ATTO XstreamCORE® 8100T

2-Port 10Gb Ethernet to 1-Port 12Gb SAS intelligent bridge

Installation and Operations Manual

ATTO
The Power Behind the Storage

155 CrossPoint Parkway
Amherst, NY 14068

P. +1.716.691.1999
atto.com

09/2024 **PRMA-0507-000**

Table of Contents

1 ATTO XstreamCORE 8100T Overview

The ATTO XstreamCORE 8100T is an accelerated intelligent bridging device that extends tape storage connectivity to up to 4 SAS-LTO Tape drives over a 10Gb Ethernet network.

ATTO XstreamCORE® intelligent bridges add shared storage benefits to SAS storage but at direct attached speeds. The 8100T provides secured and remote access through accelerated Ethernet interface to SAS tape storage providing architectural simplicity, operational flexibility, and overall system efficiency.

Use the 8100T to aggregate and share tape storage with the knowledge that it has undergone qualifications with industry leading storage and network infrastructure products. Easily integrate the 8100T into IT and Media & Entertainment workflows to provide lower operational costs through use of proprietary and patented technologies like SpeedWrite™, [1]SpeedRead™, and Advanced Data Streaming™ and built-in tools that enable configuration, device management, and troubleshooting.

Features and Benefits

The ATTO XstreamCORE 8100T is a 10-Gigabit Ethernet to 12-Gigabit SAS storage controller configured with two independent 10Gb Ethernet ports and a single 12Gb x4 mini-SAS connector.

Designed to integrate industry-leading performance and SAN capabilities into the future generation of storage solutions, the XstreamCORE 8100T uses ADSA™ (ATTO Distributed Software Architecture), a cooperative multi-tasking operating system with light-weight transactions and high-performance memory management. ADSA is optimized for storage application performance and maximum efficiency in enterprise level and application workflows looking to incorporate SAS Tape drives in their Ethernet network.

- Supports accelerated iSCSI over TCP/IP
- Integrated multi-core ARM 64bit Processor
- Two independent 10Gb Ethernet SFP+ ports
- Supports IPv4 and IPv6 connections
- Support for connection to up to 4 iSCSI initiators with two sessions each (8 total sessions supported)
- Single 12Gb SAS x4 mini-SAS HD connector
- SAS auto-negotiates to 6Gb or 12Gb
- Supports up to 4 SAS Tape Drives (LTO 5, 6, 7, 8, 9)
- Automatic SAS LUN Mapping & Management
- Support for LTFS (Linear Tape File System)
- Support for SAS TLR (Transport Layer Retries)
- System monitoring hardware
- On-chip thermal monitoring
- Dedicated 1GbE RJ45 Management port
- ACL (Access Control List) Support
- CLI over SSH
- Firmware Update over SFTP
- SpeedWrite™ and SpeedRead™ for accelerated write and read performance over iSCSI

Note ***iSCSI is only accessible on the 10Gb data ports - the 1Gb port for management only.***

Note ***[1] Patent pending***

ATTO XstreamCORE 8100T

The ATTO XstreamCORE 8100T is a simple and easy-to-use intelligent bridge that adds 10-Gigabit Ethernet connectivity to 6 and 12-Gigabit SAS Tape drives.

The XstreamCORE 8100T can be used as a desktop device or mounted in a specially designed 1U rack-mount tray (from ATTO) for easy integration into 19" racks. Each rack-mount hardware tray can support up to 4 individual units.

Dimensions

Width: 4.0 inches (103.5 mm)

Length: 9.4 inches (240 mm)

Height: 1.2 inches (30.5 mm)

Weight: approx. 2.05 pounds (0.93 kg) with SFPs

Cooling and airflow

Operating temperature: 5-40 °C external at 10,000 feet

Humidity: 10-90% non-condensing

Air enters from the front and is exhausted out the connector side. Ambient air near the inlets should not exceed 40°C. The unit automatically stops operation if the temperature goes beyond this threshold.

CAUTION ***Do not block the enclosure's vents.***

Note ***In the event of a temperature surge or overheating, the ALERT LED will turn ON, stop all data transfers and cut off power down the main rails. A full power cycle will be needed to turn the device back on.***

Power

The 8100T features an external 12V DC power jack (male) to be used with the power supply adapter that is provided with the unit.

Input: 100-240VAC ~50-60Hz, 1.4A max

Output: 12.0VDC, 5.0A. 60W

Note ***Product warranties will be voided if an alternate power supply is used.***

The power requirements of the ATTO XstreamCORE 8100T plus the power draw of other equipment in the rack must not overload the supply circuit and/or wiring of this rack.

Ethernet data ports

The dual independent 10Gb/s Ethernet ports connect the XstreamCORE 8100T to Ethernet hosts using optical SFP+ connectors or Copper SFPs (SFP+ to RJ-45 adapter) using RJ-45 cabling. Make sure all cables are anchored securely at both ends with the proper connectors.

Note ***Ethernet data ports also support direct-attach SFP+ Cabling for uplink connections to the switching fabric. This maybe suitable for short-distance connections.***

SAS ports

The 12Gb/s SAS connector (4 PHYs total) connect tape storage devices using mini-SAS HD connectors.

Note ***8100T unit supports up to 4 SAS LTO devices. Use of SAS expanders to interface with more than 4 devices is not supported. Please refer to the ATTO XstreamCORE 8200T product if connectivity to more than four tape drives is needed.***

1GbE Management port

Management is provided using the 1Gb Ethernet port accessible from the RJ-45 connector labeled with the 'wrench' icon.

LED indicators

LED indicators can be viewed from the connector (rear) side of the XstreamCORE 8100T.

LEDs include:

Power Supply: One green LED, located below the DC power jack to indicate when power is applied to the unit.

Ready/Alert: Bi-color green/yellow shared LED, located between the PWR LED and Ethernet DP1 LED. Green indicates when the unit has completed initialization and is ready for use. Yellow indicates an alert or fault condition in the unit.

DP 1 LED – Data Port 1 LED will be lit solid green for a valid link and will blink for activity.

DP 2 LED – Data Port 2 LED will be lit solid green for a valid link and will blink for activity.

Ethernet Data Port LEDs are located below the SFP+ connectors.

SAS Activity LED: A SAS activity LED is located below the mini-SAS HD connector. The LED will blink for SAS activity on any PHY in the connector

Ethernet management port: Two integrated LEDs on the RJ-45 connector indicate link and Ethernet activity. The LED on the LEFT (facing the connector, LED1) illuminates solid green when linked at 1Gb/s, off when linked at 100Mb/s or not linked. The LED on the RIGHT (LED0) blinks green to indicate activity.

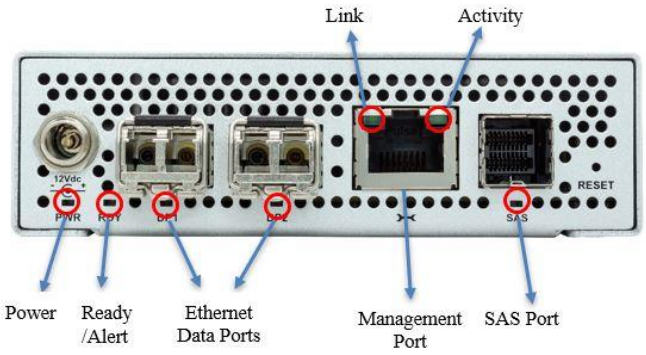


Exhibit 1 - XstreamCORE 8100T Connectors, LEDs and power receptacle on the connector (rear) side.

2 Install the XstreamCORE

Unpack the box & verify contents

- (2) 10 GbE Optical SFPs
- Power adapter and AC power cord
- The XstreamCORE 8100T
- Record the serial number, default username, and default password located on the bottom of the unit:
  S/N: _____
  Default Username: _____
  Default Password: _____
  The username and password are needed to access SSH and SFTP services via the Ethernet ports.

Install the XstreamCORE

1. Place the XstreamCORE 8100T on a stable flat surface.
2. If installing into a rack tray, install the XstreamCORE assembly horizontally within the rack so it does not reduce the air flow within the rack.
3. Connect the host computer by connecting the cable to Ethernet data port 1 or 2.
4. Connect SAS target devices with the appropriate mini-SAS HD cable.
5. Power up the target devices.
6. Connect the Ethernet data ports to your network.
7. Connect the power adapter to the XstreamCORE and to the proper AC source outlet.
8. Wait for the **XstreamCORE Ready LED** to light, indicating that the XstreamCORE has completed its power-on self-test sequence

Note ***The XstreamCORE 8100T will power on automatically and begin booting when connected to power.***

CAUTION ***The power source must be connected to a protective earth ground and comply with local electrical codes. Improper grounding may result in an electrical shock or damage to the unit. Failure to do so may cause injury or damage the unit. Also, be aware that this unit is powered on once a power source is connected. If you are using a rack, be careful not to exceed the power capabilities of the rack.***

Making an SSH connection

1. Start an SSH client.

Note ***There is more than one way to connect to the XstreamCORE using an SSH client. Your SSH client may operate differently than in the following instructions.***

2. In your SSH client, connect to the XstreamCORE. As an example, using OpenSSH, the connection would be made with the following command where username is the username set in Modify passwords, and x.x.x.x is the IP address of the XstreamCORE.
   ssh username@x.x.x.x

3. Enter your password.

To quit an SSH session, type exitConnect the Ethernet data ports to your network.

Connect to SSH using the default IP addresses

By default, the XstreamCORE 8100T is configured to use a static IP address. These addresses can be connected to using SSH and the default credentials. It is recommended to use the management port for this (MP1).

