
linux-ubuntu-modules-2.6.24-24-server | Purged |
linux-ubuntu-modules-2.6.24-23-server | Purged |
linux-image-2.6.24-24-server | Purged |
linux-image-2.6.24-23-server | Purged |
libpython2.6 | Purged |
python2.6 | Purged |
python2.6-minimal | Purged |
netcat | Purged |
telnet | Purged |
cpp-4.2 | Purged |
cpp-4.4 | Purged |
gcc-4.2-base | Purged |
gcc-4.4-base | Purged |
*****
Starting akm server.

Starting AKM...

Upgrading Quantum reserve info key metadata.

Setting metadata for Quantum reserve info key.

Generating SKM server key database backup.

The file listed below maybe transferred from the SKM server after the reboot.

Backing up SKM key server.

SKM server backup is complete.

Please pull the following file off of the SKM server using sftp:
/home/akmadmin/backups/SKM2_2KeyServer99E044405312016130536.tgz
```


- 8 When you are notified that the upgrade has completed successfully, press **Enter** to reboot the SKM server. (It will take a few minutes for the system to reboot.)

```
Upgrade to version 250Q.GC00100 from version 230Q.GC00400 has completed successfully.  
  
The SKM server will be rebooted to complete the SKM server upgrade.  
  
Press <Enter>
```

- 9 After the system reboot completes, log into the SKM server as **akmadmin** using putty or ssh.
- 10 Once you log into the system, the new version should be displayed.

```
akmadmin@skmsserver: ~  
login as: akmadmin  
akmadmin@10.60.166.243's password:  
Linux qkmsserver 2.6.32-24-server #39-Ubuntu SMP Wed Jul 28 06:21:40 UTC 2010 x86_64 GNU/Linux  
  
Scalar Key Management (SKM) Server  
Version 250Q.GC00100  
  
For SKM server setup and configuration, type  
./skmcmds  
  
You have new mail.  
Last login: Tue May 11 12:46:47 2017 from 10.60.8.57  
akmadmin@skmsserver:~$
```

- 11 Execute `akmadmin --admin-noop` to verify that the akmd process is working correctly. The return code should be all zeroes.

```
akmadmin@skmserver: ~  
login as: akmadmin  
akmadmin@10.60.166.243's password:  
Linux qkmsserver 2.6.32-24-server #39-Ubuntu SMP Wed Jul 28 06:21:40 UTC 2010 x86_64 GNU/Linux  
  
Scalar Key Management (SKM) Server  
Version 250Q.GC00100  
  
For SKM server setup and configuration, type  
./skmcmds  
  
You have new mail.  
Last login: Tue May 11 12:46:47 2017 from 10.60.8.57  
akmadmin@skmserver:~$ akmadmin --admin-noop  
Version <akmadmin Version 2.1.1>  
Tran Len <00008>  
Tran Id <1044>  
Return Code <0000>  
akmadmin@skmserver:~$
```

- 12 Copy from the system the backup that was created after the upgrade. (Backups created after the upgrade are saved at `/home/akmadmin/backups`.)
Place this backup copy where you normally keep backups.
- 13 Repeat all steps for the second SKM server in the pair.

Upgrading to Version 2.4

Upgrading from SKM version 2.2 or lower to version 2.4 must be performed by Quantum Support. Contact Quantum Support to schedule an upgrade.

Upgrading from SKM version 2.3 to version 2.4 does not require Quantum Support.

Upgrading to Version 2.3

Upgrading from SKM version 2.x to version 2.3 can be performed only by Quantum Support. Contact Quantum Support to schedule an upgrade.

Upgrading to Version 2.2

You can upgrade to SKM 2.2 directly from SKM 2.0 (or higher) or SKM 1.x.

Upgrade the servers one at a time. Make sure the first one is complete and fully upgraded before upgrading the other server. Do not upgrade them at the same time. This will protect you in case an upgrade fails, because the other server will be able to continue operations while you are recovering.

Note: The library may generate RAS/diagnostic tickets while you are performing this procedure. Once the upgrade is complete, you can ignore and close the tickets.

Equipment Required

To perform this procedure, you need:

- Remote access to the libraries that access your SKM servers.
- Physical access to your SKM servers.
- A blank, writable DVD.
- The ability to download an ISO image from Quantum Support and burn it to a DVD which you will place in the SKM server's CD or DVD ROM drive.

Procedure

- 1 Contact Quantum Support to request the upgrade. Quantum Support will send you an ISO image containing the version of software you request (the filename contains the version).
- 2 Burn the ISO image onto a DVD.
- 3 Stop all applications that require key exchanges from the SKM server pair.
- 4 Log on to the command line interface of one of the SKM servers (see [Logging on to the Command Line Interface](#) on page 92).
- 5 Access SKM Admin Commands by issuing the following command:
`./skmcmds`
- 6 At the **Command** prompt, type **u** to **Update SKM server software**.
- 7 Load the DVD containing the ISO image into the SKM server's CD or DVD ROM drive and press **<Enter>**.

The upgrade process runs.

- 8 When the upgrade process completes, press **<Enter>** to return to SKM Admin Commands.

Note: If no DVD is loaded, you are again requested for the DVD. Load the DVD and press **<Enter>**, or type **q** and press **<Enter>** to quit and return to SKM Admin Commands.

- 9 At the **Command** prompt, type **q** to quit SKM Admin Commands.
- 10 Issue the following command to verify that the new version is loaded.

```
./skmcmds -v
```

The new version should display on the screen.

- 11 Remove the DVD from the CD or DVD ROM drive.
- 12 Repeat the above steps on the other SKM server.
- 13 Back up both SKM server keystores as follows:
 - a At the prompt, access SKM Admin Commands by typing `./skmcmds`.
 - b At the **Command** prompt, type **7** to **Back up keystore**.

- c Once the backup file is created, SFTP the backup file to a safe location.
 - d At the **Command** prompt, type **q** and press **<Enter>** to quit SKM Admin Commands.
- 14 Resume using backup applications.
 - 15 Save the DVD in case you need to perform a rollback in the future.

Upgrading to Version 2.0

Upgrading from SKM version 1.0 or 1.1 to SKM version 2.0 can only be performed by Quantum Support. Contact Quantum Support to schedule an upgrade.

New VM Requirements for SKM 2.0

Version 2.0 requires the following on VM servers, which were not required in 1.0 or 1.1.

- 1 GB RAM
- Video memory must be set to 3 MB (not 4 MB)

Upgrading from Version 1.0 to Version 1.1

Upgrade the servers one at a time. Make sure the first one is complete and fully upgraded before upgrading the other server. Do not upgrade them at the same time. This will protect you in case an upgrade fails, because the other server will be able to continue operations while you are recovering.

Note: The library may generate RAS/diagnostic tickets while you are performing this procedure. Once the upgrade is complete, you can ignore and close the tickets.

Note: The name of the 1.0 (GA) version was Quantum Key Manager (QKM). The name changed to Scalar Key Manager (SKM) with 1.1. Names of menu items and some commands will therefore be different in version 1.0 and 1.1.

Equipment Required

To perform this procedure, you need:

- Remote access to the libraries that access your SKM servers.
- Physical access to your SKM servers.
- A blank, writable CD.
- The ability to download an ISO image from the Quantum Web site and burn it to a CD which you will place in the SKM server's CD ROM drive.

Procedure

- 1 Go to the Quantum SKM Web site to see if software updates exist (click Firmware):
<https://www.quantum.com/serviceandsupport/softwareanddocumentationdownloads/skm/index.aspx>
- 2 Contact Quantum Support to request the update. Quantum Support will send you an ISO image containing the version of software you request (the filename contains the version).
- 3 Burn the ISO image onto a CD.
- 4 Stop all applications that require key exchanges from the SKM server pair.
- 5 Log on to the command line interface of one of the SKM servers (see [Logging on to the Command Line Interface](#) on page 92).
- 6 Access QKM Admin Commands by issuing the following command:

