Spectra Swarm Bridge

Installation & Configuration Guide

Notices

Except as expressly stated herein, Spectra Logic Corporation makes its products and associated documentation on an "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, BOTH OF WHICH ARE EXPRESSLY DISCLAIMED. In no event shall Spectra Logic be liable for any loss of profits, loss of business, loss of use or data, interruption of business, or for indirect, special, incidental or consequential damages of any kind, even if Spectra Logic has been advised of the possibility of such damages arising from any defect or error.

Information furnished in this manual is believed to be accurate and reliable. However, no responsibility is assumed by Spectra Logic for its use. Due to continuing research and development, Spectra Logic may revise this publication from time to time without notice, and reserves the right to change any product specification at any time without notice.

Part Number

90940162 Revision A

Revision History

Revision	Date	Description
A	March 2020	Initial release

Contacting Spectra Logic

To Obtain General Information

Spectra Logic Website: www.spectralogic.com

United States Headquarters

Spectra Logic Corporation
6285 Lookout Road
Boulder, CO 80301
USA
Phone: 1.800.833.1132 or 1.303.449.6400
International: 1.303.449.6400
Fax: 1.303.939.8844

European Office

Spectra Logic Europe Ltd.
329 Doncastle Road
Bracknell
Berks, RG12 8PE
United Kingdom
Phone: 44 (0) 870.112.2150
Fax: 44 (0) 870.112.2175

Spectra Logic Technical Support

Technical Support Portal: support.spectralogic.com

United States and Canada

Phone:
Toll free US and Canada: 1.800.227.4637
International: 1.303.449.0160

Europe, Middle East, Africa

Phone: 44 (0) 870.112.2185

Deutsch Sprechende Kunden

Phone: 49 (0) 6028.9796.507
Email: spectralogic@stortrec.de

Mexico, Central and South America, Asia, Australia, and New Zealand

Phone: 1.303.449.0160

Spectra Logic Sales

Website: www.spectralogic.com/shop

United States and Canada

Phone: 1.800.833.1132 or 1.303.449.6400
Fax: 1.303.939.8844
Email: sales@spectralogic.com

Europe

Phone: 44 (0) 870.112.2150
Fax: 44 (0) 870.112.2175
Email: eurosales@spectralogic.com

To Obtain Documentation

Spectra Logic Website: support.spectralogic.com/documentation

INSTALLATION & CONFIGURATION GUIDE

This document describes the installation of the Spectra® Swarm bridge, and the necessary configuration of the appliance for use with a Spectra Logic® tape library. The Spectra Swarm bridge is a high-performance storage controller that adds 40-Gigabit Ethernet connectivity to SAS tape drives.

SPECTRA SWARM BRIDGE NETWORKING CONCEPTS

Before configuring your Spectra Swarm bridge, familiarize yourself with the following related network concepts (descriptions courtesy of Wikipedia).

CHAP

Challenge-Handshake Authentication Protocol (CHAP) is an authentication scheme used by Point-to-Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (for example, a client password).

After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.

The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.

The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.

At random intervals the authenticator sends a new challenge to the peer and repeats the above checks.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.

RADIUS uses two packet types to manage the full AAA process; Access-Request, which manages authentication and authorization; and Accounting-Request, which manages accounting.

IPsec

Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session.

RoCE

Remote direct memory access (RDMA) over Converged Ethernet (RoCE) is a network protocol that allows access over an Ethernet network. It does this by encapsulating an IB transport packet over Ethernet. Although the RoCE protocol benefits from the characteristics of a converged Ethernet network, the protocol can also be used on a traditional or non-converged Ethernet network

Network-intensive applications like networked storage or cluster computing need a network infrastructure with a high bandwidth and low latency. The advantages of RDMA over other network application programming interfaces are lower latency, lower CPU load and higher bandwidth.

INSTALL TAPE DRIVES

If necessary, install drives in your Spectra tape library using one of the following documents:

- *Spectra TSeries Drive Replacement Procedure*
- *Spectra Stack Quick Start Guide*

CREATE A PARTITION

After installing the drives, use the instructions in your library *User Guide* to create one or more partitions using the newly installed drives.

UPDATE DRIVE FIRMWARE

After creating one or more partition(s), use the instructions in your library *User Guide* to update the drive firmware of the newly installed drives.

Note: Depending on when you purchased the drives, a firmware update may not be necessary.

INSTALL THE SPECTRA SWARM BRIDGE

Use the instructions in the following sections to install the Spectra Swam bridge in a rack (optional) and to connect power, Ethernet, and SAS cables.

Install Swarm Bridge into a Rack

Use the following instructions to install the Spectra Swarm bridge into a rack.

Notes:
- The Spectra Swarm bridge can be installed on the top of a Spectra tape library. Contact Spectra Logic for assistance (see Contacting Spectra Logic on page 3).
- If you do not plan to install the bridge into a rack, or on the top of a tape library, place the bridge on a sturdy, flat work surface.

1. Using a #2 Phillips screwdriver, install the mounting brackets to the sides of the Spectra Swarm bridge.
2. Install the rack cage nuts in the 2U space where you plan to install the Spectra Swarm bridge.
3. Supporting the weight of the bridge with your hand, use a #2 Phillips screwdriver to secure the mounting brackets on the bridge to the rack cage nuts.
4. Properly ground the Spectra Swarm bridge to the rack.

Connect Cables

Use the instructions in this section to connect power, Ethernet, and SAS cables to the Spectra Swarm bridge, and to connect the SAS cables to the tape drives in your Spectra Logic tape library.

Connect Management Port Ethernet Cable

To access the Spectra Swarm web interface, connect an Ethernet cable to the management port.

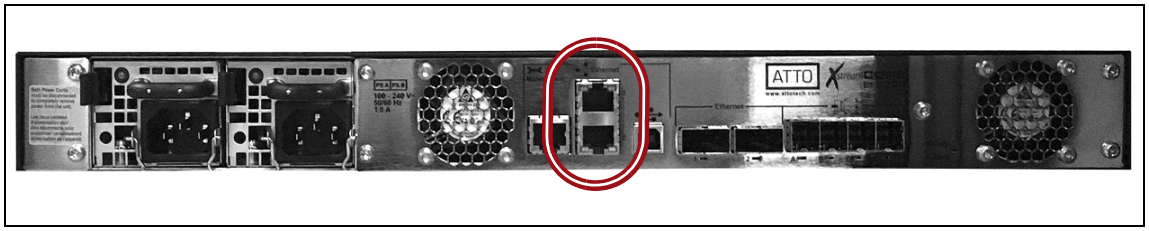

Figure 1 The management port Ethernet connectors of the Spectra Swarm bridge.

1. Connect a Category 5 Ethernet cable to either of the two RJ-45 connectors labeled “Ethernet” on the rear of the Spectra Swarm bridge.
2. Connect the other end of the cable to an active network over which a computer can access the system.

   Note: If you are connecting the Spectra Swarm bridge directly to a host computer, you may need to use a crossover cable.

Connect Data Port Ethernet Cables

Connect the Spectra Swarm bridge to Ethernet hosts or switches using one or two 40G QSFP+ optical transceivers, Direct Attached Copper (DACs) or Active Optical Cables (AOCs) cables depending on the distance required. The chart below lists the cable length restrictions for the data ports.

Note: Breakout cables are also available..

Cable Type	Max Cable Length 40 GigE
50 micron OM3	328 ft (100 m)
50 micron OM4	492 ft (150 m)
Long wave, single mode [a]	32,808 ft (10,000 m)

a. Long wave operation requires long wave QSFP+ modules (not supplied).

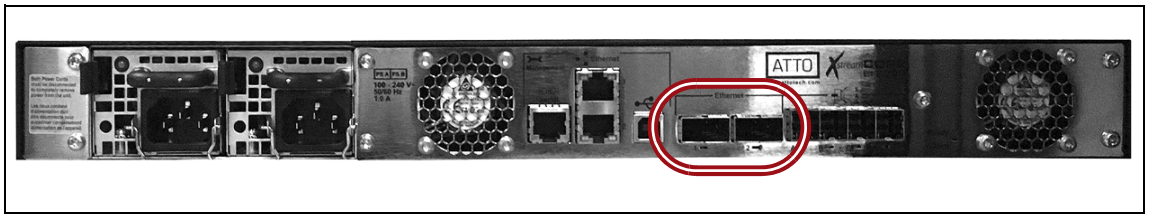

Figure 2 The data port Ethernet connectors of the Spectra Swarm bridge.

1. Connect one or two OM3 or better MTP/MPO fiber cables to the 40 GigE QFSP+ ports on the rear of the Spectra Swarm bridge.
2. Connect the other end to a host computer or compatible network switch. A breakout cable may be required.

Connect SAS Cables

Connect tape drives to the Spectra Swarm bridge using SAS cables with mini-SAS HD (SFF8644) connectors to connect to the bridge, and SFF8088 connectors to connect to tape drives. The maximum cable length supported is 32.8 ft (10 m).

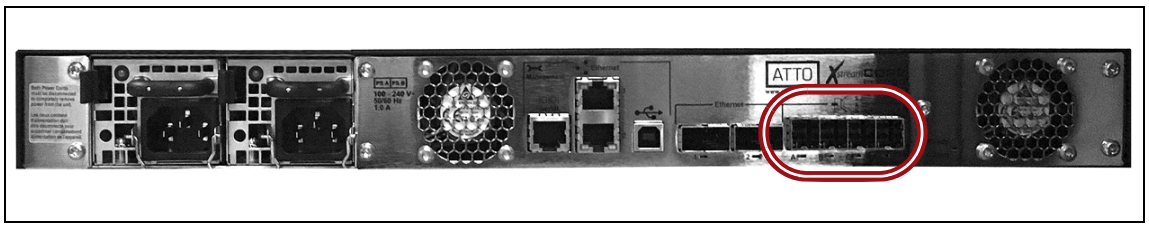

Figure 3 The SAS connectors of the Spectra Swarm bridge.

1. Connect one to four SAS cables to the SAS ports on the rear of the Spectra Swarm bridge.
2. Connect the other end of the cable into a SAS drive in your Spectra tape library.

   Note: Fan out cables may be used to connect each SAS port on the Swarm bridge to up to four SAS drives in the tape library.

Connect Power Cords

The Spectra Swarm bridge features two hot swappable power supplies and can be operated with only a single power supply inserted. Each power supply has a standard IEC320 power receptacle and cooling fan.

Note: Power is automatically supplied to the Spectra Swarm bridge when plugged into an AC outlet.

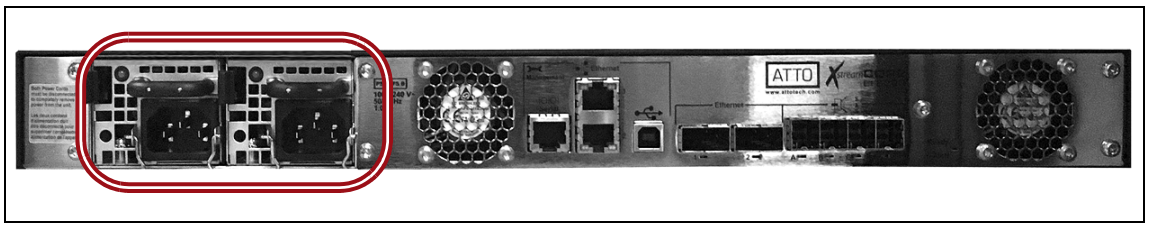

Figure 4 The power supplies of the Spectra Swarm bridge.

1. Connect one of the provided power cords to each of the power supply connectors.
2. Plug the other end of the each cord into an AC power outlet. The Spectra Swarm bridge automatically powers on.

CONFIGURE THE SPECTRA SWARM BRIDGE

Use the instructions in this section to configure the Spectra Swarm bridge for use in your storage environment.

Discover Management Port IP Address

1. From the *ATTO website*, download the QuickNAV software package appropriate for your local host operating system.
   a. Using a standard web browser, navigate to *www.atto.com*.
   b. If necessary, log in with your current account, or create a new account.
   c. Select **Support** ···⁘ **Downloads**. The Select Product & Model page displays.
   d. Select **Storage Controllers**. A list of storage controller models display in the right pane.
   e. Select the **XstreamCORE® ET 8200T** controller model. The downloads screen for the controller displays.
   f. Click the **QuickNAV** link appropriate for your operating system to download the program.

   Notes:
   - Some anti-virus programs may incorrectly identify the QuickNAV software as a virus.
   - The following instructions are for the Windows-based QuickNAV software.

