Scalar i6000 Addendum

Quantum Scalar i6000 User’s Guide Addendum
6-01244-08 Rev A
June 2011

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

COPYRIGHT STATEMENT

TRADEMARK STATEMENT

Quantum, the Quantum logo, DLT, ADIC, DLTtape, the DLTtape logo, SuperLoader, Scalar, StorNext, and DXi are registered trademarks of Quantum Corporation, registered in the U.S. and other countries. Preserving the World's Most Important Data. Yours., Backup. Recovery. Archive. It’s What We Do., the DLT logo, DLTSage, Dynamic Powerdown, FastSense, FlexLink, GoVault, MediaShield, Optyon, Pocket-sized. Well-armored, SDLT, SiteCare, SmartVerify, StorageCare, Super DLTtape, and Vision are trademarks of Quantum. LTO and Ultrium are trademarks of HP, IBM, and Quantum in the U.S. and other countries. All other trademarks are the property of their respective companies. Specifications are subject to change without notice.

OASIS and KMIP are trademarks of OASIS, the open standards consortium where the KMIP specification is owned and developed.

Purpose of this Document

This Addendum provides documentation not included in the currently published the *Scalar i6000 User’s Guide*. This addendum explains new features and provides updates to existing features.

Extended Data Lifecycle Management (EDLM)

Extended Data Lifecycle Management (EDLM) provides data protection and integrity checking by scanning your tape cartridges, providing results, and allowing supported external applications to migrate data off of bad or suspect tapes. EDLM allows you to run manual scans on any tape cartridge in the library at any time, and performs automatic scans according to schedules and policies that you set up.

EDLM is typically used to check the health of data on cartridges in long-term retention (archive or disaster recovery) that are no longer used in normal operations. (Conversely, health information for active cartridges is presented in the Media Integrity and Media Usage reports, which are part of the Advanced Reporting feature.)

Details about EDLM include:

- EDLM is a licensed feature. One license covers the entire library.
- EDLM expands upon and replaces the Media Data Integrity Analysis (MeDIA) feature previously used on the library. The MeDIA feature only included manual media scans. If you previously installed a Media Data Integrity License on the library, you will notice that the name of the license changes to Extended Data Lifecycle Management when you upgrade to version 612Q or later code, and the additional features of EDLM are added. The *Scalar i6000 User’s Guide* section “Running MeDIA Test Reports” will be replaced by Running Manual EDLM Tests on page 21 and Viewing EDLM Test Sessions and Report Details on page 24.
- One library managed partition is required for the media scans. This library managed partition is accessible only by a library administrator. It is not presented to any other applications. The library managed partition is assigned its own dedicated resources and EDLM scanning is executed in the background with no impact to normal tape operations. Cartridges are moved into the EDLM library managed partition and scanned using EDLM-scanning drives residing in the EDLM library managed partition. After being scanned, cartridges are returned to their original locations. See Creating the EDLM Library Managed Partition on page 4.
- Automatic media scanning policies are configured by partition. Each partition can have its own unique set of media scanning and action policies. See Configuring EDLM Policies on Partitions on page 6.
- You need Administrator privileges to use EDLM.

- All types of tape cartridges (data, cleaning, diagnostic, and firmware update tapes) can be scanned manually. However, only data cartridges can be scanned automatically.
- Media scan requests are initiated on a first-come, first-served basis. If no drive resources are available, the requests are queued. Queued tests are reported as "Not Completed" in the test report (see Viewing EDLM Test Sessions and Report Details on page 24).
- You may optionally use supported external applications to trigger media scans and automatically copy data off of suspect or failed tapes. To use external applications you must separately install an API client plug-in. See Configuring Access to External Applications on page 13. For a list of supported external applications and their corresponding plug-ins, see the *Scalar i6000 Release Notes*. As of library code version 612Q, the only supported external application is StorNext® version 3.5 or later with StorNext Storage Manager installed and SNAPI server component version 2.0.1 or later installed.
- In partitions configured for transparent moves, if a cartridge is being scanned and the host initiates a move request, the scan is aborted and the cartridge performs the move. The scan is not rescheduled, but the cartridge will be scanned at the next scheduled time according to the policy. The EDLM report indicates the interruption or cancellation. This ensures that normal operations are not affected by EDLM scanning.

This section covers the following topics:

- Creating the EDLM Library Managed Partition on page 4
- Configuring EDLM Policies on Partitions on page 6
- Configuring Access to External Applications on page 13
- Running Manual EDLM Tests on page 21
- Viewing EDLM Test Sessions and Report Details on page 24
- Viewing EDLM Session Report Details on page 28

Creating the EDLM Library Managed Partition

The EDLM library managed partition is a dedicated partition that you set up in the library for scanning media with EDLM. This partition exists solely for media scanning purposes and is not accessible to hosts or other applications. Tape cartridges are moved into the EDLM library managed partition and scanned using the tape drives residing in the EDLM library managed partition. When the scan is complete, the cartridges are returned to their original partitions.

Details about the EDLM library managed partition include:

- You need an EDLM license installed in order to configure the EDLM library managed partition.
- There can be only one EDLM library managed partition in the library.
- All tape drives in the EDLM library managed partition must be "EDLM-scanning drives" (not standard tape drives) which must be purchased from Quantum. Previously purchased "MeDIA drives" are the same thing and are now known as "EDLM-scanning drives." These EDLM-scanning drives are HP LTO-4 Fibre Channel or HP LTO-5 Fibre Channel tape drives. You can have

both LTO-4 and LTO-5 EDLM-scanning drives in the EDLM library managed partition.

- The EDLM library managed partition can support any number of EDLM-scanning drives (within the normal support of the physical library).
- All of the EDLM scanning drives in the EDLM library managed partition must be connected to a 7404 Fibre Channel I/O blade. The blade must not be connected to a host, nor may it be shared with drives located in another partition. Each 7404 Fibre Channel I/O blade supports up to 4 tape drives. You can use multiple 7404 blades to support the EDLM-scanning drives.
- Tape drives in the EDLM library managed partition will only be used for EDLM scanning purposes.
- All the slots in the library managed partition must be licensed slots.
- The normal library tape drive cleaning policies apply to the tape drives in the library managed partition.
- You can set up EDLM scanning policies on the EDLM library managed partition.

To create the EDLM library managed partition, do the following:

1. Install EDLM-scanning drives in the library.
2. Connect each EDLM-scanning drive to one of the four initiator ports in a dedicated 7404 Fibre Channel I/O blade. Make sure that this Fibre Channel I/O blade is not be connected to a host, and that it only has EDLM-scanning drives connected to it. If you have more than four EDLM-scanning drives, you will need to use more than one dedicated Fibre Channel I/O blade.
3. From the **Setup** menu select **Partitions > Configure**.
4. Click **Create**.
5. In the Partitions - Step 1: Choose Creation Mode dialog box, select **Expert** and click **Next**.
6. In the Partitions - Step 2: Choose Partition Properties dialog box, select the **Library Managed** check box. The name field auto-populates and you cannot change anything else on this screen. Click **Next**.
7. In the Partitions - Step 3: Choose Policy Settings dialog box, click **Next**. You cannot make any changes to this screen.
8. In the Partitions - Step 4: Select Drives dialog box, select the EDLM-scanning drives, and then click **Next**.
9. In the Partitions - Step 5: Select Storage Slots dialog box, select the slots you want to use in this partition and click **Next**.
10. In the Partitions - Step 6: Select I/E Slots, select I/E station slots and click **Next**.
11. In the Partitions - Summary Information screen, review your selections. If OK, click **Create**.
12. When the progress window completes, click **Finish**.

For more information about creating partitions, see the S*calar i6000 User's Guide* or online help.

Configuring EDLM Policies on Partitions

Automatic scanning and other EDLM policies are enabled by partition. You can set up EDLM policies on as many partitions as you want, including the EDLM library managed partition. (Some policies are not available on the EDLM library managed partition; namely, those that require external access to a host application.) You can configure the following types of policies:

Media Scan Candidate Policies	Specifies when to perform automatic scans on media in the partition. See Step 11 on page 8.
Media Scan Type Policies	Specifies which type of automatic scans to perform (quick, normal, or full). See Step 13 on page 11.
Media Scan Results Action Policies	Specifies what actions to take on suspect or failed media. These policies apply to all media in the partition, whether they were scanned manually or automatically. See Step 15 on page 12.

This section describes how to create, modify, and remove EDLM policies on partitions.

Note: Cartridges that are not capable of being read by at least one of the tape drives in the EDLM library managed partition are excluded from all scans. (For example, if the EDLM library managed partition contains only LTO-5 tape drives, then LTO-1 and LTO-2 cartridges will not be scanned.)

1 Log on as an administrator.

2 From the **View** menu, select the physical library.

3 Install the Extended Data Lifecycle Management license on the library.

   Note: If you already have the MeDIA license installed, it will automatically become the Extended Data Lifecycle Management license.

4 Create the EDLM library managed partition (see Creating the EDLM Library Managed Partition on page 4).

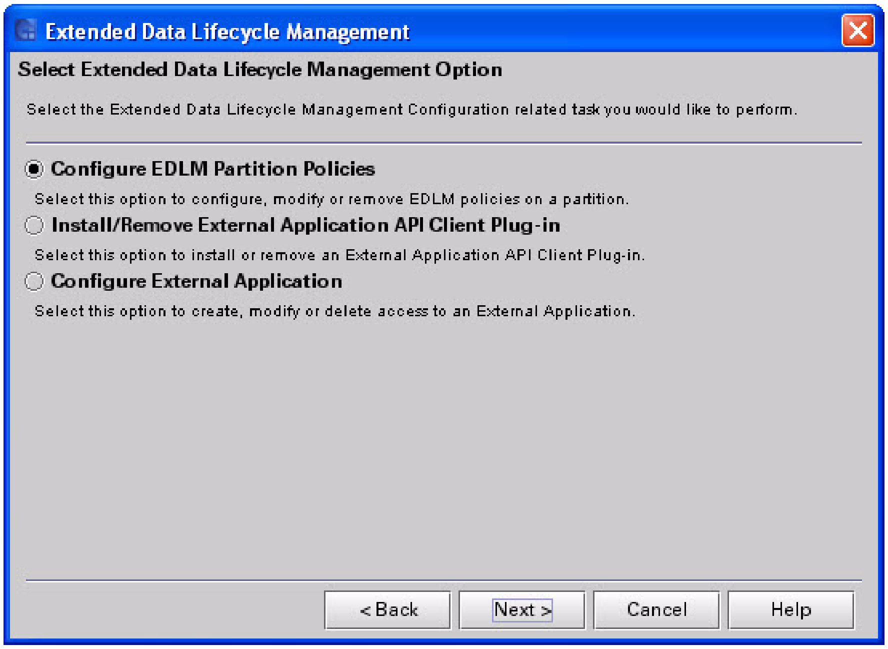
5 If you want to use a supported external application to trigger media scans or to copy data from suspect or failed tapes, you must first install the API client plug-in and configure the library to access the external application (see Configuring Access to External Applications on page 13).

6 Select **Setup > EDLM Configuration**.

   The Extended Data Life Management Configuration Wizard appears.

7 Click **Next**.

The Select Extended Data Life Management Option screen appears.



Extended Data Lifecycle Management

Select Extended Data Lifecycle Management Option

Select the Extended Data Lifecycle Management Configuration related task you would like to perform.

● **Configure EDLM Partition Policies**

Select this option to configure, modify or remove EDLM policies on a partition.

○ **Install/Remove External Application API Client Plug-in**

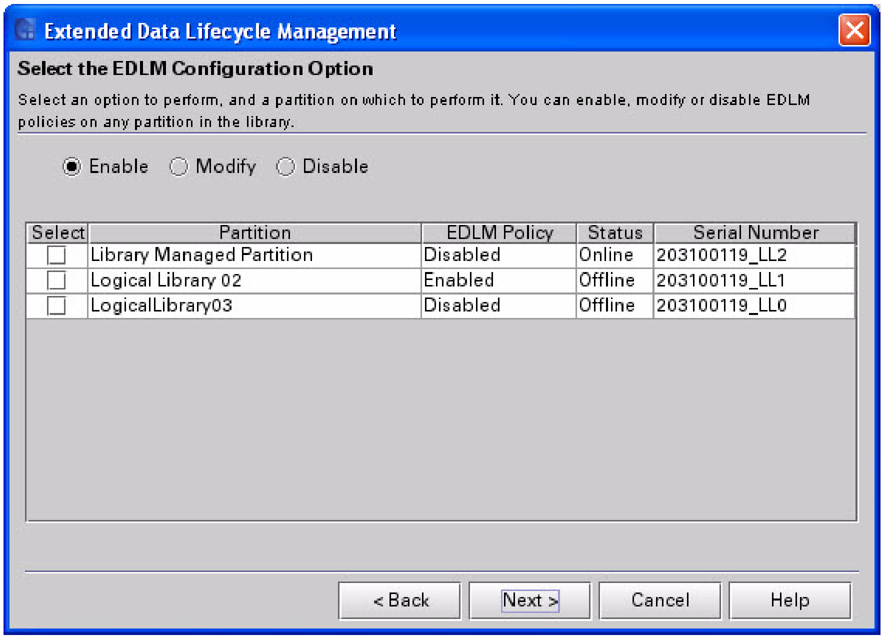
Select this option to install or remove an External Application API Client Plug-in.

○ **Configure External Application**

Select this option to create, modify or delete access to an External Application.

8 Select **Configure EDLM Partition Policies** and click **Next**.

The Select the EDLM Configuration Option screen appears. All of the library's partitions are displayed in a table. The **EDLM Policy** column indicates whether EDLM policies are enabled or disabled on the partition.



Extended Data Lifecycle Management

Select the EDLM Configuration Option

Select an option to perform, and a partition on which to perform it. You can enable, modify or disable EDLM policies on any partition in the library.

● Enable ○ Modify ○ Disable

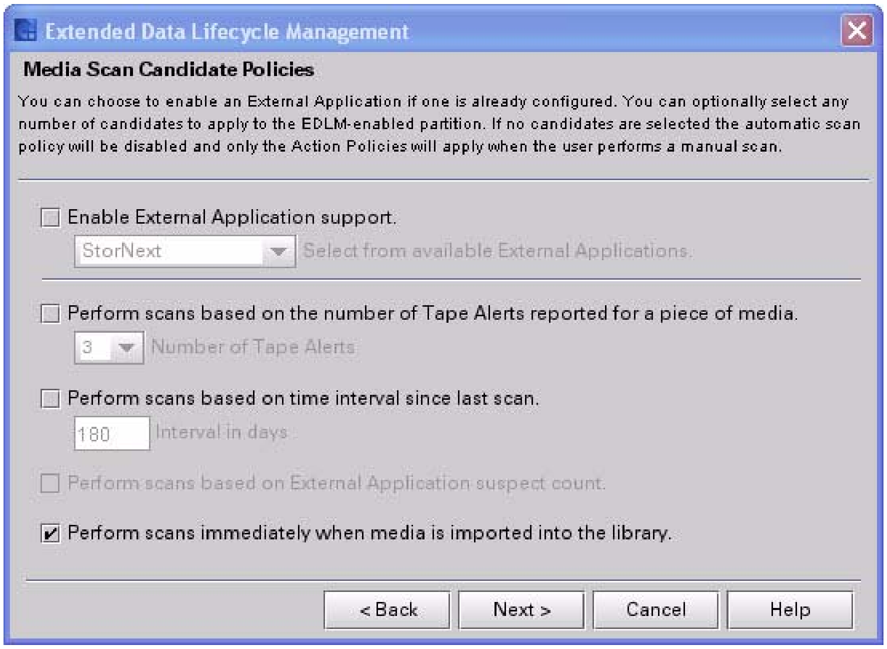
Select	Partition	EDLM Policy	Status	Serial Number
□	Library Managed Partition	Disabled	Online	203100119_LL2
□	Logical Library 02	Enabled	Offline	203100119_LL1
□	LogicalLibrary03	Disabled	Offline	203100119_LL0

9 Create, modify, or remove policies on a partition by doing one of the following:

To...	Do this...
Enable EDLM policies on a partition	**1** Select **Enable**. **2** Select a partition from the table that has EDLM policies disabled. **3** Proceed to Step 10.
Modify existing EDLM policies on a partition	**1** Select **Modify**. **2** Select a partition from the table that has EDLM policies enabled. **3** Proceed to Step 10.
Disable EDLM policies on a partition	**1** Select **Disable**. **2** Select a partition from the table that has EDLM policies enabled. **3** Click **Finish**. A confirmation dialog box appears asking you to confirm you want to disable the EDLM policies on the partition. **4** Click **Yes** to confirm. A "success" dialog box appears. **5** Click **OK** to close the dialog box. Process is complete.

10 Click **Next**.

The EDLM Media Scan Candidate Policies screen appears.



Media Scan Candidate Policies

You can choose to enable an External Application if one is already configured. You can optionally select any number of candidates to apply to the EDLM-enabled partition. If no candidates are selected the automatic scan policy will be disabled and only the Action Policies will apply when the user performs a manual scan.

□ Enable External Application support.

StorNext — Select from available External Applications.

□ Perform scans based on the number of Tape Alerts reported for a piece of media.

3 — Number of Tape Alerts

□ Perform scans based on time interval since last scan.

180 — Interval in days

□ Perform scans based on External Application suspect count.

☑ Perform scans immediately when media is imported into the library.

11 Select as many media scan candidate policies as you wish. The policies apply to all tape cartridges in the partition. Depending on your library and partition configuration, some of the options listed below may not be available.

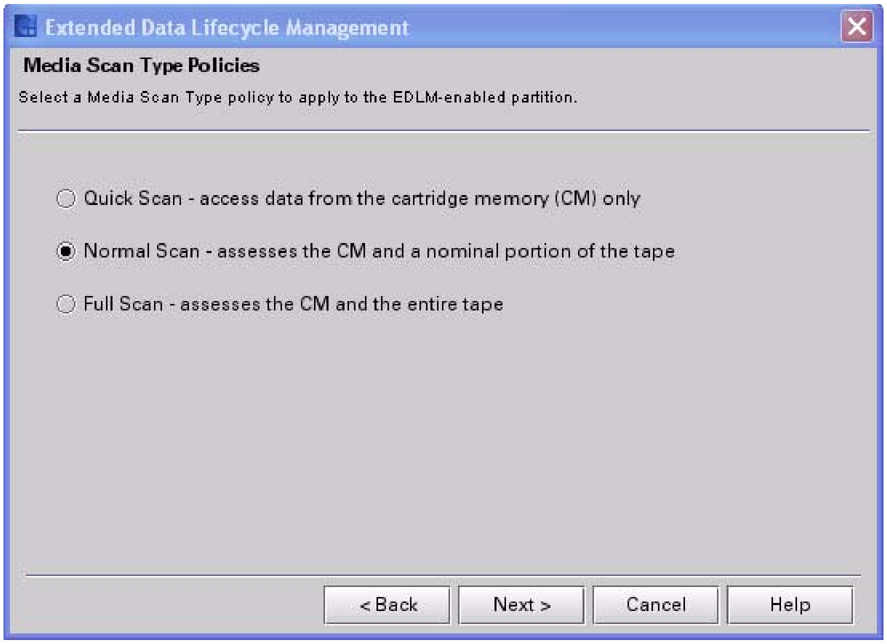
Note: You may select zero scan candidate policies by clearing all of the check boxes. This means no automatic scans will be performed on this partition. You might wish to do this to temporarily halt automatic scans on media in the partition but keep your policy drop-down list selections intact so that you can re-enable them later. You can still perform manual scans on tapes residing in the partition, and media scan action results policies (Step 15 on page 12) will remain in effect.

Media Scan Candidate Policy	Description
Enable External Application support	Allows you to use a supported external application to perform corrective action and trigger media scans. Once you enable this policy, you will be able to configure the following options: • Perform scans based on External Application suspect count. on page 10 • Request Media Copy by External Application on page 13 In order to select this policy, access to an external application must be configured (see Configuring Access to External Applications on page 13). Choose the desired external application from the drop-down list. This policy is disabled by default. This policy is not available on the EDLM library managed partition.
Perform scans based on the number of Tape Alerts reported for a piece of media.	Scans a tape if the number of Tape Alerts reported for that cartridge exceeds the specified value. From the drop-down list, select the number of Tape Alerts. The Tape Alerts included in the count are: • 01h (1)– Read Warning • 03h (3) – Hard Error • 04h (4) – Media • 05h (5) – Read Failure • 06h (6) – Write Failure • 12h (18) – Tape Directory Corrupted on Load • 33h (51) – Tape Directory Invalid on Unload • 34h (52) – Tape System Area Write Error • 35h (53) – Tape System Area Read Error • 37h (55) – Loading Failure • 3Bh (59) – WORM Medium Integrity Check Failed This policy is disabled by default. The default number of Tape Alerts is 3. This policy is not available on the EDLM library managed partition.

Media Scan Candidate Policy	Description
Perform scans based on time interval since last scan.	Scans a tape if the time interval since the last scan was performed has been exceeded. In the text box, type a time interval (in days) after which a scan will be performed. **Note:** When deciding on the interval, consider the number of tapes to be scanned in the entire library, as well as the type of scan to be performed. Full scans can take more than 2 hours on full tapes. Over-scheduling can cause delays or tapes not to be scanned as intended. This policy is disabled by default. The default interval is 180 days.
Perform scans based on External Application suspect count.	A suspect count is a means by which an external application determines when to stop writing data to tape. If you select this policy, a tape will be queued for EDLM testing when its suspect count threshold is reached. If the EDLM test indicates the tape is good, you can reset the suspect count on the external application and continue to use the tape. For more information on suspect counts and resetting suspect counts, refer to your external application's documentation. This policy is disabled by default. You can only select this policy if **Enable External Application support** is also selected (see Enable External Application support on page 9), and if the external application supports suspect counts,.
Perform scans immediately when media is imported into the library.	Scans a tape cartridge as soon as it is imported into the partition.