```
./qkmcms
```
- 7 At the **Command** prompt, type **u** to **Update SKM server software**.
- 8 Load the CD containing the ISO image into the SKM server's CD ROM drive and press **<Enter>**.

The upgrade process runs.

- 9 When the upgrade process completes, press **<Enter>** to return to SKM Admin Commands.

Note: If no CD is loaded, you are again requested for the CD. Load the CD and press **<Enter>**, or type **q** and press **<Enter>** to quit and return to SKM Admin Commands.

- 10 At the **Command** prompt, type **q** to quit SKM Admin Commands.
- 11 Issue the following command to verify that the new version is loaded.

```
./skmcmds -v
```

The new version should display on the screen.
- 12 Remove the CD from the CD ROM drive.
- 13 Repeat the above steps on the other SKM server.
- 14 Back up both SKM server keystores as follows:
 - a At the prompt, access SKM Admin Commands by typing `./skmcmds`.
 - b At the **Command** prompt, type **7** to **Back up keystore**.
 - c Once the backup file is created, SFTP the backup file to a safe location.
 - d At the **Command** prompt, type **q** and press **<Enter>** to quit SKM Admin Commands.
- 15 Resume using backup applications.
- 16 Save the CD in case you need to perform a rollback in the future.

Installing the Import/Export Utility

If you are using a version of SKM prior to SKM 2.2, but want to use the Encryption Certificate and Encryption Key import and export features available in SKM 2.2, you can download a standalone utility which provides this functionality.

The SKM Import/Export Utility is available on the Quantum Support website and must be requested from Quantum Support.

Install the utility on the servers one at a time. Make sure the first installation is complete and fully complete on the first server before installing the utility on the other server. Do not install the utility on both servers at the same time. This will protect you in case an installation fails, because the other server will be able to continue operations while you are recovering.

Note: The library may generate RAS/diagnostic tickets while you are performing this procedure. Once the upgrade is complete, you can ignore and close the tickets.

Note: The name of the 1.0 (GA) version was Quantum Key Manager (QKM). The name changed to Scalar Key Manager (SKM) with 1.1. Names of menu items and some commands will therefore be different in version 1.0 and 1.1. To access the main menu after installing the utility, type **skmcmds** and enter the administrator password.

Procedure

- 1 Contact Quantum Support to request the SKM 2.2 Utility. Quantum Support will send you an ISO image containing the version of software you request (the filename contains the version).
- 2 Download the Utility file to the computer hard drive.
- 3 Burn the Utility file onto a DVD.
- 4 Stop all applications that require key exchanges from the SKM server pair.
- 5 Log on to the command line interface of one of the SKM servers (see [Logging on to the Command Line Interface](#) on page 92).
- 6 Read and accept the End User License Agreement.
- 7 At the **Command** prompt, type **sudo ./skmieupdate-pkg.sh** to install the Utility.
- 8 Load the DVD containing the ISO image into the SKM server's DVD ROM drive and press **<Enter>**.

The utility installation process runs.

- 9 When the installation process completes, press **<Enter>** to return to SKM Admin Commands.
- 10 At the **Command** prompt, type **q** to quit SKM Admin Commands.
- 11 Issue the following command to verify that the new version is loaded.

```
./skmcmds -v
```

The new version should display on the screen:

```
./skmcmds : SKM Admin Commands (Version  
110Q.GC01100 **I/E Patch**)
```

```
./skmcmds : SKM Server Version <akmd Version  
1.0.3>
```

```
./skmcmds : SKM Server Admin Version <akmadmin  
Version 1.0.3>
```

```
akmadmin@skmsserver:~$
```

- 12 Remove the DVD from the DVD ROM drive.
- 13 Repeat the above steps on the other SKM server.
- 14 Back up both SKM server keystores as follows:
 - a At the prompt, access SKM Admin Commands by typing `./skmcmds`.
 - b At the **Command** prompt, type **7** to **Back up keystore**.
 - c Once the backup file is created, SFTP the backup file to a safe location.
 - d At the **Command** prompt, type **q** and press **<Enter>** to quit SKM Admin Commands.
- 15 Resume using backup applications.

Save the DVD in case you need to perform a rollback in the future.

Rolling Back SKM Server Software

You can only roll back from one version to the version that immediately preceded it.

Caution: You cannot perform the rollback procedure from SKM version 2.0 or higher to version 1.1. The operating system is different. If you need to go back to version 1.1 from version 2.0 or higher, contact Quantum Support for assistance.

The procedure that follows applies only to rolling back version 1.1 to 1.0.

Perform the procedure on one server at a time. Make sure it is complete before rolling back the other server. This will protect you in case a rollback fails, because the other server will be able to continue operations while you are recovering.

Note: The library may generate RAS/diagnostic tickets while you are performing this procedure. Once the rollback is complete, you can ignore and close the tickets.

Note: The name of the 1.0 (GA) version was Quantum Key Manager (QKM). The name changed to Scalar Key Manager (SKM) with 1.1. Names of menu items and some commands will therefore be different in version 1.0 and 1.1.

Equipment Required

To perform this procedure, you need:

- Remote access to your library.
- Physical access to your SKM servers.
- An SKM VM server must have a connected CD ROM drive.
- The CD used to load the current version of software.

Note: The software version on the CD must match the version currently installed on the SKM server. If it does not, you will not be able to perform the rollback. If you no longer have the correct CD, note which version of software is currently installed on the server, then contact Quantum Support for the ISO image and burn it to a new CD. To see which version is currently installed on your server, see [Viewing the SKM Server Software Version](#) on page 113.

Rolling Back From Version 1.1 to Version 1.0

- 1 Obtain the CD containing the currently installed version of software.
- 2 Stop all applications that require key exchanges from the SKM server pair.
- 3 Log on to one of the SKM servers and access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 4 Access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 5 At the **Command** prompt, type **r** to **Roll back SKM server software**.
- 6 Insert the CD into the SKM server's CD ROM drive and press **<Enter>**.
The rollback process runs.
 - If the wrong upgrade CD is loaded, the rollback stops and you receive an error message. Press **<Enter>** to return to SKM Admin Commands.
 - If no CD is loaded, you are again requested for the CD. Load the CD and press **<Enter>**, or type **q** and press **<Enter>** to quit and return to SKM Admin Commands.
- 7 When the rollback completes, press **<Enter>** to return to SKM Admin Commands.
- 8 At the **Command** prompt, type **q** to quit SKM Admin Commands.
- 9 Issue the following command to confirm that the rollback version is loaded.