- **1GbE Management port:** 192.168.0.1/24
- **10GbE Data port 1:** 10.0.0.1/8
- **10GbE Data port 2:** 172.16.0.1/12

Begin initial configuration

1. The SSH login prompt will ask the user for the username the password.
2. Type in the user name and password.
3. The ATTO CLI splash screen appears. Continue to Map Device.

Note ***The default user name and password values can be found on the bottom of the unit. The user name and the password are case sensitive.***

Security Keypairs

Keys and PEM file

The XstreamCORE controller uses a keypair that is provided to devices on a network to authenticate. The SSH and SFTP servers in the controller expects to have access to a PEM (Privacy Enhanced Mail) file containing the keypair (public and its associated private key) necessary to provide access. The keypair PEM file is generated by the controller.

Note ***The private key is only seen by the controller. Only the signature of the private key is displayed to the user and external entities.***

Keypair regeneration

The PEM file containing the keypair is regenerated by the controller if prompted by the user. Since it is the controller that generates the keypair a client services (SSH and SFTP) may report the signature as changed if they use a “known

hosts" file and may deny access to the controller unless the file is updated with the new key.

Configure the XstreamCORE

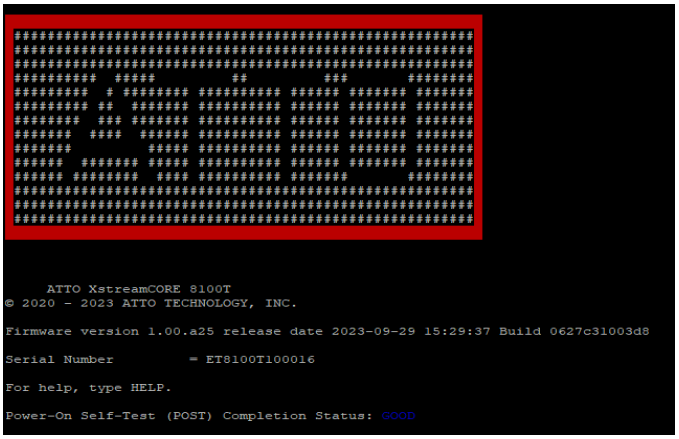
Use the Command Line Interface (CLI) to configure or view current settings for the XstreamCORE. This is accessible through an SSH terminal client. Default values are appropriate for most configurations, but may be modified.

Help is available from within the CLI by using help followed by the command name. For more information on any of these parameters, refer to the specific CLI command in Command explanations.

Preliminary steps

1. Connect to the Management Port's IP address of your XstreamCORE from an SSH client and type in your user name and password when prompted.
2. The CLI splash appears. Check default settings in **Info** to ensure they are appropriate for your configuration. Use the commands pointed to by the **Help** command to verify and change settings.

Exhibit 2 XstreamCORE 8100T SSH Splash Screen



Port configurations

1. Follow the Preliminary steps.
2. If using IPv4 DHCP to assign Ethernet port addresses then use **set IPDHCP** to enable DHCP for the selected Ethernet port(s).

Note ***If using DHCP on the management port, it is suggested the DHCP server reserve an IP address for the port's MAC address to avoid having the device's IP migrating, possibly losing CLI access.***

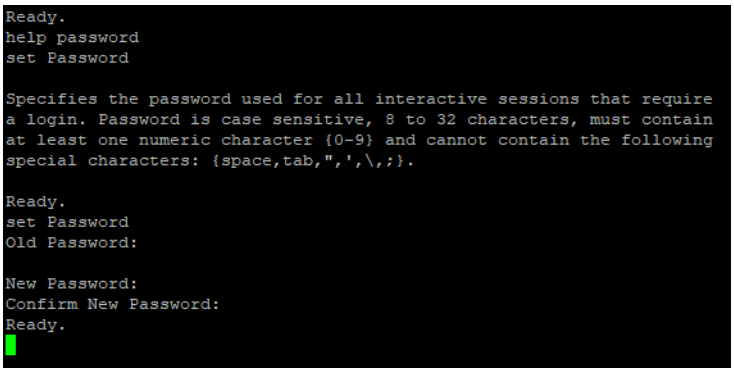
3. If using IPv6 DHCP to assign Ethernet port addresses use **set IPV6DHCP** to enable DHCP for the selected Ethernet port(s).
4. If using static IPv4 addresses then use **set IPAddress, set IPSubnetMask**, **set IPGateway** on the selected Ethernet port.
5. If using static IPv6 addresses then use **set IPV6Address, set IPV6Prefix**, **set IPV6Gateway** on the selected Ethernet port.

Modify passwords

1. Follow the Preliminary steps.
2. Use the **Password** command to begin an interactive command session
3. Enter appropriate information when prompted to enter the current password, then the new password.

If the password has been lost, the XstreamCORE 8100T can be defaulted using the reset button. Holding the reset button for 5 seconds will reset all configurations to default, including the password.

Exhibit 3 - Setting the Password



3 Map Devices

The ATTO XstreamCORE 8100T allows SAS tape devices to participate in an iSCSI fabric. iSCSI and SAS use different models to address devices. The XstreamCORE translates between these addressing models.

XstreamCORE Mapping Modes

The XstreamCORE presents a number of iSCSI target nodes on the network, each identified by an iSCSI IQN. The IQN consists of two parts: a fixed portion based on the product name and serial number, and a target name. The XstreamCORE features two mapping modes: automatic and manual. Automatic mapping creates iSCSI targets based on SAS topology without the need for user configuration. Manual mapping mode allows the user to create up to four iSCSI targets and select which tape devices to associate with each iSCSI target. A tape device may only be associated with one iSCSI target node at a time. In manual mapping the user has the ability to group multiple devices to a single iSCSI target.

Each target node can be accessed by one or more network portals. Each network portal is identified by its IP address and listening TCP port. All target names and available target portals are transmitted to a host using the standard iSCSI **sendtargets** discovery mechanism.

Tape devices connected to the XstreamCORE are viewed as Ethernet LUNs to the host computer. Each device has a unique LUN within an iSCSI target node.

CLI command **ShowDevices** will display device information for all supported tape devices currently connected.

Automatic mapping mode

The XstreamCORE 8100T is set to automatic mapping mode by default. In this mode, the XstreamCORE will create maps for each SAS PHY that has tape devices attached. Tapes and changers are grouped into targets based on what SAS PHY they are connected to. When devices are disconnected, the mappings are automatically deleted. Moving a device from one SAS PHY to another moves the device from one iSCSI target to another. Automatically created targets are accessible through both data ports by default but may be isolated to a specific data port using CLI command **iSCSISetPorts**. The **iSCSIShowMaps** command reports the fully qualified target names and LUNs associated with each target.

Exhibit 4 - Automatic iSCSI Mapping Mode

```
Ready.
get iSCSIMappingMode
Current Mapping Mode  = automatic
```

```
Ready.
showdevices
Device ID   Vendor Model SN              Type     Location  LUN iSCSI Target
     0      IBM ULT3580-TD9 1175BDF05B   drive           6    0 iqn.2016-10.com.atto:xcoreet.sn-xc8100tiolabl.6
     1      IBM 3573-TL 55L3A7801CNLLL01 changer         6    1 iqn.2016-10.com.atto:xcoreet.sn-xc8100tiolabl.6
     2      IBM ULT3580-TD9 1013000354   drive           4    0 iqn.2016-10.com.atto:xcoreet.sn-xc8100tiolabl.4
     3      IBM ULT3580-TD9 1013000357   drive           5    0 iqn.2016-10.com.atto:xcoreet.sn-xc8100tiolabl.5
     4      IBM ULT3580-TD9 1013000322   drive           7    0 iqn.2016-10.com.atto:xcoreet.sn-xc8100tiolabl.7
```

```
Ready.
iscsishowmaps
Target ID    Ports     Target name
     4       DP1 DP2   iqn.2016-10.com.atto:xcoreet.sn-xc8100tiolabl.4
                        LUN:  0 Type: drive      IBM ULT3580-TD9 1013000354

     5       DP1 DP2   iqn.2016-10.com.atto:xcoreet.sn-xc8100tiolabl.5
                        LUN:  0 Type: drive      IBM ULT3580-TD9 1013000357

     6       DP1 DP2   iqn.2016-10.com.atto:xcoreet.sn-xc8100tiolabl.6
                        LUN:  0 Type: drive      IBM ULT3580-TD9 1175BDF05B
                        LUN:  1 Type: changer    IBM 3573-TL 55L3A7801CNLLL01

     7       DP1 DP2   iqn.2016-10.com.atto:xcoreet.sn-xc8100tiolabl.7
                        LUN:  0 Type: drive      IBM ULT3580-TD9 1013000322
```

Manual mapping mode

To change mapping mode to manual mode, perform the following:

1. Run the **set iSCSIMappingMode Manual** command while there are no initiators logged in. This will delete all target nodes on the device. A reboot is required.
2. Target nodes will need to be created using the **iSCSITargetCreate** command, specifying the name of the target and which data ports the target is accessible from. Up to four iSCSI targets may be created.
3. New LUNs can be added to the target by using the **iSCSIMap** command. This command uses the target name (or the *target ID* as displayed in the **iSCSIShowMaps)** along with the *device ID* (as seen in **ShowDevices**) and the desired LUN. The LUN typically starts at zero and increments for each iSCSI target.

