



SKM Repackaging Instructions

This document details the steps required to safely prepare an SKM (Scalar Key Manager) appliance for moving, and how to properly package the SKM appliance using the supplied Move Kit components.

This document contains the following topics:

- About Packaging an SKM Server 2
- Repackaging Kit BOM 3
- About Backing Up the Servers 4
- About SKM Admin Commands 5
- Backing Up the Server 6
- Turning Off the SKM Appliance Server 9
- Removing the Server from a Rack 9
- Packaging the Server for Moving 10



About Packaging an SKM Server

Moving an SKM Appliance Server can stress the server components. To ensure safe and proper transport of the server, and to prevent voiding the warranty, carefully follow these steps, in the following order:

- [Backing Up the Server on page 6](#)
- [Turning Off the SKM Appliance Server on page 9](#)
- [Removing the Server from a Rack on page 9](#)
- [Packaging the Server for Moving on page 10](#)

Repackaging Kit BOM

Figure 1: Repackaging Kit components

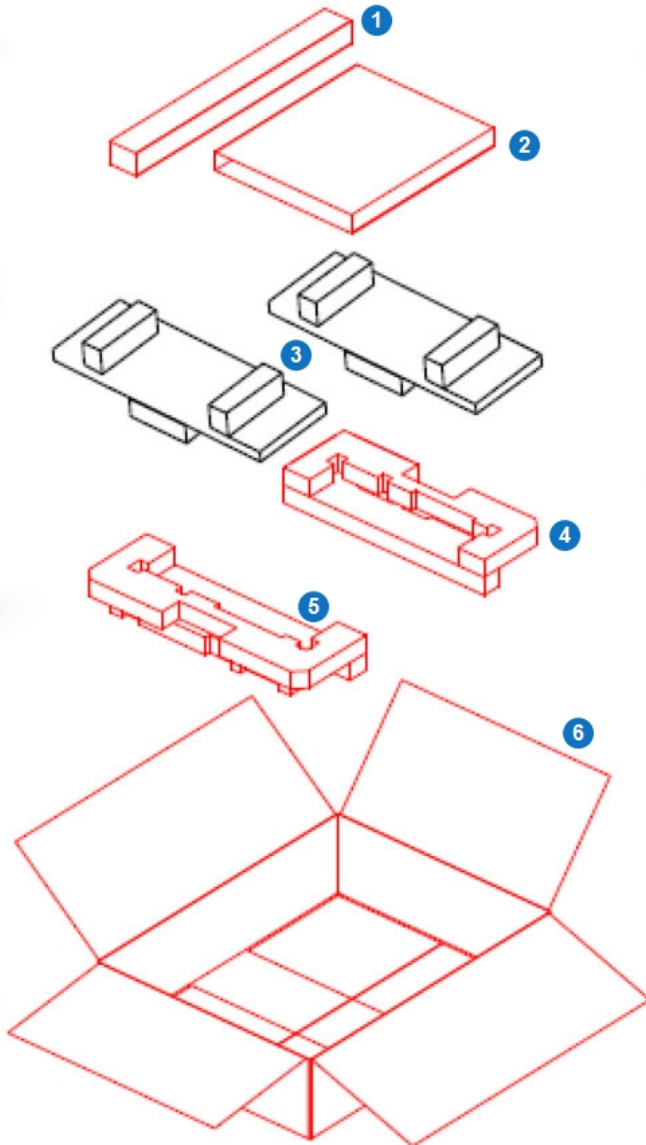


Table 1: Bill of Materials for 9-03778-xx (not shown)

Item	Part Number	Quantity	Contents
1.	3-06198-01	1	SKM Server Ship Pack Kit (shown)
2.	3-06125-01	1	48-inch Film Sheet
3.	80-2024-01	1	Packaging Tape
4.	3-06670-03	1	Shipping Label

Table 2: Bill of Materials for 3-06198-xx

Item	Part Number	Quantity	Contents
1.	3-06200-01	1	Carton Kit
2.	3-06232-01	1	Insert
3.	3-06201-01	2	Foam Top
4.	3-06202-01	1	Foam Bottom - back
5.	3-06203-01	1	Foam Bottom - front
6.	3-06199-01	1	Shipping Carton

About Backing Up the Servers

It is critical that you keep a current backup of each SKM server so that you can restore it if the server becomes inoperable.

Each SKM server generates its own unique data encryption keys, meaning that the keystore on each SKM server is different. 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 one contains different data. If a server fails and needs to be replaced, the backup is required to restore operation.