12 Click **Next**.

The EDLM Media Scan Type Policies screen appears.



Media Scan Type Policies

Select a Media Scan Type policy to apply to the EDLM-enabled partition.

○ Quick Scan - access data from the cartridge memory (CM) only

● Normal Scan - assesses the CM and a nominal portion of the tape

○ Full Scan - assesses the CM and the entire tape

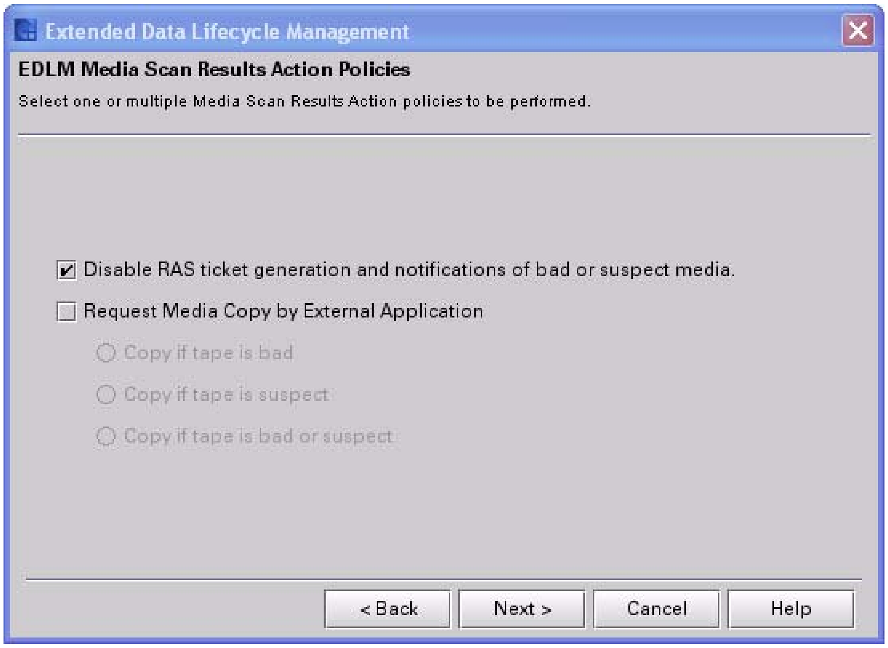
13 Select a media scan type policy.

Note: When deciding on a scan type policy, consider how the tapes are being used. Depending on the number of EDLM drives and the scan type policy you choose, scans can take a very long time to complete, and may overlap the next scheduled scan.

Media Scan Type Policy	Description
Quick Scan	Does not scan the tape. Evaluates data from the cartridge memory (CM) only. A quick scan takes less than one minute per tape. **Examples of when to use a quick scan:** • When you first import previously used scratch tapes into the library. • When you import data cartridges that have been used in other backup and archival environments and need to do a quick check to determine whether the tape cartridge is nearing end of life, at end of life, or may have had issues reading or writing.
Normal Scan (default)	Evaluates the cartridge memory (CM) and scans selected portions of the tape, focusing on areas most likely to indicate problems. A normal scan can take 20 minutes per tape. **Examples of when to use a normal scan:** • For tapes in frequent use within the library, with scanning triggered by drive-reported media Tape Alert events. • For tapes in frequent use within the library, with scanning being performed at regular time intervals.
Full Scan	Evaluates the cartridge memory (CM) and scans the entire tape. A full scan can take more than 2 hours on a full tape. **Example of when to use a full scan:** • When tape cartridges are accessed infrequently and are used primarily for onsite or offsite long-term data retention. • When tape cartridges with valuable data are introduced into the library and the state and condition of the tapes are unknown.

14 Click **Next**.

The EDLM Media Scan Results Action Policies screen appears.



Extended Data Lifecycle Management

EDLM Media Scan Results Action Policies

Select one or multiple Media Scan Results Action policies to be performed.

☑ Disable RAS ticket generation and notifications of bad or suspect media.

□ Request Media Copy by External Application

○ Copy if tape is bad

○ Copy if tape is suspect

○ Copy if tape is bad or suspect

15 Select one or more of the following media scan results action policies to be performed when media is suspect or failed.

Note: These action policies apply to all tapes scanned in this partition, whether they are scanned manually or automatically.

Media Scan Results Action Policy	Description
Disable RAS ticket generation and notifications of suspect and failed scan results.	Select this option if you do not wish to receive RAS tickets and e-mail notifications of suspect and failed scan results. RAS ticket generation is disabled by default.

Media Scan Results Action Policy	Description
Request Media Copy by External Application • Copy if scan failed (default) • Copy if scan was suspect • Copy if failed or suspect	Automatically requests a supported external application to copy all data from a suspect and/or failed tape to another tape. Once you enable this policy, you can select whether to copy failed tapes, suspect tapes, or both. A RAS ticket will be generated for each request to copy data indicating whether the request succeeds or fails. You can only select this option if a supported external application is enabled for use with EDLM on this partition (see Enable External Application support on page 9). In order for this feature to work, the partition must contain at least two tape drives (one for the suspect/failed tape from which you are copying data and one for the good tape to which you are copying data).

16 Click **Next**.

The EDLM Configuration Summary screen appears.The screen displays all of your choices.

17 Click **Finish** to apply your settings, or use the **Back** button to make changes.

A "success" dialog box appears.

18 Click **OK** to close the dialog box.

Configuring Access to External Applications

If a supported external application is managing your partition, you can use the external application with EDLM to automatically copy data off of bad or suspect tapes or to trigger media scans.

Configuring the library to use an external application is a four-part process:

1 Step 1 – Confirming the External Application is Supported on page 13

2 Step 2 – Installing the Scalar i6000 API Client Plug-in on page 14

3 Step 3 – Configuring External Application Access on page 16

4 Step 4 – Enabling the External Application for Use in EDLM Partition Policies on page 19

Step 1 – Confirming the External Application is Supported

Confirm that the **external application** managing your partition is supported by EDLM.

Note: See the release notes for a list of supported external applications. Currently the library supports only StorNext version 3.5 or later with StorNext Storage Manager installed and SNAPI server component version 2.0.1 and later installed.

Step 2 – Installing the Scalar i6000 API Client Plug-in

The application programming interface (API) client plug-in is a Quantum-provided plug-in that allows the library to communicate with a supported external application (such as StorNext Storage Manager). The API client plug-in must be installed before you can configure library access to the external application. You can install as many API client plug-ins as necessary.

Note: See the release notes for a list of supported API client plug-ins and which external applications they correspond to. Currently the library supports only SNAPI Client Plug-in version 2.0.1.

Note: If you install an API client plug-in that has the same **Name-Version** of an already installed plug-in but is at a different **Revision**, the newly installed plug-in will replace the existing plug-in. (The screen shot in Step 10 on page 16 shows the difference between version and revision.)

1 Download the API client plug-in bundle from the following Web site.

http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/S6K/Index.aspx

The plug-in bundle is a .zip file containing the following files:

- Client plug-in
- End User/Open Source License Agreement

2 Extract the files from the .zip file.

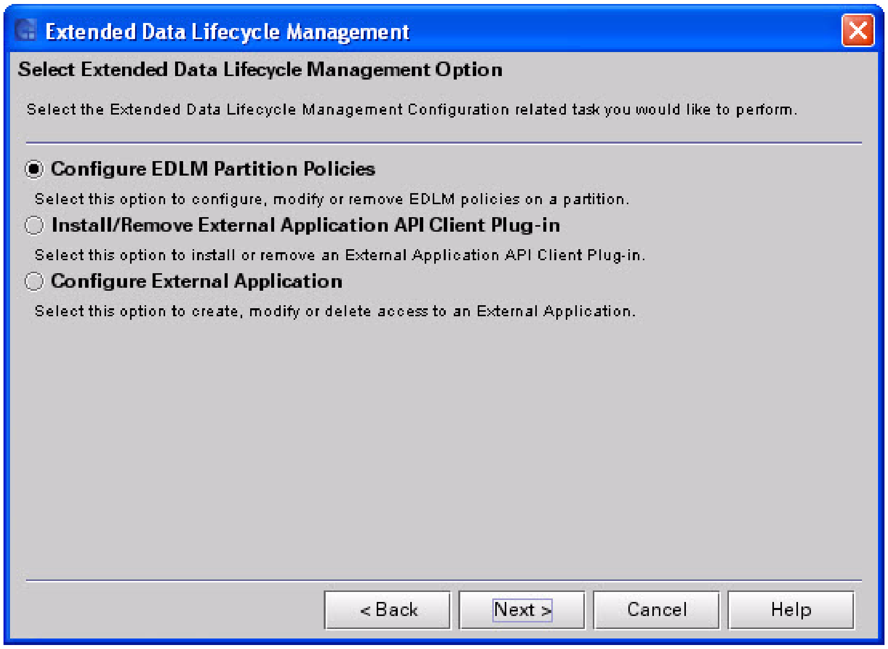
3 Read the End User/Open Source License Agreement. Installation of the plug-in implies acceptance of the license agreement.

4 Select **Setup > EDLM Configuration**.

The Extended Data Life Management Configuration Wizard appears.

5 Click **Next**.

The Select Extended Data Life Management Option screen appears.



Extended Data Lifecycle Management

Select Extended Data Lifecycle Management Option

Select the Extended Data Lifecycle Management Configuration related task you would like to perform.

● Configure EDLM Partition Policies

Select this option to configure, modify or remove EDLM policies on a partition.

○ Install/Remove External Application API Client Plug-in

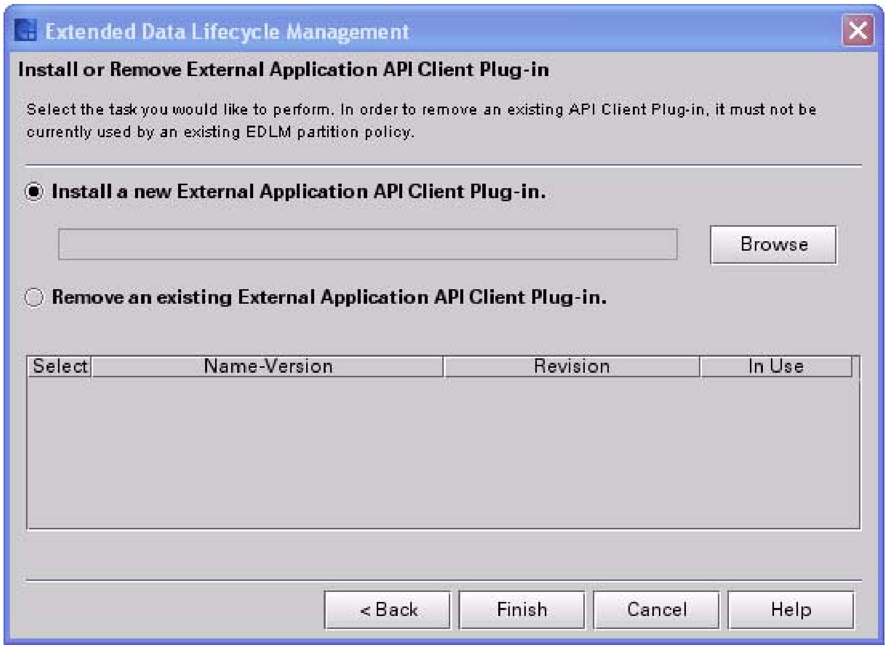
Select this option to install or remove an External Application API Client Plug-in.

○ Configure External Application

Select this option to create, modify or delete access to an External Application.

6 Select **Install/Remove External Application API Client Plug-in** and click **Next**.

The Install or Remove External Application API Client Plug-in screen appears.



Extended Data Lifecycle Management

Install or Remove External Application API Client Plug-in

Select the task you would like to perform. In order to remove an existing API Client Plug-in, it must not be currently used by an existing EDLM partition policy.

● Install a new External Application API Client Plug-in.

○ Remove an existing External Application API Client Plug-in.

Select	Name-Version	Revision	In Use

7 Select **Install a new External Application API Client Plug-in.**

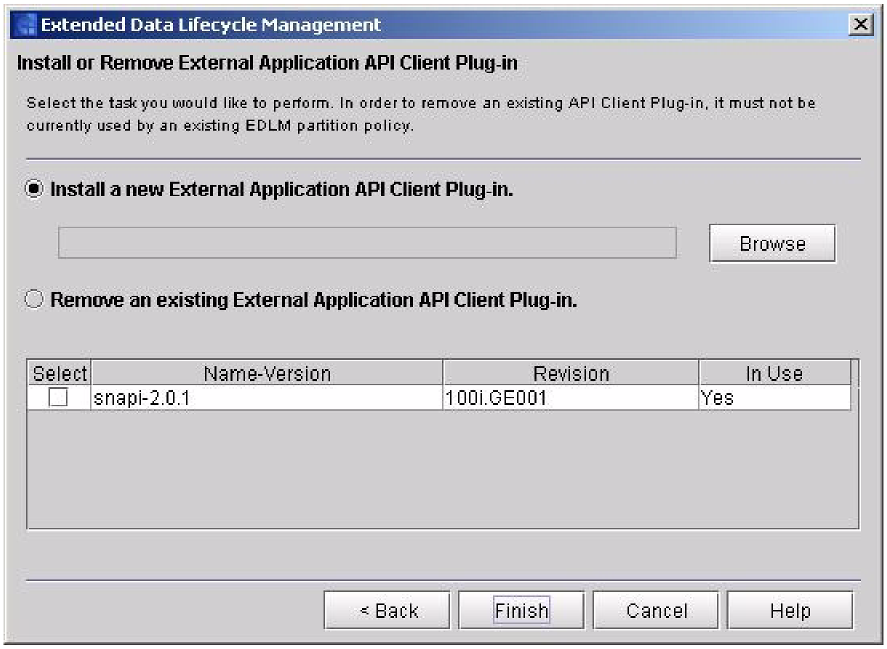
8 Click **Browse** to retrieve the plug-in file.

9 Click **Finish**.

The plug-in is installed or removed. A "success" dialog box appears.

10 Click **OK** to close the dialog box.

The installed plug-in appears on the Install or Remove External Application API Client Plug-in screen.



Install or Remove External Application API Client Plug-in

Select the task you would like to perform. In order to remove an existing API Client Plug-in, it must not be currently used by an existing EDLM partition policy.

● Install a new External Application API Client Plug-in.

○ Remove an existing External Application API Client Plug-in.

Select	Name-Version	Revision	In Use
□	snapi-2.0.1	100i.GE001	Yes

11 To remove an installed plug-in, do the following:

Note: To remove an external application API client plug-in, it must not currently be used by an existing EDLM partition policy.

a Select **Remove an existing External Application API Client Plug-in**.

b Select the plug-in(s) to remove from the list displayed in the table.

c Click **Finish**.

A confirmation dialog box appears.

d Click **Yes** to confirm you want to remove the plug-in.

12 You can now proceed to Configuring Access to External Applications on page 13.

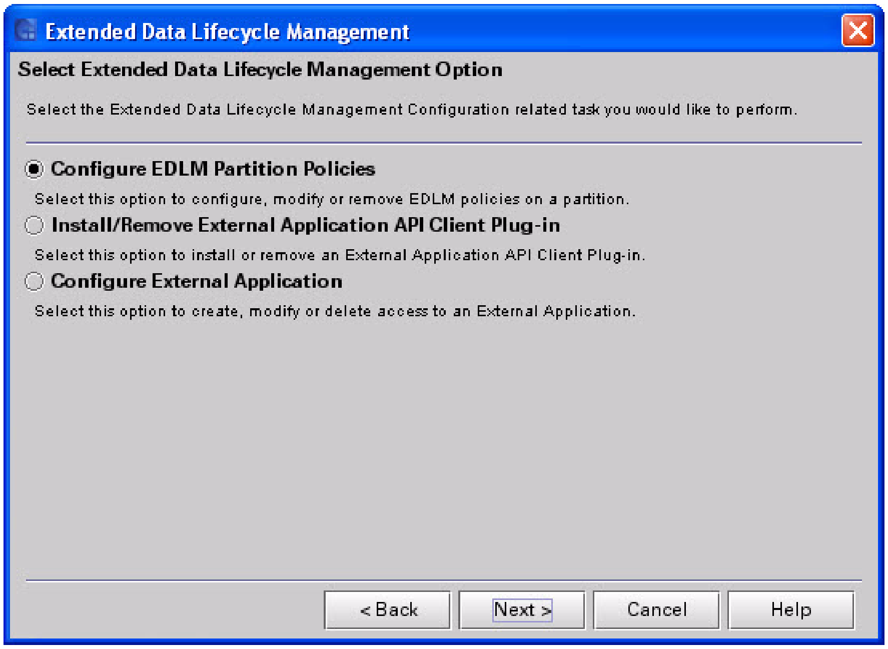
Step 3 – Configuring External Application Access

1 Select **Setup > EDLM Configuration**.

The Extended Data Life Management Configuration Wizard appears.

2 Click **Next**.

The Select Extended Data Life Management Option screen appears.



Extended Data Lifecycle Management

Select Extended Data Lifecycle Management Option

Select the Extended Data Lifecycle Management Configuration related task you would like to perform.

● **Configure EDLM Partition Policies**

Select this option to configure, modify or remove EDLM policies on a partition.

○ **Install/Remove External Application API Client Plug-in**

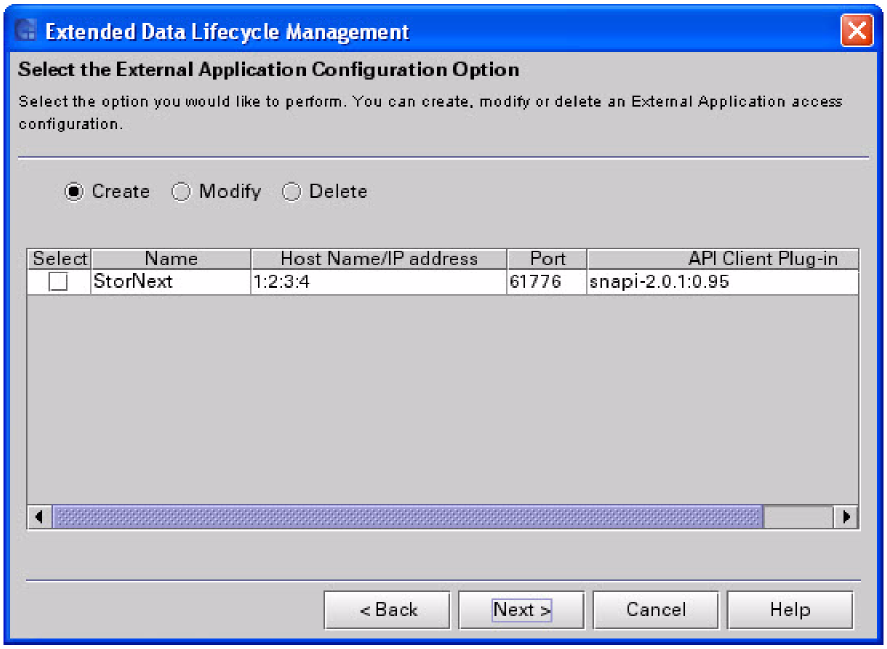
Select this option to install or remove an External Application API Client Plug-in.

○ **Configure External Application**

Select this option to create, modify or delete access to an External Application.

3 Select **Configure External Application** and click **Next**.

The Select the External Application Configuration Option screen appears.



Extended Data Lifecycle Management

Select the External Application Configuration Option

Select the option you would like to perform. You can create, modify or delete an External Application access configuration.

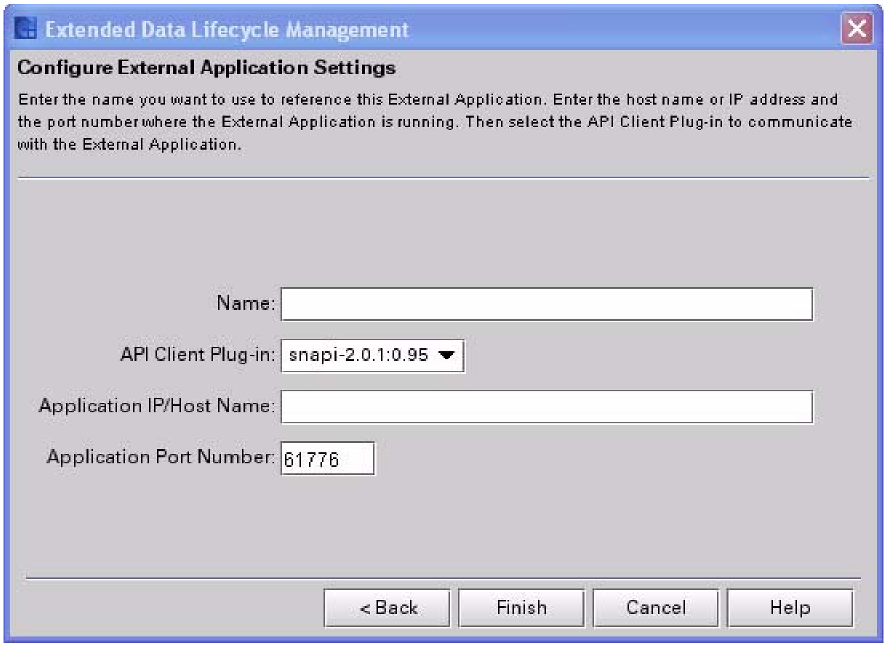
● Create ○ Modify ○ Delete

Select	Name	Host Name/IP address	Port	API Client Plug-in
□	StorNext	1:2:3:4	61776	snapi-2.0.1:0.95

4 Do one of the following:

To...	**Do this...**
Add a new external application	**1** Select **Create**. **2** Click **Next.**
Modify an existing external application	**1** Select **Modify.** **2** Select the application you want to modify from the table. **3** Click **Next**.
Delete an existing external application	**1** Select **Delete.** **2** Select the application you want to delete from the table. **3** Click **Finish**. A confirmation dialog appears. **4** Click **Yes** to confirm you want to delete the application. **5** Click **OK**. **6** Process is complete.