Note ***Some host operating systems may require a device at LUN 0 on each iSCSI target.***

Exhibit 5 - Configure Manual iSCSI Mapping Mode

```
Ready.
set iSCSIMappingMode manual

Reboot required for mapping change to take effect

Reboot now? (y/n) ? y
```

```
Ready.
get iSCSIMappingMode
Current Mapping Mode  = manual
```

```
Ready.
iSCSITargetCreate etgl all
```

```
Ready.
showdevices
Device ID   Vendor Model SN            Type    Location  LUN iSCSI Target
    0       HP MSL6480 DEC72107L3_LL03 changer        4
    1       HPE Ultrium 8036B88C07     drive          4    0 iqn.2016-10.com.atto:xcoreet.sn-aet8100t00017.etgl
    2       HPE Ultrium 8036B88BFD     drive          7    1 iqn.2016-10.com.atto:xcoreet.sn-aet8100t00017.etgl
```

```
Ready.
iSCSIMap etgl 1 0
```

```
Ready.
iSCSIMap etgl 2 1
```

```
Ready.
iSCSIShowMaps
Target ID    Ports     Target name
    0        DP1 DP2   iqn.2016-10.com.atto:xcoreet.sn-aet8100t00017.etgl
                        LUN:  0 Type: drive      HPE Ultrium 8036B88C07
                        LUN:  1 Type: drive      HPE Ultrium 8036B88BFD
```

4 XstreamCORE iSCSI Best Practices

Network Architecture

Note ***It is recommended that the XstreamCORE 8100T is used on an isolated lossless network when using iSCSI***

- When using both Ethernet data ports on the XstreamCORE 8100T each port must be assigned to an independent subnet in order to achieve full bandwidth. The XstreamCORE's Ethernet management port must also be assigned to an independent subnet. All Ethernet port subnets must not overlap.
- Spanning-tree protocol (STP) should be disabled on the switch ports being used for iSCSI traffic. This would mean ports connected to the 8100T and all iSCSI initiators.

Note ***If you do need STP enabled it is recommended that you enable the STP FastPort feature on your switch***

- Global flow control should be enabled on the switch ports and iSCSI initiators.

Note ***It is recommended that global flow control is employed for iSCSI traffic to limit dropped packets if possible.***

- It is recommended that unicast storm control is disabled on your switch.
- It is recommended that you USE broadcast and multicast storm control on your switch.
- Jumbo frames (large MTU's) should be enabled on all switch ports, the iSCSI initiators, and the 8100T data ports for optimal performance.
- If Virtual LAN (VLAN) is required, ATTO recommends configuring VLAN on your switch. A switch created VLAN is a broadcast domain, which helps separate traffic on switch ports.

iSCSI Targets and Tape Devices

- When multiple tape devices are expected to be used at the same time it is recommended to map a single tape device per iSCSI target. Automatic mapping mode does this.
- Evenly split access to multiple tape devices across both data ports. For example, if accessing two tapes across two iSCSI targets, log into one iSCSI target using the portal on data port 1 and the other using the portal through data port 2.

Jumbo Frames

- Care should be taken to ensure end-to-end path maximum transmission unit (MTU) support. Failure to provide a consistent configuration may result in packet fragmentation. All equipment on the same layer 2 network (the same LAN or VLAN) 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 can cause performance issues.

Note ***Some vendors include the headers in the size settings while others do not. This may require that equipment from different vendors be configured to different values to make the settings match.***

Network Configuration

- When configuring the IP address for Data Ports (DP1 & DP2), they should be configured on two different Ethernet LAN segments. The default port for iSCSI is 3260. DHCP should lease two separate subnets. For example:
- DP1 at 192.168.1.0/24 and DP2 at 192.168.2.0/24.

IPv6 Connections

IPv6 iSCSI connections may only be made to statically assigned or DHCP dynamically assigned IPv6 addresses on the data ports. For this reason, data port link local addresses (addresses beginning with fe80) are not shown by either the **Info** or **get IPV6Address** CLI commands.

Discovery Target Visibility

Access Control Lists (ACLs) must be enabled on a target basis to prevent initiators from discovering a particular XstreamCORE target. Once enabled, only initiators configured to be on the whitelist will be able to discover that target. If Access Control is disabled for a target, any initiator with access to the same network the XstreamCORE is located on will be able to discover and connect to that target.

Access Control Lists

Use the following steps to create an Access Control entry for any target node:

1. Create a CLI session.
2. Use **Set AccessControl [Target] enabled** to configure that target node to use ACLs.

3. For each initiator allowed to access the node, use **Set AccessEntry [Target] [Initiator IQN]** to write the initiator into the allowed initiator list.

Exhibit 6 - Access Control Lists

```
iSCSIShowMaps
Target ID    Ports     Target name
     0       DP1 DP2   iqn.2016-10.com.atto:xcoreet.sn-et8100t100016.etg1
```

```
Ready.
set AccessControl iqn.2016-10.com.atto:xcoreet.sn-et8100t100016.etg1 enabled
```

```
Ready.
set AccessEntry iqn.2016-10.com.atto:xcoreet.sn-et8100t100016.etg1 iqn.1991-05.com.microsoft:eng383
```

CHAP Configuration

To add an additional layer of security against unauthorized access to iSCSI LUNs, CHAP authentication can be configured after an Access Control entry has been created for that initiator-target pair. Access Control must be configured for all nodes except the discovery node, the discovery node cannot have Access Control Lists (ACLs) but can be configured for CHAP.

Discovery CHAP

1. Create a CLI session.
2. Use **iSCSICHAPMode** to configure the CHAP mode of the target desired, where one-way authenticates an initiator challenge from the host to the XstreamCORE and two-way additionally sends a challenge back from the XstreamCORE to the host.
3. (Two-way CHAP only) Configure the iSCSI CHAP Out Account Name and CHAP Out Secret using the **set iSCSICHAP Discovery Out** command.
4. Configure the iSCSI CHAP In Account Name and CHAP In Secret using the **set iSCSICHAP Discovery In** command.
5. See the help text for iSCSICHAP for examples of setting up discovery CHAP.

Target CHAP

1. Create a CLI session.
2. Set the target's ACL using the steps in the Access Control Lists section.
3. Use **iSCSICHAPMode** to configure the CHAP mode of the target, where one-way authenticates an initiator challenge from the host to the XstreamCORE and two-way additionally sends a challenge back from the XstreamCORE to the host.
4. (Two-way CHAP only) Configure the iSCSI CHAP Out Account Name and CHAP Out Secret using the **set iSCSICHAP [target] Out** command.
5. Configure the iSCSI CHAP In Account Name and CHAP In Secret using the **set iSCSICHAP [target] In** command. See the help text for iSCSICHAP for examples of setting up target CHAP.

5 Initiator Configuration

It is recommended that the user establish multiple sessions to the XstreamCORE 8100T from each host. Also, the user should set up one session per "Data Port" to each of the ports of the network cards. This ensures that if a link goes down a session can be restarted.

Linux

Prerequisites

- Server with a 10GbE adapter running a supported Linux kernel.
- XstreamCORE data ports configured and connected to the same network as the 10GbE adapter.

Initiator Setup Instructions

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

Install the iSCSI Initiator Utilities

For systems using apt package management, enter the following command: **apt install open-iscsi**

For systems using yum package management, enter the following command: **yum install iscsi-initiator-utils**

Note ***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.

Configure the Data Ports

1. For iSCSI applications, the in-box driver should be used to connect the 8100 to the host.
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 XstreamCORE without the use of a switch and both data ports are used, the XstreamCORE data ports must not be on the same subnet.***

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

Note ***ipaddress is the address of the XstreamCORE 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

LTFS Setup for Tape Devices

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

Open /etc/iscsi/iscsid.conf in a text editor and add the following registry settings:

node.session.iscsi.InitialR2T = No
node.session.iscsi.ImmediateData = Yes
node.session.iscsi.FirstBurstLength = 1048576
node.session.iscsi.MaxBurstLength = 16776192
node.conn[0].iscsi.MaxRecvDataSegmentLength = 4194304

and restart the server.

Note ***When using ATTO Fastframe NICs and ATTO ThunderLink with XstreamCORE 8100T, select the 8100T Tuning Profile in ATTO 360.***

Discover XstreamCORE Targets

If one-way or two-way CHAP authentication has been configured on the XstreamCORE 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 ***username and password must match the CHAP In Account Name and CHAP In Secret configured on the XstreamCORE for discovery. Both username and password are case-sensitive.***

If two-way CHAP authentication has been configured on the XstreamCORE 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

Note ***username_in and password_in must match the CHAP Out Account Name and CHAP Out Secret configured on the XstreamCORE for discovery. Both username_in and password_in are case-sensitive.***

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

Discover XstreamCORE targets by entering the following command:

iscsiadm -m discovery -t st -p ipaddress

Note ***ipaddress is the address of the XstreamCORE data port to perform discovery through.***

The command should return a list of all XstreamCORE targets available to this initiator.

Note ***If an XstreamCORE 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 XstreamCORE.

Configure Target CHAP

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

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 XstreamCORE for this target. password must match the CHAP In Secret configured on the XstreamCORE 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 XstreamCORE for this target. Both username_in and password_in are case-sensitive.***

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

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

3. 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 XstreamCORE data port used in the discovery command above.***

You can verify the initiator is connected using the command line interface's iSCSILogins command (see Appendix B).

Sample Output:

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 XstreamCORE for this target.

LTFS Partition (Tape devices only)

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 in 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

Note ***target must match the full target name returned from the discovery command above. ipaddress is the address of the XstreamCORE data port used in the discovery command above.***

Note ***You can connect/disconnect to/from all discovered targets by omitting the -T target parameter from the log in/out commands***

Windows

Prerequisites

- Server with 10GbE adapter using the latest drivers.
- XstreamCORE data ports configured and connected to the same network as the 10GbE adapter.

Setup Instructions

Configure Data Ports

1. Ports may be auto-configured if connected to a network with DHCP. Otherwise, they will need to be assigned an IP address, which can be done using the netsh command in a command prompt or PowerShell.