```
./skmcmds -v
```

The correct SKM Admin Commands version should appear on the screen.

- 10 Remove the CD from the CD ROM drive.
- 11 Repeat the above steps on the other SKM server.
- 12 Back up both SKM server keystores:
 - a At the prompt, access SKM Admin Commands by typing `./skmcmds`.
 - b At the **Command** prompt, type **7** to **Back up keystore**.
 - c Once the backup file is created, SFTP the backup file to a safe location.
 - d At the **Command** prompt, type **q** and press **<Enter>** to quit SKM Admin Commands.
- 13 Resume using backup applications.

Rolling Back From Version 2.1 or higher to Version 2.0

The procedure that follows applies only to rolling back version 2.1 or higher to 2.0. These instructions are also in the Scalar Key Manager User's Guide.

Perform the procedure on one server at a time. Make sure it is complete before rolling back the other server. This will protect you in case a rollback fails, because the other server will be able to continue operations while you are recovering.

Note: The library may generate RAS/diagnostic tickets while you are performing this procedure. Once the rollback is complete, you can ignore and close the tickets.

Equipment Required

To perform this procedure, you need:

- Remote access to your library.
- Physical access to your SKM servers.
- The CD used to load the current version of software.

Note: The software version on the CD must match the version currently installed on the SKM server. If it does not, you will not be able to perform the rollback. If you no longer have the correct CD, note which version of software is currently installed on the server, then contact Quantum Support for the ISO image and burn it to a new CD. To see which version is currently installed on your server, see [Viewing the SKM Server Software Version](#) on page 113.

Procedure

- 1 Obtain the CD containing the currently installed version of software.
- 2 Stop all applications that require key exchanges from the SKM server pair.
- 3 Log on to one of the SKM servers and access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).
- 4 At the **Command** prompt, type **r** to **Roll back SKM server software**.
- 5 Insert the CD into the SKM server's CD ROM drive and press **<Enter>**.

The rollback process runs.

- If the wrong upgrade CD is loaded, the rollback stops and you receive an error message. Press **<Enter>** to return to SKM Admin Commands.
- If no CD is loaded, you are again requested for the CD. Load the CD and press **<Enter>**, or type **q** and press **<Enter>** to quit and return to SKM Admin Commands.

- 6 When the rollback completes, press **<Enter>** to access to SKM Admin Commands.
- 7 At the **Command** prompt, type **q** to quit SKM Admin Commands.
- 8 Issue the following command to confirm that the rollback version is loaded.

```
./skmcmds -v
```

The screen should display this version: 200Q.GC01400

- 9 Remove the CD from the CD ROM drive.

- 10 Repeat the above steps on the other SKM server.
- 11 Back up both SKM server keystores:
 - a At the prompt, access SKM Admin Commands by typing:
`./skmcmds`.
 - b At the **Command** prompt, type **7** to **Back up keystore**.
 - c Once the backup file is created, SFTP the backup file to a safe location.
 - d At the **Command** prompt, type **q** and press **<Enter>** to quit QKM Admin Commands.
- 12 Resume using backup applications.



Chapter 13

Updating the SKM Keystore After Replacing a Library Control Module

If you are running SKM and you need to replace the control module in a connected library (or the chassis in a Scalar i40/i80), you must run the library serial number replacement script (named `libreplac.py`) on the SKM server to ensure you do not lose “Export Used” key export functionality.

The procedure is only necessary when the control module of a library has been replaced because it changes the physical serial number of the library so that it no longer matches what is in the metadata of the SKM server.

If you replace one of the following types of modules, you will need to run the script.

Library	Type of module being replaced
Scalar i40/i80	Chassis
Scalar i500	Control module
Scalar i6000	Control module
Scalar i3/i6	Control module

This process applies to both SKM appliance servers and SKM VM servers. These steps must be performed on both servers in the pair. This chapter covers:

- [Running the Library Serial Number Replacement Script on SKM 1.0 and 1.1 Servers \(Version 100G or 110G\)](#)
- [Running the Library Serial Number Replacement Script on SKM 2.x Servers \(Version 200G\)](#)
- [Locating the Serial Number of the Control Module/Chassis](#)

Running the Library Serial Number Replacement Script on SKM 1.0 and 1.1 Servers (Version 100G or 110G)

Note: The GA version of this product (version 1.0) is called Quantum Key Manager (QKM). Some of the commands are slightly different (for instance, `./skmcmds` is `./qkmcms` on the GA server).

- 1 Contact Quantum Support to obtain the SKM service script package. Get the file from CSWeb and send it to the customer. The name of the file is:
servicescripts-pkg.sh
- 2 Record the serial number from the old control module and the new control module. If you no longer have the module, contact Quantum Support to provide the number. See [Locating the Serial Number of the Control Module/Chassis](#) on page 229 for help in locating the serial numbers.

Old Serial Number	
New Serial Number	

- 3 Replace the library chassis/control module following the instructions in the library user's guide.

Perform all of the following steps on BOTH SKM/QKM servers.

- 4 SFTP the service script package to the following location on the SKM/QKM server:


```
/home/akmadmin
```

- 5 Log on to the command line interface of the SKM/QKM server (see [Logging on to the Command Line Interface](#) on page 92).

- 6 Verify that the service script package **servicescripts-pkg.sh** is located in the directory by issuing the following command:

```
ls -l
```

The **/home/akmadmin** directory should list **servicescripts-pkg.sh**.

- 7 Set the execute privilege for the package by issuing the following command:

```
chmod 777 servicescripts-pkg.sh
```

- 8 Install the library serial number replacement script by issuing the following command:

```
sudo ./servicescripts-pkg.sh
```

This installs the script (named **libreplace.py**) in the **/home/akmadmin/service** directory.

- 9 Verify proper installation by issuing the following command:

```
ls -l /service
```

Confirm the **/service** directory lists the script named **libreplace.py**.

- 10 Remove the service script package from the **/home/akmadmin** directory by issuing the following command:

```
rm servicescripts-pkg.sh
```

- 11 Back up the keystore as follows:

Caution: It is important to make a backup now because the script will make changes to your keystore that may be difficult or impossible to reverse. If the operation fails you will need your original backup to restore your server.

- a At the prompt, access the Admin Commands menu by typing either **./skmcmds** (for SKM version 1.1) or **./qkmcms** (for QKM version 1.0).

- b At the **Command** prompt, type **7** to **Back up keystore**.

- c Once the backup file is created, you do not need to save it to another location as you normally would. This temporary backup file will be used to restore the keystore in the event that the serial number change operation fails.
 - d At the **Command** prompt, type **q** and press **<Enter>** to quit Admin Commands.
- 12 Change to the **service** directory by issuing the following command:
- ```
cd /service
```
- 13 Invoke the library serial number replacement script by issuing the following command, replacing **<from\_sn>** with the **OLD** serial number, and **<to\_sn>** with the **NEW** serial number.

---

---

**Caution: Be careful!** Make sure you enter both the old and the new library serial numbers correctly! Incorrect entries will result in incorrect encryption key usage associations.

---

---

```
./libreplace.py <from_sn> <to_sn>
```

For example:

```
./libreplace.py A0C0123456 A0C0789012
```

- 14 Follow the script's instructions and wait for the serial number replacement operation to complete. If the operation completes successfully, the screen will display "100% Complete" and will list the number of keys updated. See sample script output in [Figure 46](#) on page 225.

---

---

**Caution: Do not interrupt the operation while it is running.**

---

---

Figure 46 Sample libreplace.py  
Script Output, SKM 1.x

```
akmadmin@qkmsserver:/service$./libreplace.py A0C0406430 A0C0088616
WARNING: If you are running this command via a VMWare console, do not press Print Screen
until execution is complete.
It is STRONGLY recommended that a keystore backup be made before proceeding. Have you
made a backup? Type 'YES' if so:
>yes
akmadmin 1053 "MD04 CT 'A0C0088616" ""
akmadmin 1053 "MD04 CT 'A0C0406430" ""