If you are creating or modifying, the Configure External Application Settings screen appears.



Extended Data Lifecycle Management

Configure External Application Settings

Enter the name you want to use to reference this External Application. Enter the host name or IP address and the port number where the External Application is running. Then select the API Client Plug-in to communicate with the External Application.

Name:

API Client Plug-in: snapi-2.0.1:0.95

Application IP/Host Name:

Application Port Number: 61776

5 If you are creating or modifying, configure the following the fields:

Field	Description
Name	Type a descriptive name you will use to identify the external application.
API Client Plug-in	Select the appropriate API client plug-in from the drop-down list. The list contains the API client plug-ins you installed in Step 2 – Installing the Scalar i6000 API Client Plug-in on page 14.
Application IP/Host Name	Type the IP address or DNS host name (if DNS is configured) of the external application server. **Note:** To use a host name, DNS must be configured on the LMC (**Setup > DNS Configuration**).
Application Port Number	Accept the default or type an external application host server port number.

6 Click **Finish**.

A “success” dialog box appears.

Caution: You may get an error dialog box that says, “Failed to validate the External Application.” This may mean that the IP address or host name is incorrect, or the server is not responding or not configured. The library will accept the settings you entered, but you should double-check that all the information is correct and modify it if necessary. If any of the configured information is incorrect, successful communication will not occur.

7 Click **OK** to close the dialog box.

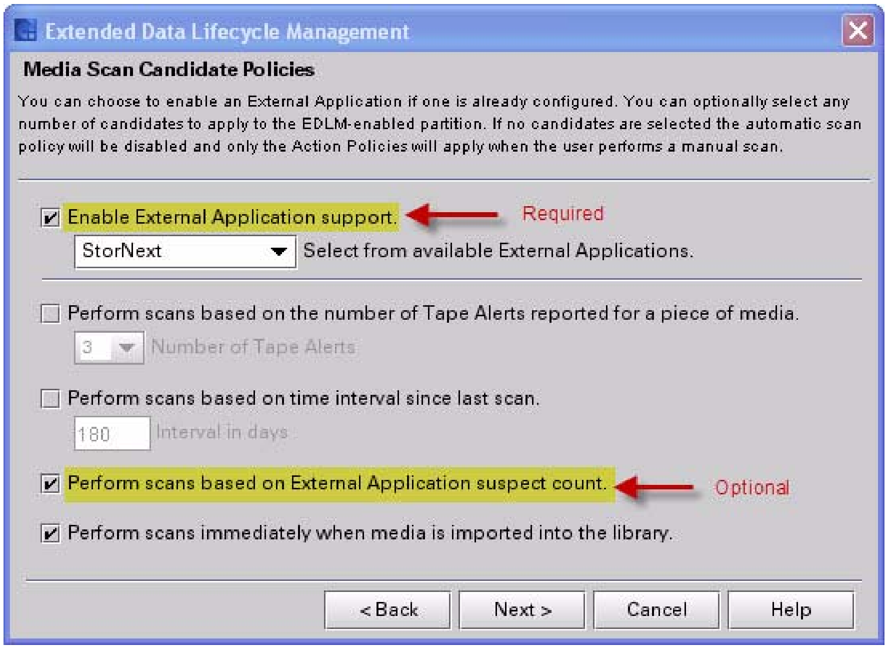
Step 4 – Enabling the External Application for Use in EDLM Partition Policies

To enable the external application for use in one or more EDLM partition policies, you need to make a few selections as shown below. You will do this when you are configuring EDLM policies on a partition (see Configuring EDLM Policies on Partitions on page 6 for complete instructions).

1 From the Media Scan Candidate Policies screen:

- Select **Enable External Application**. This will allow you to configure the policies relating to the external application. For more information, see Enable External Application support on page 9.

- Optionally, select **Perform scans based on External Application suspect count**. For more information, see Perform scans based on the number of Tape Alerts reported for a piece of media. on page 9.



Media Scan Candidate Policies

You can choose to enable an External Application if one is already configured. You can optionally select any number of candidates to apply to the EDLM-enabled partition. If no candidates are selected the automatic scan policy will be disabled and only the Action Policies will apply when the user performs a manual scan.

☑ Enable External Application support.

StorNext ▾ Select from available External Applications.

□ Perform scans based on the number of Tape Alerts reported for a piece of media.

3 ▾ Number of Tape Alerts

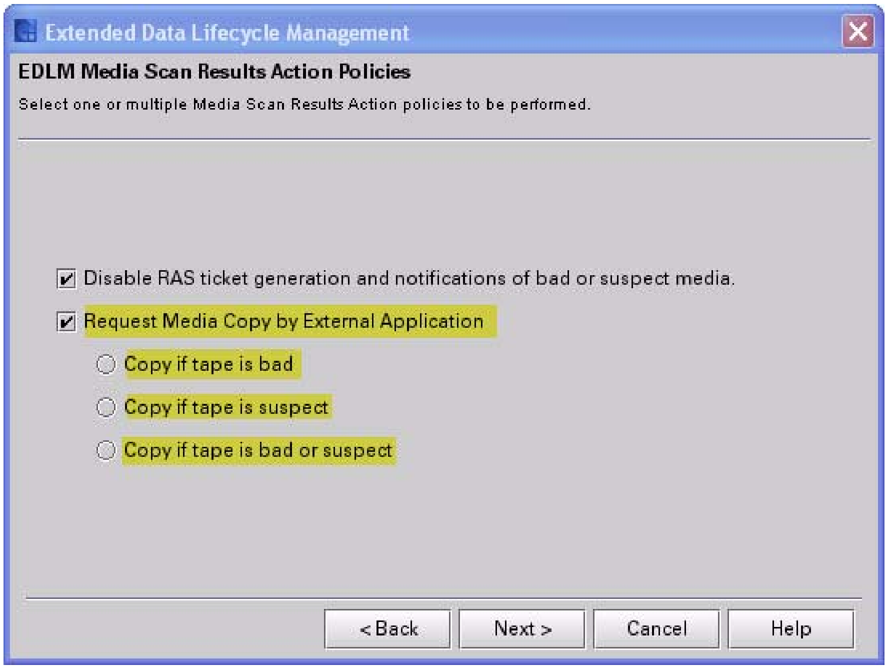
□ Perform scans based on time interval since last scan.

180 Interval in days

☑ Perform scans based on External Application suspect count.

☑ Perform scans immediately when media is imported into the library.

2 From the EDLM Media Scan Results Action Policies screen, you may optionally select **Request Media Copy on External Application**. For more information, see Request Media Copy by External Application on page 13.



EDLM Media Scan Results Action Policies

Select one or multiple Media Scan Results Action policies to be performed.

☑ Disable RAS ticket generation and notifications of bad or suspect media.

☑ Request Media Copy by External Application

○ Copy if tape is bad

○ Copy if tape is suspect

○ Copy if tape is bad or suspect

Running Manual EDLM Tests

This section replaces the current “Running MeDIA Test Reports” in the *Scalar i6000 User’s Guide*.

You may wish to evaluate media outside of the automatic scanning policies described in the sections above. You can manually scan any tape cartridge in the library at any time. The tape cartridge can be located in any partition, including the EDLM library managed partition.

Requirements for running manual tests are as follows:

- An EDLM license must be installed on the library.
- The EDLM library managed partition must be configured on the library (see Creating the EDLM Library Managed Partition on page 4).
- The tape cartridge you want to scan must be readable by a tape drive in the EDLM library managed partition.

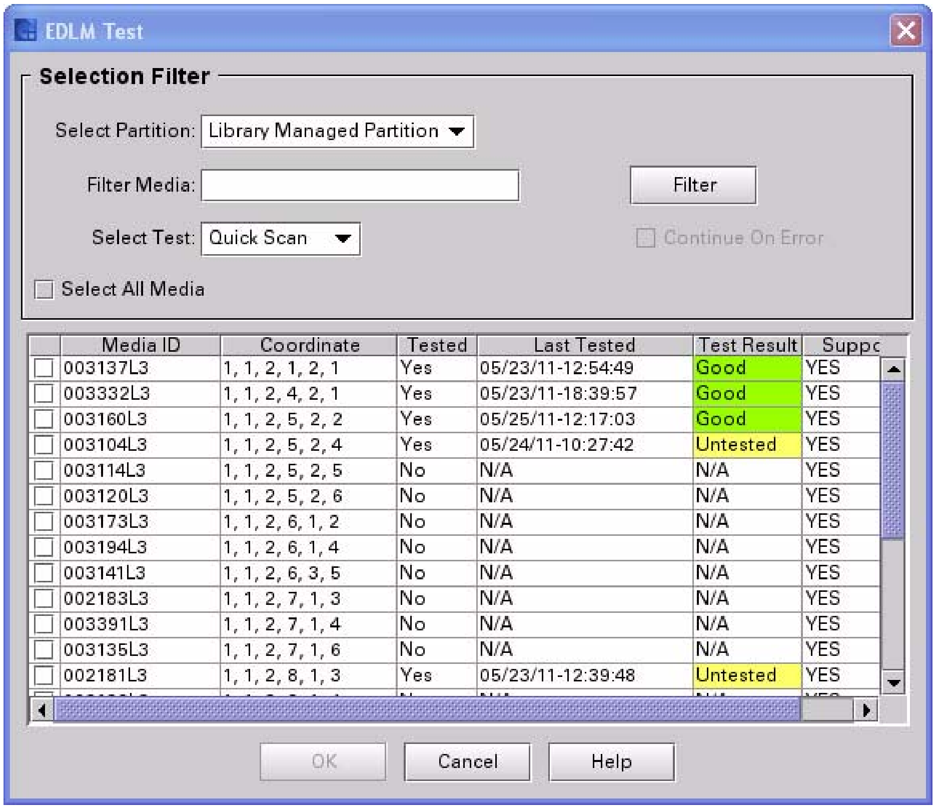
To run a manual EDLM test, do the following:

1 Log on as an administrator.

2 From the **View** menu, select the physical library or a partition on which EDLM policies are enabled.

3 From the main menu, select **Tools > EDLM Tests > Test Selection**.

The EDLM Test screen appears.



Select Partition: Library Managed Partition

Filter Media:

Select Test: Quick Scan

□ Continue On Error

□ Select All Media

	Media ID	Coordinate	Tested	Last Tested	Test Result	Suppc
□	003137L3	1, 1, 2, 1, 2, 1	Yes	05/23/11-12:54:49	Good	YES
□	003332L3	1, 1, 2, 4, 2, 1	Yes	05/23/11-18:39:57	Good	YES
□	003160L3	1, 1, 2, 5, 2, 2	Yes	05/25/11-12:17:03	Good	YES
□	003104L3	1, 1, 2, 5, 2, 4	Yes	05/24/11-10:27:42	Untested	YES
□	003114L3	1, 1, 2, 5, 2, 5	No	N/A	N/A	YES
□	003120L3	1, 1, 2, 5, 2, 6	No	N/A	N/A	YES
□	003173L3	1, 1, 2, 6, 1, 2	No	N/A	N/A	YES
□	003194L3	1, 1, 2, 6, 1, 4	No	N/A	N/A	YES
□	003141L3	1, 1, 2, 6, 3, 5	No	N/A	N/A	YES
□	002183L3	1, 1, 2, 7, 1, 3	No	N/A	N/A	YES
□	003391L3	1, 1, 2, 7, 1, 4	No	N/A	N/A	YES
□	003135L3	1, 1, 2, 7, 1, 6	No	N/A	N/A	YES
□	002181L3	1, 1, 2, 8, 1, 3	Yes	05/23/11-12:39:48	Untested	YES

4 From the **Select Partition** drop-down list, select the partition that contains the media you want to test.

5 To filter the displayed list of media, in the **Filter Media** field, type the desired Media ID (barcode label), or a portion of a Media ID, and click **Filter**. If you choose not to filter the list, skip this step.

6 From the **Select Test** drop-down menu, select the type of test you want to run.

Note: When deciding on the type of test to run, consider how the tapes are being used. Depending on the number of EDLM drives and the test type you choose, scans can take a very long time to complete.

Type of Test	Description
Quick Scan	Does not scan the tape. Evaluates data from the cartridge memory (CM) only. A quick scan takes less than one minute per tape. **Examples of when to use a quick scan:** • When you first import previously used scratch tapes into the library. • When you import data cartridges that have been used in other backup and archival environments and need to do a quick check to determine whether the tape cartridge is nearing end of life, at end of life, or may have had issues reading or writing.
Normal Scan (default)	Evaluates the cartridge memory (CM) and scans selected portions of the tape, focusing on areas most likely to indicate problems. A normal scan can take 20 minutes per tape. **Examples of when to use a normal scan:** • For tapes in frequent use within the library, with scanning triggered by drive-reported media Tape Alert events. • For tapes in frequent use within the library, with scanning being performed at regular time intervals.
Full Scan	Evaluates the cartridge memory (CM) and scans the entire tape. A full scan can take more than 2 hours on a full tape. **Example of when to use a full scan:** • When tape cartridges are accessed infrequently and are used primarily for onsite or offsite long-term data retention. • When tape cartridges with valuable data are introduced into the library and the state and condition of the tapes are unknown.

7 If desired, select the **Continue On Error** check box. You can select this check box for a **Normal Scan** or **Full Scan**. If this option is selected, the test scans the tape even if the cartridge memory (CM) test fails. If this check box is not selected, the test will not scan the tape if the CM test fails.

8 Select the check box for each tape you want to scan. To select all media listed, select the **Select All Media** check box.

Note: You can sort the media list by clicking any of the column headers. An arrow appears in the column header indicating whether the column is sorted in ascending or descending order. Click the column header again to toggle between ascending and descending order.

Note: You cannot select unsupported media.

The media selection table contains the following information:

Item	Description
Media ID	The media barcode.
Coordinate	Where the cartridge is located within the library.
Tested	Indicates whether the media has already been tested (Yes/No), or if the media is currently part of a test session that has not yet completed (Pending; cell is highlighted in yellow).
Last Tested	The date the media was last tested.
Test Result	The last test result for the media. Test results include the following: • **Good** — The tape is good. • **Bad** — The tape is bad. • **Suspect** — The tape is possibly unreliable or defective. • **Untested** — The tape could not be fully scanned, for various reasons, including: incompatible or unknown media type; tape could not be loaded; tape is encrypted but the data encryption key could not be obtained; drive not communicating with I/O blade, test was stopped. **Note:** Untested media do not initiate RAS tickets or EDLM media action policies (such as copying data from a bad or suspect tape). • **Not Completed** — The test has not completed yet.
Supported	Indicates whether the media is a supported media type (Yes/No) (meaning, it can be read by at least one of the drives in the EDLM library managed partition). For example, an LTO1 tape cannot be read by an LTO4 drive. Unsupported media cannot be selected for testing.

9 Click **OK** to start the scan.

The message **EDLM Tests have started successfully...** appears.

Note: Media scan requests are initiated on a first-come, first-served basis. If no drive resources are available, the requests are queued.

10 Click **OK** to close the message.

11 To retrieve results, go to **Tools > EDLM Tests > Test Results**. See Viewing EDLM Test Sessions and Report Details on page 24.

Viewing EDLM Test Sessions and Report Details

You can view the status of all your EDLM test sessions, including sessions that are queued but not started yet, in the EDLM Test Sessions List screen. You can stop, pause, resume, or delete test sessions. See Working with the EDLM Test Sessions List on page 24.

Each entry in the EDLM Test Sessions List screen presents an overview of a single EDLM test session. A test session includes all tapes in the library that were scheduled to be scanned at a particular point in time. Thus, a test session can include multiple tapes from different partitions.

- **Example 1:** You select 10 tapes on which to perform a manual scan. The test session includes 10 tapes.
- **Example 2:** Partition A has an automatic scan policy to scan tapes on import. You import a tape. Meanwhile, Partition B has an automatic scan policy to scan every 180 days. Ten tapes in that partition have reached the 180-day mark at the same time that you import the tape into Partition A. Because these automatic scans occur at the same time, the test session includes all 11 tapes from both partitions.

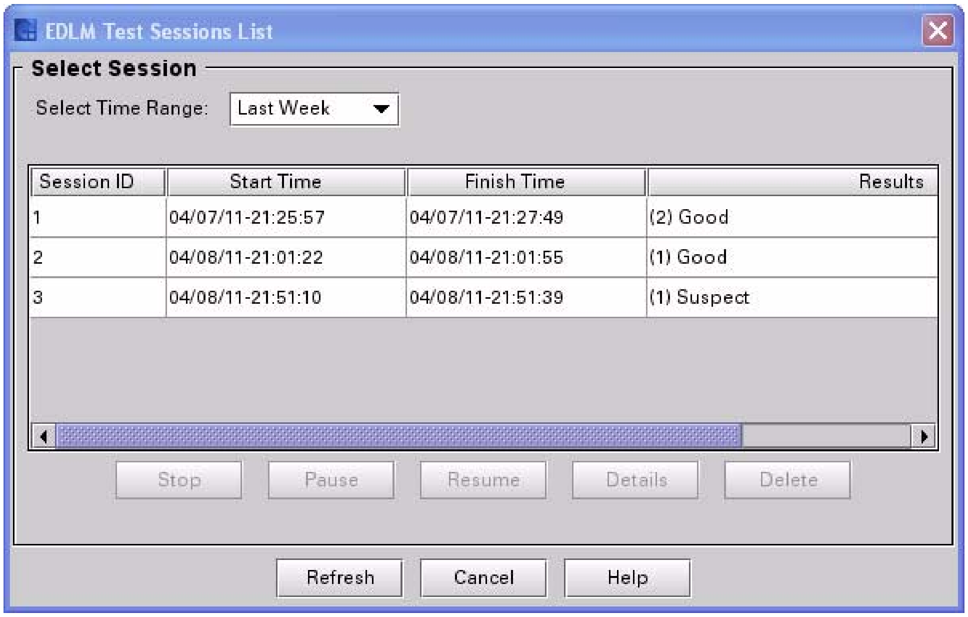
Within each test session, you view details about each tape that was scanned (see Viewing EDLM Session Report Details on page 28).

Working with the EDLM Test Sessions List

To view the status of EDLM test sessions (both automatic and manual), do the following:

1 From the menu, select **Tools > EDLM Tests > Test Results**.

The EDLM Test Sessions List dialog box appears.



Select Time Range: Last Week

Session ID	Start Time	Finish Time	Results
1	04/07/11-21:25:57	04/07/11-21:27:49	(2) Good
2	04/08/11-21:01:22	04/08/11-21:01:55	(1) Good
3	04/08/11-21:51:10	04/08/11-21:51:39	(1) Suspect

The EDLM Test Sessions List displays the set of media tests that have run based on the time range selected. Each row in the table presents an overview of a single EDLM test session.

You can sort the list by clicking any of the column headers. An arrow appears in the column header indicating whether the column is sorted in ascending or descending order. Click the column header again to toggle between ascending and descending order.

The table displays the following information about the test sessions:

Item	Description
Session ID	The session identifier, a unique number assigned to each test session that was run.
Start Time	The date and time the test session was started.
Finish Time	The date and time the test session completed. If the test session has not yet completed, “In Progress” displays. If the test session was paused, “Paused” displays.
Results	A summary of results for all media tested in the session. The reported values include the number of tapes scanned (in parentheses) for each result obtained. **Note:** To view results for individual tapes in the session, click a test session row to highlight it, and then click the **Details** button. Results are the following: • **Good** — The tape is good. • **Bad** — The tape is bad. • **Suspect** — The tape is possibly unreliable or defective. • **Untested** — The tape could not be fully scanned, for various reasons, including: incompatible or unknown media type; tape could not be loaded; tape is encrypted but the data encryption key could not be obtained; drive not communicating with I/O blade, test was stopped. **Note:** Untested media do not initiate RAS tickets or EDLM media action policies (such as copying data from a bad or suspect tape). • **Not Completed** — The test has not completed yet.

2 In the **Select Time Range** field, select the range of time for test sessions that you want displayed. The time range is based on the start time of the test session. Choose one of the following:

- **Last Week** — Test sessions that were run in the last seven days.
- **Last Month** — Test sessions that were run in the last month.
- **Last 3 Months** — Test sessions that were run in the last three months.
- **Last 6 Months** — Test sessions that were run in the last six months.
- **All** — All test sessions that were run on the library. The storage limit is 50,000 media scans. When the limit is reached, old scan results are deleted as new scan results are added.