2. Double-click the .exe file to launch the QuickNAV software. The ATTO QuickNAV wizard welcome screen displays.

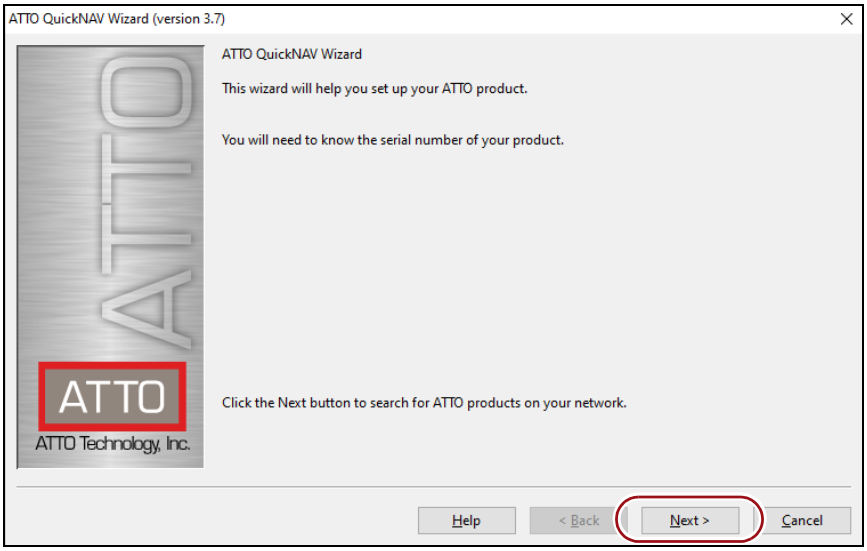

Figure 5 QuickNAV wizard welcome screen.

3. Click **Next**. The QuickNAV wizard discovery screen displays.

4. Select the controller on your local host computer to use for discovering the Spectra Swarm bridge management port IP address and click **Next**.

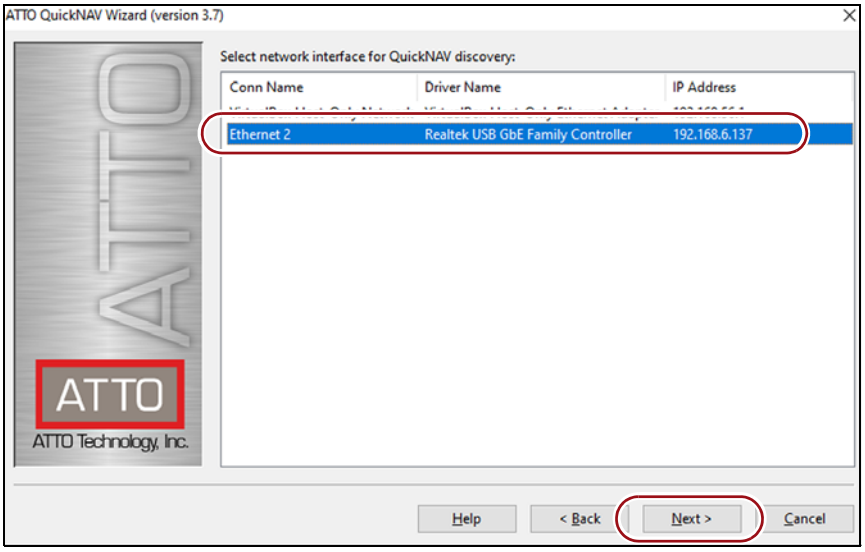

Figure 6 QuickNAV wizard discovery screen.

5. In the serial number and IP address pane, locate the serial number of the Spectra Swarm bridge to be used with a Spectra Logic tape library.

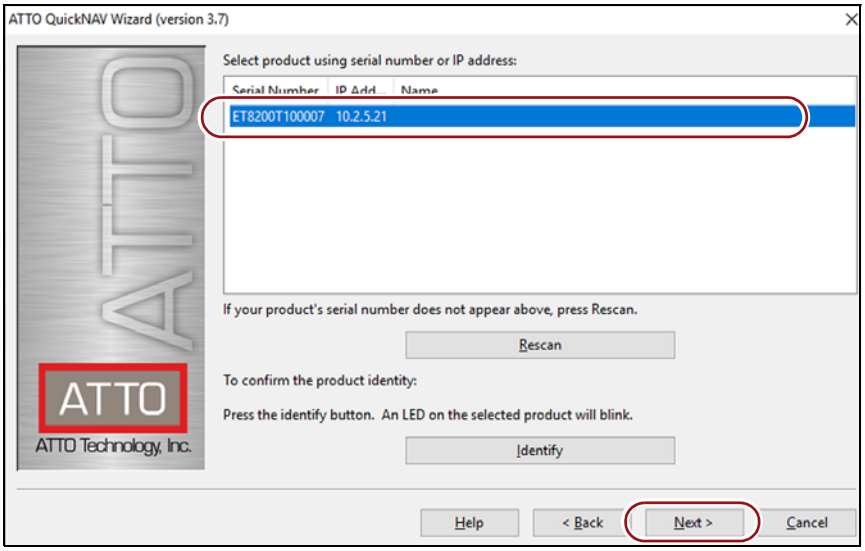

Figure 7 QuickNAV wizard serial number screen.

6. Select the row of the Spectra Swarm bridge and click **Next**.

Notes:
- If the Spectra Swarm bridge serial number is not displayed, click **Rescan** to attempt to retrieve the controller information again.
- If you have multiple Spectra Swarm bridges, it may be helpful to click **Identify** to physically confirm you are working with the correct controller.

7. The management port IP address for the Spectra Swarm bridge management port displays.

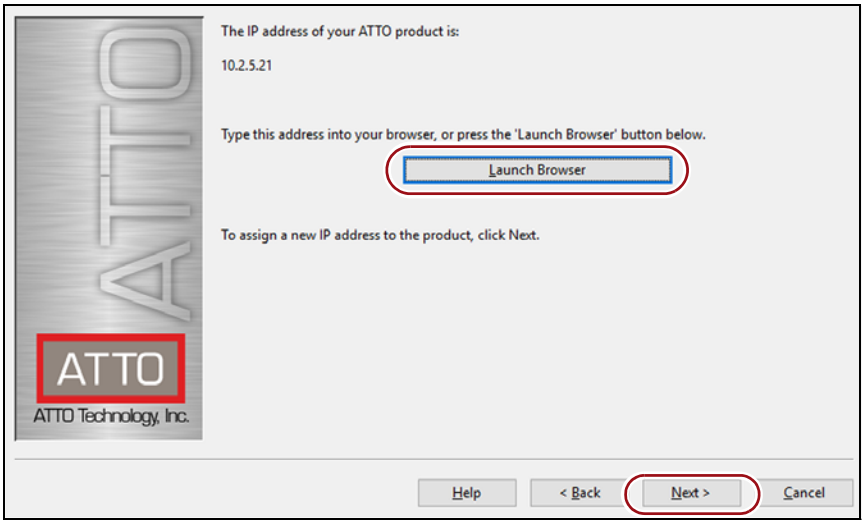

Figure 8 QuickNAV wizard IP address screen.

- To continue with the DCHP assigned IP address, click **Launch Browser** and skip to Sign In to the Spectra Swarm Bridge on page 12.
- To configure a static IP address, click **Next** and continue to Step 8.

8. On the Configure Network Settings screen, enter the desired **IPv4 Address**, **IPv4 Subnet Mask**, and optionally **IPv4 Default Gateway** and click **Next**. The ATTO QuickNAV wizard displays the newly assigned IP address.

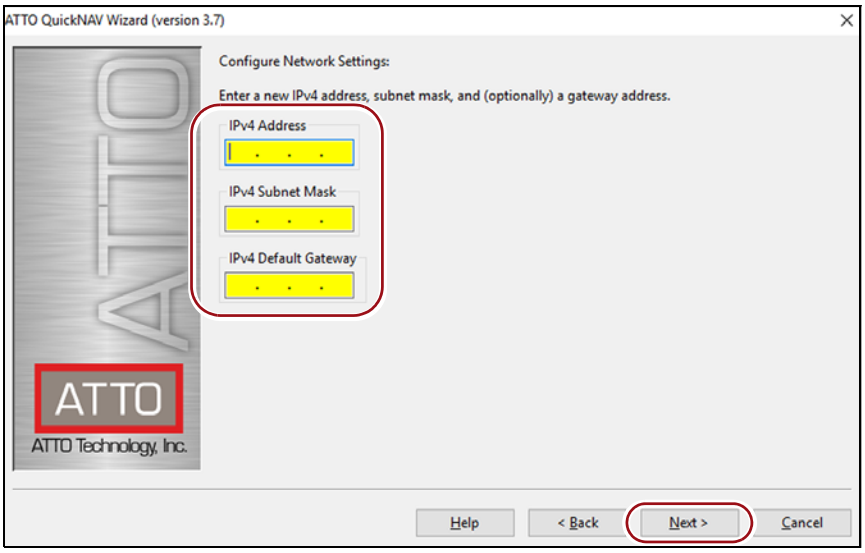

Figure 9 QuickNAV configure network settings screen.

9. Click **Reboot Now** to reboot the storage controller and continue with Sign In to the Spectra Swarm Bridge on page 12.

MANAGING THE SPECTRA SWARM BRIDGE

Use the instructions in this section to use the user interface to manage your Spectra Swarm bridge.

Sign In to the Spectra Swarm Bridge

Use the following instructions to log in to the Spectra Swarm XstreamCORE user interface.

Note: The Spectra Swarm bridge user interface is compatible with the following browsers:

- Goggle Chrome
- Mozilla Firefox
- Microsoft Edge

1. Using one of the approved web browsers, enter the IP address set or discovered in Discover Management Port IP Address on page 9.

   The Spectra Swarm bridge ships with a self-signed SSL certificate. When using the self-signed certificate, you must pass a security check every time you attempt to access the Swarm bridge user interface.

   Notes:
   - The absence of the certificate does not affect functionality.
   - If desired, you can install signed, trusted SSL certificates for your data and management ports so that you no longer need to pass the security check when accessing these ports. See the Configure Security Certificates on page 36 for more information.

2. Click **Enter here**. The Sign In dialog box displays.
3. Enter the **username** and **password** for the Spectra Swarm bridge user interface. The status screen displays.

   Note: The default username is "**admin**" and the default password is "**P@SSw0rd**" without quotes.

Change the Password

Spectra Logic recommends changing the default password for the Admin user. Use the instructions in this section to change a user's password.

Note: The instructions below reference the Admin user. The process is similar for the Read Only user.

1. In the left-hand pane, click **Controller**. The Controller Configuration screen displays.

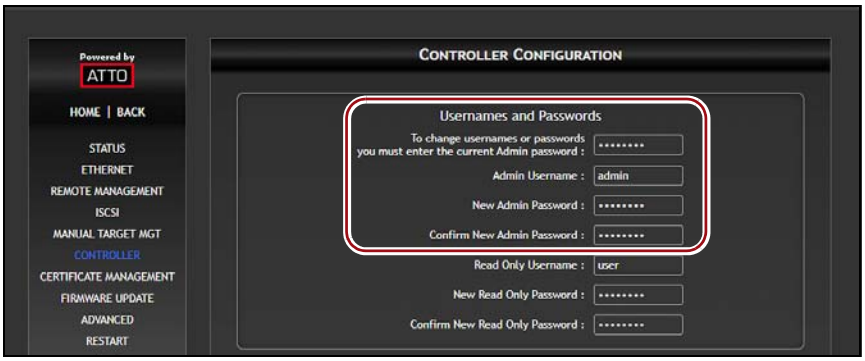

Figure 10 The Usernames and Passwords pane of the Controller Configuration screen.

2. Enter the current Admin password in the **To change usernames or passwords...** entry field.
3. If desired, change the **Admin Username**. Only lowercase letters and numbers, period (.), underscore (_), and dash (-) are supported characters.
4. Enter and confirm the **New Admin Password**. The password must be at least eight characters long, and must contain at least one number.

5. Click **Submit**. The screen refreshes and displays a message at the top of the user interface that the Spectra Swarm bridge must be restarted.

Figure 11 The password updated confirmation message.

Note: There is no error message displayed after clicking **Submit** if you entered the incorrect existing password.

