Scalar i500 User's Guide Addendum

6-01811-06 Rev A, March 2011

Purpose of this Document

The *Scalar i500 User's Guide* and the *Scalar i500 Getting Started Guide* are not being updated for this release. This Addendum explains the new features of this release, and provides updates on changes to existing features.

In particular, the user's guide and getting started guide contain inaccuracies with regard to the new features described here, so be sure to read New Features for i7 on page 3 and Updates/Changes to Existing User's Guide on page 13.

FIPS-Certified Encryption Solution

FIPS (Federal Information Processing Standard) 140-2 is a U.S. government standard relating to computer security and encryption.

With this release, the Quantum Scalar i500 now offers a FIPS 140-2 Level 1 certified encryption solution composed of the Scalar Key Manager and HP LTO-5 Fibre Channel tape drives in a Scalar i500 library. FIPS mode can be enabled on the HP LTO-5 tape drives via the library user interface. Once in FIPS mode, all encryption key communication between the tape drive and the library controller is authenticated and encrypted.

Details about configuring FIPS mode include:

- Library firmware must be at version 600G or later.
- HP LTO-5 FC tape drive firmware must be at the latest version qualified with the Scalar i500 library (see the *Scalar i500 Release Notes* for qualified firmware levels).
- An Encryption Key Management license must be installed on the library sufficient to cover the tape drive(s) on which you want to enable FIPS mode.
- A Storage Networking license must be installed on the library sufficient to cover the tape drive(s) on which you want to enable FIPS mode.
- FIPS mode is configured by partition. FIPS partitions must contain only HP LTO-5 FC tape drives.
- The partition encryption method must be set to **Enable Library Managed** in order to set FIPS mode.
- FIPS mode is disabled by default.
- Ethernet connectivity is required for the tape drives on which you want to enable FIPS mode. For most libraries, this requires one or more Ethernet Expansion blades installed on the library, unless your library consists of a single 5U control module. For 5U libraries, you can connect your tape drives directly to the Ethernet ports on the library control blade (LCB). See Tape Drive Ethernet Connectivity and the Ethernet Expansion Blade on page 6.
- The library must be connected to Scalar Key Manager. Scalar Key Manager software must be at version 2.0 or later in order to be FIPS certified.

Caution: If the Ethernet Expansion blade fails and the attached tape drives have FIPS mode enabled, all encryption operations (encrypting, decrypting, key requests) on the attached tape drives will fail. If this happens, contact Quantum Support for a replacement Ethernet Expansion blade as soon as possible.

Configuring the Library for FIPS

To configure your library for FIPS, perform the following steps:

1. Upgrade library firmware to version 600G or later.
2. For all HP LTO-5 FC tape drives that you plan to enable for FIPS, upgrade firmware to the latest version qualified with the Scalar i500 library (see the *Scalar i500 Release Notes* for qualified firmware levels).
3. Shut down the library.
4. Do one of the following:

If your library is...	Do this...
5U	Perform Cabling a 5U Library for Ethernet Connectivity on page 7.
14U or larger	Perform Installing the Ethernet Expansion Blade on page 9.

5. Power on the library.
6. Install Storage Networking and Encryption Key Management licenses on the library, if they are not already installed.
7. Enable FIPS mode (see Enabling and Disabling FIPS Mode on HP LTO-5 Tape Drives on page 4).

Enabling and Disabling FIPS Mode on HP LTO-5 Tape Drives

To operate your HP LTO-5 Fibre Channel tape drives to be compliant with FIPS, you must enable "FIPS mode." FIPS mode is configured by partition. You enable FIPS mode on a partition, which enables FIPS mode on all of the tape drives in the partition.

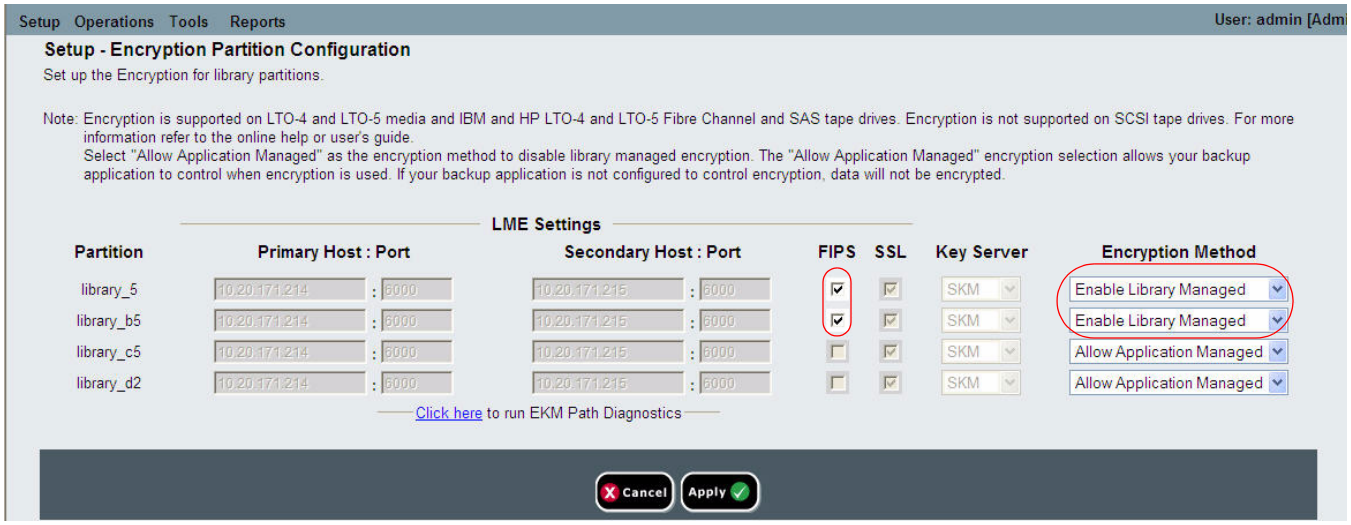
To change FIPS mode for a partition:

1. On the library web client, select **Setup > Encryption > Partition Configuration**.

   The **Setup - Encryption Partition Configuration** page displays (see Figure 1 on page 5).

   Change the Encryption Method of a partition to **Enable Library Managed**.
2. Select the **FIPS** check box to enable FIPS mode for the partition. Clear the **FIPS** check box to disable FIPS mode for the partition.
3. Click **Apply**.

Figure 1 Enabling FIPS Mode



Viewing FIPS Status on the Library

There are three ways to view FIPS status on the library:

- The Partition Configuration screen **(Setup > Encryption > Partition Configuration)** shows which partitions are enabled for FIPS. All tape drives in FIPS partitions are enabled.
- The System Information Report (**Reports > System Information)** contains a **FIPS** column in the **Library Partitions** section. The column displays "Yes" if FIPS is enabled on the partition and "No" FIPS is disabled.
- The tape drive information pop-up screen on the Library Configuration Report (**Reports > Library Configuration**) contains a **FIPS Enabled** item. This item only displays when the tape drive is an HP LTO-5 Fibre Channel tape drive. The item displays "Yes" when FIPS is enabled on the drive and "No" when FIPS is disabled.

Tape Drive Ethernet Connectivity and the Ethernet Expansion Blade

LTO-5 FC tape drives enable you to use tape drive Ethernet connectivity for FIPS-certified key exchanges, tape drive log collection, tape drive firmware updates, and tape drive firmware autoleveling via Ethernet instead of via internal serial communication. This speeds up operations and provides the security required for FIPS-certified key exchanges. 5U libraries can access tape drive Ethernet connectivity directly via the library control blade. For libraries greater than 5U, Quantum provides the Ethernet Expansion blade, which facilitates direct Ethernet connectivity between HP LTO-5 Fibre Channel tape drives and the library's internal Ethernet via the library control blade.

Details about tape drive Ethernet connectivity and the Ethernet Expansion blade include:

- Library firmware must be at version 600G or later.
- HP LTO-5 FC tape drive firmware must be at the latest version qualified with the Scalar i500 library (see the *Scalar i500 Release Notes* for qualified firmware levels).
- An Encryption Key Management license must be installed on the library sufficient to cover all the tape drives you intend to use for Ethernet operations.
- A Storage Networking license must be installed on the library sufficient to cover all the tape drives you intend to use for Ethernet operations.
- 5U libraries do not support an Ethernet Expansion blade. For 5U libraries, connect the HP LTO-5 FC tape drive to one of the internal Ethernet ports on the library control blade (see Figure 2 on page 8).
- In libraries that are greater than 5U, it is recommended that all HP LTO-5 FC tape drives be connected to an Ethernet Expansion blade. The Ethernet Expansion blade is provided as part of your FIPS-compliant solution when you purchase 8 Gb Storage Networking tape drives.
- The Ethernet Expansion blade is not in the data path and does not affect tape drive control paths.
- Each Ethernet Expansion blade has six Ethernet ports to allow you to attach up to six HP LTO-5 FC tape drives. Do not attach tape drives of any other type to the Ethernet Expansion blade.
- Do not connect the Ethernet Expansion blade to an external Ethernet source. The Ethernet Expansion blade is for internal Ethernet connectivity within the library.
- The Ethernet Expansion blade must be installed in the bottom left vertical bay in an expansion module. The empty bay to the right of the Ethernet Expansion blade must be covered by a cover plate.
- Libraries may contain both Ethernet Expansion blades and FC I/O blades.
- You may not connect a tape drive to both an Ethernet Expansion blade and an FC I/O blade.

- You are limited to a maximum of four blades per library (Ethernet Expansion blades and FC I/O blades), in any combination.
- If the tape drive Ethernet connection or an Ethernet Expansion blade fails, you will not be able to perform encryption operations on any connected tape drives that have FIPS mode enabled. You will still be able to collect tape drive logs and update tape drive firmware via internal serial communication.