3 To work with a session, click the test session row to highlight it, and then click your desired option:

Option	Description
Stop	Stops a currently running test session. Once stopped, you cannot restart the test. Any test results collected so far are listed. Tapes that did not complete testing as a result of being stopped show a test result of Untested.
Pause	Pauses a currently running test session. The tape that is being tested stays in the scanning drive. Tapes in the test session that have not been tested yet will remain queued.
Resume	Resumes a paused test session. Queued tapes are mounted and scanned.
Details	Displays the test report for the selected test session in a new window. See Viewing EDLM Session Report Details on page 28.
Delete	Deletes the selected test session from the list. Once deleted, you cannot retrieve the information again.
Refresh	Refreshes the test session list so that the latest information about the tests is displayed.

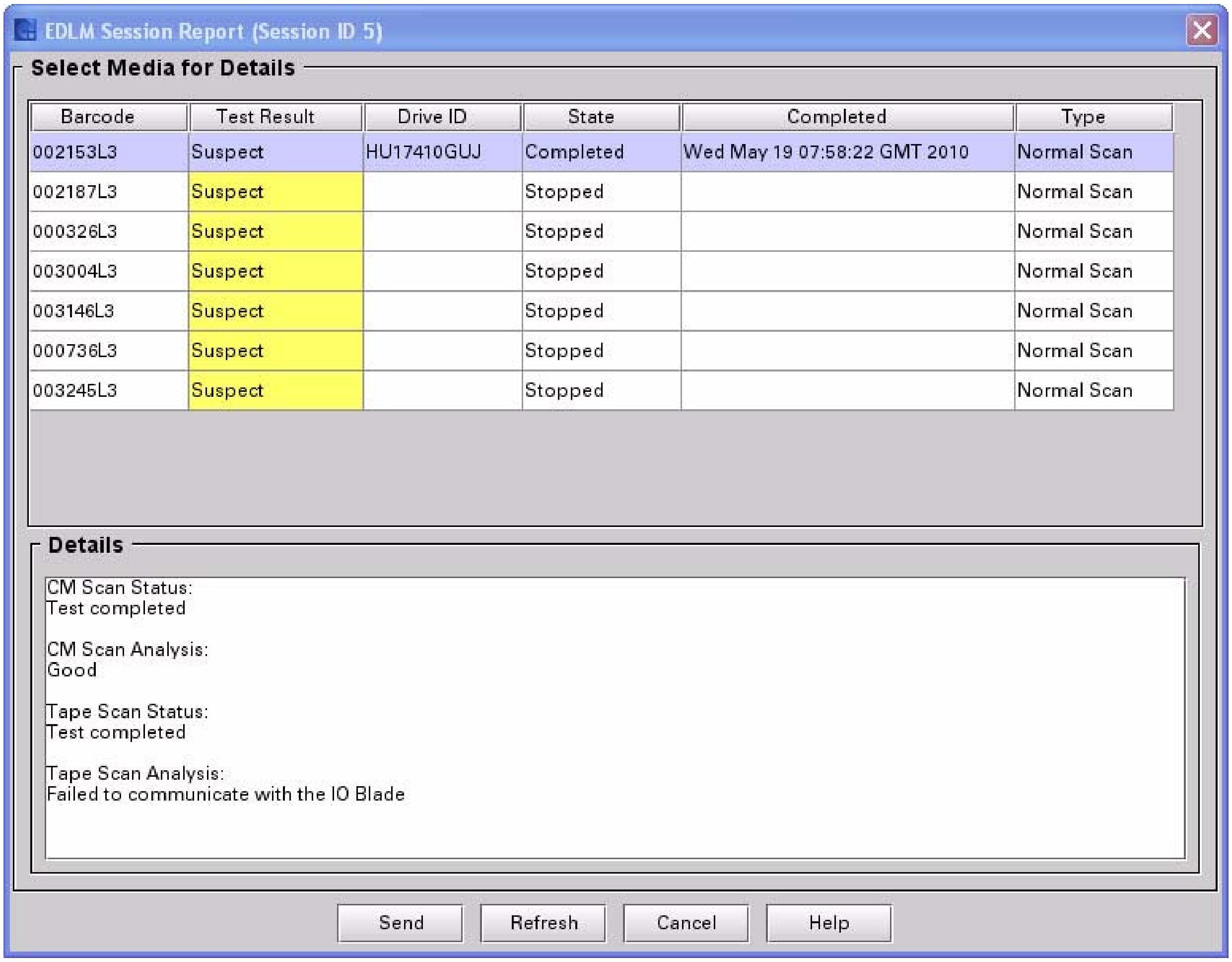
Viewing EDLM Session Report Details

To view details about a specific EDLM test session, do the following:

1 From the EDLM Test Sessions List (**Tools > EDLM Tests > Test Results**), click on a row to highlight it, and then click the **Details** button.

The test results display in a new window called EDLM Session Report (Session ID X), where X is the session ID displayed in the EDLM Test Sessions List.

You can sort the list by clicking any of the column headers. An arrow appears in the column header indicating whether the column is sorted in ascending or descending order. Click the column header again to toggle between ascending and descending order.



Barcode	Test Result	Drive ID	State	Completed	Type
002153L3	Suspect	HU17410GUJ	Completed	Wed May 19 07:58:22 GMT 2010	Normal Scan
002187L3	Suspect		Stopped		Normal Scan
000326L3	Suspect		Stopped		Normal Scan
003004L3	Suspect		Stopped		Normal Scan
003146L3	Suspect		Stopped		Normal Scan
000736L3	Suspect		Stopped		Normal Scan
003245L3	Suspect		Stopped		Normal Scan

CM Scan Status:
Test completed

CM Scan Analysis:
Good

Tape Scan Status:
Test completed

Tape Scan Analysis:
Failed to communicate with the IO Blade

The Select Media for Details section of the screen lists each tape in the test session. The following information is reported:

Item	Description
Barcode	The media barcode identifier.
Test Result	The test result displays as one of the following: • **Good** — The tape is good. • **Bad** — The tape is bad. • **Suspect** — The tape is possibly unreliable or defective. • **Untested** — The tape could not be fully scanned, for various reasons, including: incompatible or unknown media type; tape could not be loaded; tape is encrypted but the data encryption key could not be obtained; drive not communicating with I/O blade, test was stopped. **Note:** Untested media do not initiate RAS tickets or EDLM media action policies (such as copying data from a bad or suspect tape). • **Not Completed** — Test has not completed yet.
Drive ID	The serial number of the tape drive that tested the tape.
State	The current test status: Pending, In Progress, Completed, Stopped or Paused.
Completed	The date and time the test completed.
Type	The type of test that was run: Quick Scan, Normal Scan or Full Scan.

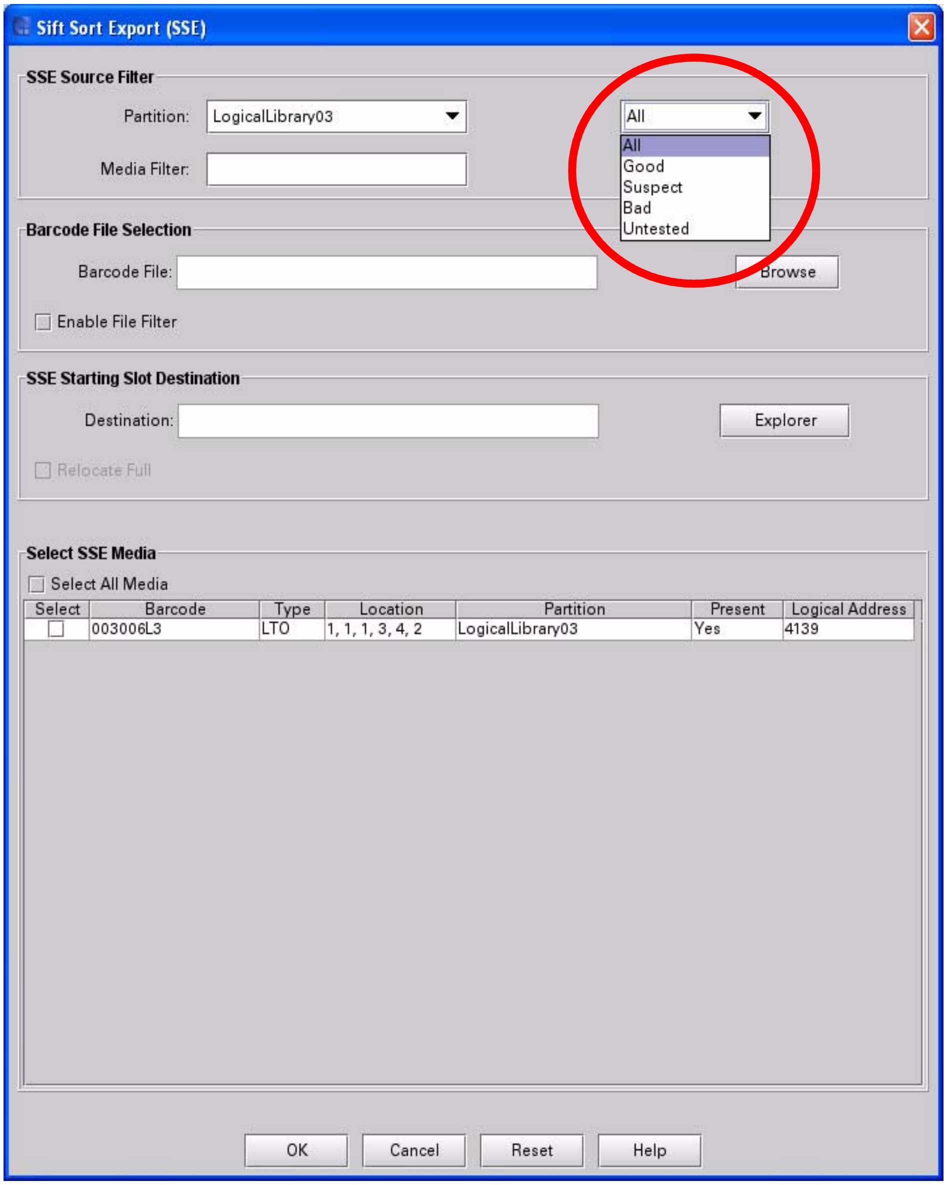
2 To view test details for a specific tape, click on a row in the **Select Media for Details** section to highlight it. Details about the test display in the Details section below. The following details display:

Item	Description
CM Scan Status	One of the following: • Test completed — Test is finished; however, the result may not be "good." You can also get this if the test was stopped. • Test paused. • Test pending. • Test in progress. • Test not run — Media was removed from library before it could be tested, or there were no drives available to test the media.
CM Scan Analysis	Summary of the cartridge memory scan (either "good" or an explanation of the result).
Tape Scan Status	One of the following: • Test completed — Test is finished; however, the result may not be "good." • Test paused. • Test pending. • Test in progress. • Test not run — Media was removed from library before it could be tested, or there were no drives available to test the media. • Test not configured — You requested a Quick Scan only so the tape was not scanned.
Tape Scan Analysis	Summary of the tape scan (either "good" or an explanation of the result).

3 To send a copy of the test session report via e-mail, click **Send**. To update the dialog with the current status, click **Refresh**.

EDLM Changes to Sift Sort Export Screen

There is a new filter in the Sift Sort Export menu (**Tools > Sift Sort > Export**) that is enabled for the library managed partition and partitions with EDLM policies configured. It allows you to filter cartridges based on their media test result: All, Good, Suspect, Bad, or Untested.



Sift Sort Export (SSE)

SSE Source Filter

Partition: LogicalLibrary03

Media Filter:

All

Barcode File Selection

Barcode File:

□ Enable File Filter

SSE Starting Slot Destination

Destination:

□ Relocate Full

Select SSE Media

□ Select All Media

Select	Barcode	Type	Location	Partition	Present	Logical Address
□	003006L3	LTO	1, 1, 1, 3, 4, 2	LogicalLibrary03	Yes	4139

KMIP-compliant Encryption Key Management

The Key Management Interoperability Protocol (KMIP®) is a specification developed by OASIS®. Its function is to standardize communication between enterprise key management systems and encryption systems. With version i8.2.1, the Scalar i6000 provides a KMIP version 1.0 compliant encryption solution.

KMIP is only supported in certain environments. Contact your Quantum representative for details.

Details about the Scalar i6000 KMIP-compliant implementation include:

- As with other encryption systems supported by the library, in order to use KMIP-compliant encryption systems with the Scalar i6000, you must have an Encryption Key Management license installed on the library.
- A minimum of two KMIP-compliant encryption servers are required for failover purposes. A total of 10 KMIP-compliant encryption servers are allowed, for increased failover capability.

See Encryption Key Management Systems on page 32 for instructions on how to configure KMIP-compliant encryption systems on the library.

Encryption Key Management Systems

Encryption key management systems generate, protect, store, and manage encryption keys. These keys are used by their respective tape drives to encrypt information being written to tape, and decrypt information being read from tape media.

The Scalar i6000 now supports four encryption key management systems:

Encryption System	Supported Tape Drives
Quantum Encryption Key Manager (Q-EKM)	IBM LTO-4 Fibre Channel IBM LTO-5 Fibre Channel
Scalar Key Manager (SKM)	HP LTO-4 Fibre Channel HP LTO-5 Fibre Channel
RSA Key Manager (RKM)	HP LTO-4 Fibre Channel HP LTO-5 Fibre Channel
KMIP-compliant key management (see KMIP-compliant Encryption Key Management on page 32).	HP LTO-4 Fibre Channel HP LTO-5 Fibre Channel

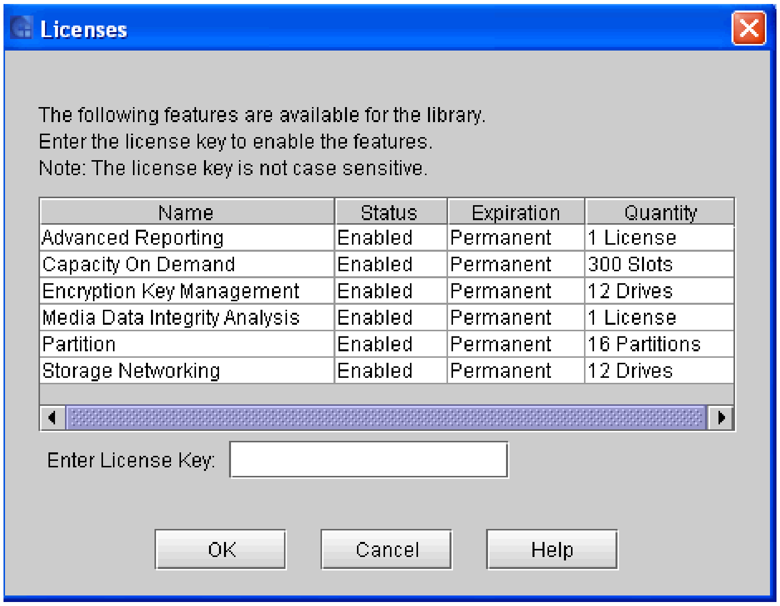
Note: The library does not support using more than one encryption key management system on a single library.

Setting up EKM on the Scalar i6000

Step 1 — Installing the EKM License Key

1 Click **Setup > Licenses**.

The Licenses dialog box appears.



The following features are available for the library.
Enter the license key to enable the features.
Note: The license key is not case sensitive.

Name	Status	Expiration	Quantity
Advanced Reporting	Enabled	Permanent	1 License
Capacity On Demand	Enabled	Permanent	300 Slots
Encryption Key Management	Enabled	Permanent	12 Drives
Media Data Integrity Analysis	Enabled	Permanent	1 License
Partition	Enabled	Permanent	16 Partitions
Storage Networking	Enabled	Permanent	12 Drives

This dialog box lists the licensed features for your library, plus Status, Expiration, and Quantity. **Quantity** refers to the number drives licensed to use this feature.

2 In the **Enter License Key** box, type the appropriate license key.

- License keys are not case sensitive and are all-inclusive. For example, J2BGL-22622-52C22 can be entered as j2bgl-22622-52c22.
- If you are using the library’s touch screen, enter the library key from the lowercase keyboard, which gives you access to the dash (-) character.
- If you cannot locate the license keys shipped with the library, you can obtain them by contacting technical support or, if you are an end user, by contacting your inside sales representative.

3 Click **OK**.

Step 2 — Preparing Partitions for Library-managed Encryption

1 If not already installed, install tape drives that are supported by the encryption system you are using (see Supported Tape Drives on page 32).

2. Ensure that the partition you are configuring for library-managed encryption contains only tape drives that are supported by the encryption system you are using.
3. 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.

Step 3 — Installing TLS Communication Certificates on the Library

Transport Layer Security (TLS) communication certificates are unique certificates that must be installed on the library in order for the library to communicate securely with attached EKM servers.

Take one the following actions, according to what encryption System you are using.

Encryption System	Action
Quantum Encryption Key Manager (Q-EKM)	Only one TLS certificate (the Root certificate) is required. Libraries with code versions 600A.GS23201 and higher generate a self-signed certificate when first booting up for Q-EKM purposes, and regenerate the certificate if it expires. You do not need to take any action unless you want to install your own Root certificate to supersede the existing certificate. If want to install your own certificate, then follow the instructions in Installing User-Provided Certificates on page 37.
Scalar Key Manager (SKM)	TLS certificates may already be pre-loaded on the library. **1** Check to see if certificates are loaded. See Checking for Current Certificates on page 35. **Note:** If certificates have already been pre-loaded by Quantum, you can replace them by installing your own certificates, if desired. **2** If needed, install certificates following the appropriate set of instructions: • Installing SKM Library TLS Certificates from Quantum CD on page 36, or • Installing User-Provided Certificates on page 37.
RSA Key Manager (RKM)	TLS certificates will be provided by your RSA RKM server administrator. Install certificates per Installing User-Provided Certificates on page 37.

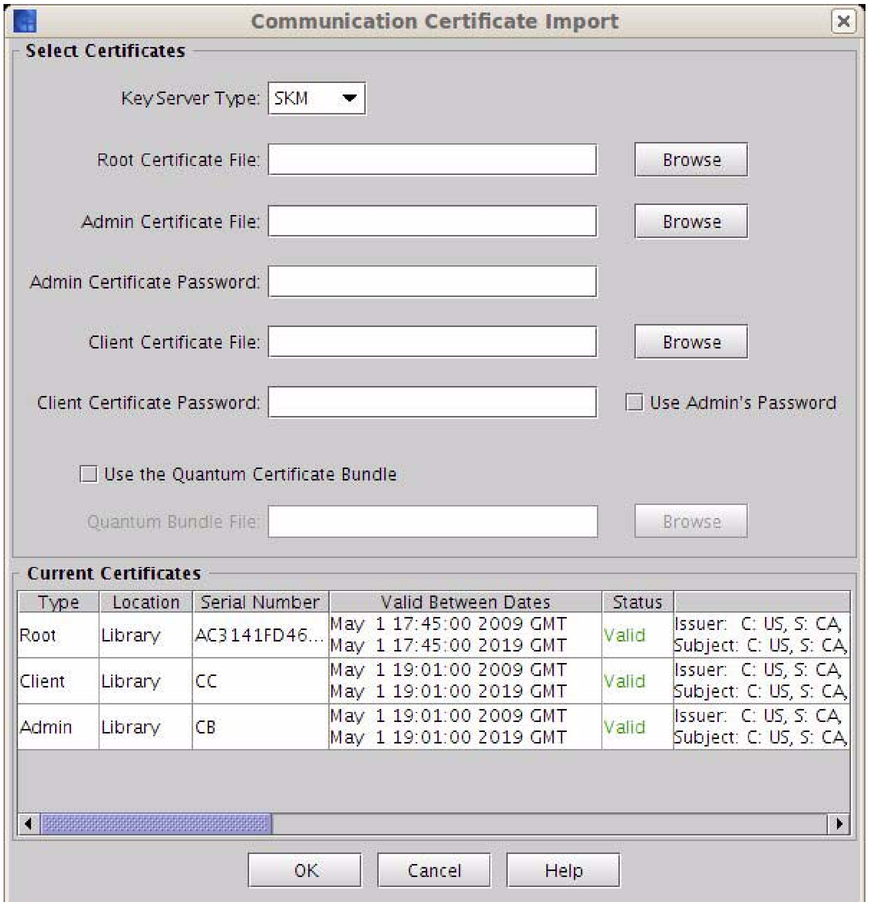
Encryption System	Action
KMIP-compliant key management	TLS certificates will be provided by your KMIP server administrator. Install certificates per Installing User-Provided Certificates on page 37.

Checking for Current Certificates

Follow the steps below to see what certificates are already loaded on your library.

1 From the Tools menu, select **EKM Management > Import Communication Certificates.**

The **Communication Certificate Import** dialog box appears.



Communication Certificate Import

Select Certificates

Key Server Type: SKM

Root Certificate File:

Admin Certificate File:

Admin Certificate Password:

Client Certificate File:

Client Certificate Password:

□ Use Admin's Password

□ Use the Quantum Certificate Bundle

Quantum Bundle File:

Current Certificates

Type	Location	Serial Number	Valid Between Dates	Status	
Root	Library	AC3141FD46...	May 1 17:45:00 2009 GMT May 1 17:45:00 2019 GMT	Valid	Issuer: C: US, S: CA, Subject: C: US, S: CA,
Client	Library	CC	May 1 19:01:00 2009 GMT May 1 19:01:00 2019 GMT	Valid	Issuer: C: US, S: CA, Subject: C: US, S: CA,
Admin	Library	CB	May 1 19:01:00 2009 GMT May 1 19:01:00 2019 GMT	Valid	Issuer: C: US, S: CA, Subject: C: US, S: CA,

Note: The **Current Certificates** section of the screen lists the certificates currently loaded on the library. If you install new certificates, they will overwrite the current certificates.