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) become inoperable, the only way to recover your keystore is by using 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.

The backup contains your keystore and certain server configuration files. The backup does not contain your password or server IP address. The backup is required for server hardware replacement, or for restoring a rebuilt SKM VM server.

⚠ 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 through 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.

i 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.

Make sure that 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 delay between key generation sessions, during which you intend to begin serving keys for encryption, you will need to perform multiple backups — one after each key generation session.

See [Backing Up the Server on the next page](#).

Source - SKM User Guide 6-66531-05RevB. Combined "Backing Up the SKM Server" and "Why You Need to Back Up Your SKM Servers" into this one topic.

About SKM Admin Commands

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

Details about these commands include:

- When you access the SKM Admin Commands, the SKM server process is stopped. This means that 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" in the *SKM User's Guide* for more information.
- You can make as many configuration changes during a session as you wish. To save your changes, type **q** at the **Command** prompt to quit the SKM Admin Commands. See "Quitting SKM Admin Commands" in the *SKM User's Guide* for more information.
- When changing configuration settings, you can press **<Enter>** to leave the current setting unchanged.
- Only one user can access the SKM Admin Commands at a time. If you try to log on, and another user is already logged on, you will receive a message that the system is already running, and you will not be able to log on.

Source - SKM User Guide 6-66531-05RevB.

Backing Up the Server

You can back up the server using the SKM Admin Commands or the command line interface (CLI). Both will stop the SKM server process prior to backup, and will restart the server process after the backup is complete. It is faster to use the command line interface unless you are already in the SKM Admin Commands.

Backing Up Using SKM Admin Commands

Perform the following steps separately for each SKM server.

1. Log on to the SKM server's command line interface.

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

- a. Connect to the SKM server.
 - **SKM appliance server:** Use SSH.
 - **SKM VM server:** Use SSH or vSphere.

i 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.

- b. At the skmserver login prompt, type the login ID:
akmadmin

- c. At the Password prompt, type your password.

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

2. Access the SKM Admin Commands.

- a. If necessary, log on to the SKM server command line interface.
- b. At the akmadmin@<hostname> prompt (where <hostname> is the SKM server hostname), type:
./skmcmds
- c. At the **Password** prompt, type your password.

A message displays, alerting you that the SKM server will be stopped.

- d. Enter **y** to agree to stop the SKM server and continue.

A message displays, stating that the SKM server is being stopped.

- e. Press **<Enter>** to continue.

The list of SKM Admin Commands displays, followed by the **Command** prompt.

Example:

```
SKM Admin Commands (Version Z10Q.TC00400)
  SKM Version <akmadmin Version 2.1.1>
Server Cert's Validity:
  /etc/akm/Certs/QKMIECertUM210275UM210276.pem
  Not Before: Feb 13 20:23:25 2013 GMT and Not After : Feb 11 20:23:25 2023 GMT
  /etc/akm/Certs/QKMServerSignedCert.pem
  Not Before: May  1 19:44:49 2009 GMT and Not After : May  1 19:44:49 2019 GMT
Admin Cert's Validity:
  /home/akmadmin/.akmadmin/Certs/QKMAdminSignedCert.pem
  Not Before: May  1 19:44:49 2009 GMT and Not After : May  1 19:44:49 2019 GMT

Current Date/Time: Fri Mar  1 07:16:49 PST 2013


-----
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.
q) Quit.
-----
Command:
```


For more information, see [About SKM Admin Commands on page 5](#).

3. At the Command prompt, type **7** (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 way, 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 if you lose a server.

⚠ Caution: Do not use SKM to encrypt the sole copy of your SKM server backup. If both servers failed, 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 the 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.

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

a. Connect to the SKM server.

- **SKM appliance server:** Use SSH.
- **SKM VM server:** Use SSH or vSphere.

i 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.

b. At the skmserver login prompt, type the login ID:
akmadmin

c. At the Password prompt, type your password.

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

2. At the **akmadmin@<hostname>** prompt (where <hostname> is the SKM server hostname), type 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<serialnumber><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 way, 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 if you lose a server.

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

Turning Off the SKM Appliance Server

1. To power off the server, press the power button and hold it in for four seconds.
2. 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.

⚡ WARNING: 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.