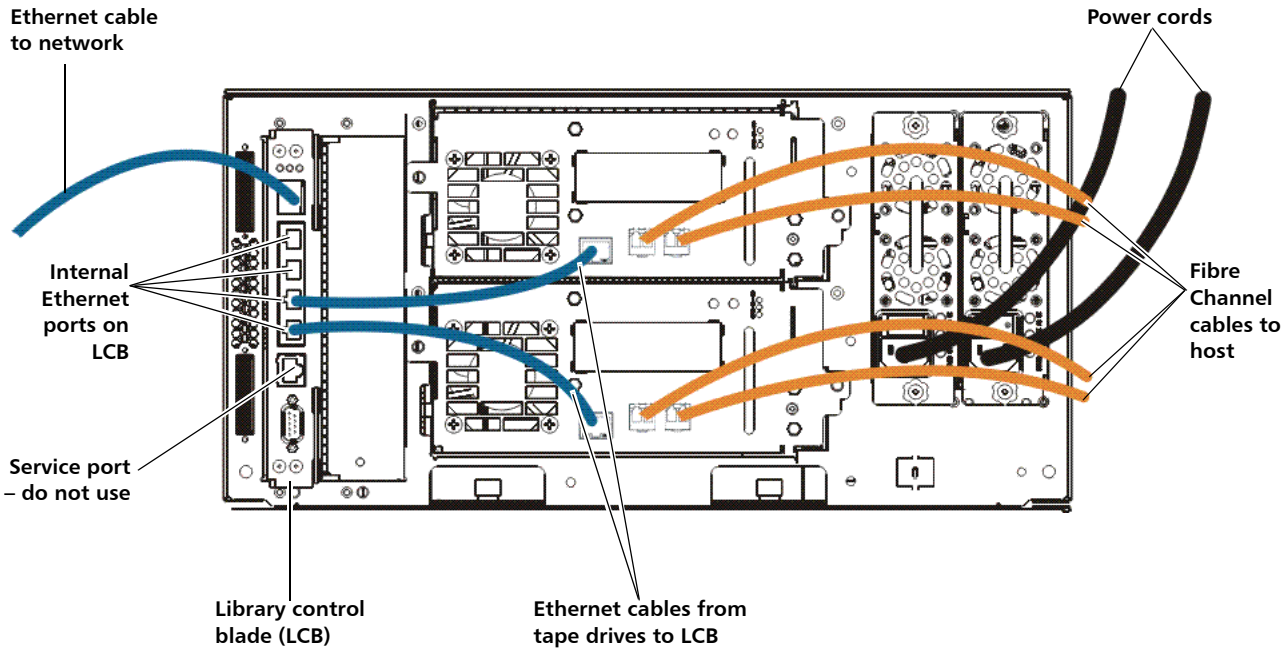
Caution: If the Ethernet Expansion blade or Ethernet connectivity fails and the attached tape drives have FIPS mode enabled, all encryption operations (encrypting, decrypting, key requests) on the attached tape drives will fail. These operations will NOT automatically continue over internal serial communication. If this happens, contact Quantum Support for a replacement Ethernet Expansion blade as soon as possible.

Cabling a 5U Library for Ethernet Connectivity

In a 5U library:

1. Upgrade library firmware to version 600G or later.
2. Upgrade tape drive firmware on all HP LTO-5 FC tape drives that you plan to connect via Ethernet to the latest version qualified with the Scalar i500 library (see the *Scalar i500 Release Notes* for qualified firmware levels).
3. Shut down the library.
4. Connect the tape drives to one of the four internal Ethernet ports on the library control blade (LCB) using Ethernet cables (see Figure 2).
5. Power on the library.

Figure 2 Ethernet Connectivity on 5U Libraries



Installing the Ethernet Expansion Blade

The Ethernet Expansion blade must be installed in the bottom left vertical bay in an expansion module. The empty bay to the right of the Ethernet Expansion blade must be covered by a cover plate.

Equipment Required

- Ethernet Expansion blade
- Cover plate
- Ethernet cables (one for each tape drive that you will connect to the Ethernet Expansion blade), plus an extra one per Ethernet Expansion blade, to connect the LCB to the expansion module in which the Ethernet Expansion blade is installed.

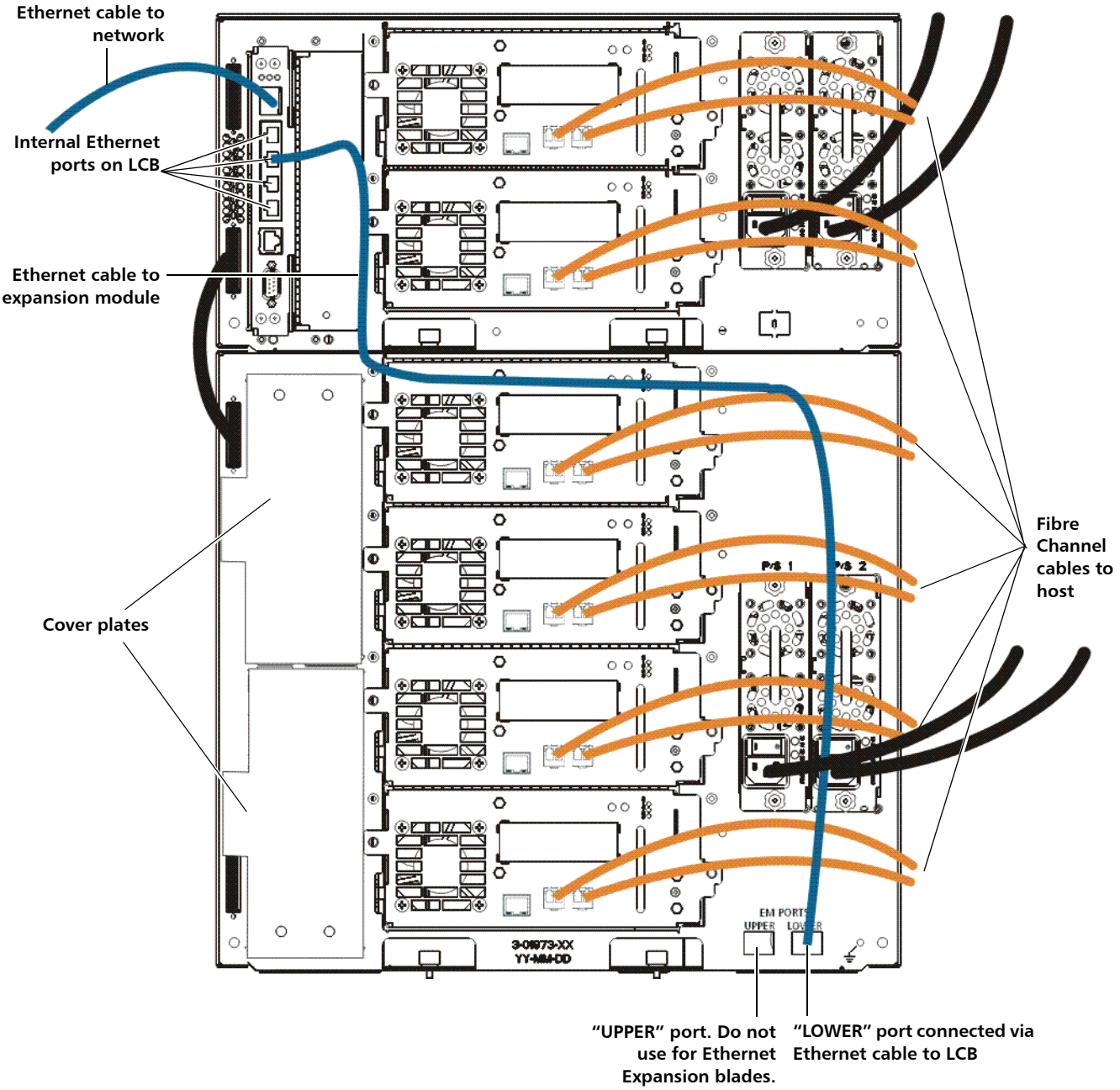
Tools Required

None

Instructions

1. Upgrade library firmware to version 600G or later.
2. Upgrade tape drive firmware on all HP LTO-5 FC tape drives that you plan to connect to the Ethernet Expansion blade to the latest version qualified with the Scalar i500 library (see the *Scalar i500 Release Notes* for qualified firmware levels).
3. Optional – Save the library configuration (see the *Scalar i500 User's Guide* for instructions).
4. Shut down the library.
5. For every expansion module that will contain an Ethernet Expansion blade, connect a standard Ethernet cable from one of the four internal Ethernet ports on the library control blade (LCB) to the Ethernet port marked "LOWER" located on the bottom right of the expansion module in which the Ethernet Expansion blade is installed. There are two ports, marked "UPPER" and "LOWER." Since the Ethernet Expansion blade must be installed in the lower bay of the expansion module, you must use the Ethernet port marked "LOWER." The "LOWER" port is on the right. See Figure 3.