6. In the left-hand pane, click **Restart**. The Restart Firmware screen displays.

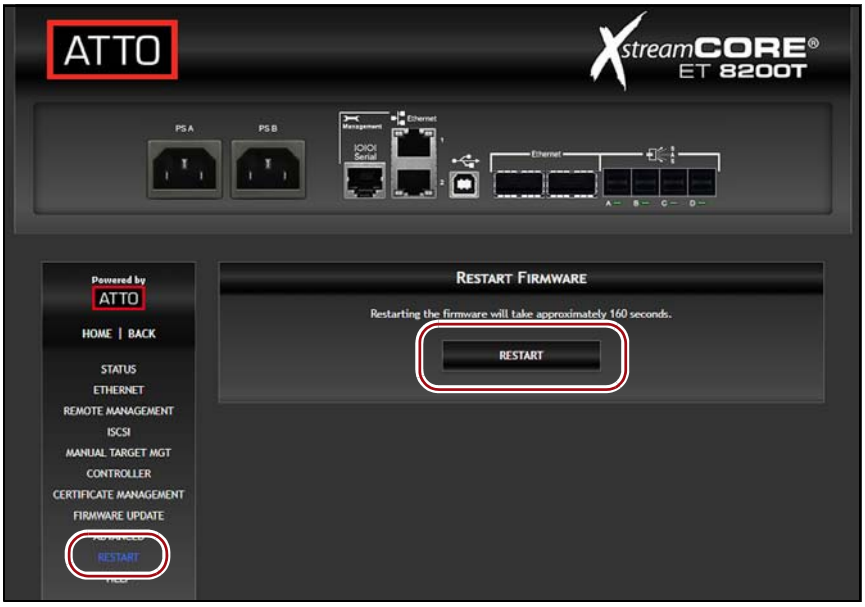

Figure 12 The Restart Firmware screen.

7. In the main window, click **Restart**. The Spectra Swarm bridge waits 160 seconds and then restarts.
8. After restarting, the sign in dialog box displays. Sign in to the Swarm bridge using the new password.

Update Firmware

The Spectra Swarm bridge uses several processors which control the flow of data. The firmware to control these processors can be upgraded in the field using either the Spectra Swarm user interface, or using a PUT command from an SFTP connection.

Using the User Interface

Use the instructions below to update the firmware of the Spectra Swarm bridge using the user interface.

Note: After upgrading to firmware version 4.0 or later, you need to update your password to comply with requirements as described in *California Senate Bill No. 327*.

1. From the *ATTO website*, download the new firmware file for the Spectra Swarm bridge.
   - **g.** Using a standard web browser, navigate to *www.atto.com*.
   - **h.** If necessary, log in to your current account, or create a new account.
   - **i.** Select **Support** ⋯ **Downloads**.
   - **j.** On the Select Product & Model page, select **Storage Controllers**. A list of storage controller models display in the right pane.
   - **k.** Select the **XstreamCORE ET 8200T** controller model. The downloads screen for the controller displays.
   - **l.** Download the desired firmware file.
2. Sign into the Spectra Swarm user interface as described in Sign In to the Spectra Swarm Bridge on page 12.
3. On the left-hand pane, click **Firmware Update**. The Firmware Update screen displays.
4. Click **Choose File** and browse to the location of the firmware file downloaded in Step 1 on page 15.
5. Click **Upload** and wait until a message displays that the upload was successful.
6. Click **Restart**.

   Note: The Spectra Swarm bridge retains a backup file in case the update process fails. After updating the firmware, verify the correct firmware version by viewing the status page and checking the firmware revision number.

Using SFTP

Use the instructions below to update the firmware of the Spectra Swarm bridge using SSH File Transfer Protocol (SFTP)

Note: After upgrading to firmware version 4.0 or later, you need to update your password to comply with requirements as described in California Senate Bill No. 327.

1. Establish an SFTP link to the storage controller that is to be flashed.

Notes:
- The storage controller SFTP server is at port 20, not the default port 22.
- The storage controller only supports one session at a time. If your client uses multiple simultaneous sessions to accelerate data transfer, the SFTP link will not work correctly.

2. As an example, using OpenSSH, the connection would be made with the following command where username is the username set in Change the Password on page 13, and x.x.x.x is the IP address of the Spectra Swarm bridge.

```
sftp –P 20 username@x.x.x.x
```

3. Enter your password when prompted.
4. Once logged in, upload the .zbd file using the "put" command:

```
PUT c:\firmware\xc8200_3_00_101F.zbd
```

5. Once the upload is complete, check the Spectra Swarm bridge log to verify successful upload, using either SSH, serial port, or USB port CLI, with the **DumpEventLog** command (see Using the Command Line Interface on page 40).
6. If the upload and firmware update were logged as successful, cycle power on the Spectra Swarm bridge using the **FirmwareRestart** command to apply the new firmware (see Using the Command Line Interface on page 40).

CONFIGURE DATA ETHERNET PORTS

Use the instructions in this section to configure the 40 GigE data Ethernet ports on the Spectra Swarm bridge.

1. In the left-hand pane of the user interface, click **Ethernet**. The Ethernet Port Configuration screen displays.

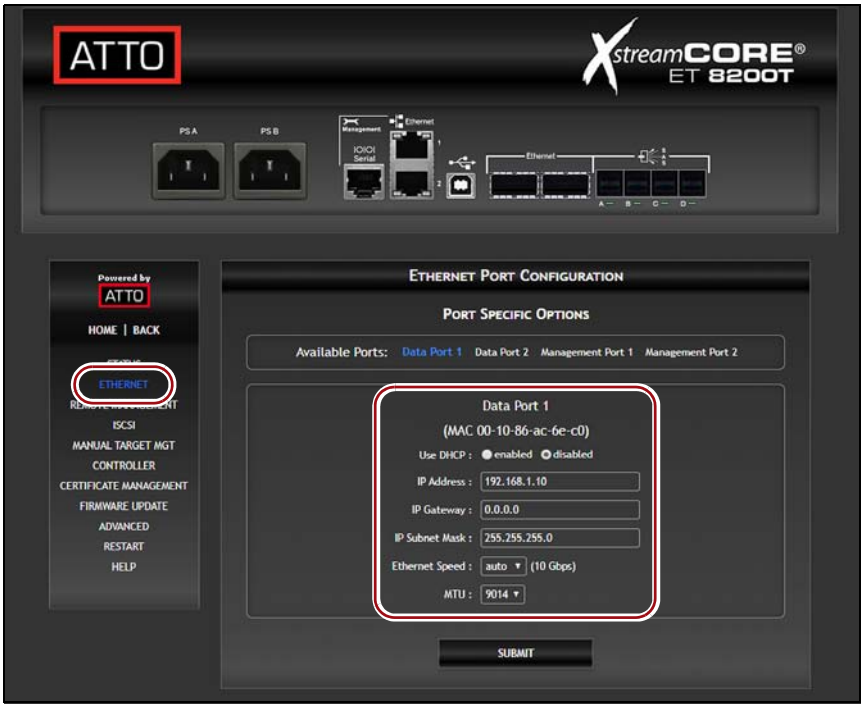

Figure 13 The Ethernet Port Configuration screen.

2. Select either Data Port 1 or Data Port 2. The screen refreshes to show the settings for the selected data port.
3. Select the appropriate **Use DHCP** radial buttons to **enable** or **disable** DHCP for the data interface.
   - If you enabled DCHP, skip to Step 6 on page 17.
   - To configure a static IP address, continue to Step 4 below.
4. Enter a valid IPv4 **IP Address**, **IP Gateway**, and **IP Subnet Mask**.
5. Use the **Ethernet Speed** drop-down menu to set the data transfer speed of the Ethernet port. Select either **10 GigE**, **40 GigE**, or **auto**.
6. Using the **MTU** drop-down menu, select the desired Maximum Transmission Unit size.

   Note: All equipment on the same network must support the same frame size. If the MTU is increased on one end device, the switch and receiving end must also be configured for larger MTUs. A mixture of devices configured for jumbo frames and standard frames on the same network may result in packet fragmentation and can cause performance issues.

7. Click **Submit**.
8. If necessary, repeat the steps in this section to configure the second Ethernet data port.

Configure Drives Using The Spectra Swarm Bridge User Interface

Use the instructions in this section to configure drives in the Spectra Swarm bridge user interface.

Note: SAS devices connected to the Spectra Swarm bridge are seen as Ethernet LUNs to the host computer.

Mapping Drives

1. In the left-hand pane of the user interface, click **Manual Target MGT**. The iSCSI Target Management screen displays.
   - To use the pre-created default target, skip to Step 2.
   - To create a new iSCSI target, in the **Add an iSCSI target** field, enter a name for a new target configuration and click **Submit**. The new iSCSI target appears in the Configure iSCSI Targets pane.

Figure 14 The iSCSI Target Management screen.

2. On the desired iSCSI target row, click **Device Maps**.

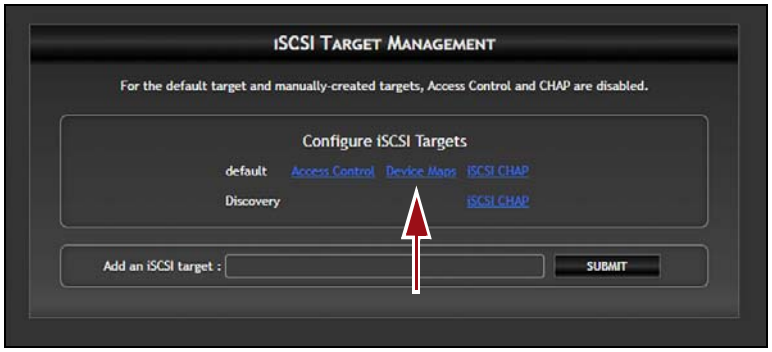

Figure 15 The Configure iSCSI Targets pane.

The iSCSI Mapping screen displays and the selected iSCSI target displays in the **FOR** drop-down menu.

3. Drag the desired device from the Unmapped Devices pane to the desired LUN. (Controller is LUN0 and cannot be changed). Repeat as needed to map all the desired drives.

Figure 16 The iSCSI Mapping screen.

4. Click **Submit**. The screen does not refresh, but the settings are saved.

Configure Access Control

If Access Control is disabled for a target, any initiator with access to the same network the Spectra Swarm bridge is located on and which has the correct discovery CHAP credentials (if any) is able to discover and connect to that target. To prevent initiators from discovering a particular Spectra Swarm bridge target, enable Access Control for that target. Once Access Control is enabled, only initiators in the list of Allowed Initiators are able to discover that target.

1. In the left-hand pane of the Spectra Swarm user interface, click **Manual Target MGT**. The iSCSI Target Management screen displays.
2. On the desired iSCSI target row, click **Access Control**.

Figure 17 The Configure iSCSI Targets pane.

The Access Control screen displays and the selected iSCSI target displays in the **FOR** drop-down menu.

3. In the Access Control row, select **Enabled**.

Figure 18 The Access Control screen.

4. Select a desired initiator from the Allowed Initiator pane and click the **Up arrow** to add it to the List of Initiators. If necessary, repeat to add additional initiators.
5. Click **Submit**. The screen does not refresh, but the settings are saved.

Configure iSCSI CHAP

If desired, use the instructions in this section to configure CHAP (Challenge Handshake Authentication Protocol) for an iSCSI initiator.

1. In the left-hand pane of the Spectra Swarm user interface, click **Manual Target MGT**. The iSCSI Target Management screen displays.

2. On the desired iSCSI Target row, click **iSCSI CHAP**.

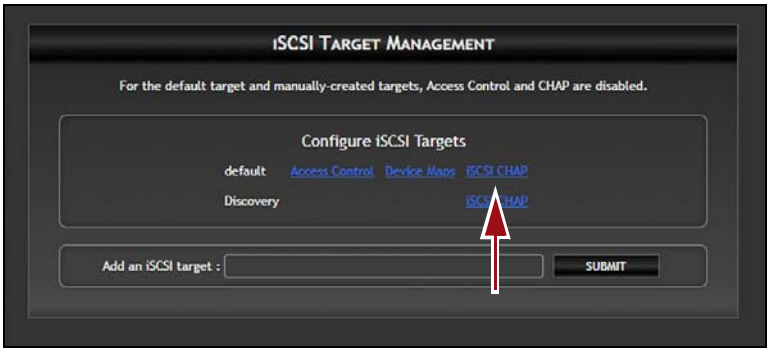

Figure 19 The Configure iSCSI Targets pane.

The iSCSI CHAP Configuration screen displays and the selected iSCSI target displays in the **FOR** drop-down menu.

3. Using the **iSCSI CHAP** drop-down menu, select **disabled**, **one-way**, or **two-way** CHAP.

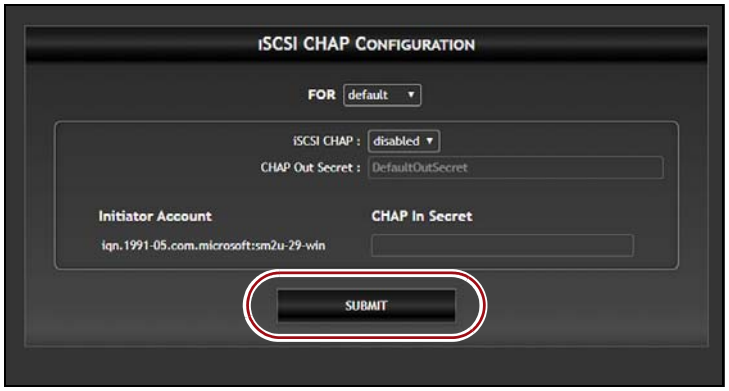

Figure 20 The iSCSI CHAP Configuration screen.