2 Confirm which certificates are appropriate for your installation.

3 Install certificates if needed, following the instructions in the following table for your encryption system.

Encryption System	Action
Q-EKM	If you wish to install your own Root certificate to supersede the existing self-generated certificate on the library, follow the instructions in Installing User-Provided Certificates on page 37.
SKM	For **SKM**, you can either: • Install from the Quantum certificate bundle on CD. Refer to Installing SKM Library TLS Certificates from Quantum CD on page 36. • Install your own certificates. Refer to Installing User-Provided Certificates on page 37.
RKM	You must use certificates provided by the RSA RKM server administrator. Refer to Installing User-Provided Certificates on page 37.
KMIP-compliant key management	You must use certificates provided by the KMIP server administrator. Refer to Installing User-Provided Certificates on page 37.

Installing SKM Library TLS Certificates from Quantum CD

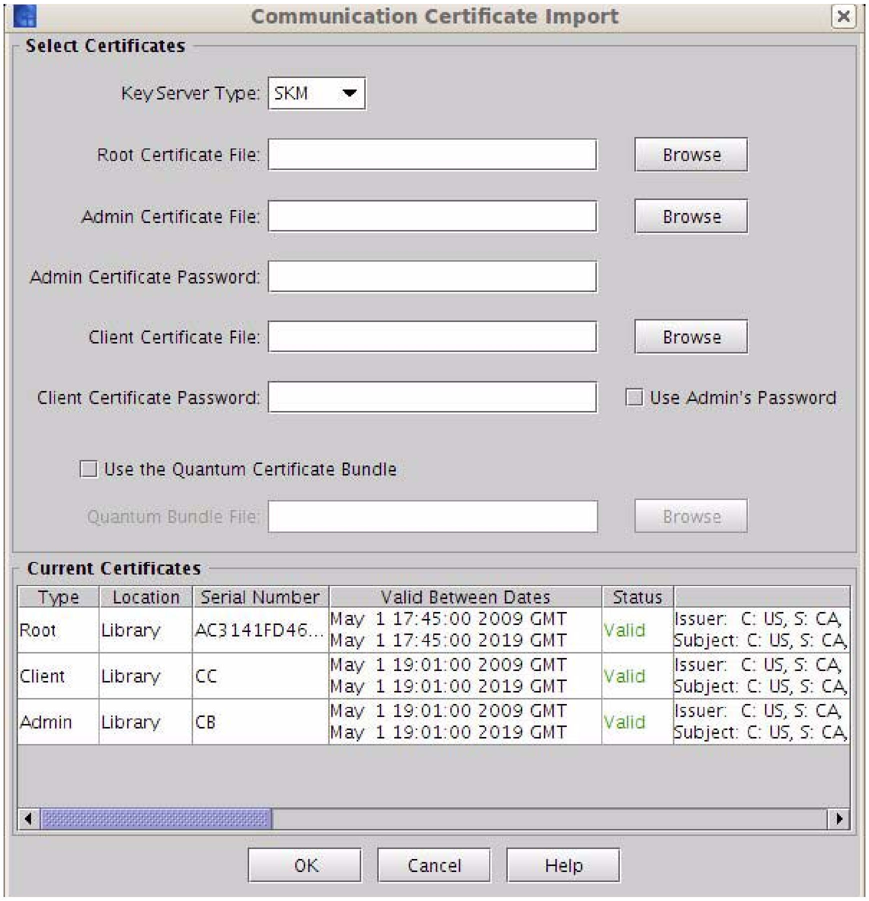
Note: The Quantum certificate bundle can be used only with SKM. Quantum TLS certificates for use with SKM may already be pre-loaded on your library. Check if these exist before adding new TLS certificates for SKM. Refer to Checking for Current Certificates on page 35.

1 Insert the CD into the CD ROM drive of your computer.

2 Either copy the file to a known location on your computer or use the CD as the location from which you will retrieve the file.

3 From the **Tools** menu, select **EKM Management > Import Communication Certificates**.

The **Communication Certificate Import** dialog box appears.



Communication Certificate Import

Select Certificates

Key Server Type: SKM

Root Certificate File:

Admin Certificate File:

Admin Certificate Password:

Client Certificate File:

Client Certificate Password: □ Use Admin's Password

□ Use the Quantum Certificate Bundle

Quantum Bundle File:

Current Certificates

Type	Location	Serial Number	Valid Between Dates	Status	
Root	Library	AC3141FD46...	May 1 17:45:00 2009 GMT May 1 17:45:00 2019 GMT	Valid	Issuer: C: US, S: CA, Subject: C: US, S: CA,
Client	Library	CC	May 1 19:01:00 2009 GMT May 1 19:01:00 2019 GMT	Valid	Issuer: C: US, S: CA, Subject: C: US, S: CA,
Admin	Library	CB	May 1 19:01:00 2009 GMT May 1 19:01:00 2019 GMT	Valid	Issuer: C: US, S: CA, Subject: C: US, S: CA,

4 In the **Select Certificates** section, select **SKM** from the **Key Server Type** drop-down list.

5 Select the **Use Quantum Certificate Bundle** check box, and then click **Browse** to locate the Quantum Bundle File.

Note: If you have installed certificates, they are listed in the Current Certificates section.

6 Click **OK**.

Installing User-Provided Certificates

Follow these instructions to install your own TLS certificates, or when installing TLS certificates for RKM or KMIP. 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.

Note: If you are using SKM, you must be running SKM 1.1 or higher on your SKM servers in order to install your own TLS certificates.

Note: If you are using RSA or KMIP, your server provider will provide TLS communication certificates.

You need to provide the following certificates:

Encryption System	Certificates Required
Q-EKM	• Root Certificate (also called the CA certificate, or Certificate Authority Certificate)
SKM	• Root Certificate (also called the CA certificate, or Certificate Authority Certificate) • Client Certificate • Admin Certificate
RKM	• Root Certificate (also called the CA certificate, or Certificate Authority Certificate) • Client Certificate
KMIP-compliant key management	• Root Certificate (also called the CA certificate, or Certificate Authority Certificate) • Client 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 Client certificates must be in pkcs12 (.p12) format, with a separate certificate and private key contained in each.

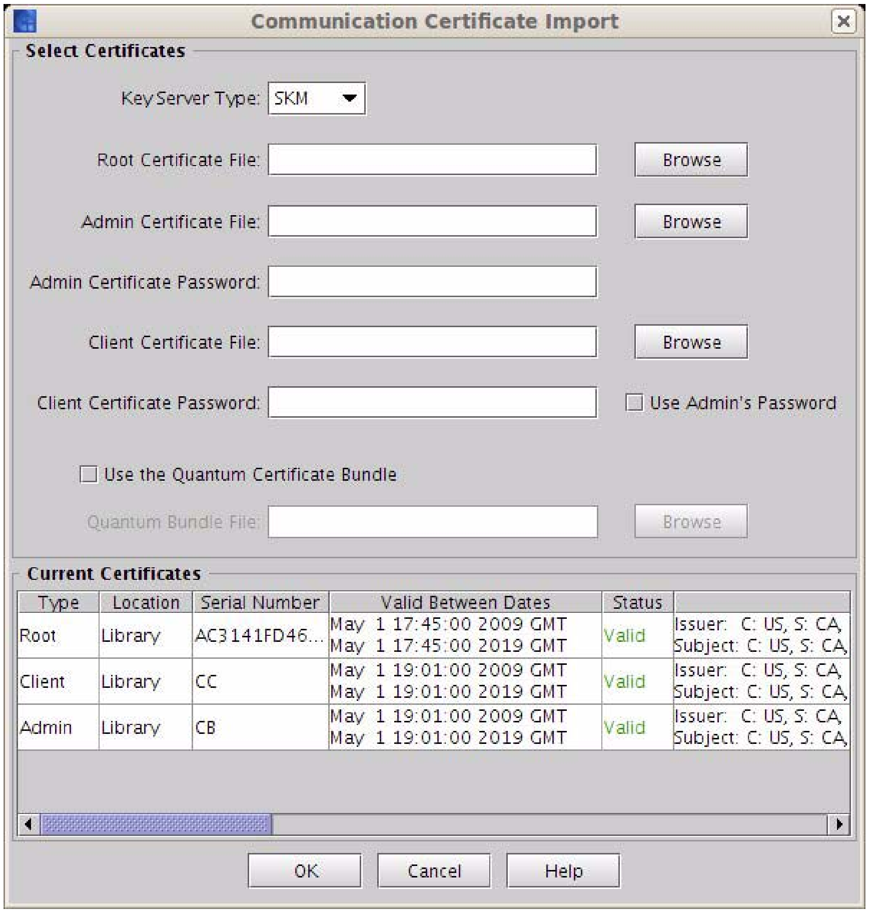
Note: The .p12 format combines the public/private key pair files in .pem file format and password protects access to such .pem certificate files.

- The Admin and Client certificates must be 1024 bits.
- The Admin and Client 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. (Only applies to SKM.)
- The same Root Certificate must be installed on the encryption key servers and the library.
- All the certificates must have a valid validity period according to the date and time settings on the encryption key server.

Follow the steps below to install your own certificates.

1. Place the certificate files in an accessible location on your computer.
2. From the **Tools** menu, select **EKM Management > Import Communication Certificates.**

   The **Communication Certificate Import** dialog box appears.



Key Server Type: SKM

Root Certificate File:

Admin Certificate File:

Admin Certificate Password:

Client Certificate File:

Client Certificate Password:

Type	Location	Serial Number	Valid Between Dates	Status	
Root	Library	AC3141FD46...	May 1 17:45:00 2009 GMT May 1 17:45:00 2019 GMT	Valid	Issuer: C: US, S: CA, Subject: C: US, S: CA,
Client	Library	CC	May 1 19:01:00 2009 GMT May 1 19:01:00 2019 GMT	Valid	Issuer: C: US, S: CA, Subject: C: US, S: CA,
Admin	Library	CB	May 1 19:01:00 2009 GMT May 1 19:01:00 2019 GMT	Valid	Issuer: C: US, S: CA, Subject: C: US, S: CA,

3 In the **Select Certificates** section, select the appropriate Key Server Type from the drop-down list.

Depending on your selection, certain fields are enabled.

4 Take the following actions, depending on which Key Server Type you selected:

For Q-EKM

- Click **Browse** to retrieve the **Root Certificate File**.

For SKM

- Click **Browse** to retrieve the **Root Certificate File**.
- Click **Browse** to retrieve the **Admin Certificate File.**
- In the **Admin Certificate Password** field, type the password used when you generated the certificate files.
- Click **Browse** to retrieve the **Client Certificate File**.
- In the **Client Certificate Password** field, type the password used when you generated the certificate files.
- If you used the same password for the client and admin certificates, you can select the **Use Admin's Password** check box.

For RKM or KMIP-compliant key managers

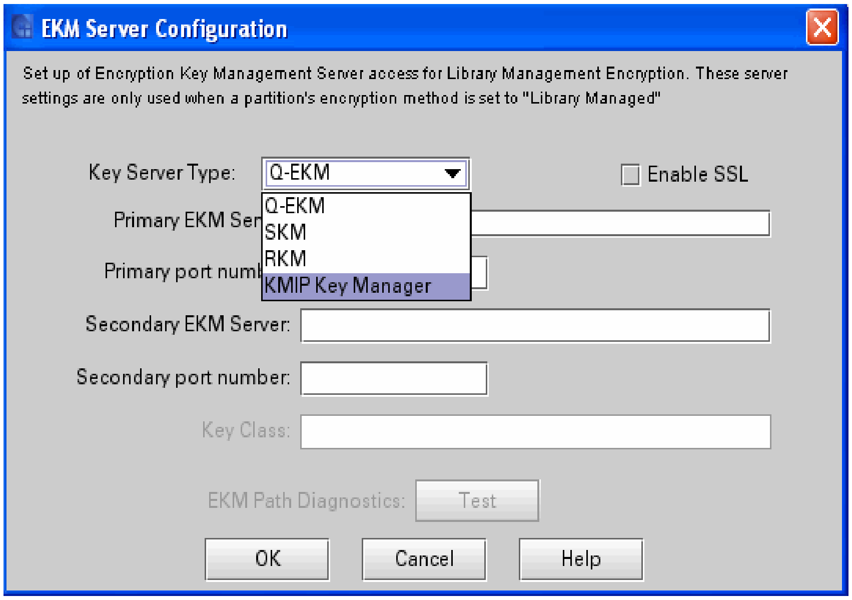
- Click **Browse** to retrieve the **Root Certificate File**.
- Click **Browse** to retrieve the **Client Certificate File**.
- In the **Client Certificate Password** field, type the password used when generating the certificate files.

5 Click **OK**.

Step 4 — Configuring the EKM Server

1 From the menu bar, click **Setup** > **Encryption** > **Server Configuration**.

The **EKM Server Configuration** dialog box appears.



EKM Server Configuration

Set up of Encryption Key Management Server access for Library Management Encryption. These server settings are only used when a partition's encryption method is set to "Library Managed"

Key Server Type: Q-EKM

2 From the **Key Server Type** drop-down list, select the server type.

3 Fill in the rest of the fields as described in the sections below for each server type: Q-EKM on page 40, SKM on page 41, RKM on page 41, or KMIP Key Manager on page 42 of this document.

For primary and secondary servers, you can enter the following:

- IPv4 address
- IPv6 address — if IPv6 is configured
- Domain name — if DNS is configured on the LMC (**Setup > DNS Configuration**)

Q-EKM

e **Enable SSL -** Select the check box if SSL communications should be enabled between the library and encryption server(s).

f **Primary EKM Server -** Type the IP address or domain name of the primary Q-EKM server.

g **Primary port number** - If SSL is enabled, the default port number is 443. If SSL is not enabled, the default port number is 3801. You can change the port number on the library, but, if you do, you must also change the port number on the key server to match or Q-EKM will not work properly. See the *Quantum Encryption Key Manager User's Guide* for information on setting the port number on the Q-EKM key server.

h **Secondary EKM Server** - Type the IP address or domain name of the optional secondary Q-EKM server.

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

i **Secondary port number** - If SSL is enabled, the default port number is 443. If SSL is not enabled, the default port number is 3801.

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

j **Key Class** - This field is not applicable for Q-EKM.

k **EKM Path Diagnostics** - Not supported for Q-EKM. The **Test** button is disabled.

SKM

a **Enable SSL** - Check box is checked automatically and field is disabled.

b **Primary EKM Server** - Type the IP address or domain name of the primary SKM server.

c **Primary port number** - Field is disabled, and port number defaults to 6000 automatically.

d **Secondary EKM Server** - Type the IP address or domain name of the secondary SKM server.

e **Secondary port number** - Field is disabled, and port number defaults to 6000 automatically.

f **Key Class** - This field is not applicable for SKM.

g **EKM Path Diagnostics** - To test the configuration, click **Test**.

The **Path Diagnostic Results** dialog box appears. For more information on EKM Path Diagnostics, see Using EKM Path Diagnostics on page 46.

RKM

a **Enable SSL** - Check box is checked automatically and the field is disabled.

b **Primary EKM Server** - Type the IP address or domain name of the primary RKM server.

c **Primary port number** - Accept the default or type the applicable port number. The default port number is 443.

Note: The port number must match the port number on the primary RKM key server.

d **Secondary EKM Server -** The secondary EKM server is not supported, therefore this field is disabled.

e **Secondary port number -** A secondary port number is not supported; therefore, this field is disabled.

f **Key Class -** Type the key class that was used during the RKM server configuration process.
The key class that was created on your RSA RKM server will be provided by the RKM server administrator.

g **EKM Path Diagnostics -** To test the configuration, click **Test.**

The Path Diagnostic Results dialog box appears. For more information on EKM Path Diagnostics, see Using EKM Path Diagnostics on page 46.

KMIP Key Manager

Note: Assign your key servers on this screen in the order in which you want failover to occur. Server 1 is the primary server; Server 2 is the secondary server; and so on. For an initial key request, the library tries Server 1 (the primary server) first. If Server 1 is not available to perform a key request, the library tries Server 2. If server 2 is not available, the library will try Server 3, and so on, in order, until it finds a server that can perform the request. Once found, this server remains the active server until it fails a key request or the library is rebooted. At that point, the library starts over and uses Server 1 for key requests. If Server 1 is not available, it will try Server 2, and so on.

a **Enable SSL** - Check box is checked automatically and the field is disabled.

b **Server 1 -** Type the IP address or domain name of the primary KMIP key manager server.

c **Port for Server 1 -** Type the applicable port number. The port number must match the configured port number on the primary KMIP key manager server. A typical port number used for communication between the KMIP key manager server and the library is port **9003**.

d **Server 2** - Type the IP address or domain name of the secondary KMIP key manager server.

e **Port for Server 2 -** Type the applicable port number. The port number must match the configured port number on the secondary KMIP key manager server. A typical port number used for communication between the KMIP key manager server and the library is port **9003**.

f Repeat Step d and Step e for up to eight additional KMIP key manager servers, in the order in which you would like failover to occur. The port number listed in each **Port** field must match the port number used on that KMIP key manager server.

g **Key Class -** This field is not applicable.

h **EKM Path Diagnostics** - To test the configuration, click **Test.**

The **Path Diagnostic Results** dialog box appears. For more information on EKM Path Diagnostics, see Using EKM Path Diagnostics on page 46.

4 Click **Close**.

5 Click **OK**.

An **Operation in Progress** dialog box appears, indicating the settings are being modified. Upon successful completion, the system returns to the main console.

Note: If using SKM, key generation begins in the background. Key generation can take one hour or more. Once SKM encryption keys have been generated, make sure to back up both SKM servers before using any encryption keys. Refer to the *Scalar Key Manager User’s Guide.*

6 Ensure all ports corresponding to the EKM servers are open on your firewall to allow the library to connect to the servers. For SKM, ports 80, 6000, and 6001 must be open.

Step 5 — Configuring Partitions for Library-managed Encryption

Encryption on the Scalar i6000 library is enabled by partition only. You cannot select individual drives for encryption; you must select an entire partition for encryption. Only partitions that are encryption-capable are displayed on the configuration screen.

Use the Partition Configuration dialog box to change the encryption method used by a partition. You can modify only one partition at a time.

Encryption Methods, Details, and Restrictions

The following encryption methods are available on the library:

- **Allow Application Managed** — Allows your host application to provide encryption support on all encryption-capable tape drives and media within the partition. This is the default setting if the partition contains encryption-capable tape drives. If you select this option, the library will not communicate with the key server on this partition. If you want an application to manage encryption, you must specifically configure the application to do so. The library will not participate in performing encryption. See your host documentation for further details.
- **Enable Library Managed** — Enables library managed encryption support via a connected key manager server—either Quantum Encryption Key Manager (Q-EKM), Scalar Key Manager (SKM), RSA Key Manager (RKM), or KMIP-compliant key server—for all tape drives and encryption-capable media assigned to the partition.

  Details and restrictions for using library managed encryption include:

  - You must have an EKM license installed on the library (Step 1 — Installing the EKM License Key on page 33) before you can select this option. Ensure the EKM license contains the appropriate quantity of drives to match or exceed what is currently installed in the library.

- Your encryption key servers must be installed, operational, and configured on the library (**Setup > Encryption > Server Configuration**), before you can enable a partition for library managed encryption (**Setup > Encryption > Partition Configuration**).
- Only LTO-4 and LTO-5 tape cartridges will be encrypted in library managed encryption partitions, unless they contain unencrypted data already, and data is appended. The partition may contain LTO-2 and LTO-3 tape cartridges, but they will not be encrypted.
- Encrypted data will never be appended to unencrypted data on tape, and unencrypted data will never be appended to encrypted data on tape.
- For data to be encrypted via library managed encryption, the media must be blank or have been written to using library managed encryption at the first write operation at the beginning of tape (BOT). If the media was previously written in a non-encrypted format, all data subsequently written to it will continue to be non-encrypted.
- Data stored on tape cartridges will not be encrypted with more than one encryption key.
- **Q-EKM** supports encryption for data cartridges using IBM LTO-4 or IBM LTO-5 Fibre Channel tape drives. If you are using Q-EKM and want to enable library managed encryption for a partition, all of the tape drives in that partition must be IBM LTO-4 and/or IBM LTO-5 Fibre Channel tape drives.

  Generating Encryption Keys for Q-EKM: Encryption keys are generated during the Q-EKM installation and configuration process.
- **SKM** supports encryption for data cartridges using HP LTO-4 or HP LTO-5 Fibre Channel drives. If you are using SKM and want to enable library managed encryption for a partition, all of the tape drives in that partition must be HP LTO-4 and/or HP LTO-5 Fibre Channel tape drives.

  Generating Encryption Keys for SKM: The library automatically generates keys as soon as you configure the SKM server. Note that you cannot change a partition to library managed encryption until after key generation is complete.

  Caution: Once encryption keys have been generated, make sure to back up both SKM servers before using any encryption keys. Refer to the *Scalar Key Manager User's Guide.*
- **RKM** supports encryption for data cartridges using HP LTO-4 or HP LTO-5 Fibre Channel drives. If you are using RKM and want to enable library managed encryption for a partition, all of the tape drives in that partition must be HP LTO-4 and/or HP LTO-5 Fibre Channel tape drives.