Figure 3 Connecting the Library Control Blade to the Expansion Module Via Ethernet



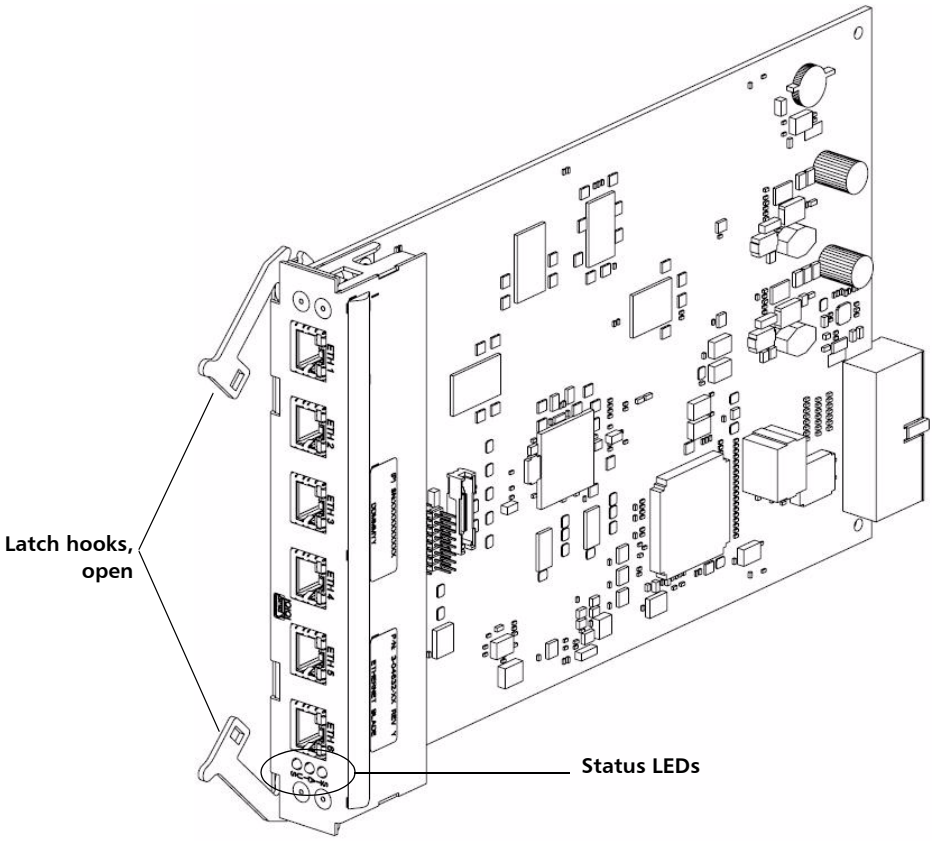
6 Prepare the library for Ethernet Expansion blade installation. The Ethernet Expansion blade must be installed in the bottom left bay of an expansion module.

- In some cases, this may require removal or relocation of an FC I/O blade and its accompanying fan blade. See the *Scalar i500 User's Guide* for detailed instructions.
- Remove the cover plate covering the two bottom left slots. To remove the cover plate, unscrew the two captive thumbscrews securing the cover plate and pull outward on the plate. Save the cover plate in case you need to use it later.

7 Remove the new Ethernet Expansion blade from the protective anti-static bag.

8 Press up and out to open the latch hooks on each side of the blade. Hold the Ethernet Expansion blade upright with the latch hooks on the left side, and the status LEDs at the bottom (see Figure 4).

Figure 4 Ethernet Expansion Blade



9 Carefully align the Ethernet Expansion blade with the guide slots in the bay.

Caution: Forcing the blade into the bay can cause the pins to bend.

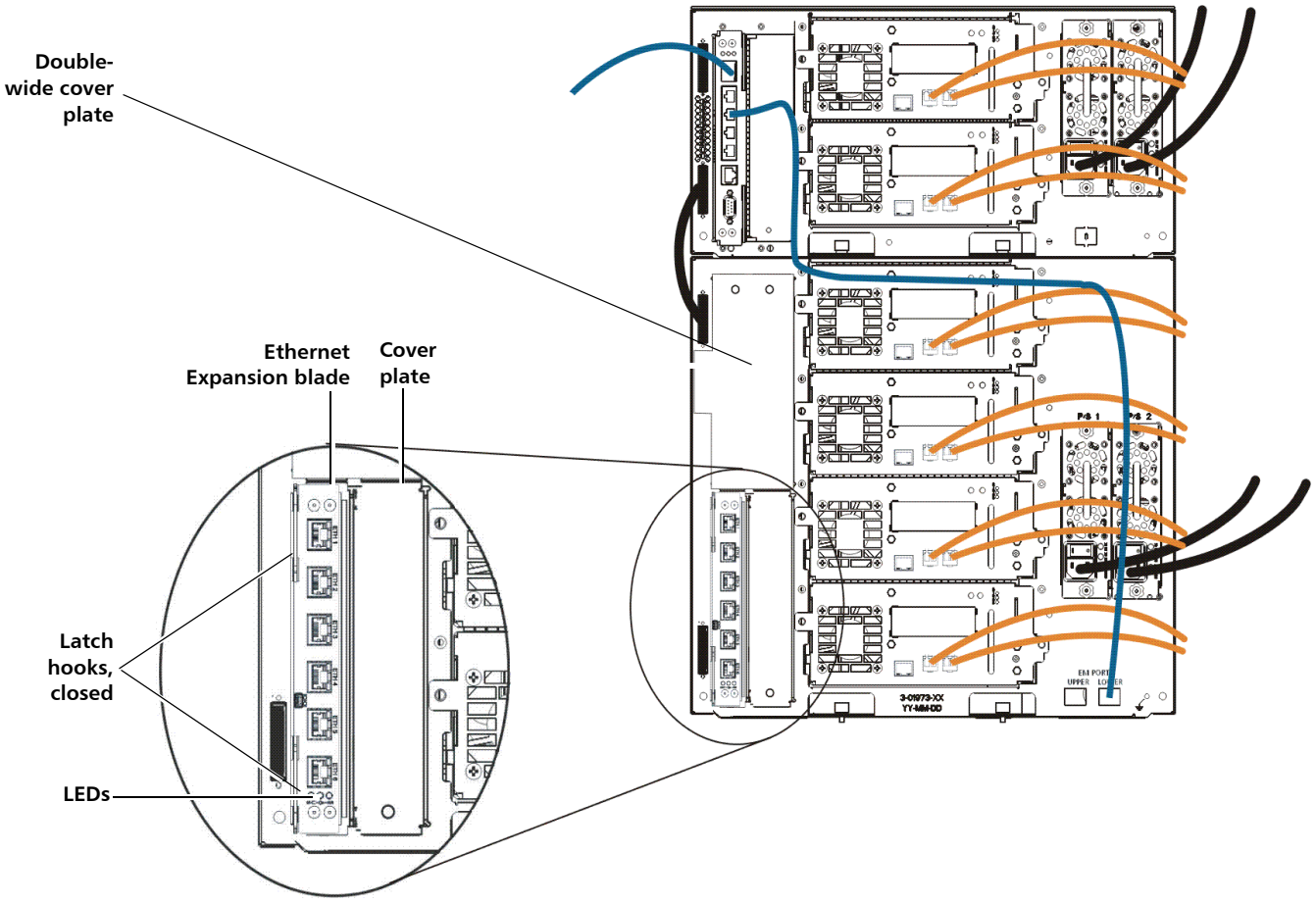
10 Evenly apply pressure to both sides of the blade and slide it into the expansion module until the latch hooks begin to move toward the middle of the blade. Push the latch hooks toward the middle of the blade and into the locked position. You will feel the blade pins connect with the expansion module's backplane as the blade locks into place.

11 Observe the status LEDs on the Ethernet Expansion blade. The blue LED should blink once every 10 seconds, indicating the blade is powered on. The green LED should blink once per second, indicating the blade's processor is working normally. The amber LED should be off.

12 Install a cover plate over the empty bay to the right of the Ethernet Expansion blade.

Caution: If the cover plate next to an Ethernet Expansion blade is not installed, Ethernet Expansion blade temperature errors will occur.

Figure 5 Installing the Ethernet Expansion Blade



13 Cable the Ethernet Expansion blade (see Cabling the Ethernet Expansion Blade on page 13).

14 Power on the library.

15 Verify the Ethernet Expansion blade is in the "Ready" state using one of these methods:

- Check the LEDs on the Ethernet Expansion blade. The green LED should blink once per second, the blue LED should blink once every 10 seconds, and the amber LED should be off.
- Use the library Web client:

  a Select **Tools > Diagnostics** to enter library diagnostics.

  A message warns you that entering diagnostics will log out all other users of the same or lower privilege level.

  b Click **OK** to agree to log all other users out.

  The diagnostics menu bar displays.

  c Select **Drives > EE Blade Control**.

  A message warns you that power cycling an Ethernet Expansion blade may cause key exchange failures if FIPS is enabled.

  d Click **OK** to proceed.

  The **Diagnostics - Ethernet Expansion Blade Control** screen displays (see Figure 7 on page 15).

  e Check the **Status** column for the Ethernet Expansion blade to be sure it says "Ready."