Migrate Keys
FROM LIBRARY:
Product : Scalar i500
Serial Number : A0C0406430
Manufacture Date: May 30, 2006
TO LIBRARY:
Product : Scalar i500
Serial Number : A0C0088616
Manufacture Date: Jul 16, 2008

This operation will modify 3103 keys - are you sure you want to continue? Type 'YES' if so:
>yes
10% Complete
20% Complete
30% Complete
40% Complete
50% Complete
60% Complete
70% Complete
80% Complete
90% Complete
100% Complete
Updated 3103 keys
akmadmin@qkmsserver:/service$
```

15 Return to the `/home/akmadmin` directory by typing the following:

```
cd /home/akmadmin
```

16 Do one of the following:

- **If the operation completed successfully**, back up the keystore like you did in [Step 11](#), except this time, copy off the backup file and store in a secure location for disaster recovery purposes as you normally would (see [Backing Up the SKM Server](#) on page 103).
- **If the operation failed**, restore the keystore backup that you created in [Step 11](#) following the restore procedure described in [Restoring the SKM Server](#) on page 107 (except that you do not need to SFTP the backup file over to the SKM server since you

left the backup file in the correct location on the server in [Step 11](#)). This will allow you to continue operations. Then contact Quantum Support for further assistance.

- 17 Log off of the command line interface by typing **exit** or **logout** at the prompt (see [Logging Off of the SKM Server Command Line Interface](#) on page 95).
- 18 Repeat [Step 4](#) through [Step 17](#) on the other SKM/QKM server in the pair.

---

## Running the Library Serial Number Replacement Script on SKM 2.x Servers (Version 200G)

- 1 Record the serial number from the old control module and the new control module. If you no longer have the module, contact Quantum Support to provide the number. See [Locating the Serial Number of the Control Module/Chassis](#) on page 229 for help in locating the serial numbers.

|                   |  |
|-------------------|--|
| Old Serial Number |  |
| New Serial Number |  |

- 2 Replace the library chassis/control module following the instructions in the library user's guide.

Perform all of the following steps on BOTH SKM servers.

- 3 Log on to a server and access SKM Admin Commands (see [Accessing SKM Admin Commands](#) on page 93).

4 Back up the SKM server as follows:

---

---

**Caution:** It is important to make a backup now because the script will make changes to your keystore that may be difficult or impossible to reverse. If the operation fails you will need your original backup to restore your server.

---

---

- a At the **Command** prompt, type **7** to **Back up SKM server**.
- b Once the backup file is created, you may leave the backup file on the server instead of copying it off as you normally would. The backup file can be used to restore the keystore in the event that the serial number change operation fails.
- c At the **Command** prompt, type **q** and press **<Enter>** to quit SKM Admin Commands and go to the command line interface.

5 Change to the **service** directory by issuing the following command:

```
cd /service
```

- 6 Invoke the library serial number replacement script by issuing the following command, replacing **<from\_sn>** with the **OLD** serial number, and **<to\_sn>** with the **NEW** serial number. Do not type the caret characters, "**<**" and "**>**".

---

---

**Caution:** **Be careful!** Make sure you enter both the old and the new library serial numbers correctly! Incorrect entries will result in incorrect encryption key usage associations.

---

---

```
./libreplace.py <from_sn> <to_sn>
```

For example:

```
./libreplace.py A0C0123456 A0C0789012
```

- 7 Follow the script's instructions and wait for the serial number replacement operation to complete. If the operation completes successfully, the screen will display "100% Complete" and will list the number of keys updated. See sample script output in [Figure 47](#).

---

---

**Caution:** **Do not interrupt the operation while it is running.**

---

---

Figure 47 Sample libreplace.py  
Script Output, SKM 2.0

```
akmadmin@skmserver:/service$
akmadmin@skmserver:/service$./libreplace.py A0C0406430 A0C0088616
WARNING: If you are running this command via a VMWare console, do not press Print Screen
until execution is complete.
It is STRONGLY recommended that a keystore backup be made before proceeding. Have you
made a backup? Type 'YES' if so:
>yes
akmadmin 1053 "MD04.CT"A0C0088616 ""
akmadmin 1053 "MD04.CT"A0C0406430 ""

Migrate Keys
FROM LIBRARY:
Product : Scalar i500
Serial Number : A0C0406430
Manufacture Date: May 30, 2006
TO LIBRARY:
Product : Scalar i500
Serial Number : A0C0088616
Manufacture Date: Jul 16, 2008

This operation will modify 3103 keys - are you sure you want to continue? Type 'YES' if so:
>yes
10% Complete
20% Complete
30% Complete
40% Complete
50% Complete
60% Complete
70% Complete
80% Complete
90% Complete
100% Complete
Updated 3103 keys
akmadmin@skmserver:/service$
```

8 Return to the /home/akmadmin directory by typing the following:

```
cd /home/akmadmin
```

9 Do one of the following:

- If the operation completed successfully, back up the keystore like you did in [Step 4](#), except this time, copy off the backup file and store in a secure location for disaster recovery purposes as you normally would (see [Backing Up the SKM Server](#) on page 103).
- If the operation failed, restore the keystore backup that you created in [Step 4](#) following the restore procedure described in [Restoring the SKM Server](#) on page 107 (except that you do not need to SFTP the backup file over to the SKM server since you

left the backup file in the correct location on the server in [Step 4](#)). This will allow you to continue operations. Then contact Quantum Support for further assistance.

- 10 Log off of the command line interface by typing **exit** or **logout** at the prompt (see [Logging Off of the SKM Server Command Line Interface](#) on page 95).
- 11 Repeat [Step 3](#) through [Step 10](#) on the other SKM server in the pair.

---

## Locating the Serial Number of the Control Module/ Chassis

This section helps you locate the serial number of your library chassis/control module.

- [Locating the Serial Number on the i3](#) on page 229
- [Locating the Serial Number on the i6](#) on page 231
- [Locating the Serial Number on the Scalar i40/i80](#) on page 233
- [Locating the Serial Number on the Scalar i500](#) on page 234
- [Locating the Serial Number on the Scalar i2000/i6000](#) on page 236

---

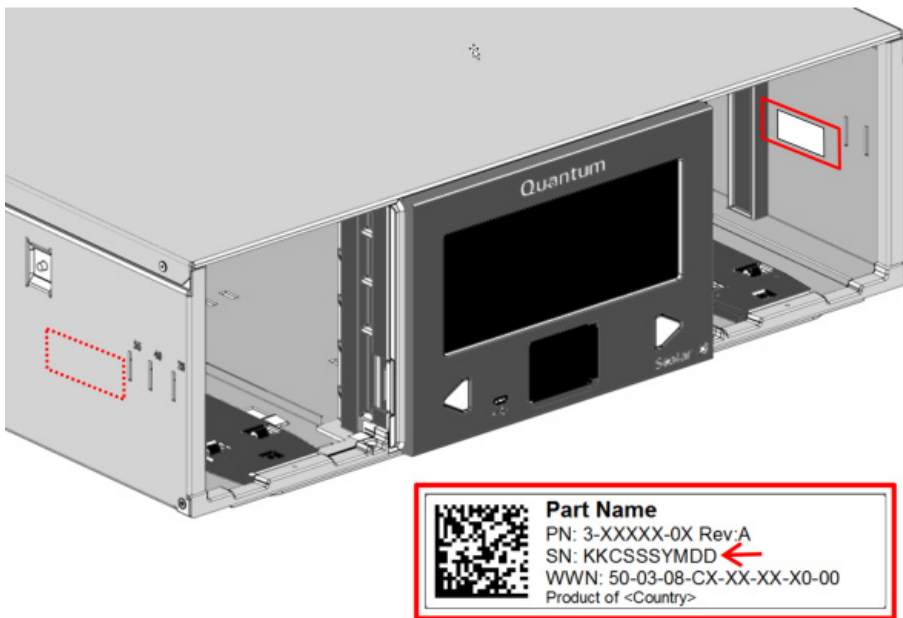
### Locating the Serial Number on the i3

---

On the Scalar i3, the serial number label is located as follows:

- On the inside of control module (CM).
  - Left or right side of the chassis.
  - You must remove the left or right magazine to view the serial number.
  - See [Figure 48](#).

Figure 48 Scalar i3 Serial Number Label Location CM



- On the outside, left-rear, of the control module ([Figure 49](#)).

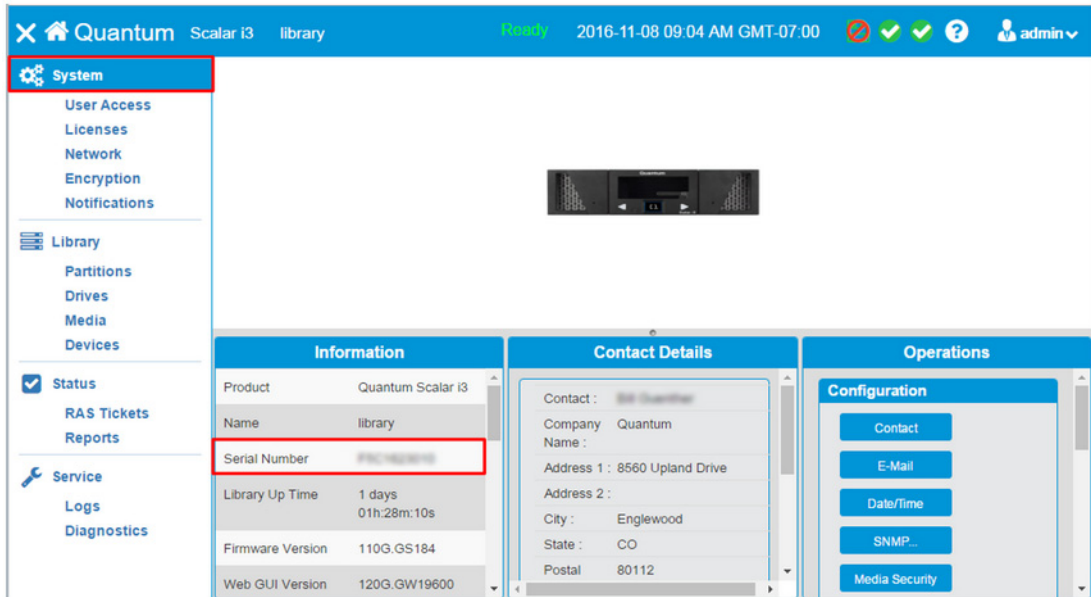
Figure 49 Scalar i3 Serial Number Label Location Side





- You can also access the serial number from the WebGUI ([Figure 50](#)).

Figure 50 Scalar i3 Serial Number Label Location WebGUI

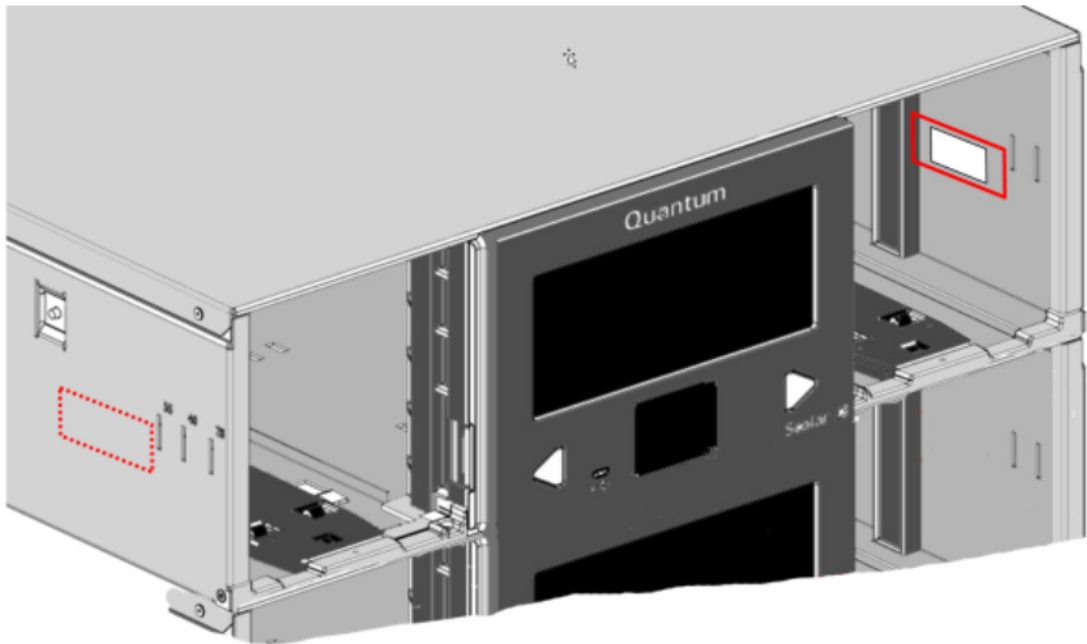


## Locating the Serial Number on the i6

On the Scalar i6, the serial number label is located as follows:

- On the inside of control module.
  - Left or right side of the chassis.
  - You must remove the left or right magazine to view the serial number.
  - See [Figure 51](#).

Figure 51 Scalar i3 Serial Number Label Location CM



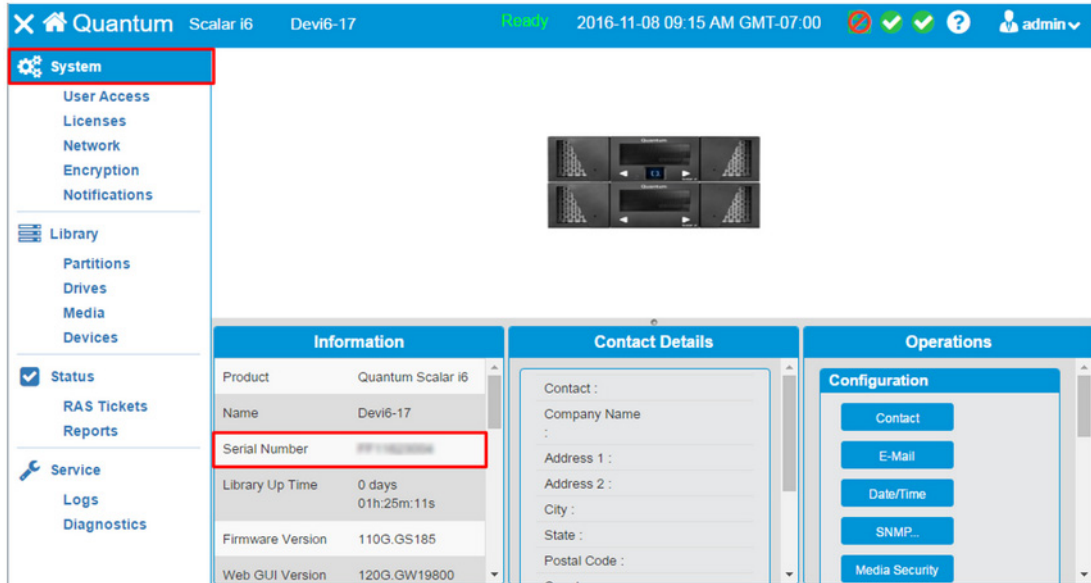
- On the outside, left-rear, of the control module ([Figure 52](#)).

Figure 52 Scalar i3 Serial Number Label Location Side



- You can also access the serial number from the WebGUI ([Figure 50](#)).

Figure 53 Scalar i6 Serial Number Label Location WebGUI



## Locating the Serial Number on the Scalar i40/i80

On the Scalar i40/i80, the serial number label is located on the rear of the chassis in the upper left corner. See [Figure 54](#).

The Scalar i40 serial number is 10 digits long and starts with **D0**; for example, D0H0029914.

The Scalar i80 serial number is also 10 digits long and starts with **D1**; for example, D1H0029914.

Figure 54 Scalar i40/i80 Serial Number Label and Location



You can also find the serial number on the library as follows:

- **Operator panel** — Select **Reports > About Library**.
- **Web client** — Select **Reports > About > Scalar i40/i80**.

### Locating the Serial Number on the Scalar i500

On the Scalar i500, the serial number label is located inside the control module, on the horizontal bar at the back of the library. To see the label, open the front door. See [Figure 55](#) for location and [Figure 56](#) for an example.

The serial number is listed first. The serial number is all of the characters following the “%SN” on the serial number label. Do not enter the “%SN” characters when typing the serial number into the SKM command line.

Figure 55 Scalar i500 Serial Number Label Location

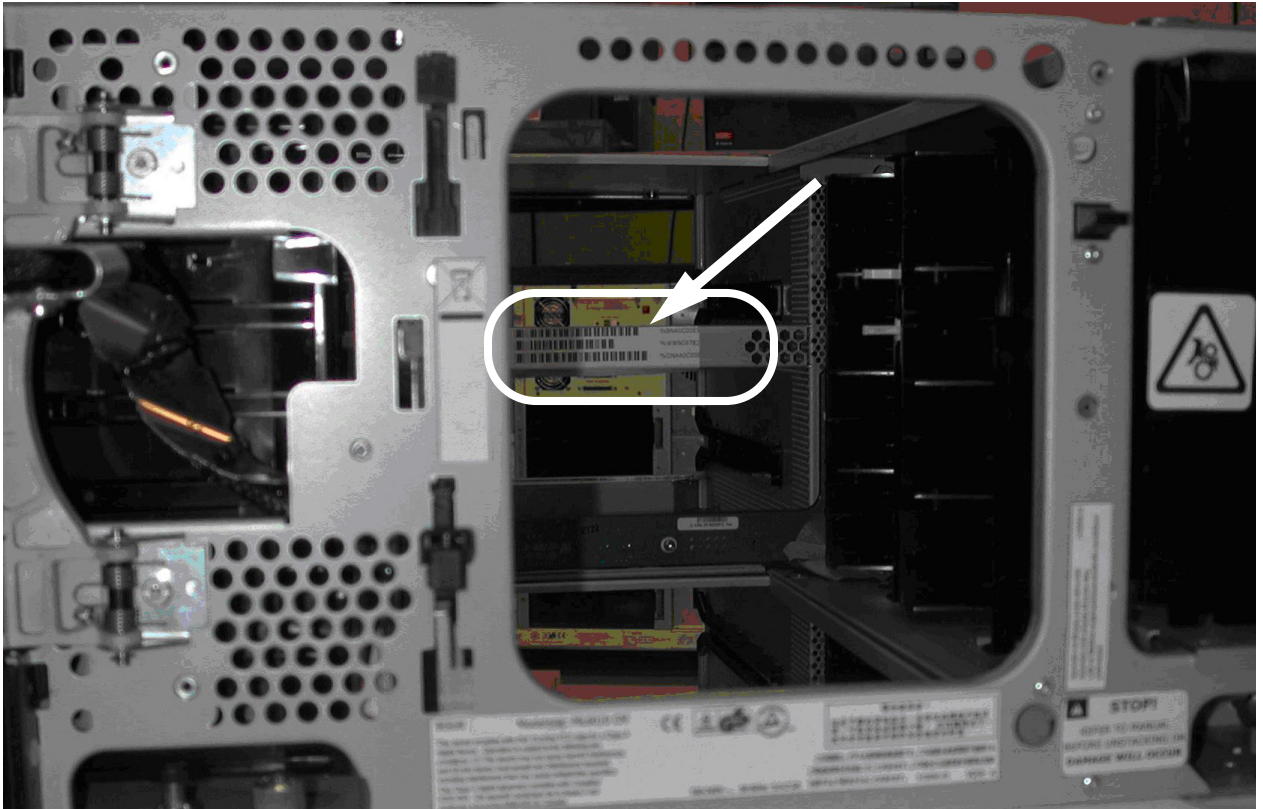


Figure 56 Scalar i500 Serial Number/WWN Label



You can also find the serial number on the library as follows:

- **Operator panel** — Select **Tools > About Library**.
- **Web client** — Select **Reports > About > Scalar i500**.

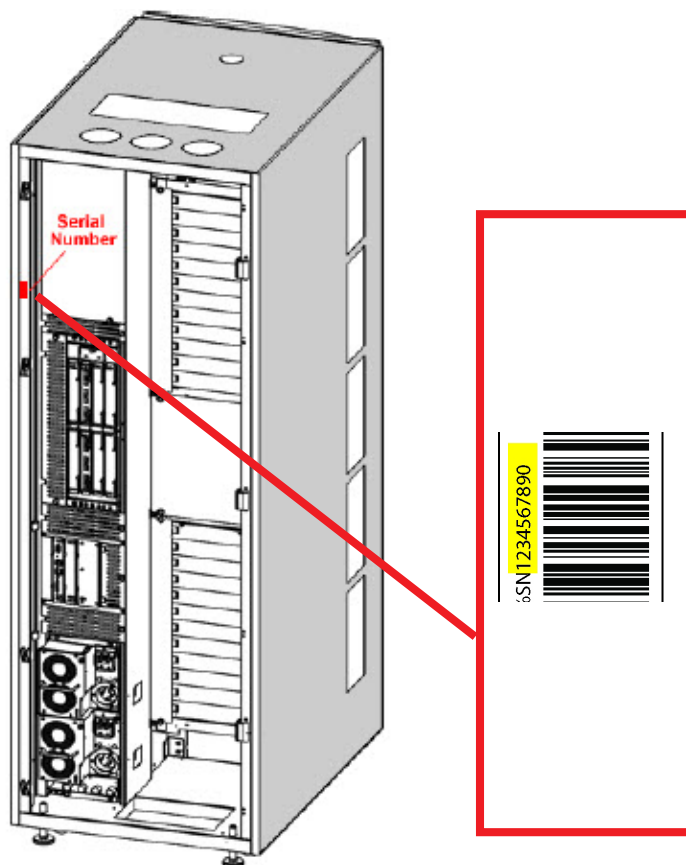
## Locating the Serial Number on the Scalar i2000/i6000

On the Scalar i2000/i6000, the serial number label is located on the left side of the library chassis from inside the rear of the library. See [Figure 57](#).

**Serial Number Format:** Serial numbers are nine digits. For new manufactured Scalar i6000 libraries, the control module serial number will begin with 2731 (for example, 273102351). However, a Scalar i2000 library upgraded to a Scalar i6000 will retain its original Scalar i2000 serial number (for example, 263104668).

The serial number is the nine digits following the “%SN” on the serial number label. Do not enter the “%SN” characters when typing these values on the SKM command line interface.

Figure 57 Scalar i2000/i6000  
Serial Number Label and  
Location



You can also find the serial number on the library as follows:

- **Library Management Console** — Select **Monitor > System**. The serial number is in the **ID** column on the first line in the **Library:<library name>** row.

Chapter 13: Updating the SKM Keystore After Replacing a Library Control Module  
Locating the Serial Number of the Control Module/Chassis





# Appendix A Specifications

---

---

## SKM Appliance Server Specifications

---

### SKM 2.7 Appliance Server (and later versions) Physical Specifications

---

**Height:** 1.69 in. (43 mm), 1U

**Depth:** 19.59 in. (497.8 mm)

**Width:** 17.11 in. (434.6 mm)

**Weight:** 18.5 lb. (8.38 kg)

**Power Supply:** 450 watt (100-127 V or 200-240 V AC nominal, auto-sensing)

**Power Cord:** The Quantum Key Management Server ships with one power cord for the one power supply.

---

### SKM 2.6 Appliance Server (and earlier versions) Physical Specifications

---

**Height:** 1.69 in. (43 mm), 1U

**Depth:** 22.7 in. (576 mm)

**Width:** 17.3 in. (439 mm)

**Weight:** 24.3 lb. (11 kg)

**Power Supply:** 300 watt (110-127 V or 200-240 V AC nominal, auto-sensing)

**Power Cords:** The Quantum Key Management Server includes the following power cords:

- IBM P/N 39M5081 - North American
- IBM P/N39M5377- Rack cord

## SKM Appliance Server Environmental Specifications

### Air Temperature

|            |                                                                                       |
|------------|---------------------------------------------------------------------------------------|
| Server on  | 50.0° to 95.0°F (10° to 35°C);<br>altitude: 0 to 3000 ft. (914.4 m)                   |
|            | 50.0° to 89.6°F (10° to 32°C);<br>altitude: 3000 ft. (914.4 m) to 7000 ft. (2133.6 m) |
| Server off | 50.0° to 109.4°F (10° to 43°C);<br>maximum altitude: 7000 ft. (2133.6 m)              |
| Shipping   | -40° to 140°F (-40° to 60°C)                                                          |

### Humidity

|            |           |
|------------|-----------|
| Server on  | 8% to 80% |
| Server off | 8% to 80% |

## SKM Appliance Server Acoustical Noise Emissions

|                        |                  |
|------------------------|------------------|
| Sound power, idling    | 6.5 bels maximum |
| Sound power, operating | 6.5 bels maximum |

## SKM Appliance Server Heat Output

Approximate heat output in British thermal units (BTU) per hour in a typical configuration:

341 BTU per hour (100 watts)

## SKM Appliance Server Electrical Input

|                                          |                                                                                                   |
|------------------------------------------|---------------------------------------------------------------------------------------------------|
| Sine-wave input                          | (50 - 60 Hz) required                                                                             |
| Input voltage low range                  | <ul style="list-style-type: none"><li>• Minimum: 100 V AC</li><li>• Maximum: 127 V AC</li></ul>   |
| Input voltage high range                 | <ul style="list-style-type: none"><li>• Minimum: 200 V AC</li><li>• Maximum: 240 V AC</li></ul>   |
| Approximate input kilovolt-amperes (kVA) | <ul style="list-style-type: none"><li>• Minimum: 0.044 kVA</li><li>• Maximum: 0.416 kVA</li></ul> |

## VM Host Specifications

### Supported VM Environments

The SKM virtual machine supports the following environments:

- VMware ESX 4.x 64-bit or 5.x 64-bit
- VMware EXSi 4.x 64-bit 5.x 64-bit
- Virtual Machine Manager 0.9.0

## Supported Libraries and Tape Drives

SKM supports the following libraries. Refer to the library documentation for information about supported tape drives:

| Library      | Tape Drives                                                                   |
|--------------|-------------------------------------------------------------------------------|
| Scalar i3/i6 | IBM LTO-6 Fibre Channel<br>IBM LTO-7 Fibre Channel<br>IBM LTO-8 Fibre Channel |

| Library        | Tape Drives                                                                                                                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scalar i40/i80 | HP LTO-4 Fibre Channel and SAS<br>HP LTO-5 Fibre Channel and SAS<br>HP LTO-6 Fibre Channel and SAS                                                                                                                             |
| Scalar i500    | HP LTO-4 Fibre Channel and SAS<br>HP LTO-5 Fibre Channel and SAS<br>HP LTO-6 Fibre Channel and SAS<br>IBM LTO-5 Fibre Channel and SAS<br>IBM LTO-6 Fibre Channel and SAS<br>IBM LTO-7 Fibre Channel<br>IBM LTO-8 Fibre Channel |
| Scalar i2000   | HP LTO-4 Fibre Channel<br>HP LTO-5 Fibre Channel<br>HP LTO-6 Fibre Channel                                                                                                                                                     |
| Scalar i6000   | HP LTO-4 Fibre Channel<br>HP LTO-5 Fibre Channel<br>HP LTO-6 Fibre Channel<br>IBM LTO-5 Fibre Channel<br>IBM LTO-6 Fibre Channel<br>IBM LTO-7 Fibre Channel<br>IBM LTO-8 Fibre Channel                                         |