4. Click **Submit**. The screen does not refresh, but the settings are saved.
5. If you selected **disabled** or **one-way** CHAP, continue to Configure Drives Using iSCSI in Windows on page 23.

   If you selected **two-way** CHAP configuration, the **CHAP Out Secret** field is now editable. To configure two-way chap, continue with Step 6 below.
6. Enter a phrase for the **CHAP Out Secret**. The phrase must be between 12 and 32 characters and cannot use the comma character (,).
7. Click **Submit**. The screen does not refresh, but the settings are saved.

   Note: The Initiator Account name for targets is not configurable. It is always the full IQN, including the product name and serial number, of that target.

CONFIGURE DRIVES USING ISCSI IN WINDOWS

Use the instructions in this section to configure drives in the iSCSI Initiator tool on your local Windows host.

1. Launch the iSCSI Initiator tool using one of the following methods:
   - From the Windows **Start** menu, launch the **iSCSI Initiator tool**.
   - Press the **Windows Key+R**. The Run dialog box displays. Enter `iscsicpl.exe` and click **OK**

   Note: Depending on your Windows configuration, the iSCSI Initiator tool may be found in the Windows Administrative Tools folder in the Start menu.

   The iSCSI Initiator Properties tool displays.
2. Select the **Discovery** tab.

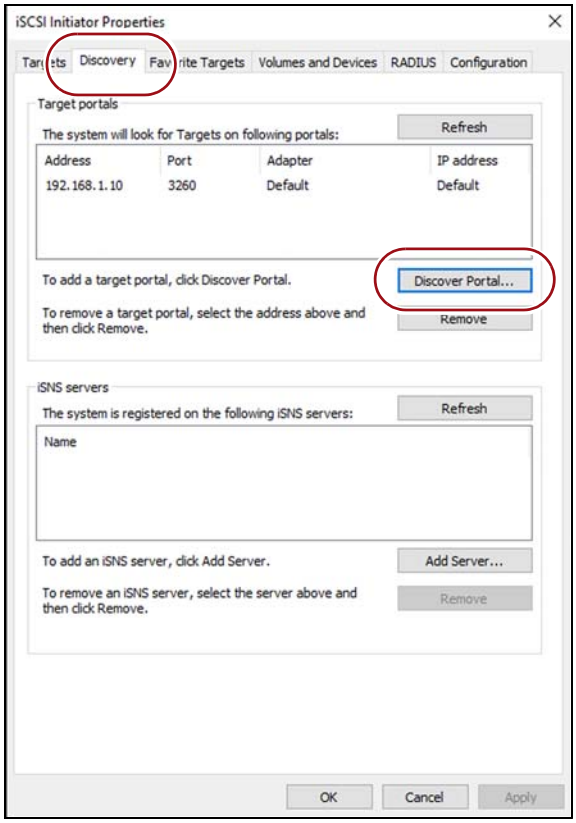

Figure 21 The iSCSI Initiator Properties Tool.

3. In the Target Portals pane, click **Discover Portal**. The Discover Target Portal dialog box displays.

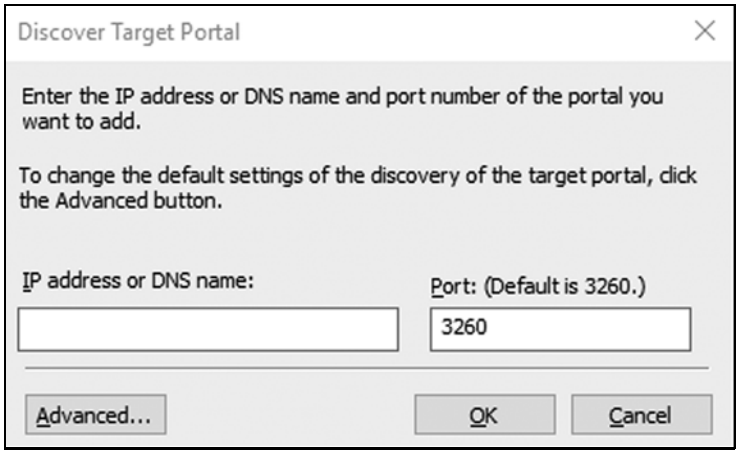

Figure 22 The Discover Target Portal dialog box.

4. Enter the IP address of the **Data Port** configured in the Spectra Swarm user interface (see Configure Data Ethernet Ports on page 17).

   Note: While the Windows iSCSI Initiator tool accepts a DNS address, the Spectra Swarm bridge is not capable of using a DNS address.

5. If necessary, change the **Port** value.

   Note: The default port value is used in most iSCSI environments.

6. Click **OK**. The target portal displays in the Target Portals pane (see Figure 21 on page 23).

7. Click the **Targets** tab. The Spectra Swarm iSCSI initiator is displayed in the Discovered Targets pane.

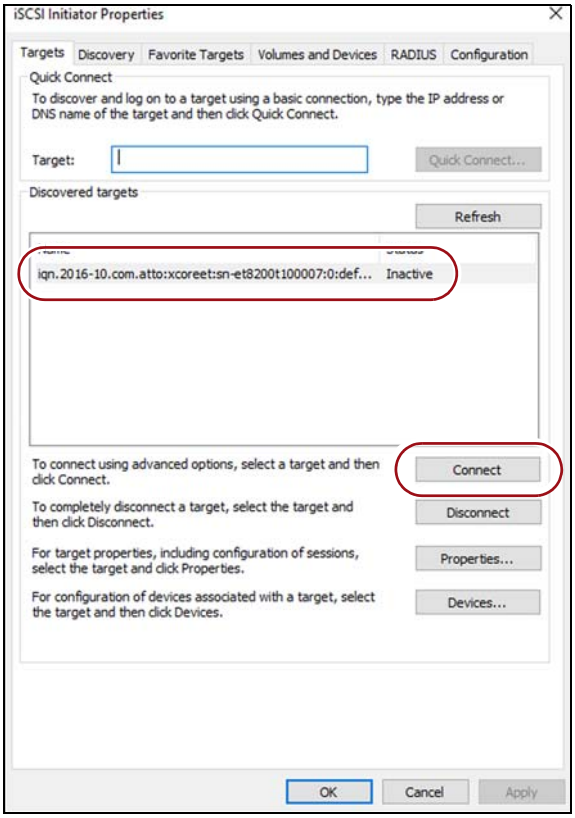

Figure 23 The iSCSI Initiator Properties Tool.

8. Select the initiator and click **Connect**. The Connect to Target window displays.

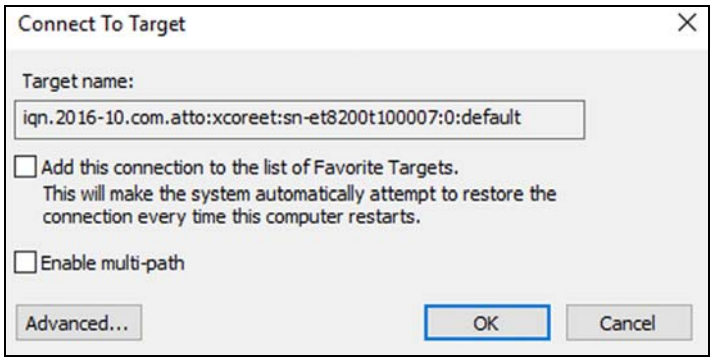

Figure 24 The Connect To Target window.

9. Click **OK** to connect to the Spectra Swarm iSCSI initiator. On the Target tab of the iSCSI Initiator Properties tool, the status of the target changes to **Connected**.
10. If desired, to display target properties, or to configure sessions, select an iSCSI target and click **Properties**. The Properties window displays. Edit properties as desired and click **OK**.

11. If desired, to configure devices associated with an iSCSI target, select an iSCSI target and click **Devices**. The Devices window displays. Edit device properties as desired and click **OK**.
12. Click **OK** to save the configuration and close the iSCSI Initiator Properties tool.

Install Tape Drivers

After configuring the Spectra Swarm initiator in the iSCSI Initiator tool, the mapped tape drives appear in the System Manager. Use the instructions in this section to install drivers for your tape drives.

1. Download or copy the appropriate driver to your local host.
2. From the Windows desktop, right-click on **This PC** and select **Properties**. The System window displays.
3. On the left-hand pane, select **Device Manager.** The Device Manager window displays.

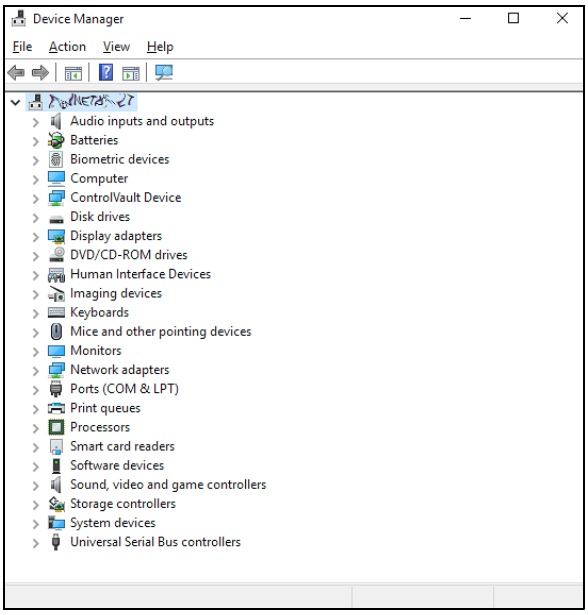

Figure 25 The Device Manager window.

4. Locate the entry for Tape Drives, and if necessary, expand the entry by clicking >.

5. Right-click on a tape drive and select **Update Driver Software**. The Update Driver Software wizard displays.

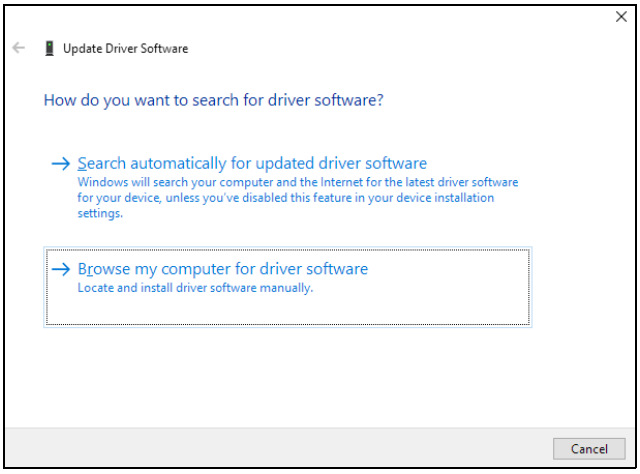

Figure 26 The Update Driver Software window.

6. Click **Browse my computer for driver software**.
7. Click **Browse**, and then select the folder that contains the tape driver.
8. Click **Next**.
9. Select the driver compatible with the tape drive and click **Next**. The driver installs on your system.
10. Click **Finish**.

Repeat these instructions for any other drives connected to your system through the Spectra Swarm bridge.

Configure iSCSI for LTFS

For iSCSI to work with LTFS, the iSCSI maximum transfer length must be set to at least 1MiB and the maximum burst length set to 4MiB. This requires modifying the registry.

Notes:
- You may need administrative access enabled in order to edit the system registry. See your IT administrator for assistance.
- Incorrectly editing a registry entry may cause system instability. Use caution when editing the system registry.

1. On your windows host, press the **Windows Key+R**. The Run dialog box displays.

2. Enter `regedit` and click **OK**. The Registry Editor window displays.

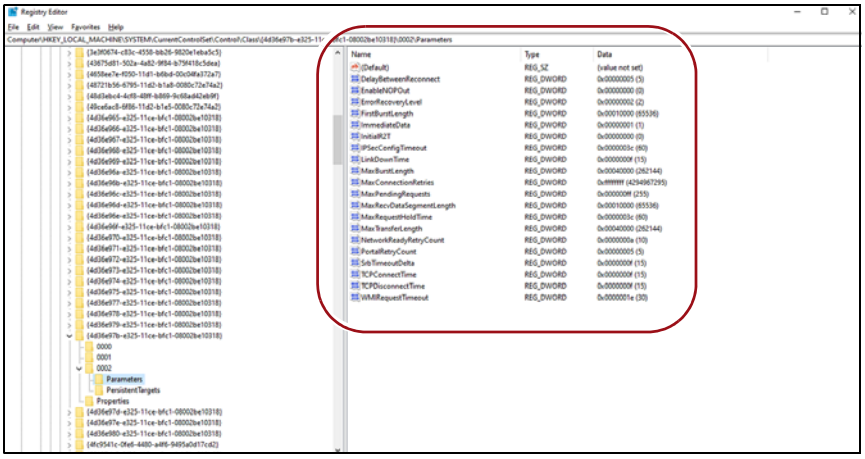

Figure 27 The Registry Editor window.