16 Save the library configuration (see the library user's guide for instructions).

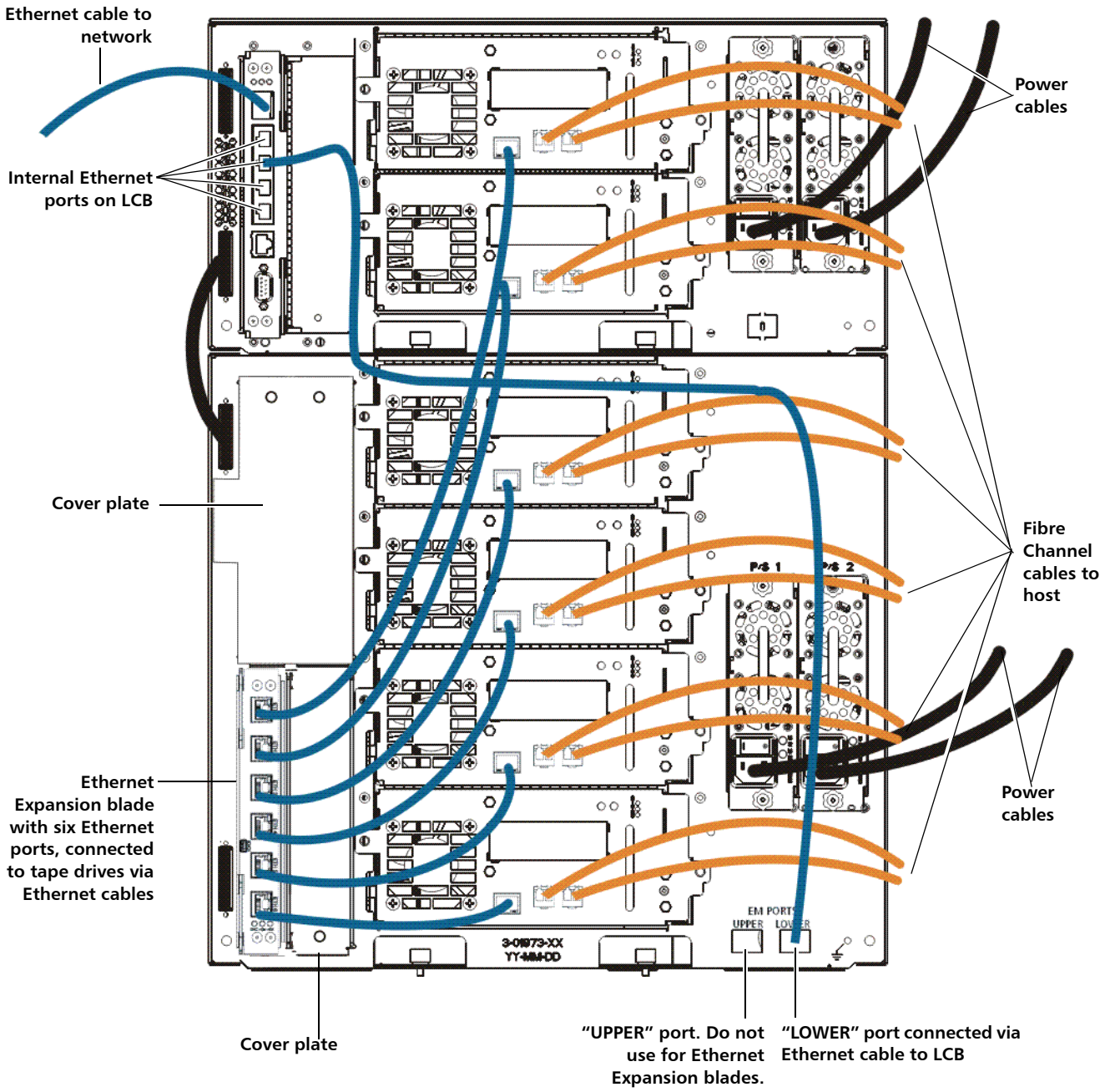
Cabling the Ethernet Expansion Blade

Cable the library and Ethernet Expansion blade as follows (see Figure 6 on page 14).

- In a 14U and higher library, it is recommended that you do not connect HP LTO-5 FC tape drives to the library control blade (LCB). Instead, you should connect the tape drives to an Ethernet Expansion blade using normal Ethernet cables.
- The Ethernet Expansion blade must be installed in the lower left slot of the expansion module. A cover plate must cover the slot next to the Ethernet Expansion blade. See Figure 6
- For every expansion module that contains an Ethernet Expansion blade, make sure a standard Ethernet cable is connected from one of the four internal Ethernet ports on the library control blade (LCB) to the Ethernet port marked "LOWER" located on the bottom right of the expansion module in which the Ethernet Expansion blade is installed. There are two ports, marked "UPPER" and "LOWER." Since the Ethernet Expansion blade must be installed in the lower bay of the expansion module, you must use the port marked "LOWER." The "LOWER" port is on the right. See Figure 6. You must do this BEFORE placing the Ethernet Expansion blade into the library as per the instructions in Installing the Ethernet Expansion Blade on page 9.

- Tape drives connected to an Ethernet Expansion blade must not be connected to an FC I/O blade. Instead, connect them to a host or switch.

Figure 6 Ethernet Connectivity on 14U and Higher Libraries



Permanently Removing or Relocating an Ethernet Expansion Blade

Library firmware monitors all Ethernet Expansion blades after they are installed in the library. Once an Ethernet Expansion blade is installed, the library expects the blade to be in the same installed location after every power cycle.

If an Ethernet Expansion blade is permanently removed from the library or relocated within the library, the library firmware must be configured to stop monitoring the EE blade. If this is not done and the library continues to monitor a removed EE blade, RAS tickets could be generated.

Note: You do not need to configure the library to stop monitoring an Ethernet Expansion blade if you are replacing a failed Ethernet Expansion blade with a new Ethernet Expansion blade in the same location (see Replacing an Ethernet Expansion Blade in the Same Location on page 16).

1. If you are permanently removing the Ethernet Expansion blade, disable FIPS mode on all Ethernet Expansion blade-connected tape drives FIRST before you remove the Ethernet Expansion blade. To disable FIPS mode, the tape drives must be Ethernet connected to allow the tape drives to reconfigure. See Enabling and Disabling FIPS Mode on HP LTO-5 Tape Drives on page 4.
2. Remove the Ethernet Expansion blade from the library's configuration as follows:
   a. On the library web client, select **Tools > Diagnostics** to enter library diagnostics.

      A message warns you that entering diagnostics will log out all other users of the same or lower privilege level.

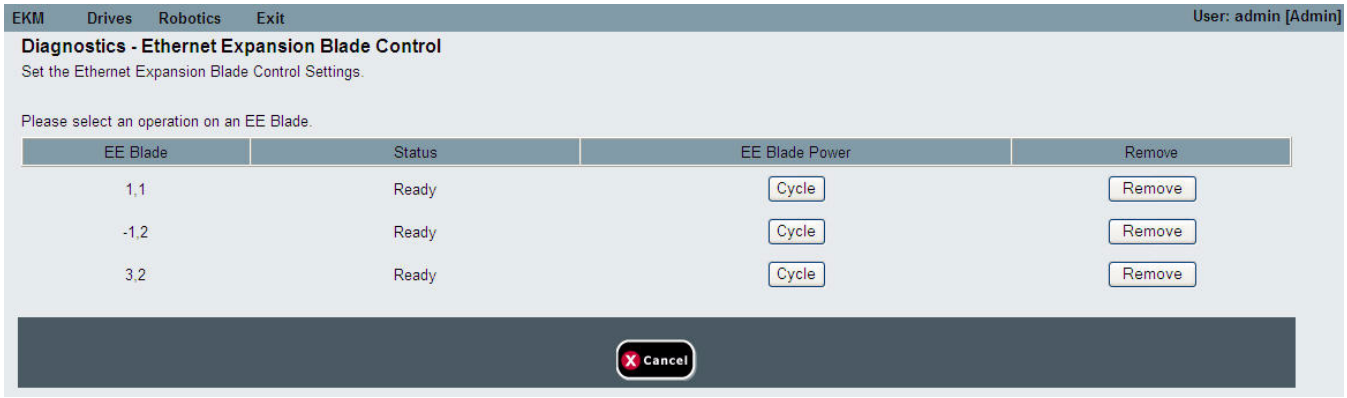
   b. Click **OK** to agree to log all other users out.

      The diagnostics menu bar displays.

   c. Select **Drives > EE Blade Control**.

      The **Diagnostics - Ethernet Expansion Blade Control** screen displays (see Figure 7).

Figure 7 Ethernet 27 Expansion Blade Control



d Click the **Remove** button corresponding to the Ethernet Expansion blade you want to remove.

Note: Removing an Ethernet Expansion blade may cause key exchange failures if FIPS is enabled. A message warns you about the possible failures and asks you to confirm that you want to proceed.

3 Click **OK** to proceed or **Cancel** to cancel the operation without removing the Ethernet Expansion blade.

4 Disconnect the Ethernet cables from the Ethernet Expansion blade.

5 Lift the latch hooks out of the lock position and push them up (see Figure 4 on page 11). You will feel the blade unplug from the library's backplane.

6 Continue lifting on the latch hooks until the Ethernet Expansion blade is totally unplugged from the backplane.

7 Slide the Ethernet Expansion blade out of the bay.

8 Remove the cover plate from the bay to the right of the Ethernet Expansion blade. Install the original double-wide cover plate over both bays. This is required for cooling and dust reduction. If you need a cover plate, contact Quantum.

9 Save the library configuration (see the library user's guide for instructions).

Replacing an Ethernet Expansion Blade in the Same Location

If you are replacing an Ethernet Expansion blade in the same location, you do not need to perform a "remove" operation via the web client as you would if you were permanently removing or relocating the Ethernet Expansion blade.

1 Disconnect the Ethernet cables from the Ethernet Expansion blade.

2 Lift the latch hooks out of the lock position and push them up (see Figure 4 on page 11). You will feel the blade unplug from the library's backplane.

3 Continue lifting on the latch hooks until the Ethernet Expansion blade is totally unplugged from the library's backplane.

4 Slide the Ethernet Expansion blade out of the bay.

5 Install the new Ethernet Expansion blade (see Installing the Ethernet Expansion Blade on page 9).

6 Save the library configuration (see the library user's guide for instructions).

Power Cycling the Ethernet Expansion Blade

Administrators can power cycle individual Ethernet Expansion blades in the library. You might want to power cycle an individual Ethernet Expansion blade when troubleshooting, such as when resolving a Reliability, Availability, and Serviceability (RAS) ticket. You can only power cycle the Ethernet Expansion blade from the Web client.

To power cycle an Ethernet Expansion blade:

1. On the Web client, select **Tools > Diagnostics** to enter library diagnostics.

   A message warns you that entering diagnostics will log out all other users of the same or lower privilege level.

2. Click **OK** to agree to log all other users out.

   The diagnostics menu bar displays.

3. Select **Drives > EE Blade Control**.

4. Click **OK** to proceed.

   The **Diagnostics - Ethernet Expansion Blade Control** screen displays (see Figure 7 on page 15).

5. Click the **Cycle** button corresponding to the Ethernet Expansion blade you want to power cycle.

   It takes approximately 1 minute to power cycle an Ethernet Expansion blade. The status displays as "Booting" during the power cycle.

Viewing Ethernet Connectivity

There are two places on the library Web client which tell you whether tape drives are connected via Ethernet (either via an Ethernet Expansion blade or connected directly to the library control blade). These two places are:

- **Tools > Drive Operations > Update tape drive firmware using a firmware image file**
- **Tools > Drive Operations > Retrieve Tape Drive Log**

The tape drive table in each of these screens has a column called **Ethernet Connected**. If the tape drive is connected via Ethernet, the tape drive IP address will be listed in the column. If the tape drive is Ethernet capable but not connected, the column displays "No." If the tape drive is not Ethernet capable, the column displays "N/A."