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

2. Test the network connection using the 'ping' command. Note the IP address of the XstreamCORE data port and then on the initiator, enter the following command:

ping ipaddress

Note ***ipaddress is the address of the XstreamCORE data port.***

Sample output:

Pinging 172.16.1.20 with 32 bytes of data:

Reply from 172.16.1.20: bytes=32 time<1ms TTL=64

Reply from 172.16.1.20: bytes=32 time<1ms TTL=64

Reply from 172.16.1.20: bytes=32 time<1ms TTL=64

Reply from 172.16.1.20: bytes=32 time<1ms TTL=64

Ping statistics for 172.16.1.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

LTFS Setup for Tape Devices

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

For iSCSI to work with LTFS, the iSCSI maximum transfer length must be set to at least 1MB and the maximum burst length set to 1MB. This will require modifying the registry. In ***[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\instance(contains Microsoft iSCSI Initiator)\Parameters]***, set

"MaxTransferLength"=dword:00100000
"MaxBurstLength"=dword:00100000
"FirstBurstLength"=dword:000100000
"MaxRecvDataSegmentLength"=dword:00400000
"LinkDownTime=dword:00000000
"MaxRequestHoldTime"=dword:00000000

and restart the server.

Note ***When using ATTO Fastframe NICs and ATTO ThunderLink with XstreamCORE 8100T, select the 8100T Tuning Profile in ATTO 360.***

Discover XstreamCORE Targets

Using iSCSI Software Initiator GUI

To open the iSCSI Software Initiator GUI, click on the **start** button to open the start menu/screen, type in **iSCSI Initiator** and press **enter**. If prompted to start the iSCSI service, click **Yes**, and type in **iSCSI Initiator** in the start menu again. You should now see a window titled iSCSI Initiator Properties.

Create Discovery Portal

1. (Two-way discovery CHAP only) Click on the **Configuration** tab along the top of the iSCSI Initiator Properties window. Click on the **CHAP...** button on the right hand side. Enter the Initiator CHAP secret.

Note ***The Initiator CHAP secret must match the CHAP Out Secret configured for discovery on the XstreamCORE. The secret is case-sensitive.***

2. Click on the **Discovery** tab near the top of the iSCSI Initiator Properties window.
3. Click on the **Discovery Portal...** button.
4. In the **Discover Target Portal** window, under **IP address**, enter the IP address of the XstreamCORE data port to connect through.
5. (Discovery CHAP disabled only) Click **OK** in the **Discovery Target Portal** window.

Discovery CHAP

This section only applies when using one-way or two-way CHAP for discovery sessions.

1. Click on the **Advanced...** button in the lower left corner of the **Discover Target Portal** window.
2. Check the box next to **Enable CHAP log on**.
3. Inside **CHAP Log on** information fill in the Name and Target Secret used for discovery.

Note ***The Name and Target Secret must match the CHAP In Account Name and CHAP In Secret configured on the XstreamCORE for discovery. Both Name and Target Secret are case-sensitive.***

4. (Two-way discovery CHAP only) Check the box next to **Perform mutual authentication**.
5. Click **OK** in the **Advanced Settings** window.
6. Click OK in the Discovery Target Portal window.

The IP address should now be displayed in the list under **Target portals**. If "Connection failure" is reported, make sure that the firewall is configured to pass iSCSI traffic. If using CHAP, ensure the name and secrets are configured correctly on both the iSCSI Software Initiator GUI and XstreamCORE for discovery.

Using iSCSI PowerShell Module

If not already done, configure the iSCSI service to start automatically. To do this open PowerShell and enter the following two commands:

Set-Service -Name msiscsi -StartupType Automatic

Start-Service msiscsi

Note ***If an "Access is denied." error is returned, run the PowerShell as an Administrator, and try again.***

Create an iSCSI Target Portal

Note ***If "Authentication Failure" is returned check to make sure the credentials and authentication type matches between the XstreamCORE and the initiator.***

No CHAP

1. Enter the following command:

New-IscsiTargetPortal -TargetPortalAddress "ipaddress" -AuthenticationType None

Note ***ipaddress is the address of the data port on the XstreamCORE through which to perform discovery.***

One-way CHAP

1. Enter the following command:

New-IscsiTargetPortal -TargetPortalAddress "ipaddress" -AuthenticationType ONEWAYCHAP -ChapUsername Username -ChapSecret Secret

Note ***ipaddress is the address of the data port on the XstreamCORE through which to perform discovery. Username must match the CHAP In Account Name configured on the XstreamCORE for discovery. Secret must match the CHAP In Secret configured on the XstreamCORE for discovery. Both username and secret are case-sensitive.***

Two-way CHAP

1. (If not already set) Enter the following command:

Set-IscsiChapSecret -ChapSecret Secret

Note ***Secret must match the CHAP Out secret configured on the XstreamCORE for discovery. The secret is case-sensitive.***

2. Enter the following command:

New-IscsiTargetPortal -TargetPortalAddress "ipaddress" -AuthenticationType MUTUALCHAP -ChapUsername Username -ChapSecret Secret

Note ***ipaddress is the address of the data port on the XstreamCORE through which to perform discovery. Username must match the CHAP In Account Name configured on the XstreamCORE for discovery. Secret must match the CHAP In Secret configured on the XstreamCORE for discovery. Both the username and secret are case-sensitive.***

Once the Target Portal is created, refresh the list of available targets by entering the following command:

Update-IscsiTarget

List all available targets by entering the following command:

Get-IscsiTarget

Connect to the Target

Using iSCSI Software Initiator GUI

1. (Two-way CHAP only) If not already done, click on the **Configuration** tab along the top of the **iSCSI Initiator Properties** window. Click on the **CHAP...** button on the right-hand side, fill in the Initiator CHAP secret, and click **OK**.

Note ***The Initiator CHAP secret must match the CHAP Out secret configured on XstreamCORE for the target. The secret is case-sensitive.***

2. In the **iSCSI Initiator Properties** window, click on the **Targets** tab.
3. Under **Discovered targets**, click on the **Refresh** button.
4. Select the name of the target, and click on the **Connect** button.
5. (CHAP disabled only) Click **OK** in the **Connect To Target** window.

CHAP

This section only applies when using one-way or two-way CHAP to connect to this target.

1. Click on the **Advanced...** button in the **Connect To Target** window.
2. Check the box next to **Enable CHAP log on**.
3. In the CHAP Log on information fill in the **Name** and **Target Secret** used for this target.

Note ***The Name and Target Secret must match the CHAP In Account Name and CHAP In Secret configured on the XstreamCORE for this target. The Name and Target Secret are both case-sensitive.***

4. (Two-way CHAP only) Check the box next to Perform mutual authentication.
5. Click **OK** in the **Advanced Settings** window.
6. Click **OK** in the **Connect To Target** window.

In the **Discovered targets list** the Status of the target should now show as Connected. If an "Authentication Failure" error message appears check that the name and secret(s) are configured correctly on both the iSCSI Software Initiator GUI and XstreamCORE for this particular target.

Using iSCSI PowerShell Module

No CHAP

Enter the following command:

Connect-IscsiTarget -NodeAddress node -AuthenticationType None

Note ***node is the full target name of the target you wish to connect to. It is listed under the NodeAddress column returned by the Get-IscsiTarget command.***

One-Way CHAP

1. Enter the following command:

Connect-IscsiTarget -NodeAddress node -AuthenticationType ONEWAYCHAP -ChapUsername Username -ChapSecret Secret

Note ***node is the full target name of the target you wish to connect to. It is listed under the NodeAddress column returned by the Get-IscsiTarget command. Username must match the CHAP In Account Name configured on the XstreamCORE for this target. Secret must match the CHAP In Secret configured on the XstreamCORE for this target. Both the username and secret are case-sensitive.***

Two-Way CHAP

1. (If not already set) Enter the following command:

Set-IscsiChapSecret -ChapSecret Secret

Note ***Secret must match the CHAP Out secret configured on the XstreamCORE for this target. The secret is case-sensitive.***

2. Enter the following command:

Connect-IscsiTarget -NodeAddress node -AuthenticationType MUTUALCHAP -ChapUsername Username -ChapSecret Secret

Note ***node is the full target name of the target you wish to connect to. It is listed under the NodeAddress column returned by the Get-IscsiTarget command. Username must match the CHAP In Account Name configured on the XstreamCORE for this target. Secret must match the CHAP In Secret configured on the XstreamCORE for this target. Both the username and secret are case-sensitive.***

Once connected the attached drives should now appear in Disk Management.

Use Action > Rescan Disks in Disk Management to detect any changes to available drives.

Disconnect from a Target

Using iSCSI Software Initiator GUI

1. Click on the **Targets** tab along the top of the **iSCSI Initiator Properties** window.
2. Under **Discovered targets**, select the name of the target, and click on the **Disconnect** button.

Using iSCSI PowerShell Module

Enter the following command:

Disconnect-IscsiTarget -NodeAddress node

Note ***node is the full target name of the target you wish to connect to. It is listed under the NodeAddress column returned by the Get-IscsiTarget command. If prompted for confirmation, enter 'A' for Yes to All***

macOS

Prerequisites

1. Server with 10GbE adapter using the latest drivers.
2. XstreamCORE data ports configured and connected to the same network as the 10GbE adapter.
3. ATTO Xtend SAN iSCSI Initiator for macOS.

Note ***macOS does not include a built in iSCSI Initiator. It is recommended to use ATTO Xtend SAN which can be purchased from the ATTO WebStore.***

To install the ATTO Xtend SAN Initiator program or when upgrading from earlier versions, you need the authorization file sent to you in an Email from ATTO Technology.

Install Xtend SAN software

Follow the instructions in the Xtend SAN manual to install the iSCSI initiator.