## Library Firmware Requirements

To access all the features of SKM, the most recent library firmware is recommended. See the Release Notes for SKM or your library for information on the minimum firmware required to run SKM, and most recent firmware versions available for your library.

---

## Tape Drive Firmware Requirements

Install the latest version of tape drive 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.

---

## Number of Data Encryption Keys Generated

Each time the SKM server generates data encryption keys in response to a library request, the number of keys generated is:

---

**Note:** SKM-attached Scalar libraries support communication certificate key lengths of 1024 bits. Communication certificates larger than 1024 bits, such as 2048 and 4096 bit key lengths, are not currently supported by all library models, but will be supported with a future prerequisite library firmware release. (Refer to the Scalar library release notes or contact Quantum/support for additional information and availability of required library firmware). Note however, that the use of communication certificates with key bit lengths larger 1024 bits will affect library performance with respect to encryption key retrieval times and encryption key generation, import and export operations. While certificate key lengths of 2048 bits slightly slow operations in single and multi-library attached SKM server environments, the use of communication certificates with a key length of 4096 bits should be avoided in SKM configuration environments where multiple Scalar tape libraries are attached to a single SKM server pair.

---

| <b>Library</b>            | <b>Number of keys generated</b> |
|---------------------------|---------------------------------|
| <b>Scalar i3/i6</b>       | 1024                            |
| <b>Scalar i40/i80</b>     | 1024                            |
| <b>Scalar i500</b>        | 1024                            |
| <b>Scalar i2000/i6000</b> | 4096                            |



# Glossary

---

This glossary defines the special terms, abbreviations, and acronyms used in this document.

---

## C

**certificate** A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated.

---

## D

**data encryption key** An alphanumeric string used to encrypt data.

---

## E

**encryption** The conversion of data into a cipher. A key is required to encrypt and decrypt the data. Encryption provides protection from persons or software that attempt to access the data without the key.

---

## H

**HDD** Hard disk drive.

---

**I**

**IP** Internet Protocol. The method or protocol by which data is transmitted from one computer (or host) to another over the Internet using a system of addresses and gateways.

**ISO image** An ISO image (International Organization for Standardization) is an archive file (also known as a disc image) of an optical disc, composed of the data contents of every written sector of an optical disc, including the optical disc file system. ISO image files typically have a file extension of .iso. ISO images are used to create CDs for SKM server upgrades.

---

**K**

**keystore** A database that contains the data encryption keys and their associated metadata.

---

**M**

**metadata** Data about data; in the case of SKM, it means information about the data in the keystore database; for example, which data encryption keys were used on which tapes.

---

**P**

**private key** One key in an asymmetric key pair, typically used for decryption.

**public key** One key in an asymmetric key pair, typically used for encryption.

---

**S**

**SFTP** Secure File Transfer Protocol; a secure version of FTP.

**SKM** Scalar Key Manager. An application that manages data encryption keys and metadata via Quantum's tape libraries.

**SKM appliance server** Physical key server purchased from Quantum.

**SKM VM server** Virtual machine key server purchased from Quantum and installed in a VMware or KVM environment.

**SSH** Secure **S**hell (or secure socket shell). A security protocol for logging onto a remote server. SSH provides an encrypted session for transferring files and executing server programs.



---

|          |            |                                                                                                                       |
|----------|------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>T</b> | <b>TCP</b> | Transmission Control Protocol. Works in conjunction with IP to ensure that packets reach their intended destinations. |
|          | <b>TLS</b> | Transport Layer Security.                                                                                             |

---

|          |           |                                                                                                                                                 |
|----------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>V</b> | <b>VM</b> | Virtual machine. A virtual machine is a software implementation of a machine (i.e., a computer) that executes programs like a physical machine. |
|----------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------|





# Index

---

---

## A

airflow 10  
akmadmin login ID 92  
asymmetric encryption 5

---

## B

backing up the server 7, 90, 103  
beep codes 166

---

## C

CD/DVD  
    drive activity LED 22  