You can also view the location coordinates and Ethernet Expansion blade status in the library System Information Report:

- **Reports > System Information**

Ethernet Expansion Blade Status LEDs

The status LEDs for the Ethernet Expansion blade are located at the bottom of the Ethernet Expansion blade below ETH 6 (see Figure 8 on page 18).

Figure 8 Ethernet Expansion Blade LEDs

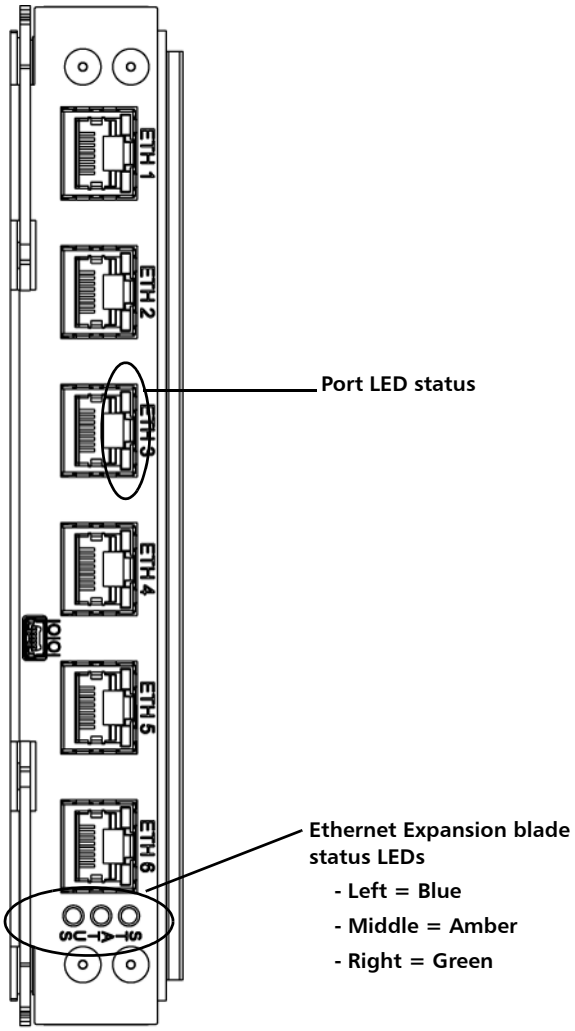


Table 1 Ethernet Expansion Blade Status LED Descriptions

LED Color	Represents	Blade Status
Green	Processor status	• Solid OFF — Blade's main processor is not operating (or blade is booting). • Solid ON — Blade's main processor is not operating. • Blinks once per second (1 Hz) — Normal.
Amber	Health status	• Solid OFF — Normal. • Solid ON — Failure or blade is autoleveling. In conjunction with the blue LED blinking once very 10 seconds, this is a normal condition. Autoleveling takes about three minutes per blade, and blades autolevel in series. Never remove a blade when the amber LED is solid ON unless it has been on continuously for at least 10 minutes.
Blue	Power control status	• Solid OFF — Blade is not receiving power. • Solid ON — Blade is not operational. • Blinks once every second (1 Hz) — Powered off. Ready to remove. • Blinks once per 10 seconds (flash) — Normal. Blade is powered on.

Table 2 Explanation of Ethernet Expansion blade Ethernet Port LED States

LED Color	Blade Status
Green	• Solid ON — Link is up; data can be sent or received through the Ethernet port. • Solid OFF — Link is down; data cannot be sent or received through the Ethernet port.
Amber	• Flashes at irregular intervals — Data activity is occurring through the Ethernet port. • Solid OFF — No data activity is occurring through the Ethernet port.

Data Path Failover

Data Path Failover is a new 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 latest version.

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. The library issues a RAS ticket when automatic 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, unless the reason Port 2 is active is due to a forced failover (see Forcing Data Path Failover on page 22). If you forced a failover to Port 2 and then reset the tape drive, the library and host will continue to use Port 2 until failover occurs again or the library is rebooted.

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.

If desired, you can manually switch the active port (see Forcing Data Path Failover on page 22).

Note: If you are NOT using data path failover on a tape drive, then only Port 1 is used for data path or control path transmission. Port 2 is only recognized by the library or host when data path failover is enabled on the tape drive.

Requirements for Data Path Failover

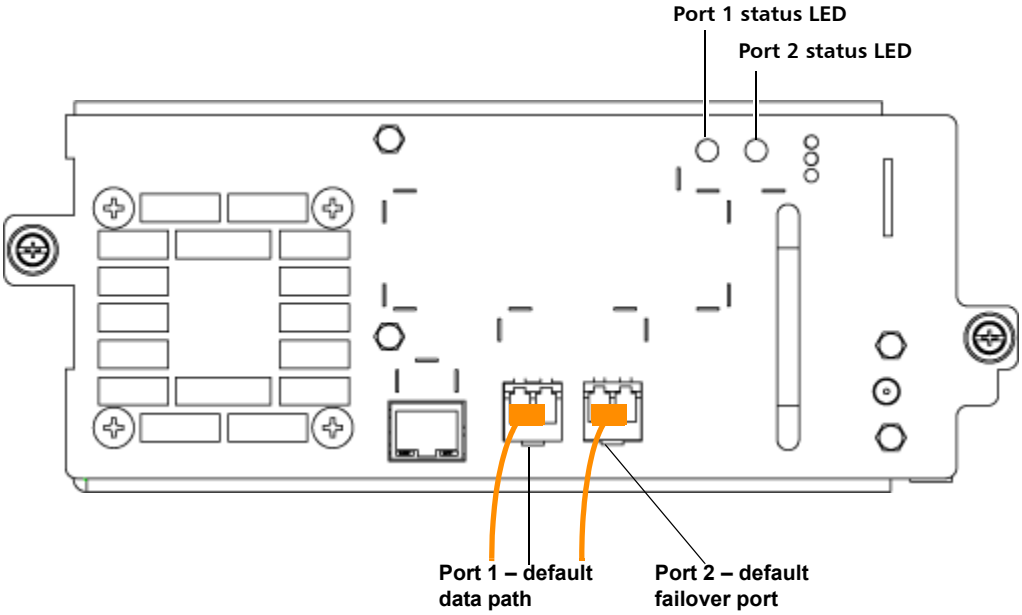
- The tape drives must be HP LTO-5 Fibre Channel tape drives.
- HP LTO-5 FC tape drive firmware must be at the version qualified with the Scalar i500 library (see the *Scalar i500 Release Notes* for qualified firmware levels).
- The library must have a Storage Networking license sufficient to cover the 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 Data Path Failover

To enable data path failover:

1 Connect both tape drive Fibre Channel ports (Port 1 and Port 2) to a host or switch (see Figure 9).

Figure 9 HP LTO-5 Fibre Channel Tape Drive Ports



2 From the library **Setup** menu, click **Drive Settings**.

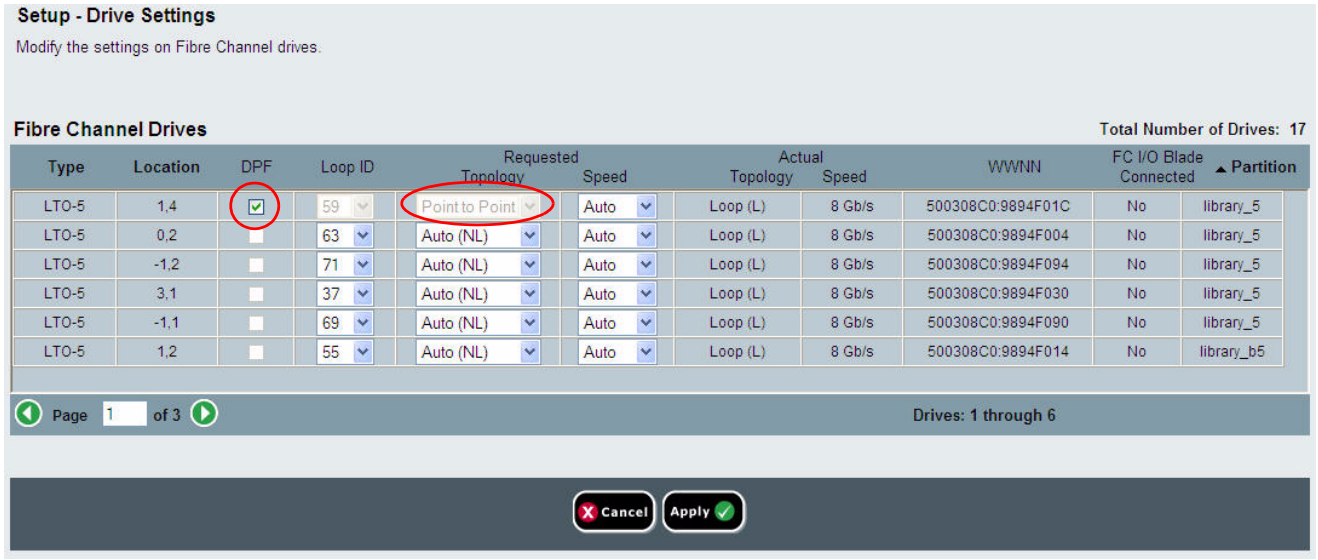
The **Setup - Drive Settings** page displays (see Figure 10).

3 For each tape drive on which you want to enable data path failover, do the following:

- **a** First, change the **Requested Topology** setting to **Point to Point.**
- **b** Then select the **DPF** check box.

4 Click **Apply**.

Figure 10 Enabling Data Path Failover



Forcing Data Path Failover

You can manually switch the active Fibre Channel port on a DPF-enabled tape drive by forcing a failover. You might want to force a failover to check that the non-enabled port still works, or to switch back to using Port 1 once the issue that originally caused it to fail over is fixed.