3. Browse to the location listed below:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\<*instance_number*>\Parameters

   Note: The "instance number" varies by system.

   The registry information displays in the right-hand pane (see Figure 27).

4. Double-click **MaxTransferLength**. The Edit DWORD dialog box displays.

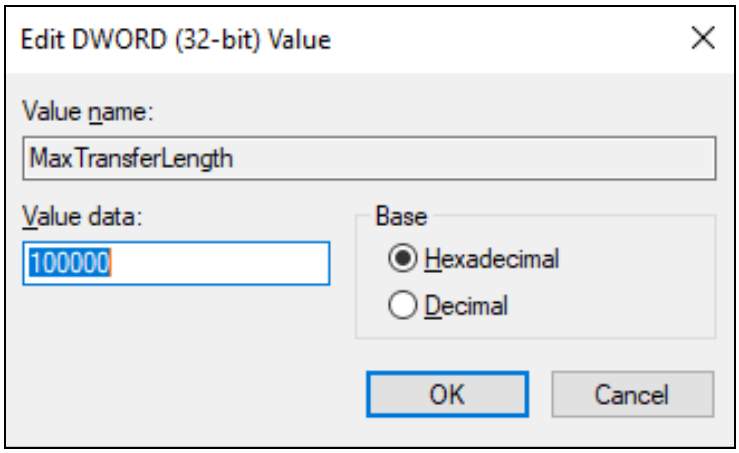

Figure 28 The Edit DWORD dialog box for MaxTransferLenth.

5. Do one of the following:
   - Click **Hexadecimal**, enter `100000` in the **Value data** entry box, and click **OK**.
   - Click **Decimal**, enter `1048576` in the **Value data** entry box, and click **OK**.
6. Double-click **MaxBurstLength**. The Edit DWORD dialog box displays.

7. Do one of the following:
   - Click **Hexadecimal**, enter `400000` in the **Value data** entry box, and click **OK**.
   - Click **Decimal**, enter `4194304` in the **Value data** entry box, and click **OK**.
8. Close the Registry Editor.

CONFIGURE DRIVES USING iSCSI IN LINUX

Use the instructions in this section to configure drives in the iSCSI initiator on your local Linux host.

Note: If any command fails with permission denied, prefix the command with `sudo`, and try again.

Install the iSCSI Initiator Utilities

1. To determine which package management software is used by your Linux distribution, use the following command:

   ```
   which yum
   ```

If the output is similar to /bin/yum, this distribution uses yum, otherwise it uses apt.

2. For systems using apt package management, execute the following command:

   ```
   apt install open-iscsi
   ```

3. For systems using yum package management, execute the following command:

   ```
   yum install iscsi-initiator-utils
   ```

Configure the Data Ports

1. For iSCSI applications, the in-box driver should be used to connect the Spectra Swarm bridge to the host.

   For iSER (iSCSI extensions for RDMA) applications, load the appropriate driver that supports RDMA on your host installed NIC.

2. Ports may be auto-configured if connected to a network with DHCP. Otherwise, they will need to be assigned an IP address using the ipconfig command.

   Note: If Ethernet ports are direct-connected to the Spectra Swarm bridge without the use of a switch and both data ports are used, the Spectra Swarm bridge data ports must not be on the same subnet. The default subnet mask for the Spectra Swarm bridge is 255.255.0.0

3. Test the network connection using the ping command. Note the IP address of the Spectra Swarm bridge data port and then on the initiator, enter the following command:

   ```
   ping ipaddress
   ```

   where “ipaddress” is the address of the Spectra Swarm bridge data port.

   Sample output:

   ```
   PING 172.16.1.20 (172.16.1.20) 56(84) bytes of data.
   ```

   64 bytes from 172.16.1.20: icmp_seq=1 ttl=64 time=0.144 ms

   64 bytes from 172.16.1.20: icmp_seq=2 ttl=64 time=0.111 ms

   64 bytes from 172.16.1.20: icmp_seq=3 ttl=64 time=0.116 ms

Tape Drives

If using tape devices, install Linear Tape File System (LTFS) software provided by the tape device manufacturer.

If using iSER with tape devices, set max sectors to 2048 before attempting to mount or create a LTFS partition. To do this execute the following two commands:

```
rmmod ib_iser
```

```
modprobe ib_iser max_sectors=2048
```

Note: The ib_iser change is not persistent across reboots. To make the changes persistent, you should add a kernel module configuration file. This modification will take place whenever the ib_iser module is started.

- Create the file /etc/modprobe.d/ib_iser.conf
- Add the max sectors modification option the file options ib_iser max_sectors=2048

Discover Spectra Swarm Targets

If one-way or two-way CHAP authentication has been configured on the Spectra Swarm bridge for the discovery session, open /etc/iscsi/iscsid.conf in a text editor and add or modify the following lines:

```
discovery.sendtargets.auth.authmethod = CHAP
discovery.sendtargets.auth.username = username
discovery.sendtargets.auth.password = password
```

Note: The username and password must match the CHAP In Account Name and CHAP In Secret configured on the Spectra Swarm bridge for discovery. Both username and password are case-sensitive.

If two-way CHAP authentication has been configured on the Spectra Swarm bridge for discovery, also add or modify the following lines in /etc/iscsi/iscsid.conf:

```
discovery.sendtargets.auth.username_in = username_in
discovery.sendtargets.auth.password_in = password_in
```

Notes:
- The username_in and password_in must match the CHAP Out Account Name and CHAP Out Secret configured on the Spectra Swarm bridge for discovery. Both username_in and password_in are case-sensitive.
- You must log out of any current sessions and re-perform discovery for the CHAP settings to take effect.

Discover Spectra Swarm bridge targets by entering the following command:

```
iscsiadm -m discovery -t st -p ipaddress
```

where “ipaddress” is the address of the Spectra Swarm bridge data port to perform discovery through.

The command should return a list of all Spectra Swarm bridge targets available to this initiator.

Note: If an Spectra Swarm bridge target exists but is not returned through discovery, check that this initiator is in the list of Allowed Initiators for that target (see Target Access Control in Section 5).

If “Login failed to authenticate with target” is returned, check that the credentials set in /etc/iscsi/iscsid.conf match the credentials configured on the Spectra Swarm bridge.

Configure Target CHAP

This section only applies when one-way or two-way CHAP authentication has been configured on the Spectra Swarm bridge to connect to a target. If not using CHAP, skip to Connect to the Target below.

1. Enter the following commands:

```
iscsiadm -m node -T target -o update
-n node.session.auth.authmethod -v CHAP
```

```
iscsiadm -m node -T target -o update
-n node.session.auth.username -v username
```

```
iscsiadm -m node -T target -o update
-n node.session.auth.password -v password
```

Note: "target" must match the full target IQN returned by the discovery command above. "username" must match the CHAP In Account Name configured on the Spectra Swarm bridge for this target. "password" must match the CHAP In Secret configured on the Spectra Swarm bridge for this target. Both username and password are case-sensitive.

2. (Two-way CHAP only) Enter the following commands:

```
iscsiadm -m node -T target -o update -n
node.session.auth.username_in -v username_in
```

```
iscsiadm -m node -T target -o update -n
node.session.auth.password_in -v password_in
```

Note: "target" must match the full target IQN returned by the discovery command above. "username_in" must match the full target IQN returned by the discovery command above. "password_in" must match the CHAP Out Secret configured on the Spectra Swarm bridge for this target. Both username_in and password_in are case-sensitive.

You must log out of any current sessions and re-perform discovery for the CHAP settings to take effect.

Connect to the Target

1. (iSER only) Change the connection mode to iSER by entering the following command:

```
iscsiadm -m node -T target -o update -n iface.transport_name
-v iser
```

Note: "target" must match the full target name returned from the discovery command above.

2. Log in to the target by entering the following command:

```
iscsiadm -m node -T target -p ipaddress -l”
```

Note: “target” must match the full target name returned from the discovery command above. “ipaddress” is the address of the Spectra Swarm bridge data port used in the discovery command above.

In the user interface, click on Advanced on the left hand side of the screen, enter DisplayInitiators under Enter a CLI command, and click Submit.

Note: You can also verify the initiator is connected using the command line interface's DisplayInitiators command (see the *ATTO 8200T User Guide*).

Sample Output:

Initiator : Target : Transport

;==============================

iqn.1994-05.com.redhat:767dbe5a936e : default : ISER

iqn.1994-05.com.redhat:767dbe5a936e : default : ISER

If using an iSER connection, verify that the initiator IQN is listed with "iSER" in the transport column.

Drives mapped to that target should now appear in the /dev/ directory as new SCSI devices, for example /dev/sdc.

To refresh available drives enter the following command:

```
iscsiadm -m session -rescan
```

If “iSCSI login failed due to authorization failure” is reported, ensure the CHAP credentials (if any) entered above match those configured on the Spectra Swarm bridge for this target.

LTFS Partition

Note: Some manufacturers’ drivers use non-standard names for tape devices.

- To create an LTFS partition, enter the following command:

```
mkltfs /dev/IBMtapeX
```

Note: “stX” is the tape device to create a partition on.

- To mount an LTFS partition, enter the following command:

```
ltfs /path/to/mount -o devname=/dev/IBMtapetX
```

Note: /path/to/mount is the desired directory on which to mount the partition. “stX” is the tape device where the LTFS partition resides.

Disconnect from the Target

To log out from a target, enter the following command:

```
iscsiadm -m node -T target -p ipaddress -u
```

Notes:
- "target" must match the full target name returned from the discovery command above. "ipaddress" is the address of the Spectra Swarm bridge data port used in the discovery command above.
- You can connect/disconnect to/from all discovered targets by omitting the `-t target` parameter from the log in/out commands.

TEST DRIVES

Once the drives are configured in the Spectra Swarm bridge user interface, test the connection to each drive.

- From your host system, verify the drives are discovered by the system.
- Verify the data path by writing and reading back a small amount of data.

LED Indicator Status

Use the chart below to help troubleshoot problems with the Spectra Swarm bridge.

LED Indicators on Front of Controller

LED Indicator	Description
Power Supplies	One LED for each supply. Green indicates on and ready while amber indicates an unplugged or a failed supply.
Controller Power	A lit green LED indicates power has been turned on to the storage controller.
Ready	A lit green LED indicates ready, and OFF indicates not ready.
Alert	A lit yellow LED indicates an alert condition.
Ethernet Data Activity	A lit green port activity LED indicates traffic on the port, and OFF indicates no port activity.
Ethernet Data Port Speed	A bi-color port speed LED is lit as follows: ▪ Green = 40 GigE ▪ Yellow = 10 GigE ▪ OFF = No link or 1 GigE.
SAS Device Activity	A lit green LED for each SAS connector indicates port activity on at least one PHY in the connector, and OFF indicates no port activity.

LED Indicators on Rear of Controller

LED Indicator	Description
Power Supplies	One LED for each supply. Blue indicates on and ready. Blinking blue indicates power is applied but power supply is not on. Blinking Red indicates an unplugged or failed power supply.
Ready / Alert	Bi-color shared LED lit green means ready, yellow indicates an alert condition.
Ethernet Management Port	The left green LED on the RJ45 connector indicates speed, while the right green LED indicates an active link/activity.
Ethernet Data Port	Port LEDs are located below the QSFP+ connectors. A lit green LED indicates link, and OFF indicates no link.

LED Indicator	Description
SAS Connection	SAS LEDs are located below the mini-SAS HD connector. A lit green LED indicates a link has been established on at least one PHY, and OFF indicates there are no links.

BEST PRACTICES

The best practices listed below help you achieve maximum data transfer performance for the Spectra Swarm bridge.