    eject button 22  
certificate  
    exporting 140, 146  
    importing 140, 146  
certificates, encryption 5  
chassis replacement script 221  
command line  
    help menu 112  
    logging on 92

    operations 112  
configuring  
    appliance server 28, 33  
    library 83  
    multiple libraries 90  
    VM server 39, 41, 49, 54  
connectors  
    rear panel 22  
control module replacement script  
    221  
cooling 10  
cover, opening 10

---

## D

data encryption keys  
    assignment 3  
    depletion of 137  
    exporting 140, 149  
    generating 136  
        at initial setup 136  
        automatic 137  
        manual 138  
    importing 140, 149  
    list of 120  
    number of 117

    overview 4  
date  
    and TLS certificates 168  
    setting 100  
diagnostic tickets 165  
disabling library managed  
    encryption 138  
disaster  
    planning 12  
    recovery 181, 183  
drive code 242, 243  
drive, see hard disk drive

---

## E

EKM path diagnostics 142  
electrostatic considerations 16  
encrypted media 160  
encryption  
    algorithms 4  
    asymmetric encryption 5  
    certificate 5  
    keys 4  
    overview 2  
    planning 9

- private key 5
- public key 5
- symmetric encryption 5
- encryption key import warning log 127
- encryption-capable media 2
- encryption-capable tape drive 2
- encryption-enabled tape drive 2
- encryption-enabled tape library 3
- end user license agreement 34, 116
- Ethernet activity LED 25
- Ethernet link LED 25
- Ethernet port 1 24
- Ethernet port 2 24
- Ethernet ports 34
- exiting 95
- exporting
  - data encryption keys 140, 142, 146, 149
  - encryption certificates 140, 141, 145, 146

---

## F

- failover 3
- fan 10
  - noisy 167
- firmware
  - downgrading 216
  - rolling back 216
- firmware requirements
  - library 242
  - tape drive 242
- frequently asked questions 159
- front panel, appliance server 32, 33

---

## G

- generating data encryption keys

- 136
- glossary 245

---

## H

- hard disk drive
  - activity LED 21, 22
  - mirroring 6, 174
  - replacing 174
  - status LED 22
- hard drive, see hard disk drive
- help menu, command line 112
- hostname, configuring 100

---

## I

- importing
  - data encryption keys 140, 142, 146, 149
  - encryption certificates 140, 142, 145, 146
  - TLS certificates on SKM server 59, 70
- installing
  - appliance server 28, 29
  - VM server 39, 49
- IP address
  - changing 98
  - port 1 24
  - port 2 24
  - setup port 24

---

## K

- keys
  - see also data encryption keys 4
  - asymmetric 5
  - encryption
    - overview 4
  - private 141, 144
  - public 141, 144

- symmetric 5, 141, 144
- keystore 6
  - update after library control module replacement 221

---

## L

- LEDs
  - error indicators 161
- library 3
  - control module replacement script 221
  - template 121
- library managed encryption
  - disabling 138
  - overview 2
- library user's guides xvi
- logging off 95
- logging on 92
- login ID 68, 71, 92
- logs
  - encryption key import warning 127
  - retrieving via command line 114
  - retrieving via SKM server 115
  - SKM server 114
  - verbosity 117

---

## M

- MAC address, configuring 43
- media
  - encrypted 160
  - encryption capable 2
- metadata 6
- mirrored hard disk drives 6, 174
- multiple libraries 11, 90

---

**O**

ova image 41

---

**P**

password  
     changing 35, 47, 56, 97  
     lost 97, 169

planning the SKM environment 9

POST beep codes 166

POST error codes 166

power button 21

power cord connector 24

power failure 26

powering off the appliance server 26

powering on the appliance server 26

private key 141, 144

public key 141, 144

publications xv

---

**Q**

quitting 95

---

**R**

rack 11

RAID rebuild 22, 165, 179

RAS tickets 165

rear panel, appliance server 22, 31

replacement procedures  
     hard disk drive 174  
     library control module 221  
     SKM appliance server 181  
     SKM VM server 183

reset button 21

restoring the server 107

running out of keys 137

---

**S**

serial connector 24

serial number  
     Scalar i2000/i6000, locating 236  
     Scalar i40/i80, locating 233  
     Scalar i500, locating 234  
     SKM server, locating 170

server  
     backing up 103  
     configuration 12  
     cover, opening 10  
     error LED 21  
     powering off 26  
     powering on 26  
     replacing  
         appliance 181  
         VM 183  
     restoring 107  
     software 113

setup wizard 96

sharing encrypted tapes offsite 141, 144

SKM  
     overview 2  
     process 3

snapshot, capturing 114, 115

software  
     version, SKM server 113

specifications 239

symmetric encryption 5

symmetric key 141, 144

systems-management connector 24

---

**T**

tape drive  
     encryption capable 2  
     encryption-enabled 2

tape drive code 242, 243

template, library 121

terminology 245

time zone, changing 99

time, setting 100

TLS certificates  
     displaying on SKM server 101  
     installing on Scalar i40/i80/i500 library 84  
     installing on SKM server 59, 70  
     requirements, user provided 60

trace level logging 117

troubleshooting 159

---

**U**

USB connectors 21, 24

user's guides, library xvi

---

**V**

verbosity in logs 117

video card settings 44

video connector 24