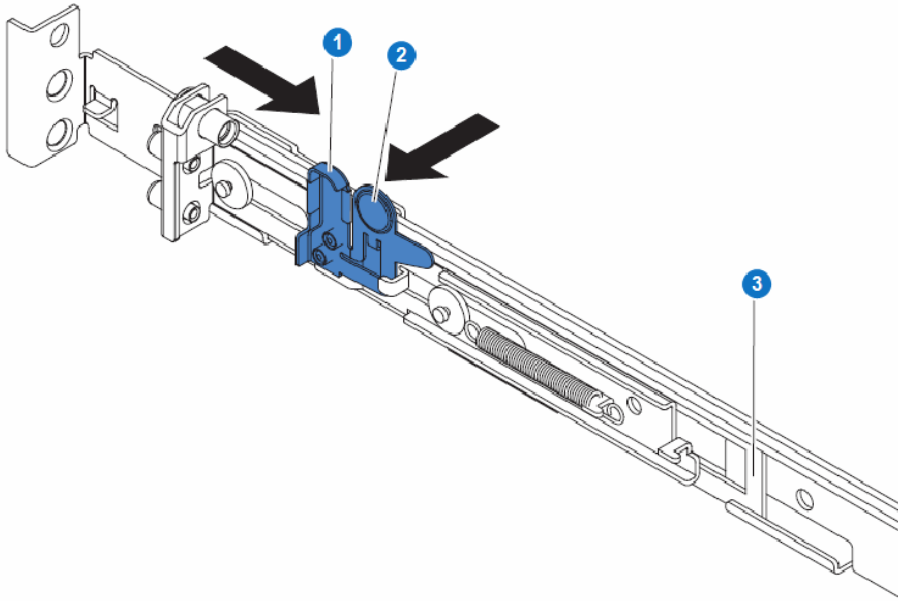
Removing the Server from a Rack

Used 6-67122-01A as source and reverse engineered from step 9... since most of the steps involve putting the rails in, it's a quick removal.

1. Remove the cables from the rear of the server and place them in the the insert box (see [Figure 1 on page 3](#)).
2. Disengage the server from the front mounting flanges by loosening the captive thumbscrews and pulling the server straight out of the server rack.
3. Loosen and remove any screws securing the slide rails to the server rack.

4. Remove each rack slide rail from the server rack by pressing on the rail adjustment bracket (3) and tabs (1 and 2), then sliding the rail carrier inward to release the end of the rail from the rack. Remove the released end of the slide rail from the rack. Repeat for the other end of the rack slide rail.

Figure 2: Rack slide rail

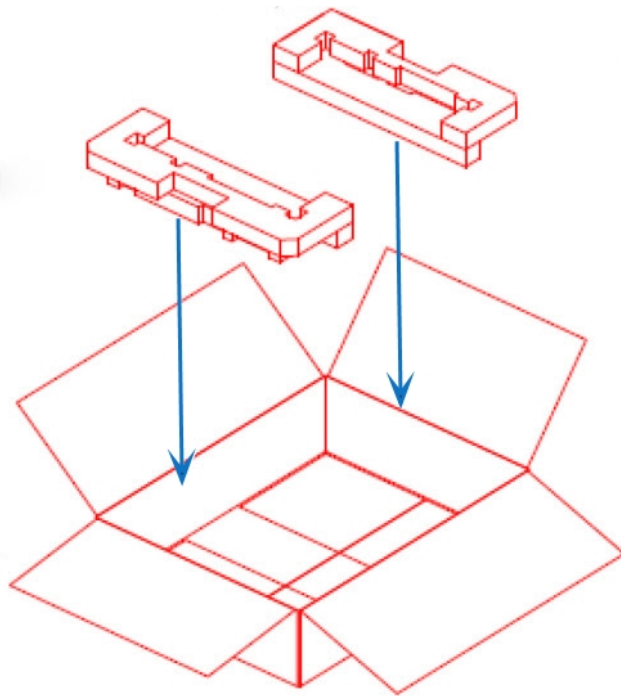


5. Place the rack slide rails and any removed screws in the carton kit box (see [Figure 1 on page 3](#)).

Packaging the Server for Moving

1. Place the foam bottom front and back pieces in the open carton so that they sit on opposite ends of the box, as shown:

Figure 3: Foam bottom front and back pieces in carton



2. Lay the film sheet on top of the foam bottom front and back pieces.
3. Place the server in the carton on top of the film sheet and foam bottom pieces so that the server is snugly secured in the carton. Wrap the film sheet around the server.
4. Place the two foam top pieces on top of the server in the carton.
5. Place the carton kit, and the insert, on top of the two foam top pieces in the carton.
6. Seal the carton with shipping tape (not provided).