You can only force a failover on one tape drive at a time. Both Fibre Channel ports must be connected to a host or switch.

To force a failover:

1 From the **Tools** menu, select **Drive Operations**.

The **Tools - Drive Operations** screen displays (see Figure 11).

Figure 11 Forcing Data Path Failover

2 Select **Force Data Path Failover** and click **Next**.

The **Force Data Path Failover** page displays (see Figure 12). All of the tape drives that have data path failover enabled are listed. The port currently being used as the data path is listed in the **Active Port** column. The **Active Port** column will state "No Link" if neither port is connected.

Figure 12 Forcing Data Path Failover

3 Select the tape drive on which you want to force the failover.

Note: The tape drive must be in the "ready" state in order to be selected.

4 Click **Apply**.

The new active port displays in the **Active Port** column.

Note: If the new active port does not display, refresh the page in the browser.

Note: The library will issue a RAS ticket if the forced failover fails. The library will not issue a RAS ticket if the forced failover succeeds.

Automatic SKM Key Generation

When an SKM server has used 80 percent of the data encryption keys assigned to a particular library, that library attempts to automatically generate data encryption keys on the SKM server. In previous releases, you had to manually generate data encryption keys.

Both SKM servers must be running and operational in order for automatic key generation to succeed.

- **If automatic key generation succeeds**, a RAS ticket informs you the keys were generated and instructs you to back up both SKM servers as soon as possible.
- **If automatic key generation fails**, the library tries again every time a new key is requested, until the keys are 90 percent depleted. At that point, the library stops trying to auto-generate keys and issues a RAS ticket stating that you must manually generate keys. See the library user's guide for instructions on how to manually generate keys.

Forcing Control Path Failover

Control path failover is an existing feature that is available with HP LTO-5 tape drives and a Storage Networking license. This release expands this feature, allowing you to force a control path failover.

You might want to force a failover to check that the non-active tape drive still works, or to switch back to the original control path tape drive once the issue that originally caused the failover has been fixed.

To force a control path failover:

1 From the Web client, click **Tools > Drive Operations**.

The **Tools - Drive Operations** screen displays (see Figure 13).

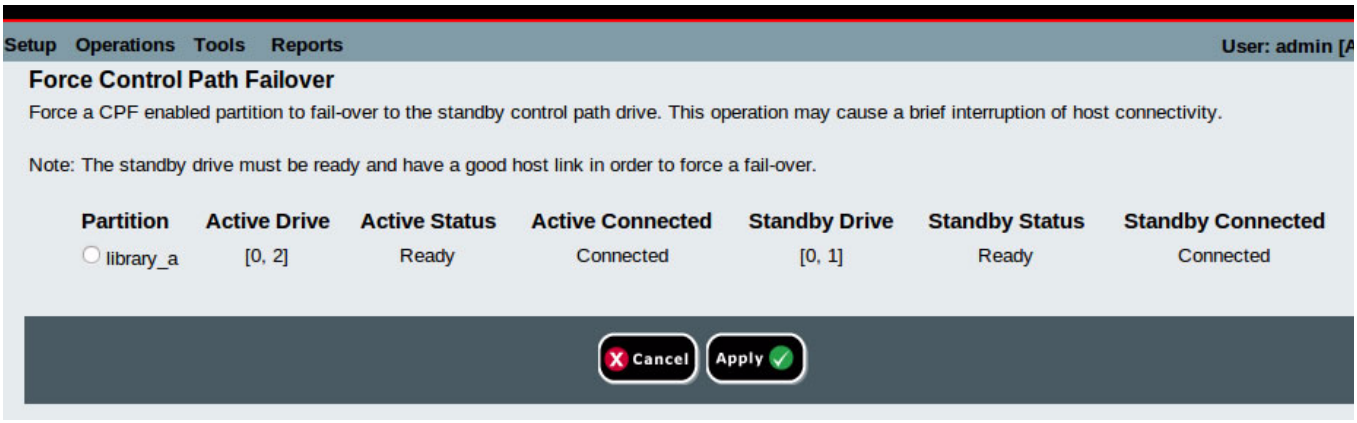
Figure 13 Forcing Control Path Failover

2 Select **Force Control Path Failover** and click **Next**.

The **Force Control Path Failover** screen displays (see Figure 14). All of the partitions that have control path failover enabled are listed. The location and status of the tape drive that is currently serving as the control path are listed in the **Active** columns. The location and status of the tape drive that is currently serving as the standby control path are listed in the **Standby** columns. For each partition, the following information is listed:

Column	Indicates
Active Drive	Location of the current control path tape drive.
Active Status	Ready status of the current control path tape drive.
Active Connected	Whether the current control path tape drive is connected and has a working link.
Standby Drive	Location of the standby tape drive.
Standby Status	Ready status of the standby tape drive.
Standby Connected	Whether the standby tape drive is connected and has a working link.

Figure 14 Forcing Control Path Failover



3 Select the partition on which you want to force the failover.

Note: The standby tape drive must be "ready" and "connected" in order to force a failover.

4 Click **Apply**.

The new active tape drive location displays in the **Active Drive** column. The new standby tape drive location displays in the **Standby Drive** column.

Note: If the new tape drive locations do not display, refresh the browser.

Updates/Changes to Existing User's Guide

This section provides updates to the current text in the *Scalar i500 User's Guide*.

LTO-5 Tape Drive Ports

The library handles the Ethernet and Fibre Channel ports on LTO-5 tape drives differently depending on the tape drive. With the addition of Ethernet Expansion blades and data path failover in this release, this information has changed since the last release.

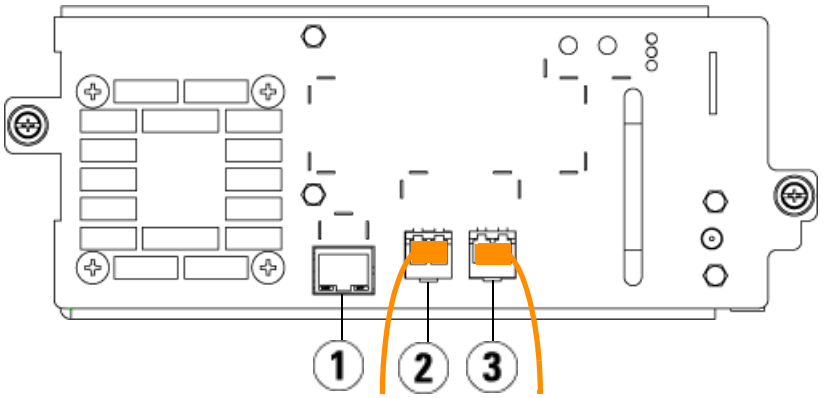
See Figure 15, Figure 16, and Figure 17 for details.

Caution: LTO-5 Fibre Channel tape drives can be configured for speeds of up to 8 Gb/s. If they are configured for 8 Gb/s, you should connect them directly to a host or switch and not to an FC I/O blade, because the FC I/O blade only allows speeds up to 4 Gb/s. If you connect an LTO-5 Fibre Channel tape drive to an FC I/O blade, the speed will autonegotiate 4 Gb/s.

Caution: If you enable data path failover, control path failover, or host access control, do not connect the tape drive to an FC I/O blade.

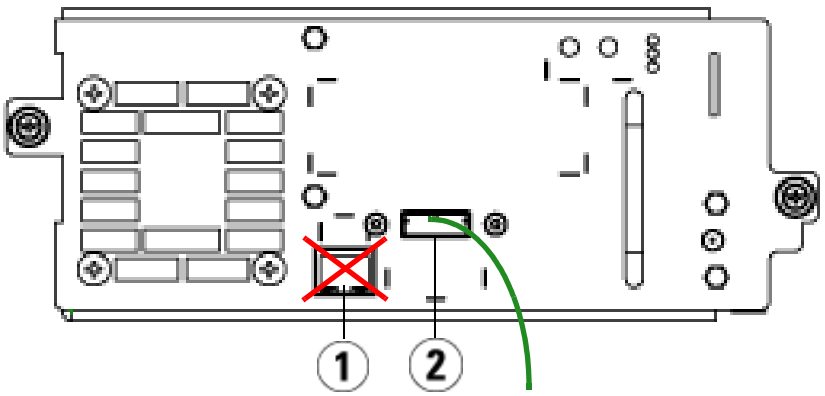
Caution: Do not connect a tape drive to both an FC I/O blade and an Ethernet Expansion blade.

Figure 15 HP LTO-5 Dual Port Fibre Channel Tape Drive



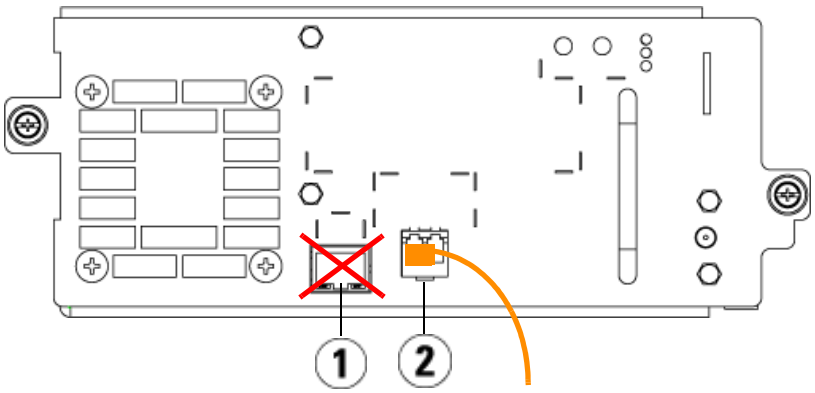
1 Ethernet port — Use for Ethernet connectivity in conjunction with FIPS.
2 Fibre Channel port 1 — Default data port. If you are only using one port, use this port.
3 Fibre Channel port 2 — Default failover port (for use with data path failover).