- The Spectra Swarm bridge supports both iSER and iSCSI over Ethernet. iSER runs over RDMA eliminating the TCP/IP stack so it is much more efficient and provides higher throughput with deterministic latency. iSCSI runs over TCP/IP and will have higher latency with slower performance than iSER.
- Spectra Logic recommends that the Spectra Swarm bridge is used on an isolated physical, lossless network when using iSCSI.
- When using the Spectra Swarm bridge, each data port must be assigned to an independent subnet in order to achieve full bandwidth.
- Spanning-tree protocol (STP) should be disabled on the switch ports used for iSCSI traffic.
- Flow control (XON/XOFF) should be enabled on the switch ports and the iSCSI initiators.
- Spectra Logic recommends disabling UNICAST storm control on your switch.
- Spectra Logic recommends that you USE broadcast and multicast storm control on your switch.
- Jumbo frames (large MTUs) should be enabled on all switch ports, the iSCSI initiators, and the Spectra Swarm bridge data ports for optimal performance.

CONFIGURE SECURITY CERTIFICATES

The Spectra Swarm bridge uses a certificate that is provided to devices on a network to authenticate the controller. The HTTPS, SSH, and SFTP services running on the controller expect to have access to a PEM (Privacy Enhanced Mail) file containing the keypair (a certificate and its associated private key) necessary to provide access. The initial keypair PEM file has been generated by the controller.

Note: The private key is only seen by the controller.

Keypair Regeneration

The PEM file containing the keypair is regenerated by the controller if:

- It expires. This will be noted in the Spectra Swarm event log. Additionally, the approaching expiration of the keypair is logged one month prior to its expiration.
- The IP configuration of an Ethernet port changes. The certificate used on the controller uses the IP configurations of the Ethernet ports (but not the DNS name of the controller). If an Ethernet port IP configuration changes, the keypair will be regenerated to reflect the change.
- User-provided certificate attributes change.

In all cases, since it is the controller that generates the keypair, the certificate within will be self-signed. This will result in a client web browser warning advisement when a connection attempt is made to the controller.

Note: Even if an externally signed certificate is present on the XstreamCORE, a self-signed certificate will be generated to replace it if the conditions above are met.

Keypair PEM File Requirements

If a self-signed certificate is not desirable, an externally signed certificate and its associated private key can be uploaded to the controller. The file containing this keypair must meet several requirements:

- It must be named httpspem.pem.
- It must be in the PEM format.
- The contents of the file must include both the certificate and the private key.
- It must not be encrypted (if generated via OpenSSL's "req" command, specify "-nodes").
- The private key must be an RSA private key.
- The certificate must be SHA256 signed.
- The certificate must have the same attributes as the controller displays in the "get HttpsCertParams" command (see below).

The file format should appear as follows (note that the actual contents have been abbreviated):

-----BEGIN PRIVATE KEY-----

MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDaJU8l iMAIZREs

… <snip>

uU0m3t4sxrOlF5WarwTYQWKE

-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

MIIDIjCCAgqgAwIBAgIJANYizZ6isr/
gMA0GCSqGSIb3DQEBCwUAMDoxCzAJBgNV

… <snip>

/GAqJDXDoFDpHrHGEXtOi9AP1VKxREo+J/L9eb+CuOE/EPFaHlM=

-----END CERTIFICATE-----

Installing a Keypair PEM File

1. Sign in to the Spectra Swarm user interface (see Sign In to the Spectra Swarm Bridge on page 12).
2. On the left-hand pane, click **Certificate Management**. The Certificate Management screen displays.
3. In the **Upload PEM File** pane, click **Choose File** and browse to the location of the PEM file.
4. Click **Upload**.

REMOTE INTERFACE OPTIONS

If you do not want to use the Spectra Swarm user interface, you can access and manage the Spectra Swarm bridge using one of the following remote interfaces.

Using the Serial Port Connection

The Spectra Swarm bridge supports remote service operations over the RS-232 serial port using standard terminal emulation software available with most systems.

1. With the Spectra Swarm bridge powered off, connect a cable from Spectra Swarm bridge RS-232 serial port to the serial (COM) port on a personal computer.

   Notes:
   - The serial cable must be less than 6.5 ft (2m).
   - A gender changer or DB-9 to DB-25 converter may be needed depending on the cables being used.

2. Power on the Spectra Swarm bridge by connecting power cables to the rear of the controller.
3. Start a terminal emulation program on the personal computer, and use it to connect to the Spectra Swarm bridge. For example, if you are using HyperTerminal on a computer running a Windows operating system, type Spectra Swarm bridge in the New Connection dialog box.
4. Click **OK**.

5. In the Connect To dialog box, for the **Connect using** field, select the COM port number to which your serial cable is connected.
6. Click **OK**.
7. In the COM Properties dialog box select the following values:
   - **Bits per second**: 115200
   - **Data Bits**: 8
   - **Parity**: None
   - **Stop Bits**: 1
   - **Flow Control**: None
   - **Terminal type**: ASCII
   - **Echo**: on
8. Click **OK**.
9. After you connect to the Spectra Swarm bridge, start-up messages are displayed. These messages are only displayed when the controller is starting up (power is connected to the controller but the Ready LED indicator is not yet lit). If the Ready LED indicator is lit before the user connects the serial cable or starts/sets up the terminal program, you will need to press **Enter** to receive a Ready message prompt.
10. In serial port sessions, there is no prompt on the line below the word Ready. Begin typing commands in the blank line where the cursor is resting. No user name or password is required for serial port access.
11. To verify that you have connected successfully, type `help` after the Ready prompt and press **Enter**.

Using the USB Port Connection

The Spectra Swarm bridge supports remote service operations over the USB port using standard terminal emulation software available with most systems.

1. With the Spectra Swarm bridge powered off, connect a USB cable from the USB-B management port to a USB port on a personal computer.
2. Power on the Spectra Swarm bridge by connecting power cables to the rear of the controller.
3. After the Spectra Swarm bridge boots, the computer should detect the USB port and load the appropriate serial USB driver. For example, in a Windows environment, the OS will detect the USB cable installed and try to find and load a serial to USB driver.
4. Start a terminal emulation program on the personal computer, and use it to connect to the Spectra Swarm bridge. For example, if you are using HyperTerminal on a computer running a Windows operating system, type Spectra Swarm bridge in the New Connection dialog box.
5. Click **OK**.

Using an SSH Connection

Up to two SSH sessions can be conducted simultaneously. A serial port session can use the CLI while SSH sessions are open. Whichever session issues the first set CLI command can continue to issue **set** commands, while the other session can only issue **get** commands or display information. Once a connection is established, refer to Using the Command Line Interface on page 40.

1. Start an SSH client.

   Note: There is more than one way to connect to the Spectra Swarm bridge using an SSH client. Your SSH client may operate differently than in the following instructions.

2. In your SSH client, connect to the Spectra Swarm bridge. As an example, using OpenSSH, the connection would be made with the following command where username is the username set Change the Password on page 13, and x.x.x.x is the IP address of the Spectra Swarm bridge.

   ```
   ssh username@x.x.x.x
   ```

3. Enter your password or the default password if you did not configure a new password.
4. To quit an SSH session, type `exit` and press **Enter**.

USING THE COMMAND LINE INTERFACE

The command line interface (CLI) provides access, configuration, and monitoring for the Spectra Swarm bridge through a set of ASCII commands. CLI commands may be entered through a serial port connection, USB connection, active telnet session, or the Advanced page on the Spectra Swarm user interface.

- CLI commands are context sensitive and generally follow a standard format:

  [*Get*|*Set*] Command [*Parameter1*|*Parameter2*] followed by the return or enter key.

- CLI commands are case insensitive: you may type all upper or all lower case or a mixture. Upper and lower case in this manual and the help screen are for clarification only.
- Commands generally have three types of operation: get, set, and immediate.
- The get form returns the value of a parameter or setting and is an informational command.
- Responses to get commands are followed by Ready.
- The set form is an action that changes the value of a parameter or configuration setting. It may require a SaveConfiguration command and a restart of the system before it is implemented. The restart can be accomplished as part of the SaveConfiguration command or by using a separate FirmwareRestart command. A number of set commands may be issued before the SaveConfiguration command.

- Responses to set commands are either an error message or Ready. The asterisk character (*) indicates you must use a SaveConfiguration command to finalize the set command. SaveConfiguration asks if you want to restart the system or not.
- Immediate commands are set commands which are executed right away and do not require a SaveConfiguration command.
- Responses to Immediate commands are either an error message or data results followed by Ready.

Command Conventions

Symbols, typefaces and abbreviations used to indicate functions and elements of the command line interface.

Symbol	Indicates
[ ]	Required entry
< >	Optional entry
|	Pick one of
...	Repetition of preceding item
\n	End of line
-	A range (ex 6-9 = 6, 7, 8, 9)
el	Ethernet LUN (0 <= el <= 1024)
dp	Ethernet Data port number (1<= dp <= 2)
sasConn	SAS connector name (A, B, C, D)
mp	Ethernet Management port number (1<= mp <= 2)

CLI Error Messages

The following error messages may be returned by the command line interface:

- ERROR. Invalid Command. Type 'Help' for command list.
- ERROR. Wrong/Missing Parameters
- Usage: <usage string>
- ERROR. Command Not Processed

CLI Summary Reference

A summary of the command line interface commands, their defaults, and example use of the command. Commands which have no default values associated with them have a blank entry in that column of the table.

Command	Default	Example
AccessControl	disabled	get AccessControl default
AccessEntry		set AccessEntry default iqn.1994-05.com.CENTOS.host
BootEthernetDelay	0	get BootEthernetDelay
BootOldestImage		BootOldestImage
ClearCliLog		ClearCliLog
ClearEventLog		ClearEventLog
ControllerLun	enabled	get controllerlun
ControllerModel		get controllermodel
ControllerName	" "	set controllername Omega6
CoreDumpInfo		CoreDumpInfo
Date	10/25/2016 (with SNTP disabled)	set date 03/03/2019
DeleteAllMaps		deleteallmaps
DisplayInitiators		DisplayInitiators
DPMTU	1514	get DPMTU all
DumpCliLog		DumpCliLog
DumpConfiguration		dumpconfiguration
DumpEventLog		dumpeventlog
EmailFromAddress	" "	get emailfromaddress
EmailNotifyAddress	" "	set emailnotifyaddress 5 bw@abc.com
EmailPassword		set emailpassword Password12345
EmailServerAddress	0.0.0.0	get emailsesrveraddress
EmailUsername	" "	set emailusername beta321
EthDpConnectorInfo		get EthDpConnectorInfo all
EthernetPort	enabled	set EthernetPort mp1 disabled
EthernetSpeed	auto	set ethernetspeed mp1 100
EthPortList		EthPortList

Command	Default	Example
Exit		exit
FirmwareRestart		firmwarerestart
FlashImages		flashimages
Help		help AccessControl
HttpsCertInfo		HttpsCertInfo
HttpsCertParams	Country (C) = "" State (ST) = "" Locality (L) = "" Organization (O) = "" Organization Unit (OU) = "" Common Name (CN) = ""	get HttpsCertParams
IdentifyController	disabled	set identifycontroller enabled
IdentifyLUN		IdentifyLUN default 3
Info		info
IPAddress	With IPDHCP disabled: DP1 = 10.0.0.1 DP2 = 10.0.0.2 MP1 = 10.0.0.3 MP2 = 10.0.0.4	get ipaddress mp1
IPDHCP	enabled	set ipdhcp mp1 disabled
IPDNSServer	127.0.0.1	get ipdnsserver
IPGateway	0.0.0.0	set ipgateway mp1 200.10.22.3
IPSubnetMask	With IPDHCP disabled: 255.255.0.0	get ipsubnetmask mp1
iSCSIAlias	“ “	Set iSCSIAlias Backup_Cluster_1
iSCSICHAP	disabled	get iSCSICHAP all
iSCSICHAPSecret		set iSCSICHAPSecret default in iqn.1994-05.com.CENTOS.host Password12345
iSCSIDeletedTargets		iSCSIDeletedTargets
iSCSIFastReTx	enabled	Set iSCSIFastReTx disabled
iSCSIRestoreDeletedTarget		iSCSIRestoreDeletedTarget all
iSCSISACK	enabled	Set iSCSISACK disabled
iSCSITarget		
iSCSITargetCopy		

Command	Default	Example
iSCSITargetNameDisplay		iSCSITargetNameDisplay
iSCSITargetRename		iSCSItargetrename TargetA targetB
IsReserved		IsReserved
MaxOpTemp	65	get maxoptemp
MinOpTemp	0	set minoptemp 10
OEMConfigFile	ATTO	get oemconfigfile
OpTempWarn	10	set optempwarn 15
Password	P@SSw0rd	set password Password12345
Performance		get performance
Ping		ping mp1 192.42.155.155
ReadOnlyPassword	P@SSw0rd	set readonlypassword Password12345
ReadOnlyUsername	user	get readonlyusername
Reserve		reserve
RestoreConfiguration		restoreconfiguration default
Route		Route TargetA default 3
RouteDisplay		routedisplay iscsi
SASConnectorInfo		get sasconnectorinfo all
SASPortList		sasportlist
SASTargets		sastargets
SaveConfiguration		saveconfiguration restart
SerialNumber		get serialnumber
SNMP	disabled	set SNMP enabled
SNMPDumpEngineID		snmpdumpengineid
SNMPDumpMIB		snmpdumpmib
SNMPExtendedTraps	disabled	get snmpextendedtraps
SNMPTrapAddress	0.0.0.0 none	set snmptrapaddress 6 192.42.155.155 all
SNMPTraps	disabled	set snmptraps enabled
SNMPUsername		snmpusername
SNTP	enabled	get sntp

Command	Default	Example
SNTPServer	MAIN - 129.6.15.30 AUX1 - 128.138.140.44 AUX2 - 128.138.141.172	set sntpserver 129.6.15.30
StopIdentifyLUN		StopIdentifyLUN default 3
Temperature		get temperature
Time		set time 03:32:30
TimeZone	EST (-05)	set timezone pst
Uptime		get uptime
Username	admin	set username Barbara
VerboseMode	enabled	set verbosemode disabled

CLI Command Explanations

AccessControl

AccessControl enables or disables access control on a target node. Access to the target node is keyed to the iSCSI qualified name of white listed initiators.