Note ***You must have administrator access to install the program. Remote installations will not work. You must install directly on the MAC.***

CAUTION ***Disable macOS Power Management when running Xtend SAN to avoid losing connections.***

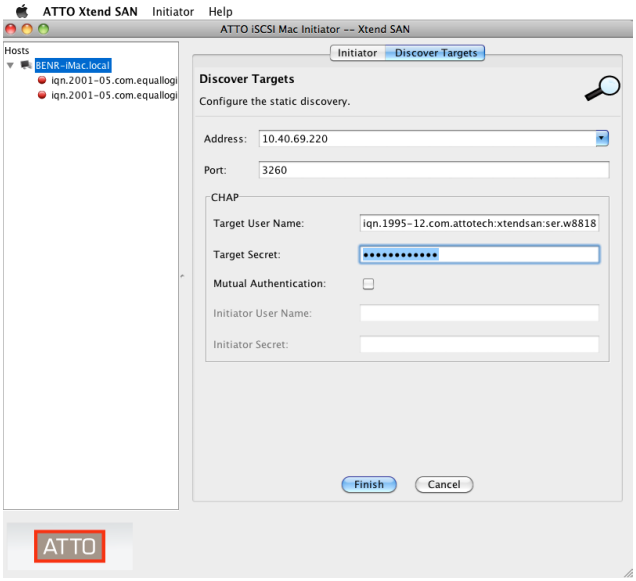
Target Discovery

DNS/IP discovery is a mechanism that directly contacts an iSCSI target device. The initiator queries the iSCSI target to determine what targets are available to the initiator. You can select all or some of these available targets and the ATTO iSCSI Initiator creates connections to these targets.

You must know the hostname or IP address for each of the iSCSI targets to be discovered. Please have this information available before proceeding.

1. Double click the Xtend SAN icon to open the application. Initiators are listed in the left-hand panel.
2. Click on the initiator with which you wish to work. The central panel contains tabs for **Initiator** and **Discover Targets**.
3. Click on the **Discover Targets** tab.
4. Click on Discover by DNS/IP.
5. Type in the IP address or hostname of the device with targets you wish to discover.
6. The default Port Number is **3260**. Edit the port number if the port number for your target device is different.
7. If authentication is required:
   a. Type in the **Target Secret**.
   b. If the initiator requires mutual authentication, click on the **Mutual Authentication** check box.
8. Type in the Initiator **User Name** and the **Initiator Secret**.
9. Click on Finish.
10. The discovered targets are listed in the central panel. Continue to Add targets

Exhibit 7 - Target Discovery



Add Targets

The ATTO iSCSI Initiator maintains a list of added targets that have been discovered after the Mac is reconnected to a network.

Targets are listed under **Discovered Targets** in the central panel. Targets that have been previously added appear as light grey.

1. Highlight the target(s) to be added. Multiple targets may be highlighted at one time.
2. Click on **Add**.

The highlighted targets appear in the left-hand panel.

- If you want to add more targets, return to Step 1.
- If you want to discover more targets, return to DNS/IP discovery
- If you want to manage targets, continue to Managing Targets

Managing Targets

After discovering targets, ATTO Xtend SAN software allows you to connect to and remove targets, configure security, and view or configure a number of useful features.

ATTO Xtend SAN software provides the capability to:

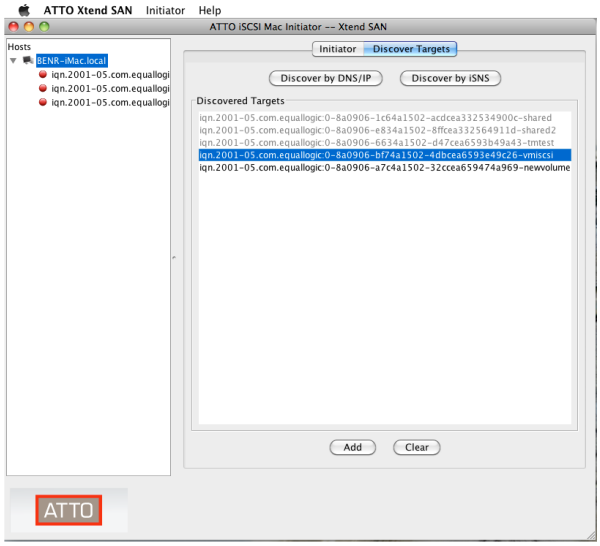
- Select target ports for connection.
- Specify automatic login at boot time.
- Connect to targets.
- Remove targets.
- Configure security for each target.
- View the iSCSI login parameters established during a connection.
- Configure iSCSI login parameters for each connection.
- View a list of LUNs exposed by the target.

You must first **select targets** in order to manage them. Targets are listed in the left-hand panel. Icons next to each target indicate the status of the target:

- Red indicates not connected.
- Green indicates connected.
- X indicates the target is unavailable.

Click on the target you wish to manage. The central panel contains tabs for **Setup**, **Status** and **LUNs**. Use the following instruction for the task you wish to accomplish.

Exhibit 8 - Adding Targets



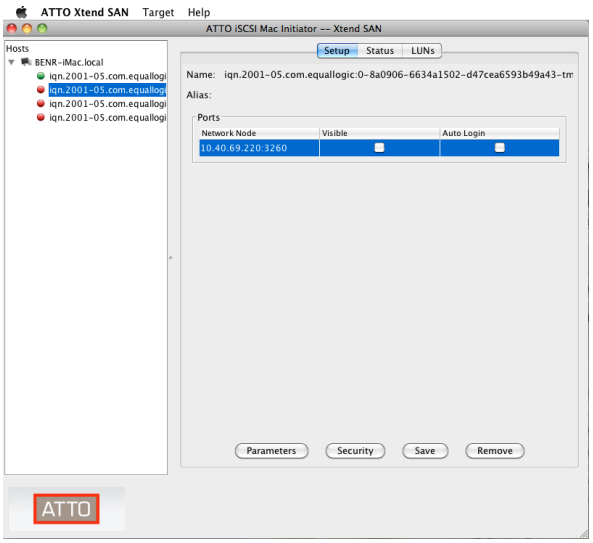


Exhibit 9 – Selecting Targets

Select Target Ports for Connection

iSCSI targets may be accessed through one or more ports. The ATTO iSCSI Initiator presents all the ports identified by a target during the discovery process. You must select each port and identify if the port is visible for connection and if a visible port requires auto login. All ports for a target are listed in the **Setup** tab while only visible ports are listed in the **Status** tab.

You may automatically log into a target at system boot by clicking the **Auto Login** check box during target setup.

1. Click on the **Setup** tab. A list of one or more ports is displayed. Set up each port individually to connect to the target.

   Highlight one of the target's ports. Click the **Visible** check box if you want to connect using this port.
   - Click the **Auto Login** check box if you want to automatically connect to this port after the system boots.
   - Click on **Security** if your system requires CHAP security**.** Refer to Configure security.
   - Click on **Parameters** if the default iSCSI login parameters are not correct for your target. Refer to Configure iSCSI login parameters.
2. Set up the remaining ports by highlighting each port and selecting the options listed in Step 2.
3. When you have set up all the ports, click on **Save** to save the configuration.
4. Continue to manage additional targets or continue to Connect to targets.

Configure security using CHAP

CHAP is a mechanism for authenticating the device at the other end of a network link. CHAP requires that the target device challenges the initiator first (Target Challenge) and that the initiator challenges the target second (Initiator Challenge).

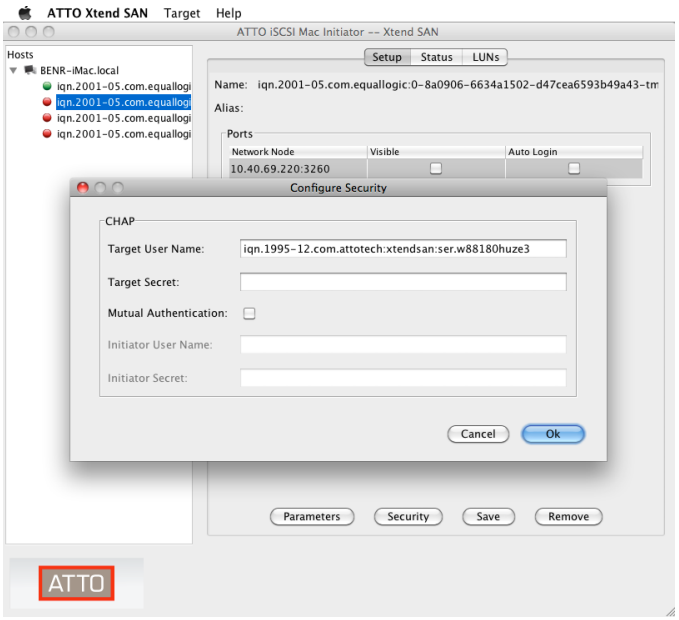
The CHAP challenge mechanism requires that both ends know the Target Secret and the Initiator Secret. The Target Secret answers the Target Challenge and the Initiator Secret answers the Initiator Challenge.

Be sure to have the secrets when configuring security. The ATTO iSCSI Initiator does not impose rules for formatting CHAP secrets. However, many iSCSI targets have formatting rules which determine the format of the ATTO iSCSI CHAP secrets. In general, secrets should follow these guidelines:

- Do not use a tab or space.
- Use ASCII printable characters: do not use special control characters.
- Secrets are case sensitive: you may use all upper case, all lower case or a combination of upper and lower case.
- Secrets should be longer than 12 characters.

1. Click on the **Setup** tab.
2. Click on **Security**.
3. The **Configure Security** screen appears.
4. Type in the **Target Secret**. If the initiator requires mutual authentication, click on the **Mutual Authentication** check box.
5. Type in the Initiator User Name and the Initiator Secret.
6. Click **OK** when you have completed your choices.
7. Click **Save** to save your configuration.