Figure 16 HP LTO-5 Single Port SAS Tape Drive



1 Ethernet port - do not use.
2 SAS port - use this port.

Figure 17 IBM LTO-5 Single Port Fibre Channel Tape Drive



1 Ethernet port - do not use.
2 Fibre Channel port - use this port.

Automatic RAS Ticket Closure

Automatic ticket closure is an new optional feature that closes all currently open RAS tickets when you reboot the library. If any errors occur during the reboot, the library issues new tickets.

In order for automatic ticket closure to occur, a user must intentionally initiate a reboot, either by restarting the library, shutting down the library, or upgrading library firmware. Automatic ticket closure will not occur if the library shuts down unexpectedly or if the power cord is unplugged.

You can always view closed tickets on the library Web client by selecting **Tools > All RAS Tickets** and clicking the **Include Closed Tickets** check box. Tickets that were auto-closed are designated as "Canceled."

Automatic ticket closure is enabled by default. You can enable or disable this feature from the operator panel. Select **Tools > System Settings** and then select or clear the **Auto-Ticket Closure** check box.

Web Client - Library View Removed

The "library view" has been removed as an optional view from the Web client home page.

Password Length

The maximum length for library user and administrator passwords has been increased from 12 to 16 characters.

Upgrading Firmware

You can no longer download library or tape drive firmware directly from the Quantum Web site. Instead, you must contact Quantum Support to receive the firmware upgrade file.

- To find out the latest version of library firmware, see the release notes or check the Quantum Web site at: http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SI500/Index.aspx.
- To find out the latest version of tape drive firmware, see the release notes.

Release notes and instructions for upgrading library and tape drive firmware can be found here: http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SI500/Index.aspx.

Viewing the Control Path for Partitions Configured for Control Path Failover

When control path failover is configured for a partition, the partition uses a virtual port as the control path communication port. The World Wide Port Name (WWPN) for this virtual port is listed in the System Information Report in the Library Partitions section under Control Path (**Reports > System Information**).

Handling LTO Tape Cartridges

The following text replaces/adds to the current text in the user's guide:

- For external long-term vaulted storage, store cartridges in a vertical orientation.
- If cartridges must be stacked horizontally for moving and handling, do not stack cartridges more than five high.
- The operating temperature range for Linear Tape Open (LTO) cartridges is 50ºF to 113ºF (10ºC to 45ºC). The operating relative humidity range is 10% to 80% (non-condensing). The storage temperature range is 60.8ºF to 89.6ºF (16º to 32ºC). Temperatures above 125.6ºF (52ºC) can cause permanent damage.

Tape Cartridge Barcode Labels

A maximum of 12 characters is recommended. A barcode label with more than 12 characters may not be printable according to the Code 39 label specifications for the tape cartridge area to which the label is attached. The effective tape cartridge barcode label length, including any media ID, may be limited to a maximum of 12 characters.

Automatic EKM Path Diagnostics - Test Warning Threshold

The current user's guide incorrectly states that you can set the test warning threshold when running Q-EKM or SKM. You can only set this if you are running Q-EKM.

Installing SKM User-Supplied TLS Certificates on the Library

In the current user's guide, the server and admin certificates are called different names. Also, there are additional requirements now.

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

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

You need to provide the following certificates:

- Root Certificate (also called the CA certificate, or Certificate Authority Certificate)
- Admin 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.
- 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.
- The same Root Certificate must be installed on the SKM servers and the library.
- All the certificates must have a valid validity period according to the date and time settings on the SKM server.

Manually Generating SKM Data Encryption Keys Using the Library

The following caution should be noted when manually generating data encryption keys via the library:

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

Exporting SKM Native Encryption Certificates

Previously, both SKM servers needed to be connected and operational in order to export the native encryption certificate. Since the native encryption certificate is the same for both servers in an SKM server pair, you may now export the native encryption certificate when only one SKM server is connected/ operational.

Exporting "Current" SKM Encryption Keys

You can now export current keys in addition to used and selective keys from the library.

The **Export Current** selection exports all the keys that were used to encrypt the tape cartridges that are currently in the library performing this export. This includes storage slots, I/E stations, and tape drives. If a tape cartridge is no longer in the library, the key used to encrypt it will not be exported.

To perform this function, click **Tools > EKM Management > Encryption Key > Export**.

Special Instructions for Replacing a Control Module in a Library Running SKM

If your library is running SKM and you replace a control module, the function to **Export Used** SKM encryption keys via the library Web client will not export all used keys correctly unless you run a special script on the SKM server after you replace the control module. This will correct the library serial number associations in the key server database. Refer to *the Scalar Key Manager 2.x User's Guide* for instructions.

When running the script, you will need to enter the serial numbers of both the non-functioning control module as well as the serial number of the new replacement control module. Before you send the control module back to Quantum, record the serial numbers so you can provide them when required. If you have already returned the failed control module to Quantum, contact Quantum Support to obtain its serial number.

Locating the Serial Number on the Scalar i500

On the Scalar i500, the serial number label is located inside the control module, on the horizontal bar at the back of the library. To see the label, open the front door. See Figure 18 for location and Figure 19 for an example.

The serial number is listed first. The serial number is all of the characters following the "%SN" on the serial number label. Do not enter the "%SN" characters when typing the serial number into the SKM command line.

Figure 18 Scalar i500 Serial Number Label On Control Module Seen Through Open Front Door

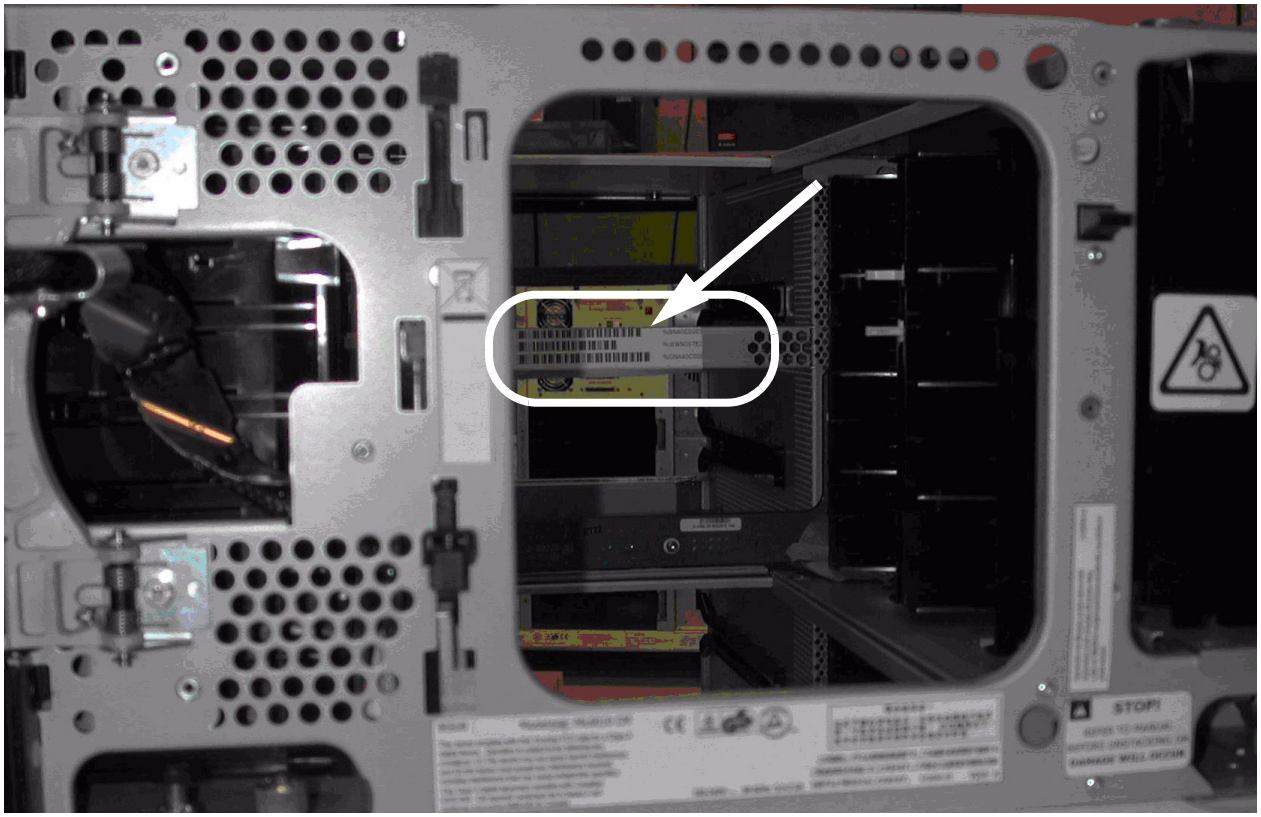
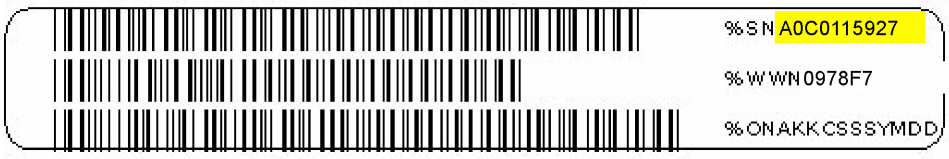


Figure 19 Scalar i500 SN/WWN Label



You can also find the serial number on the library as follows:

- **Operator panel** — Select **Tools > About Library**.
- **Web client** — Select **Reports > System Information**. The serial number is in the **Physical Library** table in the **Serial Number** column.

Reboot Brings Offline Tape Drives Online

Rebooting the library brings any offline tape drives back online.

Secure LDAP Support

You can optionally configure Secure LDAP on the regular LDAP configuration screen (**Setup > User Management > Remote Authentication**) using one of two methods (do not use both).