  Generating Encryption Keys for RKM: Encryption keys are generated during the RKM installation and configuration process.
- **KMIP-compliant key management** supports encryption for data cartridges using HP LTO-4 or HP LTO-5 Fibre Channel drives. If you are using KMIP-compliant key servers and want to enable library managed encryption for a partition, all of the tape drives in that partition must be HP LTO-4 and/or HP LTO-5 Fibre Channel tape drives.

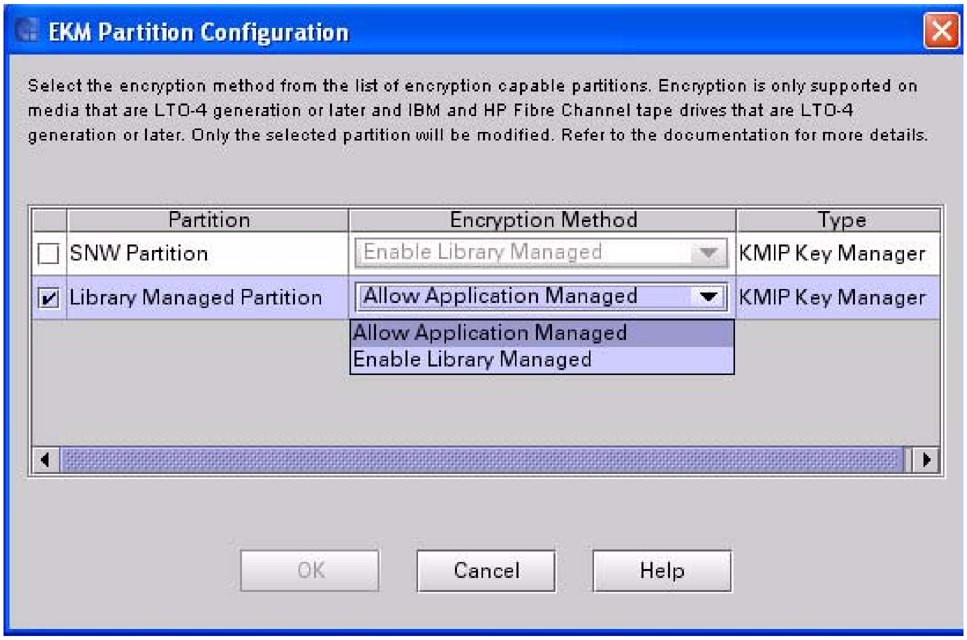
Generating Encryption Keys for KMIP-compliant key servers: Encryption keys are generated one at a time, as needed, upon request.

Changing the Encryption Method

1 If you are not already viewing the physical library, click **View** and select the name of the physical library.

2 Click **Setup > Encryption > Partition Configuration**.

The **EKM Partition Configuration** dialog box appears. Each partition’s current encryption method is listed under Encryption Method.



EKM Partition Configuration

Select the encryption method from the list of encryption capable partitions. Encryption is only supported on media that are LTO-4 generation or later and IBM and HP Fibre Channel tape drives that are LTO-4 generation or later. Only the selected partition will be modified. Refer to the documentation for more details.

	Partition	Encryption Method	Type
□	SNW Partition	Enable Library Managed	KMIP Key Manager
☑	Library Managed Partition	Allow Application Managed	KMIP Key Manager

3 If you want to change a partition’s encryption method, make sure that the tape drives in that partition do not have cartridges loaded. If there are cartridges in the tape drives, you cannot change the encryption method.

4 Select the check box for the partition whose encryption method you want to change.

5 Change the encryption method by selecting from the Encryption Method drop-down list:

Encryption Method	Description
Allow Application Managed	This is the default setting if you have encryption-capable tape drives in the partition. This option should remain selected ***unless*** you are connecting the library to an external EKM server. This option allows an external backup application to provide encryption support to all encryption-capable tape drives and media within the partition. **Note:** If you want an application to manage encryption, you must specifically configure the application to do so.
Enable Library Managed	Enables encryption support via connected EKM servers to the partition. Choose this option for Q-EKM, SKM, RKM, or KMIP key servers.

Note: When you change a partition from Enable Library Managed to Allow Application Managed, any encrypted data that was written to the tapes while the partition was configured for library managed encryption can no longer be read, until you change the partition back to Enable Library Managed.

6 Click **OK**.

The dialog box is closed and you are returned to the main console.

If the partition encryption settings were not successfully configured, follow the screen instructions to resolve any issues.

Step 6 — Saving the Library Configuration

When you are finished configuring the library, save the library configuration (**Tools > Save/Restore**).

Using EKM Path Diagnostics

EKM Path Diagnostics is a series of short tests performed by the library to determine whether the EKM servers are connected and operating properly.

Note: This feature is not available for Q-EKM.

You can perform EKM Path Diagnostics tests manually at any time, or automatically in the background at regular intervals:

- **Manual** — You can perform manual EKM Path Diagnostics at any time by clicking the **Test** button on the EKM server setup screen (**Setup > Encryption > Server Configuration**).
- **Background** — You can configure the library to automatically perform background EKM Path Diagnostics tests at regularly scheduled intervals and notify you via RAS tickets if any problems arise. To do this, go to **Setup > Physical Library**. Under **EKM Path Diagnostics**, select the **Enable** check box.

Note: This feature is enabled by default. You can disable it for SKM but you cannot disable it for RKM or KMIP key managers. Unless directed by Quantum Support to disable this feature, the background EKM Path Diagnostics should always be enabled so the library can monitor SKM server status and report issues as soon as they arise.

The tests performed are:

- **Ping** — Verifies the Ethernet communication between the library and the key servers.
- **Path** — Verifies that SKM/RKM/KMIP services are running on the key servers.
- **Config** — Verifies that the key servers are capable of serving encryption keys.

Troubleshooting EKM Path Diagnostics Problems

If this occurs...	Do this...
The Ping test fails	Either the referenced server is not running, or the server address may not have been entered correctly.
The Ping test passes, but the Path test fails	Check the key server to make sure all required services are running.
The Ping and Path tests pass, but the Config test fails	There is either an issue with the communication certificates required for exchanging keys, or, in the case of RKM, the key class entered in the Encryption Server Configuration screen does not match the one set up on the server.

Monitoring EKM Server Status

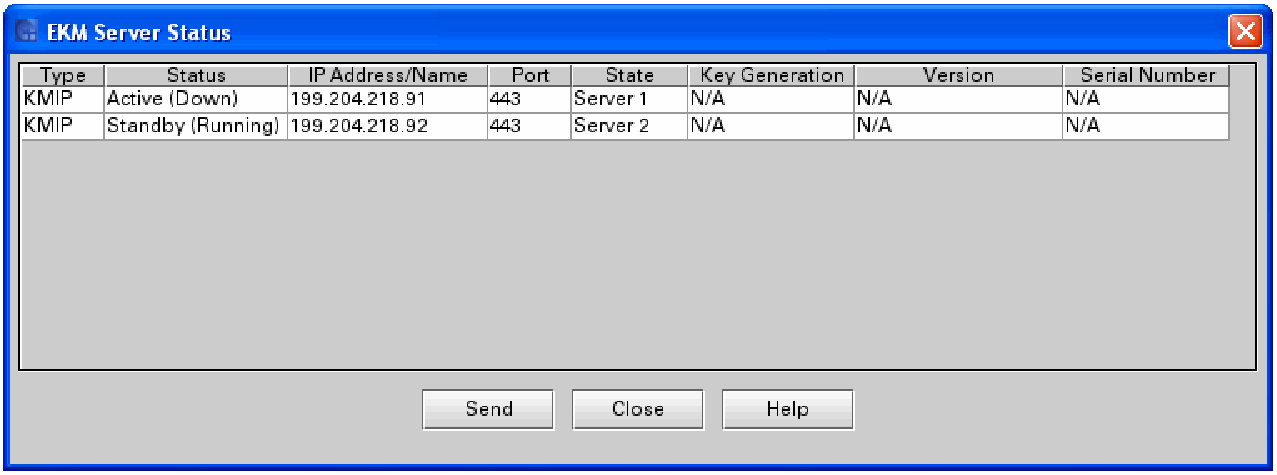
You can monitor all configured EKM servers using the EKM Server Status dialog box.

Monitoring EKM Server Status

1 From the **View** menu, select the name of the physical library or partition that communicates with the EKM servers you want to monitor.

2 On the menu bar, click **Monitor** > **EKM Servers**.

The **EKM Server Status** dialog box appears.



EKM Server Status

Type	Status	IP Address/Name	Port	State	Key Generation	Version	Serial Number
KMIP	Active (Down)	199.204.218.91	443	Server 1	N/A	N/A	N/A
KMIP	Standby (Running)	199.204.218.92	443	Server 2	N/A	N/A	N/A

For each server, the EKM Server Status dialog box displays the following information:

Element	Description
Type	The encryption server type (Q-EKM, SKM, RKM, or KMIP)
Status	The current status of the server: **Note:** "Active" status indicates that this server will receive the next key request. Q-EKM — Active, Standby or Not Configured SKM — Active Running, Standby Running or Down, or Not Configured RKM — Active Running or Down, Standby Running or Down, or Not Configured KMIP — Active Running or Down, Standby Running or Down, or Not Configured
IP Address/Name	The IP address or host name of the server
Port	The server port number: Q-EKM — Default 3801 for non-SSL and 443 for SSL SKM — 6000 (fixed) RKM — Default 443 KMIP — No default

State	Q-EKM, SKM, RKM — Whether the server is Primary or Secondary. KMIP — Order of failover. Server 1 is primary, Server 2 is secondary, and so on.
Key Generation	Applies to SKM only: Yes — encryption key generation in progress. No —encryption key generation not in progress.
Version	Applies to SKM only: Software version number
Serial Number	Applies to SKM only: Server serial number

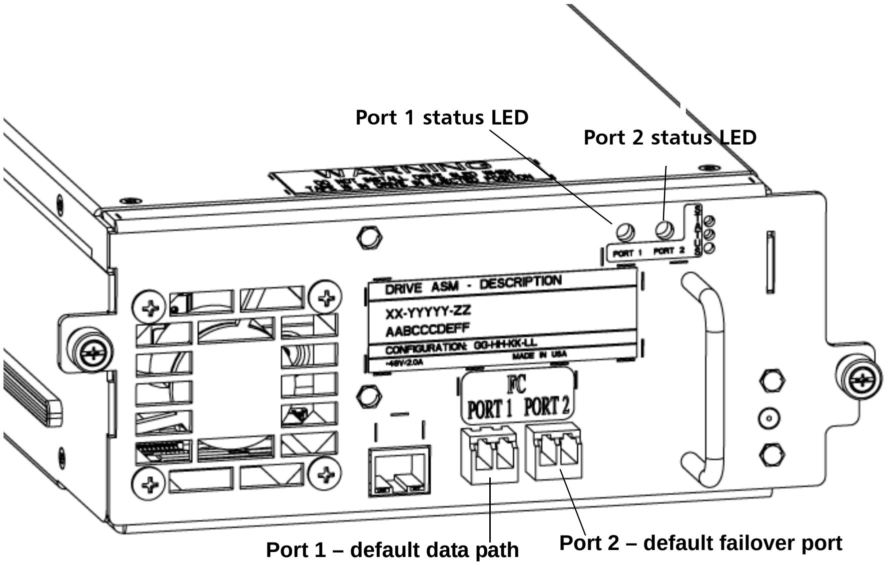
3 You can mail, save, or print status information by using the **Send** button.

Data Path Failover

Data Path Failover is a feature provided as part of the Storage Networking license and applies to HP LTO-5 Fibre Channel tape drives only. If you previously installed a Storage Networking license, you can use this feature once you upgrade library firmware to the appropriate version. Verify firmware version requirements in the *Scalar i6000 Release Notes*.

Data Path Failover provides an alternate data path when a preferred data path fails. The Data Path Failover functionality is provided as part of the Storage Networking license and applies to HP LTO-5 Fibre Channel tape drives only.

The HP LTO-5 Fibre Channel tape drives have two Fibre Channel ports. If you enable Data Path Failover on the tape drive, one port is used as the “active port” for data transmission, and the other port stands by for use if the active port fails. If the tape drive loses its Fibre Channel link with the active port, it will automatically “fail over” and use the standby port to continue drive operations.



The library issues a RAS ticket when automatic data path failover occurs. In addition, the library monitors the standby port and issues a RAS ticket if the standby port does not report a good Fibre Channel link status.

The library uses Port 1 for data path transmission unless a failover occurs. Once failover occurs, the library uses Port 2 until failover occurs again or the library is rebooted. Similarly, if a tape drive configured for data path failover is the control path for a partition, the host uses Port 1 for media changer commands unless a failover occurs. Once failover occurs, the host uses Port 2 until failover occurs again or the library is rebooted.

Note: Performing a drive reset operation is another way to make Port 1 the active port again.

A tape drive can be configured for both data path failover and control path failover. If both are configured, the control path will not fail over to another tape drive unless both ports on the control path tape drive fail.

Requirements for Data Path Failover

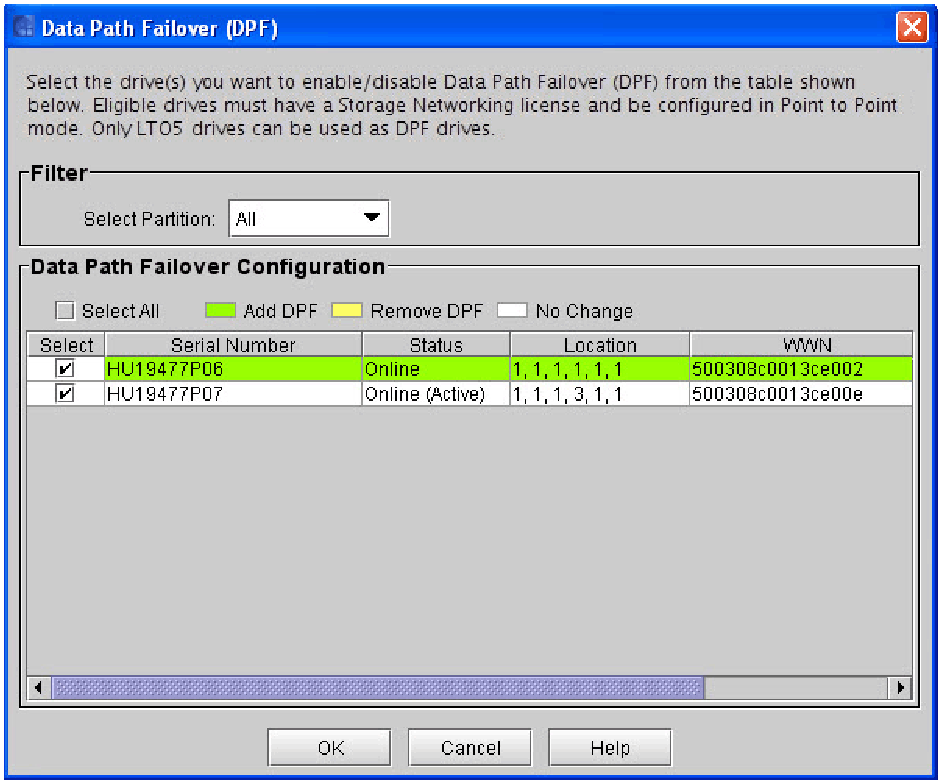
- The tape drive must be HP LTO-5 Fibre Channel tape drives and the drive must be connected to an Ethernet Expansion Blade (EEB).
- HP LTO-5 FC tape drive firmware must be at the version qualified with the Scalar i6000 library (see the Scalar i6000 Release Notes for qualified firmware levels).
- The library must have a Storage Networking license sufficient to cover the tape drive(s) on which you want to configure data path failover.
- Both FC ports on the tape drive must be connected to a host or switch. Neither tape drive port may be connected to a Fibre Channel I/O blade.
- Data path failover must be enabled on the tape drives (data path failover is disabled by default).
- Tape drive topology settings must be set to Point to Point.

Enabling/Disabling Data Path Failover

To enable or disable data path failover functionality:

4 From the main console, select **Setup > Partitions > Data Path Failover**.

The **Data Path Failover (DPF)** dialog box appears.



Data Path Failover (DPF)

Select the drive(s) you want to enable/disable Data Path Failover (DPF) from the table shown below. Eligible drives must have a Storage Networking license and be configured in Point to Point mode. Only LTO5 drives can be used as DPF drives.

Filter

Select Partition: All

Data Path Failover Configuration

□ Select All 🟩 Add DPF 🟨 Remove DPF □ No Change

Select	Serial Number	Status	Location	WWN
☑	HU19477P06	Online	1, 1, 1, 1, 1, 1	500308c0013ce002
☑	HU19477P07	Online (Active)	1, 1, 1, 3, 1, 1	500308c0013ce00e

5 Under **Data Path Failover Configuration**, select the drive(s) you want to enable (or disable) Data Path Failover on.

Current Data Path Failover status is indicated:

- Green - Enable Data Path Failover
- Yellow - Disable Data Path Failover
- White - no changes to the drive have been made

6 Click **OK**.

An **Operation in Progress** dialog box appears.

Data Path Failover configuration is now complete.

Monitoring Drive Status

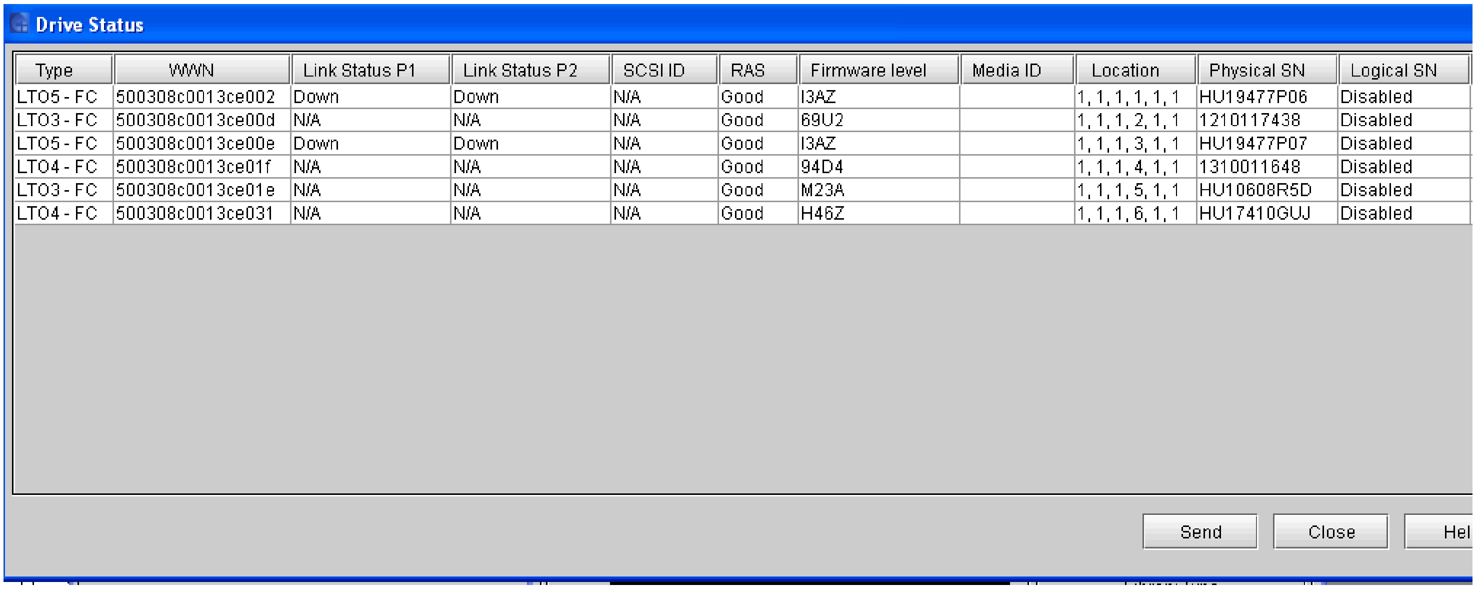
Drive status monitoring has been extended to show whether a drive is configured as a Control Path, a Control Path Failover drive, if Data Path Failover is enabled or disabled, and also provides link status for port 1 and port 2.

The **Drive Status** dialog box displays status information for tape drives in the currently selected partition. If you are viewing the physical library, status information for all drives appears. You can perform this procedure while viewing either the physical library or a partition.