Default: disabled

`set AccessControl` [default | *target Name*] [enabled | disabled]

`get AccessControl` [default | *target Name* | all]

AccessEntry

AccessEntry allows the addition or deletion of an initiator entry from the access control list of a target node. The initiator name must be formatted as an iSCSI qualified name and must be between 16 and 223 characters, is case sensitive and cannot be 'all'.

`set AccessEntry` [default | *target name*] [*initiator name* <delete> | all <delete>]

`get AccessEntry` [default | *target name* | all]

BootEthernetDelay

BootEthernetDelay sets the delay (in seconds) after startup before enabling the Ethernet ports. The value “0” disables the delay.

Default: 0

`set BootEthernetDelay` [0 - 255]

`get BootEthernetDelay`

BootOldestImage

The BootOldestImage command allows the user to boot the appliance using the oldest stored flash image.

`BootOldestImage`

ClearCliLog

Clears the contents of the CLI command log.

`ClearCliLog`

ClearEventLog

ClearEventLog clears the contents of the event log.

`ClearEventLog`

ControllerLun

ControllerLun controls the automatic generation of a controller device at LUN 0.

Default: enabled

`set ControllerLun` [enabled | disabled]

`get ControllerLun`

ControllerModel

ControllerModel reports the specific model and firmware information to the CLI.

`get ControllerModel`

ControllerName

ControllerName provides a descriptive ASCII name assigned to the unit. This field is used by applications to identify individual units. The specified name can be up to a maximum of 32 characters. If the name contains spaces, it must be enclosed in quotation marks. Unlike other non-immediates, changes to ControllerName take effect immediately.

`set ControllerName` [*name*]

`get ControllerName`

CoreDumpInfo

Displays information concerning a core dump stored by a prior fault.

`CoreDumpInfo`

Date

Date sets/displays the current date. The date range is 10/25/2016 to 01/18/2038.

Default: 10/25/2016 (with SNTP disabled)

`set Date` [*MM*/*DD*/*YYYY*]

`get Date`

DeleteAllMaps

Removes all mapped devices from the map table. Upon the subsequent POST, if no maps are present the default maps will be loaded.

`DeleteAllMaps`

DisplayInitiators

Displays a list of currently logged-in iSCSI initiators the target they are logged into and the transport type. No WWN.

`DisplayInitiators`

DPMTU

DPMTU controls the MTU, or maximum transmission unit (Frame Size), used by the data port. Changes to these settings are applied when a SaveConfiguration command is executed.

Default: 1514

`set DPMTU` [dp[*n*] | all] [1514 | 9014]

`get DPMTU` [dp[*n*] | all]

DumpCliLog

Dumps the contents of the CLI command log to the current CLI session. The column EvLog# is the current event log number as seen in DumpEventLog. The keyword EXCEPT indicates an exception occurred while processing the command, and the keyword RESTART indicates the unit was restarted. An optional numeric parameter specifies the maximum number of entries to display from the end of the log.

`DumpCliLog` <*NumEntries* | all>

DumpConfiguration

Dumps the system configuration.

`DumpConfiguration`

DumpEventLog

DumpEventLog can be used to dump the contents of the event log to an RS-232, USB, or telnet session. With no parameters, the last 2048 entries will be displayed. The optional parameter "all" specifies all entries will be displayed. An optional numeric parameter specifies the maximum number of entries to display from the end of the log.

`DumpEventLog` <*NumEntries* | all>

EmailFromAddress

EmailFromAddress configures the email address that this system will use to talk to the email server. Full email address is a fully qualified Internet email address, not more than 128 characters long.

`set EmailFromAddress` [*full email address*]

`get EmailFromAddress`

EmailNotify

EmailNotify turns on and off email notification.

Default: disabled

`set EmailNotify` [enabled | disabled]

`get EmailNotify`

EmailNotifyAddress

EmailNotifyAddress configures notification addresses. Index is a number between 1 and 5, inclusive. Full email address is a fully qualified Internet email address, not more than 128 characters long. The level can be "all", "informational", "warning", "critical" or "none". This is the minimum level of severity in order for the event to trigger an email notification.

`set EmailNotifyAddress` [index] [*full email address*] [all | informational | warning | critical | none]

`get EmailNotifyAddress` [index | all]

EmailPassword

EmailPassword sets the password used to authenticate the login to the SMTP email server. The password must not be more than 64 characters. A password is not required if the email server does not require authentication.

`set EmailPassword`

EmailServerAddress

EmailServerAddress configures the address of the server that should be contacted in order to send out emails. Either an IP address or a fully qualified domain (e.g. mail.myserver.com) may be specified.

Default: 0.0.0.0

`set EmailServerAddress` [*IP address* | *name*]

`get EmailServerAddress`

EmailUsername

EmailUsername sets the username used to authenticate the login to the SMTP email server. The username must not be more than 128 characters. A username is not required if the email server does not require authentication.

`set EmailUsername` [*username*]

`get EmailUsername`

EthDpConnectorInfo

EthDpConnectorInfo displays information about the specified Ethernet Data Port QSFP Connector. Valid connector names are DP0, DP1, etc.

`get EthDpConnectorInfo` [*ethConn* | all]

EthernetPort

The EthernetPort command is used to enable or disable an ethernet port.

Default: enabled

`set EthernetPort` [dp[*n*] | mp[*n*]] [enabled | disabled]

`get EthernetPort` [dp[*n*] | mp[*n*] | all]

EthernetSpeed

EthernetSpeed determines the speed of any Ethernet port(s). If Auto is enabled then the Ethernet speed will be negotiated and the value in parentheses returned by the 'get' command indicates the current speed of the Ethernet connection. Changes to these settings are applied when a SaveConfiguration command is executed.

Default: auto

`set EthernetSpeed` [dp[*n*] [10Gb | 40Gb | auto] | mp[*n*] [100 | 1Gb | auto] | all auto]

`get EthernetSpeed` [dp[*n*] | mp[*n*] | all]

EthPortList

Lists the available Ethernet ports and their current status. Valid status values are: Up or Down

`EthPortList`

Exit

Exit terminates the current CLI session over SSH. This command has no effect if used during a serial RS-232 session or USB connection.

`Exit`

FirmwareRestart

FirmwareRestart resets and reinitializes the firmware.

`FirmwareRestart`

FlashImages

FlashImages displays the metadata for software images currently stored in the Flash device. The optional parameter "validate" also validates the CRC of the flash images. Note that the CRC validation causes a multi-second delay.

`FlashImages` <validate>

Help

The Help command issued with no parameters displays a list of available CLI commands. When a CLI Command name is specified, a command usage string and command description is presented on the CLI.

`Help` <*command name*>

HttpsCertInfo

Displays information about the current HTTPS certificate.

`HttpsCertInfo`

HttpsCertParams

Displays or sets the attributes used to generate the HTTPS certificate. All attributes are optional. C is Country with a fixed length of 2 characters. ST is State with a max length of 128 characters. L is Locality with a max length of 128 characters. O is Organization with a max length of 64 characters. OU is Organization Unit with a max length of 64 characters. CN is Common Name with a max length of 64 characters. Changes made to the HTTPS attributes will take effect on reboot.

Default: Country (C) = ""

State (ST) = ""

Locality (L) = ""

Organization (O) = ""

Organization Unit (OU) = ""

Common Name (CN) = ""

`set HttpsCertParams` [C | ST | L | O | OU | CN] [*nn...nn*]

`get HttpsCertParams`

IdentifyController

IdentifyController causes the 'Alert' LED to blink to enable identification of this system. Disable this option to cancel the blinking.

Default: disabled

`set IdentifyController` [enabled | disabled]

`get IdentifyController`

Info

Info displays version numbers and other product information for key components. Use the optional 'brief' parameter to show a more concise subset of system information.

`Info` <brief>

IPAddress

IPAddress controls the current IP address of any Ethernet port(s). If IPDHCP is enabled, then the 'get' command reports the current IP address assigned by the network DHCP server, followed by the (DHCP) identifier. Changes to these settings are applied when a SaveConfiguration command is executed.

Default (when IPDHCP is disabled):

DP1 = 10.0.0.1

DP2 = 10.0.0.2

MP1 = 10.0.0.3

MP2 = 10.0.0.4

`set IPAddress` [dp[*n*] | mp[*n*] | all] [xxx.xxx.xxx.xxx]

`get IPAddress` [dp[*n*] | mp[*n*] | all]

IPDHCP

IPDHCP allows acquisition of an IP address from a network DHCP server. When this option is disabled, the IP address used will be specified by the IPAddress CLI command. Changes to these settings are applied when a SaveConfiguration command is executed.

Default: enabled

`set IPDHCP` [dp[*n*] | mp[*n*] | all] [enabled | disabled]

`get IPDHCP` [dp[*n*] | mp[*n*] | all]

IPDNSServer

Controls the current DNS Server address. If IPDHCP is enabled, then this value is automatically detected. If IPDHCP is disabled, then this value must be manually set.

Default: 127.0.0.1

`set IPDNSServer` [xxx.xxx.xxx.xxx]

`get IPDNSServer`

IPGateway

IPGateway controls the current default gateways used by any Ethernet port(s). If IPDHCP is enabled, the 'get' command reports the current IP gateway assigned by the network DHCP server. Changes to these settings are applied when a SaveConfiguration command is executed.

Default: 0.0.0.0

`set IPGateway` [dp[*n*] | mp[*n*] | all] [xxx.xxx.xxx.xxx]

`get IPGateway` [dp[*n*] | mp[*n*] | all]

IPSubnetMask

IPSubnetMask controls the current subnet masks used by any Ethernet port(s). If IDHCP is enabled, the 'get' command reports the current IP subnet mask assigned by the network DHCP server. Changes to these settings are applied when a SaveConfiguration command is executed.

Default: 255.255.0.0 (with IPDHCP disabled)

`set IPSubnetMask` [dp[*n*] | mp[*n*] | all] [xxx.xxx.xxx.xxx]

`get IPSubnetMask` [dp[*n*] | mp[*n*] | all]

iSCSIAlias

iSCSIAlias assigns a human-readable name to this system. Aliases may be 1 to 64 characters in length and may contain spaces if enclosed in quotes.

`set iSCSIAlias` [*alias*]

`get iSCSIAlias`

iSCSICHAP

Specifies the type of CHAP (Challenge-Handshake Authentication Protocol) to be used for initiator logins. In 'One-way' authentication, the target authenticates the initiator using the 'in' CHAP secret, but the initiator does not authenticate the target. In 'Two-way' authentication, an additional level of security enables the initiator to authenticate the target using the 'out' CHAP secret. 'Disabled' means no authentication will be enforced and any initiator will have access to the target. If 'discovery' is specified, the selected CHAP authentication will apply to discovery sessions. NOTE: Access Control must be enabled on the target for CHAP authentication to occur.

Default: disabled

`set iSCSICHAP` [default | *target name* | discovery] [disabled | one-way | two-way]

`get iSCSICHAP` [default | *target name* | discovery | all]

iSCSICHAPSecret

Specifies the incoming and outgoing passwords for iSCSI CHAP sessions. Secrets are case sensitive, 12 to 32 characters, and cannot contain spaces. 'In' and 'out' secrets must be different for each name. The 'in' secret is for authentication of the initiator by the target. It is used for both one-way and two-way authentication. There is only one 'out' secret per target. The default account name for out secret is 'root'. If 'discovery' is specified, the setting will apply to CHAP during discovery sessions. There is a single account name for discovery CHAP, which is overwritten when the discovery account name is changed. NOTE: Access Control must be enabled and iSCSICHAP set to one-way or two-way for the CHAP secret to apply.