- **LDAPS** — You may enable LDAP over SSL (LDAPS) by entering a URI in the form of "ldaps://hostname" in the **Server URI** field. This will use SSL to send secure communication via port 636. If the LDAP server does not support LDAPS or does not have LDAPS enabled, then login operations will fail. LDAPS has been deprecated in favor of using StartTLS (see option below). Do not use LDAPS if you are using StartTLS. Once you apply LDAPS, StartTLS will not be available.
- **StartTLS** — Select this check box to configure secure LDAP communication using TLS. StartTLS uses the same port as regular LDAP (389). If TLS mode is not supported on your LDAP server, then login operations will fail. You cannot use StartTLS if you want to use LDAPS.

Optionally, if you are using one of the above methods, you can install a TLS CA certificate.

- **Install TLS CA certificate** — Provides additional verification of the LDAP server. If the certificate is installed, the library verifies that the LDAP server has not been compromised. The certificate must be the same certificate that is installed on your LDAP server and must be in .pem format. The maximum size the file can be is 4 KB. The library will only perform the verification if you have configured Secure LDAP (either LDAPS or StartTLS). Place a copy of the certificate file in an accessible location on your computer and use the **Browse** button to locate and install it. Once a certificate is installed, you can remove it by selecting the **Remove TLS CA certificate** check box. The library reboots after you install or remove a TLS CA certificate.

Simultaneous Snapshots Prohibited

You can configure the library to automatically attach a library snapshot to certain RAS ticket e-mail notifications (**Setup > Notifications > E-Mail Configuration**). If the library is in the process of capturing an automatic snapshot, you will not be able to manually capture a snapshot via the Web client until the automatic snapshot is complete. If this happens, an error message will display. Wait about 10 minutes and try again.

Control Path Failover – Additional Requirements

Tape drive control path failover is a feature that requires a Storage Networking license and HP LTO-5 tape drives. Two additional requirements for this feature are:

- In order for control path failover to work, both the control path tape drive and the failover tape drive must have their topology configured as Point to Point. Previously, the library allowed you to change the topology once control path failover was configured, even though this prevented the feature from working. Now, the library will not enable control path failover unless both the control path and failover tape drives are configured as Point to Point, and will not allow you to change the topology from Point to Point on any tape drives configured for control path failover.
- The control path and failover tape drives must be connected to an NPIV-enabled switch on the same fabric. They must not be connected to an FC I/O blade.

Media Integrity Report Enhancement

The Media Integrity Report now includes the last 10 drive error codes for each TapeAlert. These are displayed in the downloaded .csv report under the column headings **Error #1**, **Error #2**, and so on. The drive error codes are only present in the downloaded report, and are not displayed in the onscreen report.

Limits on Downgrading Library Firmware

If your library is running firmware version 600G or later, you can only downgrade library firmware to version 410G or later. If you need to downgrade to a version earlier than 410G, contact Quantum Support for assistance.

Limits on Restoring a Saved Configuration

If your library is running firmware version 600G or later, you can only restore a saved configuration that was created with firmware version 410G or later. If you need to restore a configuration created with a firmware version earlier than 410G, contact Quantum Support for assistance.

Logical SCSI Element Addressing

The library uses standard industry conventions to logically number every storage slot, I/E station slot, and tape drive in the library. Host software is designed to understand this addressing system, and generally there are no problems relating to tape cartridge slots. However, hosts sometimes have problems relating to tape drives, particularly when tape drives, library control modules, or library expansion modules are added or removed, or empty tape drive slots exist. This section explains how the library logically addresses tape drives and slots, so that you can avoid common problems with host software.

Tape Drive Logical SCSI Element Addressing

Tape drive logical element addresses are assigned by partition. The numbering is sequential within a partition and starts over with each partition. The addresses start with the lowest library module in a partition. The top tape drive in the module and partition is always number 256. The tape drive beneath that is 257, and so on until all tape drives in that module/partition have been accounted for.

Numbering continues with the top tape drive in the next module up. Empty tape drive slots are skipped (they are not given an element address).

Host software may have problems recognizing tape drives when tape drives, control modules, or expansion modules are added, removed, or replaced; or when partitions are added, deleted, or modified, because existing logical element addresses can change. Therefore, after making any of these types of modifications, you must refresh the configuration of any backup application that manages the library to reflect new tape drive positions. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

See Figure 9 on page 18 for a simple example of element addressing in a 14U library with a single partition, six tape drives installed and no empty tape drive slots. Note that multiple partition can create complexity. If you need help with the element addressing in your library, contact Quantum Support.

Cartridge Slot Logical SCSI Element Addressing

Tape cartridge slots are assigned logical element addresses by partition. The numbering is sequential within a partition and starts over with each partition. Numbering begins at the top left slot (as you look at the library from the front) in the lowest module in the library and moves sequentially down the left-most column. The top left slot of every partition is always number 4096, the slot beneath that is 4097, and so on. When the numbering reaches the bottom of the column, it continues to the top slot in the next column to the right (as long as it is in the same module and partition) and moves down that column. When all of the slots in the lowest module belonging to a partition have been accounted for, numbering continues to the top left slot in the next module above (as long as it is in the same partition). The numbering can get tricky when partitions span modules and do not use all of the slots in a module.

Tape cartridge slots are assigned a logical element address whether they contain a cartridge or not. Cartridges themselves are not given a logical element address; only the slot is. Slot element addresses change when slots are added or removed; partitions are added, removed, or modified; or cleaning slots are added or removed.

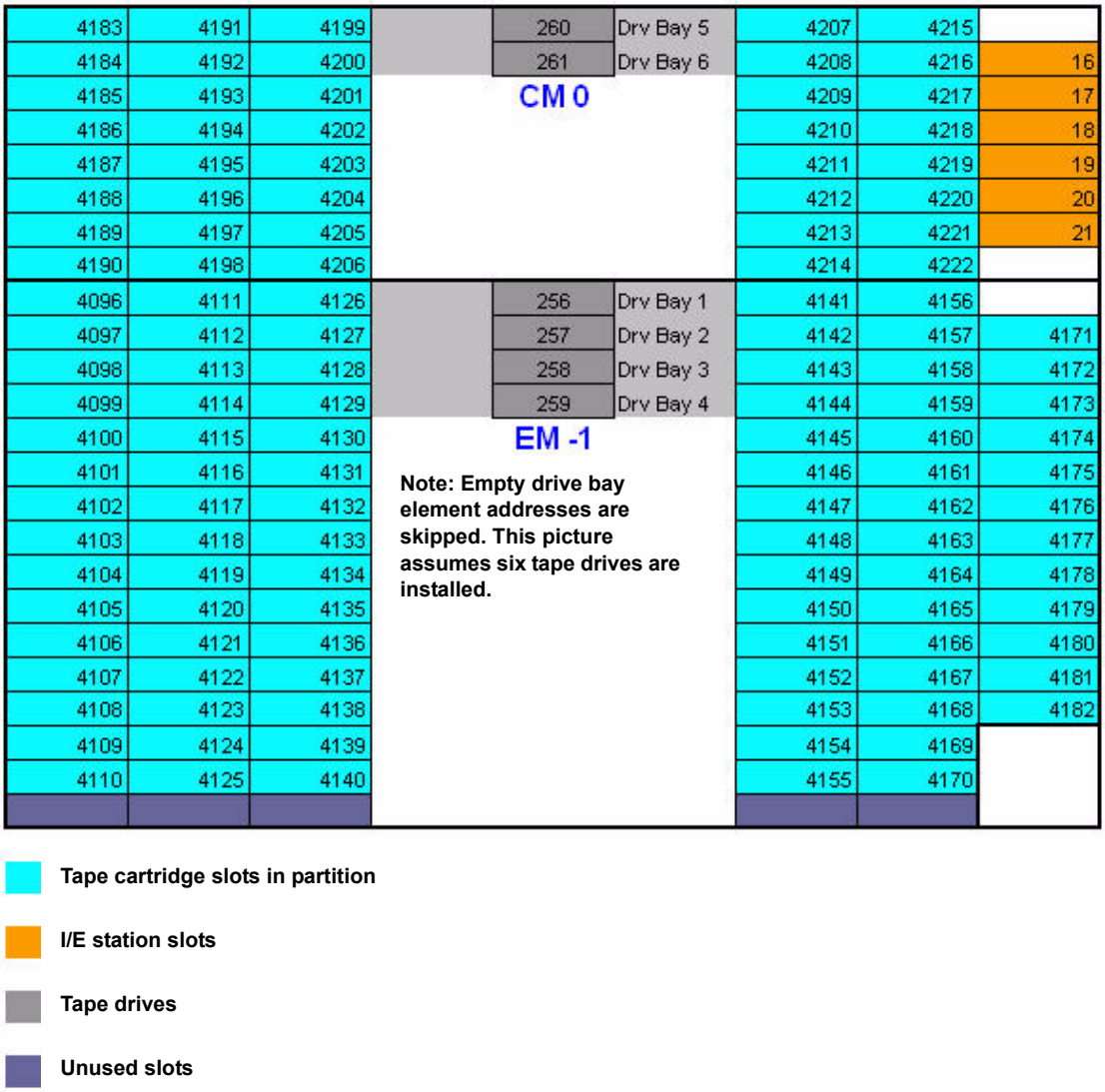
I/E station slots are numbered differently from partitions. Numbering begins at the top I/E station slot in the uppermost module that contains I/E station slots, and continues sequentially downward. This top slot has element address 16. The slot beneath that is 17, and so on.

Cleaning slots belong to the System partition and are not reported to the host. Cleaning slots are skipped (they are not given a logical element address), so adding or removing a cleaning slot will renumber all of the slots in a partition.

Generally, host software easily recognizes logical slot element addresses, even when they change. The next time the host issues a READ ELEMENT STATUS command, it will process the new number and recalculate all of the slot addresses.

See Figure 9 on page 18 for a simple example of element addressing in a 14U library with a single partition.

Figure 20 Logical Element Addressing, 14U, One Partition, Six Tape Drives Installed



Quantum's Knowledge Base

Quantum keeps a dynamic listing of frequently asked questions, troubleshooting tips, and service bulletins for all of its products. To access the knowledge base, go to the Quantum Support Web site and click on Knowledge Base:

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