1 Click **Monitor** > **Drives**.

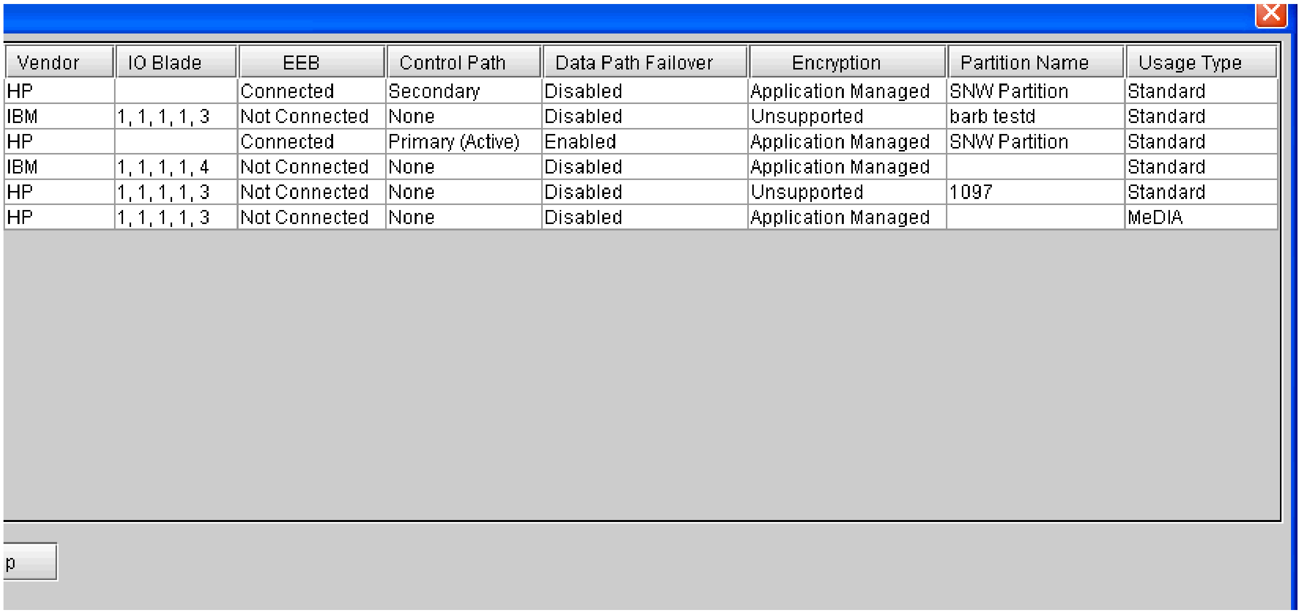
The **Drive Status** dialog box appears.

Left-side view of Drive Status dialog box



Type	WWN	Link Status P1	Link Status P2	SCSI ID	RAS	Firmware level	Media ID	Location	Physical SN	Logical SN
LTO5 - FC	500308c0013ce002	Down	Down	N/A	Good	I3AZ		1, 1, 1, 1, 1, 1	HU19477P06	Disabled
LTO3 - FC	500308c0013ce00d	N/A	N/A	N/A	Good	69U2		1, 1, 1, 2, 1, 1	1210117438	Disabled
LTO5 - FC	500308c0013ce00e	Down	Down	N/A	Good	I3AZ		1, 1, 1, 3, 1, 1	HU19477P07	Disabled
LTO4 - FC	500308c0013ce01f	N/A	N/A	N/A	Good	94D4		1, 1, 1, 4, 1, 1	1310011648	Disabled
LTO3 - FC	500308c0013ce01e	N/A	N/A	N/A	Good	M23A		1, 1, 1, 5, 1, 1	HU10608R5D	Disabled
LTO4 - FC	500308c0013ce031	N/A	N/A	N/A	Good	H46Z		1, 1, 1, 6, 1, 1	HU17410GUJ	Disabled

Right-side view of Drive Status dialog box



Vendor	IO Blade	EEB	Control Path	Data Path Failover	Encryption	Partition Name	Usage Type
HP		Connected	Secondary	Disabled	Application Managed	SNW Partition	Standard
IBM	1, 1, 1, 1, 3	Not Connected	None	Disabled	Unsupported	barb testd	Standard
HP		Connected	Primary (Active)	Enabled	Application Managed	SNW Partition	Standard
IBM	1, 1, 1, 1, 4	Not Connected	None	Disabled	Application Managed		Standard
HP	1, 1, 1, 1, 3	Not Connected	None	Disabled	Unsupported	1097	Standard
HP	1, 1, 1, 1, 3	Not Connected	None	Disabled	Application Managed		MeDIA

The following table describes the elements on the **Drive Status** dialog box.

Element	Description
Type	The type of drive.
WWN	For a Fibre Channel drive only, the World Wide Name of the drive.
Link Status P1	Reports the link status for port 1 on the drive: Active - Signal detected, port initialization complete, and process login complete Passive - Signal detected Down - Not connected to SAN Unknown - Drive is offline/varied off so state is unknown
Link Status P2	Reports the link status for port 2 on the drive: Active - Signal detected, port initialization complete, and process login complete Passive - Signal detected Down - Not connected to SAN Unknown - Drive is offline/varied off so state is unknown
SCSI ID	For a SCSI drive only, the SCSI ID of the drive.
RAS	The status of the drive as reported by the RAS system (for example, Good or Failed).
Firmware level	The firmware level of the drive.
Media ID	The barcode of the loaded cartridge.
Location	The drive coordinate location within the library.
Physical SN	The physical serial number of the particular drive.
Logical SN	The logical serial number that the library assigns to a drive in a specific location. This is not the serial number of the particular drive (see **Physical SN** in this table). If a drive is replaced by another drive in the same library location, the logical serial number remains the same. From the host's perspective, the replacement drive is the same as the original one. If the logical serial number addressing feature is disabled for the library, **Disabled** appears in this field.
Vendor	The name of the drive vendor.
IO Blade	The location of the I/O blade to which the drive is attached. Locations are indicated by means of a coordinate system.
EEB	Indicates whether or not the drive is connected to an EEB (Ethernet Expansion Blade). Only HP LTO-5 drives can be connected to an EEB. **Note:** A drive can be connected to either an I/O Blade or an EEB, not both.
Control Path	Reports if a drive is a primary (CP) or a secondary (CPF) drive. The values are Primary, Secondary, or None. It also reports which drive is currently the active drive by displaying "(Active)", example "Primary (Active)".

Element	Description
Data Path Failover	Indicates whether Data Path Failover is enabled or disabled.
Encryption	Indicates whether or not encryption is set up as Application Managed or Library Managed.
Partition Name	The name of the partition to which the drive is assigned.
Usage Type	Indicates whether the drive is a Standard drive (used for data read/write) or an EDLM scanning drive (part of a library managed partition for testing media integrity).

Determining Control Path Configuration

The following information is included in the current *Scalar i6000 Installation Guide,* however edits were requested after publishing. This information will be included in the next release of the Scalar i6000 User's Guide. The content in the Control Path Matrix on page 57 below refers to the corresponding sections in the *Scalar i6000 User's Guide*.

You must define a control path for each library partition. The control path is used to connect a partition to a host application. The Scalar i2000/i6000 does not automatically assign a control path when you create a partition. Each partition control path can occur through one of several different physical connection points depending on the hardware configuration of your library.

The procedure for setting up and defining the control path for a partition depends on which physical connection point you choose to use. For more information, refer to the *Scalar i6000 Installation Guide*

Note: In regards to the Control Path configuration, only HP LTO-5 drives can be configured for control path bridging. Only HP LTO-5 drives with SNW licenses can be configured for control path failover. Currently, IBM LT0-5 drives cannot be configured for control path

Note: A partition can be LUN mapped through any FC I/O blade, but you must manually configure LUN mapping to present the partition to specific hosts.

WARNING: When configuring a control path using an FC I/O blade connection, the partition LUN can be presented multiple times through any FC I/O blade and even the MCB at the same time. In a direct attached control path configuration, you can choose the drive to present the partition and it remains dedicated to the drive until you change it to another drive.

Table 1 Control Path Matrix

GUI Menu Path	User Guide Procedures	MCB Direct Connection	FC I/O Blade Connection	HP LTO-5 EEB Direct Connection[a]	HP LTO-5 EEB Connection w/SNW License[b]
Setup > Partitions > Configure	Creating Partitions	**Step 1**	**Step 1**	**Step 1**	**Step 1**
Setup > Connectivity	Configure FC I/O Blade Port Configuration FC Host Port Failover Enabling a Target Port Configuring Datapath Conditioning		**Step 2**		
Setup > Connectivity	Port Configuration	**Step 2**			
Setup > Device > Access	FC Host LUN Mapping Channel Zoning Creating SCSI Host LUN Mapping Assignments Using the LUN Mapping Wizard	**Step 3**	**Step 3**		
Setup > Partitions > Control Path	Configuring Control Path (if appropriate, Control Path Failover)			**Step 2**	**Step 2**
Setup > Device > Access > SNW Drives	Selecting a Storage Networking Drive				**Step 3**

Table 1 Control Path Matrix

GUI Menu Path	User Guide Procedures	MCB Direct Connection	FC I/O Blade Connection	HP LTO-5 EEB Direct Connection[a]	HP LTO-5 EEB Connection w/SNW License[b]
Setup > Device > Access > SNW Host	SNW (Storage Networking) Host				**Step 4**

[a] Only HP LTO-5 drives support control path bridging.
[b] Only HP LTO-5 Storage Networking licensed drives can be configured for control path failover.

Control Path Failover

The Scalar i6000 provides support for configuring the HP LTO-5 SNW licensed drive for control path failover. When control path failover is used, one drive is assigned as the primary control path and another drive as the control path failover (secondary) drive. The control path failover drive is used whenever the primary control path drive fails, becomes inoperable, or loses connectivity.

To configure a control path failover drive, you must have a Storage Networking License (SNW). Storage Networking (SNW) is a licensable feature that allows you to take advantage of the control path failover and host access configuration features of 8 GB/ HP LTO-5 tape drives, without those drives being connected to a 4 GB/Fibre Channel I/O blade.

For instructions on adding a license key, refer to "Setting Up EKM on the Scalar i6000" in *Scalar i6000 User's Guide*.

Note: A control path and failover drive consumes two drive counts from the SNW license.

The existing Control Path (CP) feature can be enabled or disabled by selecting or deselecting the Enable Control Path check box on the Control Path dialog box. If the partition has multiple drives covered by the SNW license, then you can select a Control Path Failover (CPF) drive from the CPF Selection table. This drive will be used as the active CP drive in the case where the primary CP drive fails.

Functionality exists to manually "failover" and "failback" among the configured control path drives to allow control path and drive diagnostics. For information about CPF configuration requirements, refer to CPF Configuration Guidelines on page 6.

CPF Configuration Guidelines

A logical library partition's media changer control path can be configured via a control path drive. In such configuration, the library control path is hosted by the drive's physical FC port and uses the same World Wide Port Name (WWPN) associated with the selected tape drive. While the tape drive (SSC device) responds as LUN 0 at the WWPN, the partition media changer (SMC device) responds as LUN 1 at the WWPN.

For example, consider such a drive configured to host the library control path. A switch could detect the tape drive as LUN 0 with WWPN 500308c0:9e2c3001 and detect the media changer as LUN 1 with WWPN 500308c0:9e2c3001 also via switch port 1:

```
[11:0:0:0]   tape         fc:0x500308c09e2c3001 ,   0x010100       /dev/st0  /dev/
sg2

[11:0:1:1]   mediumx    fc:0x500308c09e2c3001,     0x010101        /dev/sg3
```

If two drives are configured for library control path failover functionality, then the library control path will be able to failover to the configured redundant failover drive. In this type of configuration, the library control path is not hosted by a drive's physical FC port, but via a virtual port with a unique WWPN, reporting the SMC device also as LUN 0. Such configuration also requires that the two configured control path drives (primary and secondary) are connected to the same switch, which must support N-Port ID Virtualization (NPIV), and that the drives connect with point-to-point connection topology.

Virtual port WWPNs are based on the library's WWNN and are identified by the WWPN’s last 12 bits. A partition’s control path configured via a virtual port would end in 0x7FF for the first partition, 0x7FE for the second partition, 0x7FD for the third partition and so on. The partition's virtual port is presented by only one of the configured failover drives. If the active path to the media changer fails due to a FC cable issue, a drive failure or even a drive removal, the library control path will switch to the secondary drive and appear to the SAN via the same WWPN.

For example, consider two drives configured for control path failover configured within the first partition. A switch could detect the two tape drives as LUN 0 with WWPNs 500308c0:9e2c3001 and 500308c0:9e2c3005 at switch ports 1 and 2, and detect the media changer also as LUN 0 with WWPN 500308c0:9e2c37ff via switch port 1:

```
[11:0:0:0]   tape         fc:0x500308c09e2c3001 ,   0x010100       /dev/st0  /dev/
sg2

[11:0:1:0]   mediumx    fc:0x500308c09e2c37ff,      0x010101        /dev/sg3

[11:0:2:0]   tape         fc:0x500308c09e2c3004,    0x010200       /dev/st1  /dev/
sg4
```

If the drive hosting the library control path fails, or the link from switch port 1 to the hosting drive fails, the control path failover drive would take over and the switch would detect the media changer device no longer on port 1, but port 2:

```
[11:0:1:0]   mediumx    fc:0x500308c09e2c37ff,      0x010201        /dev/sg3

[11:0:2:0]   tape         fc:0x500308c09e2c3004,    0x010200       /dev/st1  /dev/
sg
```

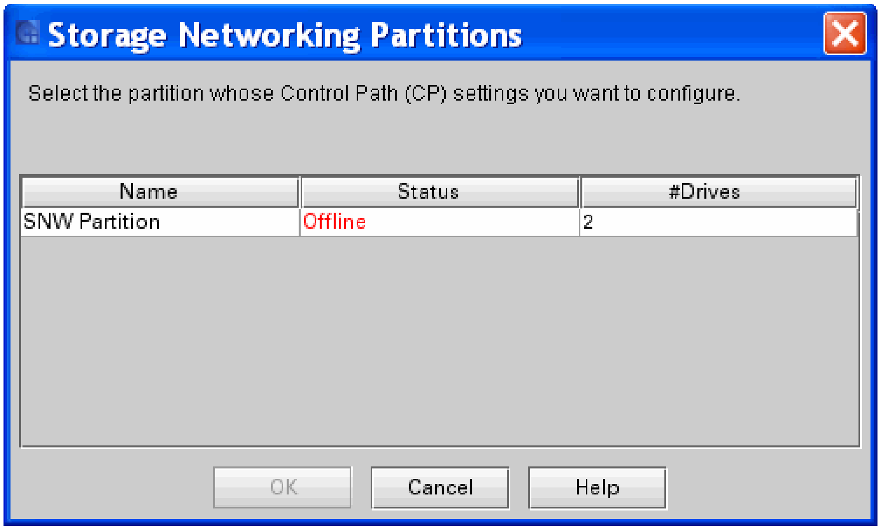
Configuring Storage Networking Partitions

Follow the steps below to select a partition and configure the control path.

1 Log on as an administrator.

2 From the main console, select Setup > Partitions > Control Path.

The Storage Networking Partitions dialog box appears.



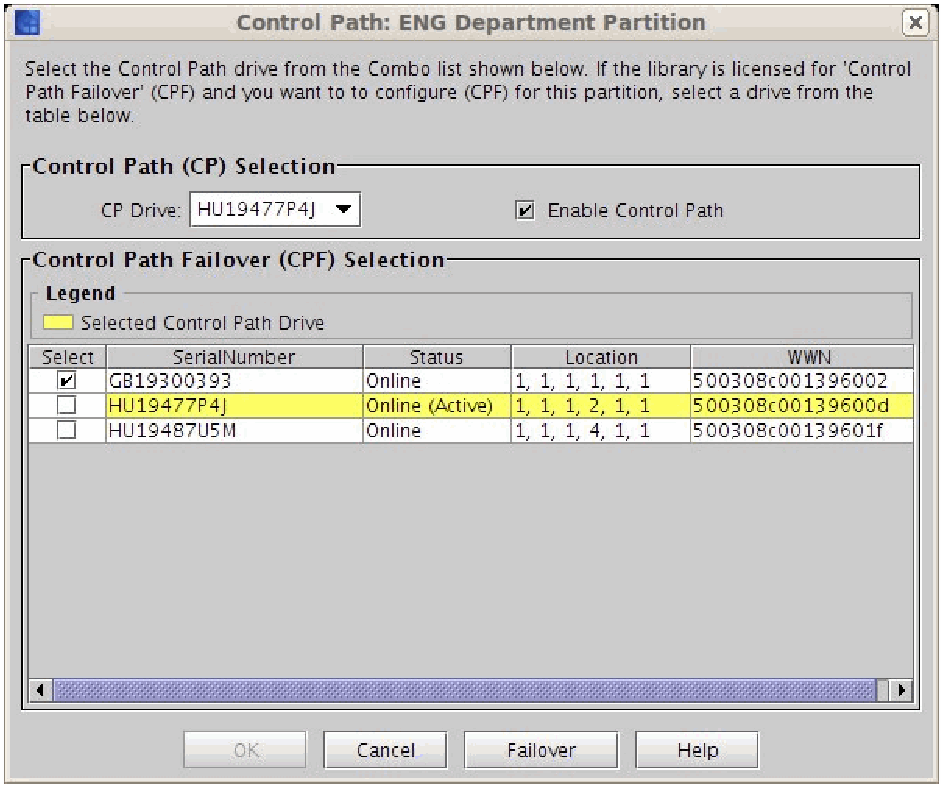
Storage Networking Partitions

Select the partition whose Control Path (CP) settings you want to configure.

Name	Status	#Drives
SNW Partition	Offline	2

3 Highlight the partition you want to configure, and click **OK**.

The **Control Path** dialog box appears.



Control Path: ENG Department Partition

Select the Control Path drive from the Combo list shown below. If the library is licensed for 'Control Path Failover' (CPF) and you want to to configure (CPF) for this partition, select a drive from the table below.

Control Path (CP) Selection

CP Drive: HU19477P4J

☑ Enable Control Path

Control Path Failover (CPF) Selection

Legend

🟨 Selected Control Path Drive

Select	SerialNumber	Status	Location	WWN
☑	GB19300393	Online	1, 1, 1, 1, 1, 1	500308c001396002
□	HU19477P4J	Online (Active)	1, 1, 1, 2, 1, 1	500308c00139600d
□	HU19487U5M	Online	1, 1, 1, 4, 1, 1	500308c00139601f

4 Click the **Enable Control Path** check box.

5 A check box appears and the **CP Drive** drop-down list is enabled.

6 From the **CP Drive** drop-down list select the drive you want to configure as the control path.

7 The primary CP drive you selected is highlighted in yellow.

Note: You must have a SNW license with sufficient drive counts to configure a CPF drive.

8 To select a CPF drive, click the **Select** check box for the desired drive.

9 Click **OK**.

10 An **Operation in Progress** dialog box appears.

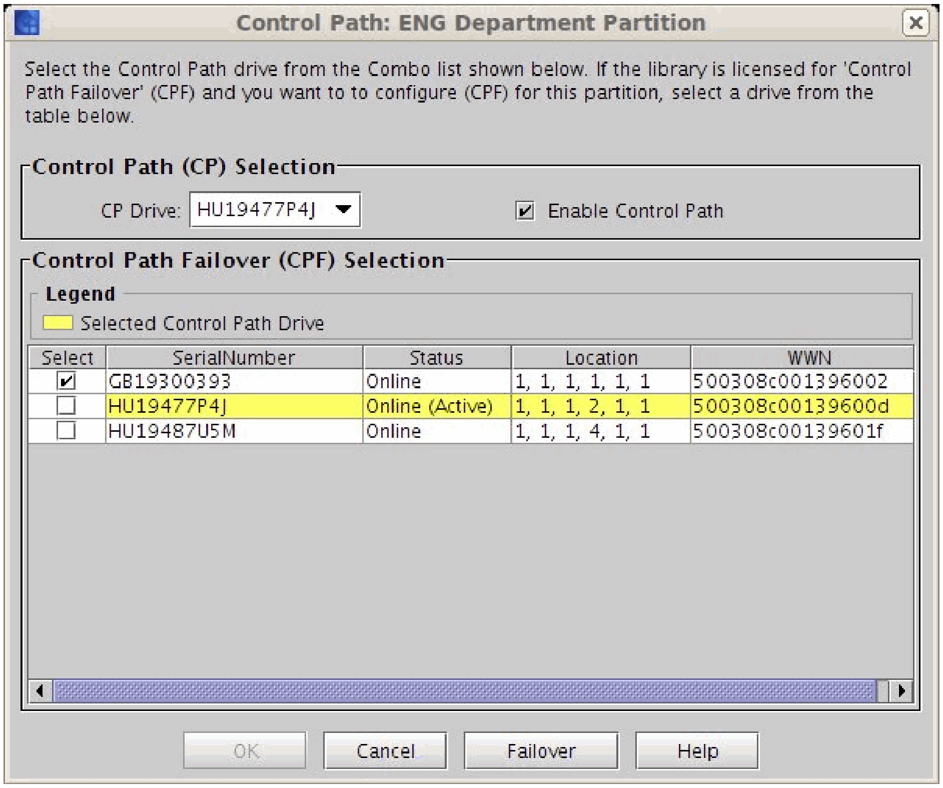
11 The CP and CPF drives are configured.

Manual Failover / Failback between Drives

If maintenance needs to be carried out on the currently active CP drive, you can force that drive to failover to the non-active CP drive.

12 From the main console, select **Setup** > **Partitions** > **Control Path**.

The **Control Path** dialog box appears, with the CP drive highlighted, and the CPF drive checked.



Control Path: ENG Department Partition

Select the Control Path drive from the Combo list shown below. If the library is licensed for 'Control Path Failover' (CPF) and you want to to configure (CPF) for this partition, select a drive from the table below.

Control Path (CP) Selection

CP Drive: HU19477P4J

☑ Enable Control Path

Control Path Failover (CPF) Selection

Legend

🟨 Selected Control Path Drive

Select	SerialNumber	Status	Location	WWN
☑	GB19300393	Online	1, 1, 1, 1, 1, 1	500308c001396002
☐	HU19477P4J	Online (Active)	1, 1, 1, 2, 1, 1	500308c00139600d
☐	HU19487U5M	Online	1, 1, 1, 4, 1, 1	500308c00139601f

13 Click the **Failover / Failback** button.

14 A warning message appears informing that switching the active CP drive could cause temporary loss of communication to the host application.