Exhibit 10 – Configuring CHAP



Connect to Targets

The ATTO iSCSI Initiator provides manual and automatic login/logout to iSCSI target ports. Automatic login occurs immediately after the system is booted or after the network interface is re-established. The **Auto Login** check box must be selected to provide automatic logins.

Note ***You can manually log in to any visible iSCSI targets from the Status tab.***

1. Click on the **Status** tab. A list of one or more ports is displayed.
2. Select the target port.
3. Click **Login** at the bottom of the tab. The highlighted target status changes to **connected**.
4. Continue selecting other ports or view the iSCSI parameters established for each port during login.
    - Highlight the target's port.
    - Click on **Parameters**. A popup dialog box displays the **Login Parameters**.
5. When you have finished viewing the parameters, click on **Close**.
6. Click on the **LUNs** tab. View LUNs exposed by the target.

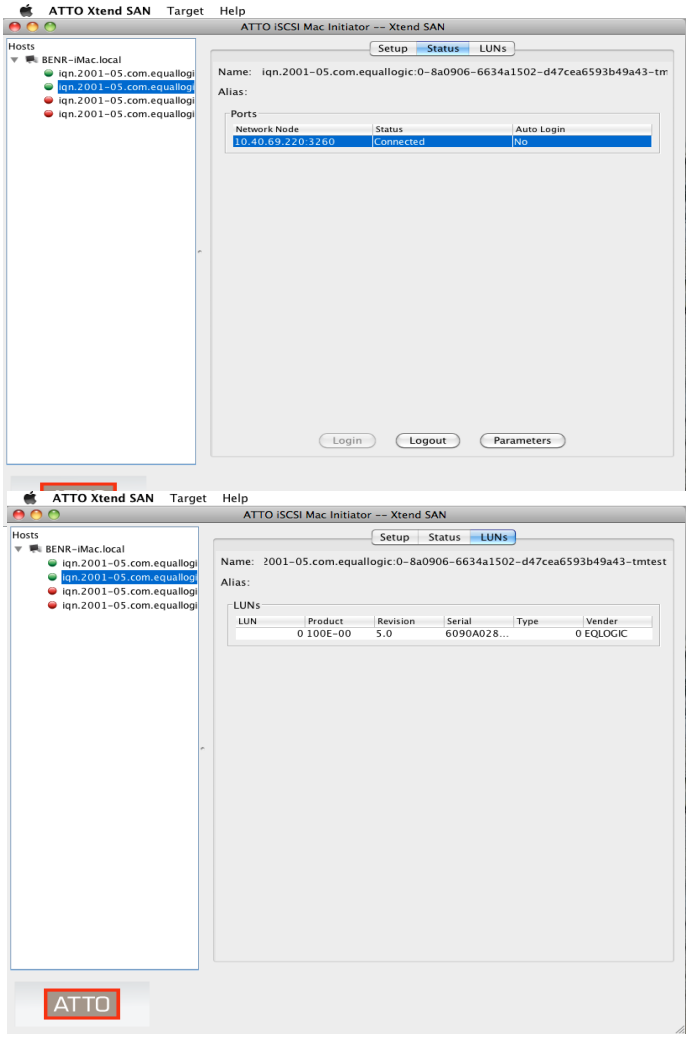


Exhibit 11 – Connecting to Targets

6 Update Firmware

The firmware on the ATTO XstreamCORE 8100T is field upgradable. From time to time new firmware may be released to include the latest enhancements, new features, and bug fixes.

The XstreamCORE firmware is distributed as a **.zbd** file from the ATTO Technology web site at **www.atto.com**. Download the file and note the filename.

Using SFTP

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

Note ***The storage controller SFTP server is at port 20, not the default port 22.***

2. As an example, using OpenSSH, the SFTP connection is made with the following command using username 'sftp', the password set in **Modify passwords**, and x.x.x.x as the IP address of the XstreamCORE.

   sftp sftp@<x.x.x.x>
3. Enter your password when prompted.
4. Once logged in, upload the zbd file using the "put" command.
   For example:
   put c:\firmware\xc8100_3_00_101F.zbd
5. The firmware update process may take several minutes. Use CLI command **FlashStatus** to check the progress of the firmware update. FlashStatus will indicate when the update has completed pending a restart.
6. Upon a successful firmware update, restart the XstreamCORE using the **FirmwareRestart** CLI command to apply the new firmware.

7 Appendix A Cabling

ATTO XstreamCORE SAS connections connect SAS storage devices into the Ethernet Storage Area Network (SAN). Make sure all cables are anchored securely at both ends with the proper connectors.

SAS Connections

The XstreamCORE 8100T supports 12Gb & 6Gb SAS LTO Tape Drives.

Note ***The lengths in the table are for passive copper cables***

SAS PHY auto-negotiates the appropriate sync rates with the connected devices. Check the type of cable and cable length limit.

Keep cable lengths as short as possible to ensure the highest signal quality and performance. These cable lengths include the wiring inside the devices.

Cable Type		Max Cable Length	Max Speed
SFF 8644 – SFF 8644		1m, 3m	12Gb/s
SFF 8644 – SFF 8088		1m, 3m	6Gb/s
SFF 8644 – 4x SFF 8644		1m, 3m	12Gb/s
SFF 8644 – 4x SFF 8088		1m, 3m	6Gb/s
SFF 8644 – 2x SFF 8644 & 2x SFF 8088		2m	12Gb/s

Note ***Visit the ATTO web store at http://www.atto.com/store to purchase compatible cables.***

Ethernet Data Connection

Ethernet technology offers a variety of cabling options. The type of cable required varies depending upon the application, environment and distance.

The 10Gb Ethernet data ports provide host connectivity. The table shows optical connections:

Note ***Visit the ATTO web store at http://www.atto.com/store to purchase compatible cables.***

Note ***The table shown is for optical cabling with SFP+ modules***

Note ***For RJ45 interface, Cat6a (or) greater at a maximum of 30m is recommended.***

Cable Type	10Gb/s
50 µm OM2	82m
50 µm OM3	300m
50 µm OM4	400m

Note ***1GbE is not supported on the data port***

Ethernet Management Connection

The 100/1000 RJ-45 Ethernet port provide dedicated monitoring, management, and diagnostics capabilities, supporting CLI over SSH, and File Transfer over SFTP.

When you connect an Ethernet cable between the XstreamCORE and a 100/1000 RJ-45 connection, you may need a crossover cable connecting directly to a computer.

The ATTO XstreamCORE auto detects the Ethernet speed by default.

Note ***It is recommended to use a good quality Cat 5e or better cable***

Appendix B CLI Provides ASCII-based Interface

The command line interface (CLI) provides access, configuration, and monitoring for ATTO XstreamCORE services through a set of ASCII commands. CLI commands are entered through the SSH session.

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 restart of the system before it is implemented. The restart can be accomplished by using a separate *FirmwareRestart* command if not prompted to reboot. A number of set commands may be issued before restart command.
- Immediate commands are set commands which are executed right away and do not require a Save Configuration command.
- Responses to Immediate commands are either an error message or data results followed by Ready.

Exhibit 2 Symbols, typefaces and abbreviations used to indicate functions and elements of the command line interface used in this manual

Command conventions

Symbol	Indicates
[ ]	Required entry
<>	Optional entry
|	pick one of
…	Ellipses, repetition of preceding item
\n	end of line
-	a range (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)
mp	Ethernet Management port number (mp1)

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 and their defaults is given below. Only those commands which have a "set" component that can be stored in non-volatile memory have a default listed. Commands which have no default values associated with them have a blank entry in that column of the table. Commands which are not present in the specified unit list "N/A" in that column.

Command	Default Value
AccessControl	disabled
AccessEntry	
CertGen	
CertInfo	
ClearCliLog	
ClearEventLog	
ControllerName	
CoreDumpInfo	
Date	
DNSDomain	
DNSNameServer	
DumpCliLog	
DumpConfiguration	
DumpEventLog	
EncryptionKey	Unique keys
EthCongestionAlgorithm	cubic
EthFlowControl	DP1 enabled DP2 enabled MP1 auto
EthMTU	DP1 9000 DP2 9000 MP1 1500

EthPort	
EthSack	enabled
EthStats	
Exit	
FirmwareRestart	
FlashStatus	
Help	
Info	
IPAddress	DP1 10.0.0.1 DP2 172.16.0.1 MP1 192.168.0.1
Iperf3Server	disabled
IPDHCP	DP1 disabled DP2 disabled MP1 disabled
IPGateway	
IPSubnetMask	DP1 255.0.0.0 DP2 255.240.0.0 MP1 255.255.0.0
IPV6Address	DP1 fd00::2 DP2 fd00::3 MP1 fd00::1
IPV6DHCP	DP1 disabled DP2 disabled MP1 disabled
IPV6Gateway	
IPV6Prefix	DP1 64 DP2 64 MP1 64
iSCSIChangeTargetSuffix	
iSCSICHAP	
iSCSICHAPMode	disabled
iSCSILatency	
iSCSILogins	
iSCSIMap	

iSCSIMappingMode	automatic
iSCSISetPorts	
iSCSIShowMaps	
iSCSITargetCreate	
iSCSITargetDelete	
iSCSIUnMap	
Licenses	
Password	Unique. See the bottom of the unit for default password
Ping	
RestoreConfiguration	
SASConnectorStats	
SASPortList	
SendEOMDeferredError	disabled
SFPInfo	
ShowDevices	
Temperature	
Timesync	enabled
TimesyncServer	
TimeZone	Time zone: America/New_York
TimeZoneList	
Uptime	

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 whitelisted initiators in the target's access control list.

set AccessControl [Target Name | target ID] [enabled | disabled]
get AccessControl [Target Name | target ID | all]

AccessEntry

AccessEntry allows the addition (or) deletion of an initiator entry from the access control list of a target node. The initiator name is converted to lower case and must be between 16 and 223 characters.
NOTE: For 'set AccessEntry','delete' is optional when specifying an initiator name, but is required if specifying 'all'.

set AccessEntry [Target name | target ID] [initiator name <delete> | all [delete]]
get AccessEntry [Target name | target ID | all]

CertGen (Immediate)

Deletes existing self-signed HTTPS certificates and generates new self-signed HTTPS certificates. This operation could take several minutes to complete.