`set iSCSICHAPSecret` [default | *target name* | discovery] [in [*account name* | all] | out [*account name*] | delete [*account name* | all]] <*Secret*>

`get iSCSICHAPSecret` [default | *target name* | discovery] [in [*account name* | all] | out [root]]

iSCSIDeletedTargets

Displays a list of deleted iSCSI target names.

`iSCSIDeletedTargets`

iSCSIFastReTx

Configures TCP fast retransmits for iSCSI connections.

Default: enabled

`set iSCSIFastReTx` [enabled | disabled]

`get iSCSIFastReTx`

iSCSIRestoreDeletedTarget

Enables the controller to automatically recreate a deleted iSCSI target after the next system reboot.

`iSCSIRestoreDeletedTarget` [*target name* | all]

iSCSISACK

Configures TCP Selective ACK for new iSCSI connections. Selective ACK must be configured on both the host and the target in order to be enabled. This command only affects new connections. To change existing iSCSI connections use the host to log out, then log back in.

Default: enabled

`set iSCSISACK` [enabled | disabled]

`get iSCSISACK`

iSCSITarget

iSCSITarget creates/deletes an iSCSI target. The target name is appended to the standard iSCSI qualified name and may not exceed 16 characters. The 'default' target cannot be deleted.

`iSCSITarget` [*target name*] <delete>

iSCSITargetCopy

iSCSITargetCopy creates a copy of an iSCSI target.

`iSCSITargetCopy` [*original target name*] [*copy target name*]

iSCSITargetNameDisplay

iSCSITargetNameDisplay displays the iSCSI target names.

`iSCSITargetNameDisplay`

iSCSITargetRename

iSCSITargetRename renames an iSCSI target.

`iSCSITargetRename` [*original target name*] [*new target name*]

IsReserved

IsReserved displays the reservation status of the current services session/ interface.

`IsReserved`

MaxOpTemp

Regulates/displays the maximum enclosure temperature alarm of the Spectra Swarm bridge in degrees Celsius. If the temperature of the Spectra Swarm bridge rises above the maximum MaxOpTemp, thermal control event handling occurs.

Default: 65

`set MaxOpTemp` [55-65]

`get MaxOpTemp`

MinOpTemp

Regulates/displays the minimum enclosure temperature alarm of the Spectra Swarm bridge in degrees Celsius. If the temperature of the Spectra Swarm bridge falls below the minimum MinOpTemp, thermal control event handling occurs.

Default: 0

`set MinOpTemp` [0-30]

`get MinOpTemp`

OEMConfigFile

Returns the "name" (the contents of the first record) of the OEM configuration file stored in persistent memory.

Default: ATTO

`get OEMConfigfile`

OpTempWarn

Regulates/displays the number of degrees in Celsius before a warning is sent to the user. Valid entries are between 0 degrees and 15 degrees.

Default: 10

`set OpTempWarn` [0-15]

`get OpTempWarn`

Password

Password specifies the password used for all sessions: SSH, SFTP and the graphical user interface. The password must be 8 to 32 characters long, must contain at least one numeric character {0-9}, and may not contain the following: {' \ ; tab or the space character}.

Default: P@SSw0rd

`set Password` [*password*]

Performance

Returns system performance data for the user-specified data port(s). Data consists of the average rate (MB/s) and number of I/Os (IO/s) measured over the previous sampling period (approximately one second). Successful SCSI Read (28h, 88h, A8h) and Write (2Ah, 8Ah, AAh) commands are considered I/Os. Factors that may affect reported performance include port availability and saturation, transfer size, target device speeds, and overall system utilization.

`get Performance` <dp[*n*]>

Ping

Ping will send an ICMP echo request to the specified host.

`Ping` [dp[*n*] | mp[*n*]] [*IP Address*] <count <*size*>>

ReadOnlyPassword

ReadOnlyPassword specifies the password used for all sessions: SSH, SFTP and the graphical user interface. The password must be 8 to 32 characters long, must contain at least one numeric character {0-9}, and may not contain the following: {' \ ; tab or the space character}.

Default: P@SSw0rd

`set ReadOnlyPassword` [*password*]

ReadOnlyUsername

ReadOnlyUsername specifies the username used for all sessions: SSH, SFTP and the graphical user interface. Username must be all lowercase, 1 to 32 characters long, start with an alphabetical character, and may only contain the following: {a-z,0-9,-,_.}.

Default: user

`set ReadOnlyUsername` [*username*]

`get ReadOnlyUsername`

Reserve

Reserve prevents other CLI sessions from modifying the Spectra Swarm bridge. When the Spectra Swarm services interface is reserved, set commands are unavailable to other sessions, but get commands are available. Executing a SaveConfiguration or RestoreConfiguration command releases the Spectra Swarm bridge so that other CLI sessions may make setting changes.

`Reserve`

RestoreConfiguration

Restores configuration to either the default configuration or the configuration last saved into non-volatile memory. The saved option undoes any changes made since the last save.

`RestoreConfiguration` [Default | Saved]

Route

Route assigns a SAS destination device to an iSCSI protocol address on the specified target from the default target's map list. The device is mapped at the target's next available LUN. The "delete" identifier removes the map from the specified target. In verbose mode, overwriting a map requires secondary confirmation of the action.

`Route` <iSCSI> [*target name*] [default [LUN] | delete [LUN]]

RouteDisplay

RouteDisplay will display a list of iSCSI to SAS address mappings. The optional 'Target Name' parameter will display all mappings for that target.

`RouteDisplay` <iSCSI> <*target name*>

SASConnectorInfo

SASConnectorInfo displays information about the specified SAS connector. Valid connector names are A through D.

`get SASConnectorInfo` [*sasConn* | all]

SASPortList

Lists the status of all available SAS ports.

`SASPortList`

SASTargets

Lists the physical devices that are connected to all SAS connectors and PHYs.

`SASTargets`

SaveConfiguration

Many commands require a SaveConfiguration command to be executed as indicated by the return Ready. *. When you invoke a SaveConfiguration command, the current configuration is permanently saved in the Spectra Swarm bridge and the new configuration becomes the active configuration. If a firmware restart is required to make the requested change permanent, you are asked to confirm the restart. You can override this request by indicating the override value on the command line. You may make several changes through commands before implementing the restart, but once you have restarted the Spectra Swarm bridge, all the command changes created before the restart and save are implemented. If you select the restart option, the Spectra Swarm bridge executes its complete start up cycle.

`SaveConfiguration` <Restart | NoRestart>

SerialNumber

Reports the Spectra Swarm bridge serial number. The serial number, unique for each Spectra Swarm bridge, is a 13-character field. The first seven alphanumeric characters are an abbreviation of the Spectra Swarm bridge name while the remaining six numbers are the individual Spectra Swarm bridge board number.

`get SerialNumber`

SNMP

Enables/disables SNMP functionality.

Default: disabled

`set SNMP` [enabled | disabled]

`get SNMP`

SNMPDumpEngineID

Dumps the SNMPv3 Engine ID of this device.

`SNMPDumpEngineID`

SNMPDumpMIB

Dumps the contents of the specified private SNMP MIB to the current CLI session. If no parameter is specified, the Controller private MIB is dumped. For further assistance with SNMP, consult your network administrator.

`SNMPDumpMIB` <Controller | Product | ISCSI | SMI | TC>

SNMPExtendedTraps

SNMPExtendedTraps enables and disables Extended (i.e., Device Error) SNMP trap functionality.

Default: disabled

`set SNMPExtendedTraps` [enabled | disabled]

`get SNMPExtendedTraps`

SNMPTrapAddress

Sets/displays the IP trap addresses and levels. Consult your network administrator for further assistance with SNMP.

Index: value between 1 and 6

IPAddress: standard IP address for the host receiving messages; must be in the same subnet as the Spectra Swarm bridge

Trap Level: event severity required to trigger a trap

None: no traps are sent to configured IP addresses

All: traps are sent for all triggering events

Warning: only warning and critical events are sent

Critical: only critical events are sent

Default: 0.0.0.0 none

`set SNMPTrapAddress` [Index] [*IPAddress*] [*Trap Level*]

`get SNMPTrapAddress`s <Index | All>

SNMPTraps

Enables/disables SNMP trap functionality. Consult your network administrator for further assistance with SNMP.

Default: disabled

`set SNMPTrap`s [enabled | disabled]

`get SNMPTraps`

SNMPUsername

Sets the SNMPv3 username and password or displays the SNMPv3 username. The username must be 1 to 32 characters long, and may only contain the following: {a-z, A-Z, 0-9}.The password must be 8 to 32 characters long, and may only contain the following: {a-z, A-Z, 0-9}. SNMP must be enabled to run this command.

`SNMPUsername`

`get SNMPUsername`

SNTP

SNTP controls whether SNTP time server functionality is enabled.

Default: enabled

`set SNTP` [enabled | disabled]

`get SNTP`

SNTPServer

SNTPServer sets/displays the IP addresses used to retrieve the SNTP time. Index range is 1-3 indicating the server slot to set/display. Enter 0.0.0.0 to disable a time server slot.

Default:

1 - MAIN - 129.6.15.30

2 - AUX1 - 128.138.140.44

3 - AUX 2 - 128.138.141.172

`set SNTPServer` [Index] [*IP address*]

`get SNTPServer` <Index | All>

StopIdentifyLUN

Stops lighting the LED of a disk drive associated with an iSCSI Target LUN.

`StopIdentifyLUN` [*target name*] [*lun*]

Temperature

Displays the current internal temperature of the Spectra Swarm bridge in degrees Celsius.

`get Temperature`

Time

Sets/displays the current time in a 24-hour format. If SNTP is enabled and at least one ethernet port is connected to a reachable SNTP time server, the time is retrieved from one of the configured SNTP time servers, and manual attempts to change the time will have no effect. If SNTP is disabled or SNTP server synchronization is not possible, the system time starts from Spectra Swarm bridge last known system time stamp, and the time may be changed manually.

`set Time` [*HH:MM:SS*]

`get Time`

TimeZone

Sets/displays the time zone. Setting may be EST, CST, MST, PST, or a numerical offset from GMT in the format +/- HH. When SNTP is enabled, Spectra Swarm bridge applies the time zone setting to the time retrieved from a specified SNTP time server to determine the local time.

Default: EST (-05)

`set TimeZone` [[EST | CST | MST | PST] | [[+|-][*HH*]]]

`get TimeZone`

Uptime

Returns the time [days hrs:min:sec] since the last reboot.

`Uptime`

Username

Username specifies the username used for all sessions: SSH, SFTP and the graphic user interface. Username must be all lowercase, 1 to 32 characters long, start with an alphabetical character, and may only contain the following: {a-z,0-9,-,_.}.

Default: admin

`set Username` [*username*]

`get Username`

VerboseMode

Controls the level of feedback returned by the command line interface. Disabling this option removes CLI Help command descriptions and removes CLI command display headers and parameter names from get and immediate commands.

Default: enabled

`set VerboseMode` [enabled | disabled]

`get VerboseMode`

REGULATORY INFORMATION

FCC Notices (US Only)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment under FCC rules.

Compliance with ICES-003

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Compliance with EU Regulations

Marking by the "CE" symbol indicates compliance of this ATTO device to the EMC Directive and the Low Voltage Directive of the European Union.

The ATTO XstreamCORE ET 8200T complies with Directive 2011/65/EC on the Restriction of the Use of Hazardous Substances in Electrical and Electronic Equipment RoHS2 (recast) and take the following exemptions:

6(c)- Copper allot containing up to 4% lead by weight.

7(a) -Lead in high melting temperature type solders (i.e. lead based alloys containing 85% by weight or more lead).

7(c)-l -Electrical and electronic components containing lead in a glass or ceramic other than dielectric ceramic in capacitors, e.g. piezoelectronic devices, or in glass or ceramic matrix compound.

UL60950-1/CSA C22.2 No. 60950-1

UL62368-1/CSA C22.2No.62368-1

The product has been certified and bears the Mark, as applicable, of the EMC and Product Safety authorities as indicated below:

Safety: TUV 72141224/72171382, EN 60950-1/62368-1, CE, CSA 60950-1, UL 60950-1/62368-1 CB IEC60950-1/IEC62368-1 (all national deviations)

Emissions/Immunity: FCC Part 15 Class A, ICES-003, CE - EN55032, EN55024, IEC61000-3-2, IEC61000-3-3