15 If you still want to perform this operation, click **Yes** to continue.

The new active CP drive is configured.

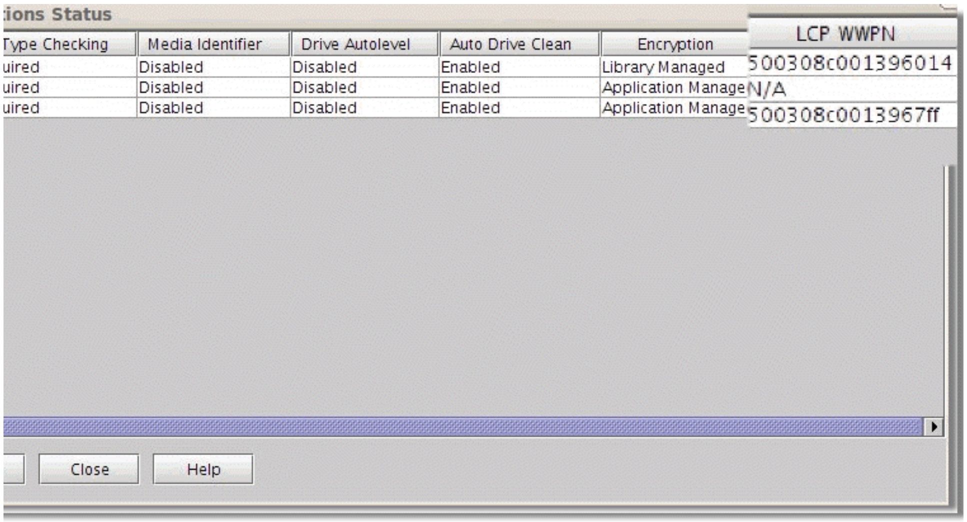
World Wide Port Name (WWPN) Listed for CP Failover Partition

When using the CP failover feature the partition is given a virtual WWPN. The GUI now displays the WWPN for each virtual partition. You will need this WWPN to build zoning for the partition.

The following dialog boxes are changed to display the WWPN.

1 Click **Monitor** > **Partitions.**

The **Partition Status** dialog box appears.



:ions Status

Type Checking	Media Identifier	Drive Autolevel	Auto Drive Clean	Encryption	LCP WWPN
uired	Disabled	Disabled	Enabled	Library Managed	500308c001396014
uired	Disabled	Disabled	Enabled	Application Manage	N/A
uired	Disabled	Disabled	Enabled	Application Manage	500308c0013967ff

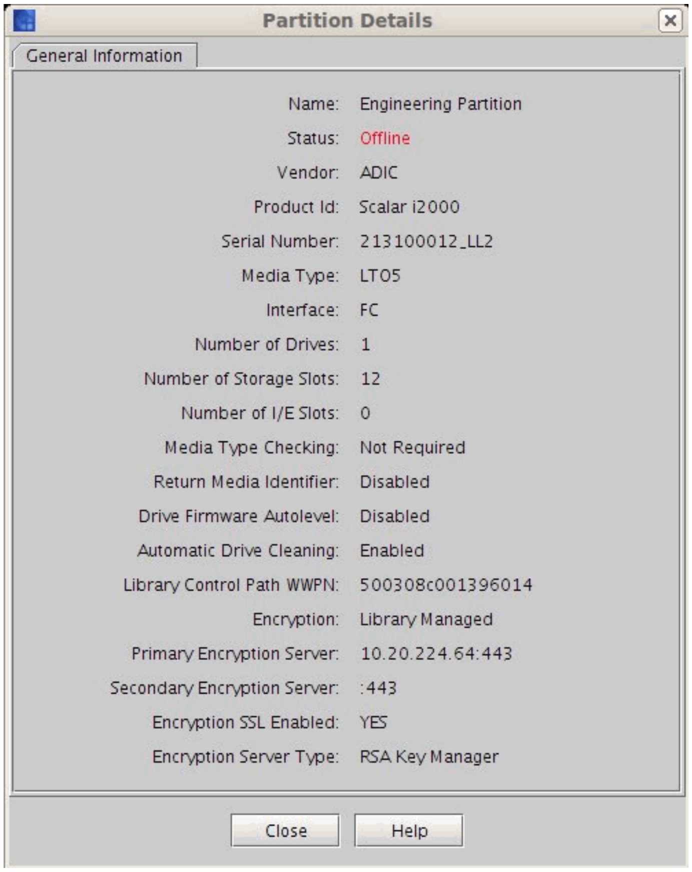
The following table describes the elements on the **Partitions Status** dialog box.

Element	Description
Name	The name of the partition.
Status	The status of the partition (Online or Offline).
Media Type	The type of media used in the partition (LTO-1, LTO-2, LTO-3, LTO-4, LTO-5, or DLT).
Interface	The type of interface used to connect to the host (FC or SCSI).
#Drives	The number of tapes drives in the partition.
#Storage Slots	The number of storage slots in the partition.
#I/E Slots	The number of I/E station slots in the partition.
Media Type Checking	The current setting for media type checking (Required, Not Required, or Disabled).
Media Identifier	The current setting for return media identifier (Suffix, Pass Through, Prefix, or Disabled).

Element (Continued)	Description
Drive Autolevel	The current setting for drive firmware autoleveling (Enabled or Disabled).
Auto Drive Clean	The current setting for automatic drive cleaning (Enabled or Disabled).
Encryption	Reports whether the media is encrypted. The values are Not Supported, Application Managed, or Library Managed.
LCP WWPN	The Library Control Path (LCP) World Wide Port Name (WWPN) for a virtual partition.

2 To view partition details, click **Details.**

The **Partition Details** dialog box appears.



Name: Engineering Partition
Status: Offline
Vendor: ADIC
Product Id: Scalar i2000
Serial Number: 213100012_LL2
Media Type: LTO5
Interface: FC
Number of Drives: 1
Number of Storage Slots: 12
Number of I/E Slots: 0
Media Type Checking: Not Required
Return Media Identifier: Disabled
Drive Firmware Autolevel: Disabled
Automatic Drive Cleaning: Enabled
Library Control Path WWPN: 500308c001396014
Encryption: Library Managed
Primary Encryption Server: 10.20.224.64:443
Secondary Encryption Server: :443
Encryption SSL Enabled: YES
Encryption Server Type: RSA Key Manager

This dialog box provides a summary of the partition configuration. Refer to the *Scalar i6000 User’s Guide* for field descriptions.

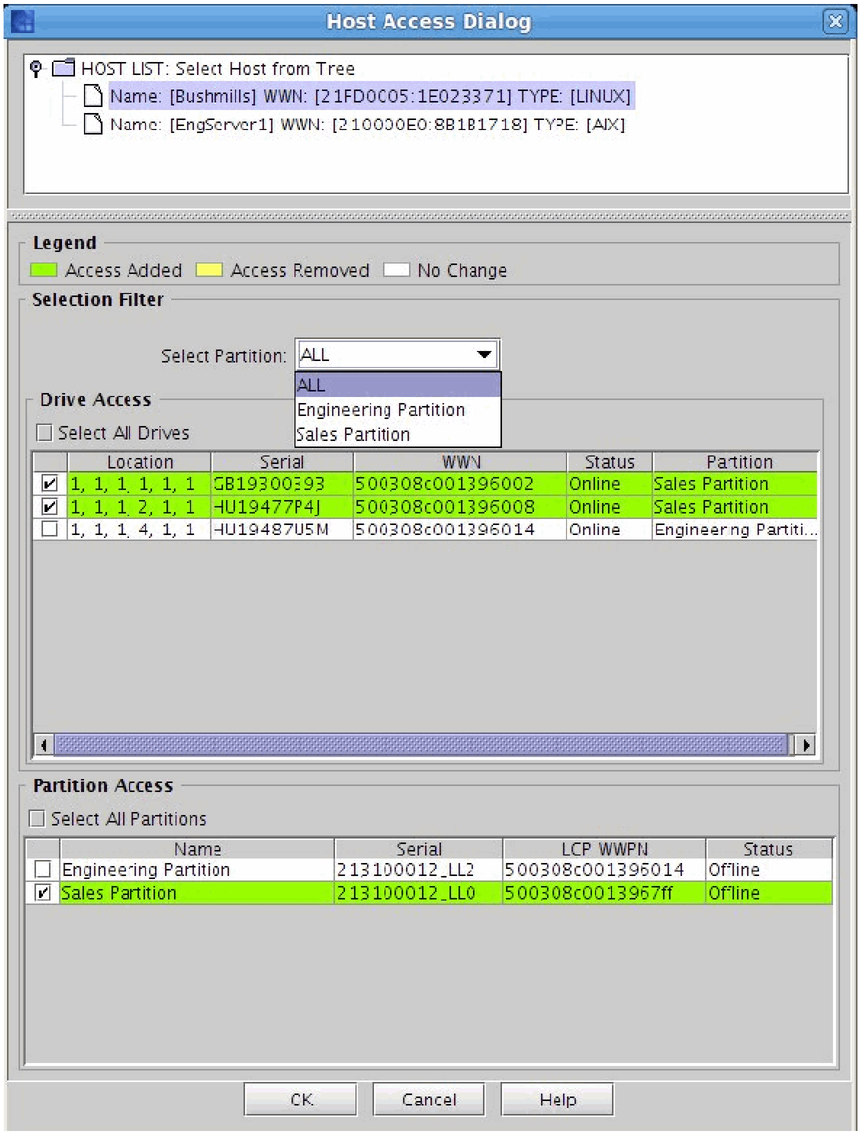
Accessing the SNW Host Device

The list of hosts and partitions on the **Host Access** dialog box includes both the WWN (World Wide Name) and WWPN (World Wide Port Name).

1 Select **Setup** > **Device** > **Access** > **SNW Host**.

2 In the **Host Configured** section, select the appropriate host or click the check box for **Select All Hosts**.

3 On the **Storage Networking Host Configuration** dialog box, click **Access**.



HOST LIST: Select Host from Tree
- Name: [Bushmills] WWN: [21FD0C05:1E023371] TYPE: [LINUX]
- Name: [EngServer1] WWN: [210000E0:8B1B1718] TYPE: [AIX]

Legend

🟩 Access Added 🟨 Access Removed ☐ No Change

Selection Filter

Select Partition: ALL

- ALL
- Engineering Partition
- Sales Partition

Drive Access

☐ Select All Drives

	Location	Serial	WWN	Status	Partition
☑	1, 1, 1, 1, 1, 1	GB19300393	500308c001396002	Online	Sales Partition
☑	1, 1, 1, 2, 1, 1	HU19477P4J	500308c001396008	Online	Sales Partition
☐	1, 1, 1, 4, 1, 1	HU19487U5M	500308c001396014	Online	Engineering Partiti...

Partition Access

☐ Select All Partitions

	Name	Serial	LCP WWPN	Status
☐	Engineering Partition	213100012_LL2	500308c001396014	Offline
☑	Sales Partition	213100012_LL0	500308c0013967ff	Offline

Updated Glossary Definitions

Control Path Failover (CPF)

The Scalar i6000 provides support for configuring the HP LTO-5 drive for control path failover. To configure a control path failover drive, you must have a Storage Networking License (SNW).

When control path failover is used, one drive is assigned as the primary control path and another drive as the control path failover (secondary) drive. The control path failover drive is used whenever the primary control path drive fails or is inoperable.

Storage Networking (SNW)

A licensable feature that allows you to take advantage of the control path failover and host access configuration features of 8 GB/ HP LTO-5 tape drives, without those drives being connected to a 4 GB/Fibre Channel I/O blade.

Data Path Failover

You can use Data Path Failover to allow an alternate data path when a preferred data path fails. Data Path Failover is provided as part of the Storage Networking license and applies to HP LTO-5 Fibre Channel tape drives only.

The HP LTO-5 Fibre Channel tape drives have two Fibre Channel ports. If you enable Data Path Failover on the tape drive, one port will be used as the "active port" for data transmission, and the other port will stand by to be used if the active port fails. If the tape drive loses its Fibre Channel link with the active port,

it will automatically "fail over" and use the standby port to continue drive operations.

Custom Verification Test

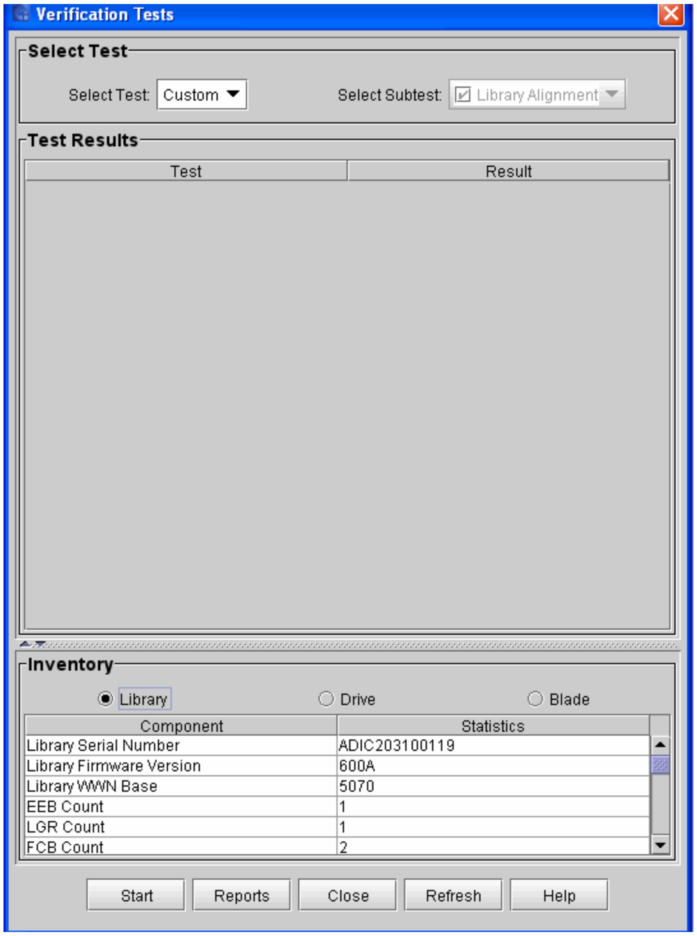
A new custom test has been added. This feature enables you to run the Library Alignment sub-test on a per-rack basis.

For future releases, this functionality will be expanded to allow you to create a custom test comprised of chosen sub-tests.

Running Custom Tests

1. Make sure that you are viewing the physical library. From the View menu, click the name of the physical library.
2. Click **Tools > Verification Tests**.

The Verification Tests dialog box appears.



Verification Tests

Select Test

Select Test: Custom

Select Subtest: ☑ Library Alignment

Test Results

Test	Result

Inventory

● Library ○ Drive ○ Blade

Component	Statistics
Library Serial Number	ADIC203100119
Library Firmware Version	600A
Library WWN Base	5070
EEB Count	1
LGR Count	1
FCB Count	2

3 From the **Select Test** drop-down list, click **Custom**.

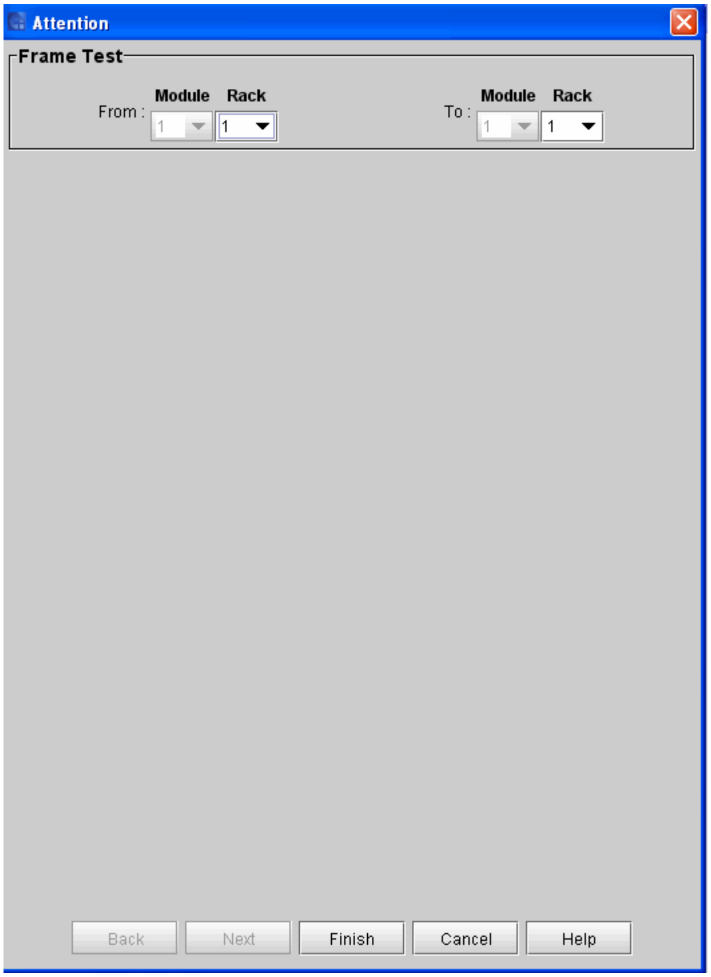
The **Select Subtest** field defaults to the Library Alignment subtest and cannot be changed.

4 Click **Start**.

5 If prompted to take the library offline, click **Yes**.

6 Click **Start**.

The following dialog box appears.

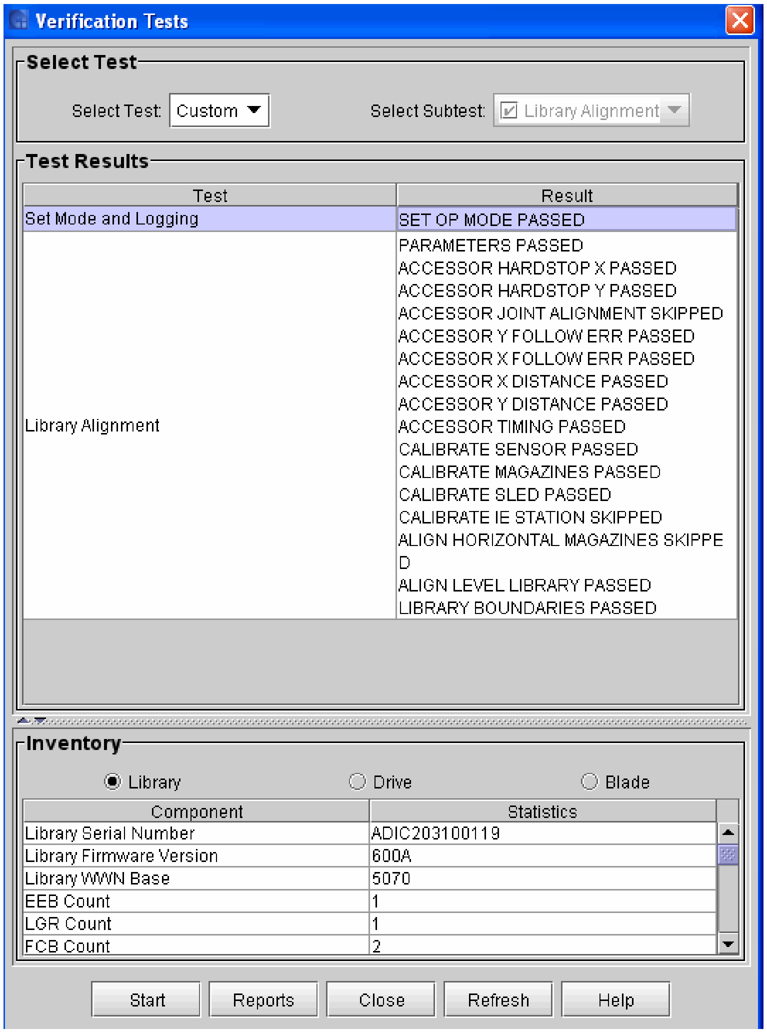


7 Select the starting Module (frame) and Rack as well as the ending Module (frame) and Rack where you want to perform the tests.

8 Click **Finish**.

The test is initiated.

Test progress is shown in the **Verification Tests** dialog box.



Select Test

Select Test: Custom

Select Subtest: ☑ Library Alignment

Test Results

Test	Result
Set Mode and Logging	SET OP MODE PASSED
Library Alignment	PARAMETERS PASSED ACCESSOR HARDSTOP X PASSED ACCESSOR HARDSTOP Y PASSED ACCESSOR JOINT ALIGNMENT SKIPPED ACCESSOR Y FOLLOW ERR PASSED ACCESSOR X FOLLOW ERR PASSED ACCESSOR X DISTANCE PASSED ACCESSOR Y DISTANCE PASSED ACCESSOR TIMING PASSED CALIBRATE SENSOR PASSED CALIBRATE MAGAZINES PASSED CALIBRATE SLED PASSED CALIBRATE IE STATION SKIPPED ALIGN HORIZONTAL MAGAZINES SKIPPE D ALIGN LEVEL LIBRARY PASSED LIBRARY BOUNDARIES PASSED

Inventory

● Library ○ Drive ○ Blade

Component	Statistics
Library Serial Number	ADIC203100119
Library Firmware Version	600A
Library WWN Base	5070
EEB Count	1
LGR Count	1
FCB Count	2

9 After the test is complete, click **Reports** to view the current or historical reports.