CertGen

CertInfo (Immediate)

Displays information about the current HTTPS certificates.

CertInfo

ClearCliLog (Immediate)

Clears the contents of the CLI command log.

ClearCliLog

ClearEventLog (Immediate)

Clears the contents of the event log.

ClearEventLog

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.

set ControllerName [name]
get ControllerName

CoreDumpInfo (Immediate)

Displays information concerning all core dumps stored by a prior fault.

CoreDumpInfo

Date

Sets/displays the current date and time, in the format of YYYY-MM-DD HH:MM:SS.

NOTE: When using this command to configure the date, "Timesync" must already be disabled.

set Date [YYYY-MM-DD] [HH:MM:SS]
get Date

DNSDomain

Configures the global value for the DNS domain.
Up to 6 domains can be specified, each seperated by a space. The list can be cleared by calling set with 'Clear' as the value.

set DNSDomain [domain url] x 6 | Clear]
get DNSDomain

DNSNameServer

Configures the global value for the DNS name server.
Up to 3 IPv4 or IPv6 name servers can be specified, each seperated by a space. The list can be cleared by calling set with 'Clear' as the value.

set DNSNameServer [[IPv4 Address | IPv6 Address] x 3 | Clear]
get DNSNameServer

DumpCliLog (Immediate)

Dumps the contents of the CLI command log to the current CLI session.

DumpCliLog

DumpConfiguration (Immediate)

Dumps the configuration of the unit.

DumpConfiguration

DumpEventLog (Immediate)

Dumps the contents of the event log to the current CLI session. With no parameters, the last 2048 entries are displayed. The optional parameter "all" specifies all entries will be displayed. An optional numeric parameter specifies the maximum number of newest entries to display.

DumpEventLog <NumEntries | all>

EncryptionKey (Immediate)

Allows the SSH/SFTP server-side encryption keys to be generated (or) displayed. Displaying the encryption keys will cause all available server-side public keys to be displayed, as well as the signatures of the server-side private keys. Revoking existing keys can be performed with the Generate option.

EncryptionKey [Generate | Display]

EthCongestionAlgorithm

Configures the congestion algorithm for Ethernet traffic on the unit's data ports.

set EthCongestionAlgorithm [cubic | reno]
get EthCongestionAlgorithm

EthFlowControl

Sets the PAUSE frame behavior for the given data port(s). The "enabled" and "disabled" settings affect both rx and tx.

set EthFlowControl [DP[n] | all] [enabled | disabled]
get EthFlowControl [DP[n] | all]

EthMTU

Configures the MTU, (or) maximum transmission unit (Frame Size), used by the specified ethernet port. Standard equates to 1500 and jumbo 9000.

set EthMTU [DP[n]] [296 - 9024 | standard | jumbo]
get EthMTU [DP[n] | MP[n] | all]

EthPort

Lists the available Ethernet ports, current status (Up/Down), and link speed. Specifying a port name followed by enabled (or) disabled configures the port to be persistently enabled (or) disabled, respectively.

set EthPort [DP[n] | MP[n] | all] [enabled | disabled]
get EthPort

EthSack

Configures the SACK (Selective Acknowledgements) networking parameter. SACK is a refinement of TCP's traditional "cumulative" acknowledgements.

set EthSack [enabled | disabled]
get EthSack

EthStats

Displays port statistics for the selected Ethernet port.

get EthStats [DP[n] | MP[n] | all]

Exit (Immediate)

Terminates the current CLI session over SSH. This command relaunches the CLI interface if used during a serial RS-232 session.

Exit

FirmwareRestart (Immediate)

Causes an immediate reboot of the unit.

FirmwareRestart

FlashStatus (Immediate)

Displays the status of a firmware update in progress, (or) the most recent firmware update if no update is in progress. By default, only fifteen lines of status are displayed. The argument "verbose" will result in up to two hundred lines of status being displayed, including the status of a root filesystem update in progress, (or) the most recent root filesystem update if no update is in progress.

FlashStatus <verbose>

Help (Immediate)

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>

Info (Immediate)

Displays version number and other system information for key components of the unit.

Info

IPAddress

Configures the current IP address of any Ethernet port(s). If IPDHCP is enabled, the 'get' command reports the current IP address assigned by the network DHCP server, followed by the (DHCP) identifier.

set IPAddress [DP[n] | MP[n]] [xxx.xxx.xxx.xxx]
get IPAddress [DP[n] | MP[n] | all]

IPDHCP

Configures the current DHCP setting. DHCP allows acquisition of an IP address from a network DHCP server. When this option is disabled, the IP address used is specified by the "IPAddress" command.

set IPDHCP [DP[n] | MP[n] | all] [enabled | disabled]
get IPDHCP [DP[n] | MP[n] | all]

Iperf3Server

Enable (or) disable an iperf3 server to aid network configuration and troubleshooting.

set Iperf3Server [enabled | disabled]
get Iperf3Server

IPGateway

Configures the current default gateway used by the specified Ethernet port.

set IPGateway [DP[n] | MP[n] | all] [IP Address]
get IPGateway [DP[n] | MP[n] | all]

IPSubnetMask

Configures the current subnet masks used by the specified Ethernet port.

set IPSubnetMask [DP[n] | MP[n] | all] [xxx.xxx.xxx.xxx]
get IPSubnetMask [DP[n] | MP[n] | all]

IPV6Address

Configures the current IPv6 address of any Ethernet port(s). If IPV6DHCP is enabled, the 'get' command reports the current IP address assigned by the network DHCP server, followed by the (DHCP) identifier.

set IPV6Address [DP[n] | MP[n]] [IPv6 Address] | [IPv6 Address/Prefix]
get IPV6Address [DP[n] | MP[n] | all]

IPV6DHCP

Configures the current DHCPv6 setting. DHCP allows acquisition of an IP address from a network DHCP server. When this option is disabled, the IP address used is specified by the "IPV6Address" command.

set IPV6DHCP [DP[n] | MP[n] | all] [enabled | disabled]
get IPV6DHCP [DP[n] | MP[n] | all]

IPV6Gateway

Configures the current default gateway used by the specified Ethernet port.

set IPV6Gateway [DP[n] | MP[n] | all] [IP Address]
get IPV6Gateway [DP[n] | MP[n] | all]

IPV6Prefix

IPV6Prefix controls the current IPv6 prefix of any Ethernet port(s).

set IPV6Prefix [DP[n] | MP[n]] [Prefix length]
get IPV6Prefix [DP[n] | MP[n] | all]

iSCSIChangeTargetSuffix (Immediate)

Automatic mapping mode only. Change the default iSCSI qualified name (IQN) suffix.

The changeable suffix begins following the serial number in the IQN formatted as follows:

iqn.yyyy-mm.<naming authority>:<unit serial number>.<changeable suffix>

The changeable suffix must be 1-32 characters in length. Executing the command without providing an argument reverts the changeable suffix to the default.

iSCSIChangeTargetSuffix [Target ID | name] <new changable suffix>

iSCSICHAP

Specifies the incoming and outgoing usernames/passwords for iSCSI CHAP sessions.

Passwords are case sensitive, 12 to 16 characters, and cannot contain spaces, tabs, (or) the following characters: ( ) . ; ' " `

Usernames are case sensitive, 4 to 223 characters, and cannot contain the following characters:
*~ ! @ # $ ^ & ( ) + [ ] { } * ; : ' " . , % | < > ? / \ = `*

The 'in' password 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' username/password pair per target.

If 'discovery' is specified, the setting will apply to CHAP during discovery sessions.

NOTE: Access Control must be enabled and iSCSICHAPMode set to one-way (or) two-way for the CHAP password to apply.

EXAMPLES:

Display CHAP credentials for discovery and for all targets
get iSCSICHAP all

Display CHAP credentials for target ID 0's access entry 'iqn.initiator.00'
get iSCSICHAP 0 iqn.initiator.00

Display CHAP credentials for target name 'iqn.target.1' with an access entry of 'iqn.initiator.01'
get iSCSICHAP iqn.target.1 iqn.initiator.01

Set the 'in' CHAP credentials for target ID 2's access entry 'iqn.initiator.0A, with username 'user1' and password 'pa$$worD35410'
set iSCSICHAP 2 in iqn.initiator.0A user1 pa$$worD35410

Set the 'out' CHAP credentials for the target name 'iqn.target.3', with username 'user2' and password 'P@ssW0Rd!8833'
set iSCSICHAP iqn.target.3 out user2 P@ssW0Rd!8833

Set the 'in' CHAP credentials for discovery, with username 'user_discovery' and password 'p@$$wOrDdiscover'
set iSCSICHAP discovery in user_discovery p@$$wOrDdiscover

set iSCSICHAP [[Target name | target ID] [in [Access entry] | out] | [discovery] [in | out]] [username] [password]
get iSCSICHAP all | discovery | [[Target name | target ID] <Access entry>]

iSCSICHAPMode

iSCSICHAP specifies the type of CHAP to be used for initiator logins.

In 'One-way' authentication, the target authenticates the initiator using the 'in' CHAP password, 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 password.

'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.

set iSCSICHAPMode [Target Name | target ID | discovery] [disabled | one-way | two-way]
get iSCSICHAPMode [Target Name | target ID | discovery | all]

iSCSILatency (Immediate)

Captures and reports iSCSI read and write latency on a per-target basis. All times are in microseconds and are an average of multiple commands sampled during a short period when this CLI command is executed. Reads (or) writes must be occurring when executing this command.

Length represents the command length in bytes seen during the sampling period.

Response time is the time from receipt of an iSCSI command until a response and possibly data has been transmitted back to the initiator.

Queue time is how long a command that's ready has waited before being submitted to the device. Applies to writes only.

Device time represents how long the SAS device took to complete a command.

Response to Command time is the time between transmitting a response for one command and beginning iSCSI processing of the next. Includes host delay.

R2Ts are the number of Ready to Transfer messages that were needed to fetch all data for a write command. Applies to writes only.

iSCSILatency

iSCSILogins (Immediate)

Displays details of the initiators currently logged in (active), and optionally of initiators previously logged in as well (inactive). Displays active logins by default and both active and inactive if the 'all' argument is specified.

iSCSILogins <all>

iSCSIMap (Immediate)

Manual mapping mode only. Map a device to an iSCSI target. Use CLI commands iSCSIShowMaps and ShowDevices to see the target and device IDs.

iSCSIMap [Target ID | name] [Device ID] [LUN]

iSCSIMappingMode

Changes the iSCSI mapping mode. In automatic mode devices are assigned to predefined iSCSI targets based on SAS topology. iSCSI targets are only accessible when devices are attached. Manual mode allows user creation and deletion of iSCSI targets and user mapping of devices to targets. Changing the mapping mode may require a reboot before taking effect.

set iSCSIMappingMode [automatic | manual]
get iSCSIMappingMode

iSCSISetPorts (Immediate)

Configure the iSCSI target data port accessibility.

iSCSISetPorts [Target ID | name] [DP1 | DP2 | all | none]

iSCSIShowMaps (Immediate)

Display mapping details between iSCSI targets and devices.

iSCSIShowMaps

iSCSITargetCreate (Immediate)

Manual mapping mode only. Create an iSCSI target. The target name is formatted as follows:

iqn.yyyy-mm.<naming authority>:<unit serial number>.<IQN suffix>

The provided IQN suffix must be between 1-32 characters.

iSCSITargetCreate [IQN suffix] [DP1 | DP2 | all | none]

iSCSITargetDelete (Immediate)

Manual mapping mode only. Delete an iSCSI target.

iSCSITargetDelete [Target ID | name]

iSCSIUnMap (Immediate)

Manual mapping mode only. Remove a mapping between device and iSCSI target. Use CLI commands iSCSIShowMaps and ShowDevices to see the target and device IDs.

iSCSIUnMap [Device ID]

Licenses (Immediate)

Displays the collection of relevant open source licenses used by the unit.

Licenses

Password

Specifies the password used for all interactive sessions that require a login. Password is case sensitive, 8 to 32 characters, must contain at least one numeric character {0-9} and cannot contain the following special characters: {space, tab, ", ', \, ;}.

set Password

Ping (Immediate)

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

Ping [DP[n] | MP[n]] [IP Address] <count <size>>

RestoreConfiguration (Immediate)

Restores the configuration back to defaults. Use the default option to revert the SSH/SFTP admin password back to the original password. All Ethernet configuration settings and iSCSI maps are also reset to defaults. The default option is equivalent to pressing and holding the reset button for 5 seconds to restore settings. The unit will reboot as part of the process.

RestoreConfiguration <default>

SASConnectorStats (Immediate)

Displays SAS PHY error statistics. The argument "verbose" will print out the legend for the header values.

SASConnectorStats <verbose>

SASPortList (Immediate)

Displays SAS PHY link information.

SASPortList

SendEOMDeferredError

End Of Medium (EOM) deferred error configuration controls early warning deferred errors generated by SpeedWrite. Enable this setting if there are issues with end of tape handling.

set SendEOMDeferredError [enabled | disabled]
get SendEOMDeferredError

SFPInfo

SFPInfo displays information about the specified SFP(s).

get SFPInfo [DP1 | DP2 | all]

ShowDevices (Immediate)

Display SAS device details.

ShowDevices

Temperature

Displays the current operating temperatures of the various temperature sensors in degrees Celsius.

get Temperature

Timesync

Configures the "timesync" service. Timesync automatically adjusts the system date and time based on well-known time servers.

set Timesync [enabled | disabled]
get Timesync

TimesyncServer

Sets/displays timesync servers.

Assign up to three timesync servers separated by spaces or use 'delete' to remove all.

set TimesyncServer [List of up to 3 timesync servers | delete]
get TimesyncServer

TimeZone

Timezone sets/displays the time zone.

set TimeZone [[EST | CST | MST | PST] | [Index from TimeZoneList command]]
get TimeZone

TimeZoneList (Immediate)

Displays available time zones for setting the timezone.

TimeZoneList

Uptime (Immediate)

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

Uptime

Appendix C Standards and Compliances

The equipment described in this manual generates and uses radio frequency energy. If this equipment is not used in strict accordance with the manufacturer's instruction, it can and may cause interference with radio and television reception.

Regulatory Notices

Notice for USA (FCC)

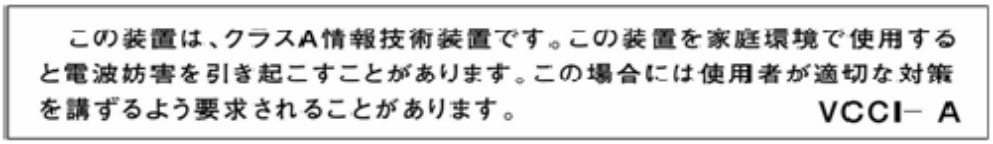
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Notice for Canada (ICES)

This Class A digital apparatus complies with Canadian CAN ICES-003(A) / NMB-003(A).

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

Notice for Japan (VCCI)



Translation: This is Class A equipment. Operation of this equipment in a residential environment could cause radio interference. In such a case, the user may be required to take corrective actions. VCCI-A

Notice for European Union (CE Mark)

This equipment is in compliance with the European Union EMC Directive 2014/30/EU, Low Voltage Directive 2014/35/EU, RoHS 2011/65/EU, (EU) 2015/863

Standards:

This equipment is in conformity with the following standards or documents.

Electromagnetic Compatibility (Class A):	Product Safety
FCC CFR 47 Part 15 Subpart B:2023	IEC 62368-1:2018 (CB Scheme)
ICES-003 Issue 7	EN IEC 62368-1:2020+A11:2020
EN 55032:2015/A11:2015	UL 62368-1:2019
BS EN 55032:2015/A11:2015	CSA C22.2 N0. 62368-1:19
AS/NZS CISPR 32:2015 +AMD 1:2020	EN/IEC60825-1, Class 1 Laser **
VCCI CISPR 32:2016	
EN55035:2017/A11:2020	
BS EN55035:2017/A11:2020	** When used with approved optical modules

Appendix D Warranty Information

ATTO Technology, Inc. limited warranty

ATTO Technology, Inc. (“ATTO”) warrants to the original purchaser of this product (“Product”) that the Product is free from defects in material and workmanship for the term described for this specific Product on ATTO's website (www.atto.com). ATTO's liability shall be limited to replacing or repairing any defective product at ATTO's option. There is no charge for parts or labor if ATTO determines that this product is defective.

PRODUCTS WHICH HAVE BEEN SUBJECT TO ABUSE, MISUSE, ALTERATION, NEGLECT, OR THOSE PRODUCTS THAT HAVE BEEN SERVICED, REPAIRED OR INSTALLED BY UNAUTHORIZED PERSONNEL WILL NOT BE COVERED UNDER THIS WARRANTY. DAMAGE RESULTING FROM INCORRECT CONNECTION OR AN INAPPROPRIATE APPLICATION OF THIS PRODUCT SHALL NOT BE THE RESPONSIBILITY OF ATTO. LIABILITY UNDER THIS LIMITED WARRANTY IS LIMITED TO ATTO PRODUCT(S). DAMAGE TO OTHER EQUIPMENT CONNECTED TO ATTO PRODUCT(S) IS THE CUSTOMER'S RESPONSIBILITY. THIS LIMITED WARRANTY IS MADE IN LIEU OF ANY OTHER WARRANTIES, EXPRESS OR IMPLIED. ATTO DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE TO THE EXTENT IMPLIED WARRANTIES CANNOT BE EXCLUDED, SUCH IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD APPLICABLE TO THE PRODUCT. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON THE DURATION OF IMPLIED WARRANTIES, THE ABOVE MAY NOT BE APPLICABLE. ATTO'S RESPONSIBILITY TO REPAIR OR REPLACE A DEFECTIVE PRODUCT IS THE SOLE AND EXCLUSIVE REMEDY PROVIDED TO THE CUSTOMER FOR BREACH OF THIS WARRANTY.

ATTO IS NOT RESPONSIBLE FOR DAMAGE TO OR LOSS OF ANY DATA, PROGRAMS OR ANY MEDIA. THE PRODUCTS ARE NOT INTENDED FOR USE IN: (I) MEDICAL DEVICES OR THE MEDICAL FIELD; OR (II) USE IN RUGGED APPLICATIONS.

ATTO IS NOT LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, IRRESPECTIVE OF WHETHER ATTO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. NO ATTO DEALER, AGENT OR EMPLOYEE IS AUTHORIZED TO MAKE ANY MODIFICATION, EXTENSION OR ADDITION TO THIS WARRANTY.

This warranty gives you specific legal rights, and you may also have other rights which vary from state to state.