ATTO Technology, Inc.

ATTO Xtend SAN

iSCSI Initiator for Mac OS X

Installation and Operation Manual

ATTO Technology, Inc.

155 CrossPoint Parkway
Amherst, New York 14068 USA

www.attotech.com

Tel   (716) 691-1999
Fax   (716) 691-9353

Sales support: sls@attotech.com
Technical support: Monday -- Friday, 8am-8pm EST
                    techsupp@attotech.com

1/2009   PRMA-0398-000

Contents

1   ATTO Xtend SAN iSCSI Initiator for Mac OS X

ATTO Xtend SAN is an iSCSI initiator which allows Mac® OS X users to connect to iSCSI Storage Area Networks (SANs), enabling access to iSCSI storage from OS X workstations or OS X laptops.

ATTO Xtend SAN, the ATTO Technology iSCSI Initiator for Mac OS X, allows Mac users to use and benefit from Internet SCSI (iSCSI), one of the fastest growing storage networking protocols today.

iSCSI allows you to take advantage of your existing Ethernet expertise and infrastructure while reaping the benefits of network attached storage, avoiding the cost and complexity associated with Fibre Channel.

iSCSI enables key applications including collaborative digital video/audio workflows, laptop connectivity to SANs and remote backups. With iSCSI, small business and workgroups can take full advantage of a SAN environment, even with limited IT budgets and resources.

ATTO Xtend SAN has been rigorously tested against products from leading iSCSI manufacturers, ensuring a high degree of interoperability with existing equipment.

The simplicity of iSCSI makes it the ideal storage networking protocol for Mac OS X users who are accustomed to the legendary ease-of-use of Mac OS X, as even non-technical users can set up and manage a server with just a few mouse clicks. ATTO Xtend SAN lessens the effort associated with the implementation of an iSCSI SAN by providing features designed with ease-of-use in mind, including an updated GUI which reflects the elegance and simplicity Mac OS X users have come to expect.

In addition to Xtend SAN, ATTO also produces an extensive line of iPBridges which provide iSCSI connectivity to either SCSI or Fibre Channel storage. The combination of Xtend SAN and the iPBridge allows you to create a heterogeneous SAN that combines Apple storage and servers with other, non-Apple storage. Using ATTO Xtend SAN and ATTO iPBridges also allows you to use the Internet to transport data across long distances, ensuring that you can implement remote backup solutions which aid compliance with regulatory measures for sensitive data.

The ATTO iSCSI solutions for Apple also enable collaborative workflows with SCSI storage. ATTO iPBridges provide iSCSI connectivity for SCSI storage, making storage that was previously direct-attached into network-addressable storage. Mac OS X workstations, including laptops, running ATTO Xtend SAN can then collaborate on projects using data on that storage, providing for more efficient workflows.

With a wide range of OS X-compatible iSCSI products, ATTO is the premier provider of iSCSI solutions for Mac OS X users.

Features

- High performance – capable of supporting multiple streams of uncompressed video
- iSCSI error handling and recovery
- Advanced CLI for addressing iSCSI Targets
- Intuitive GUI-based installation and management
- Support for Digests with Class 1 error recovery
- Compatible with Mac OS X 10.4.x and later
- Compatible with leading Ethernet switches and network interface cards
- Compatible with leading ISV solutions
- Challenge-Handshake Authentication Protocol (CHAP) support
- Internet Storage Name Service (iSNS) Client support
- Login redirect and asynchronous logout functionality
- Compatible with all ATTO iPBridges and leading iSCSI target devices

ATTO Technology Inc.

Exhibit 1-1   An example of an iSCSI SAN setup.
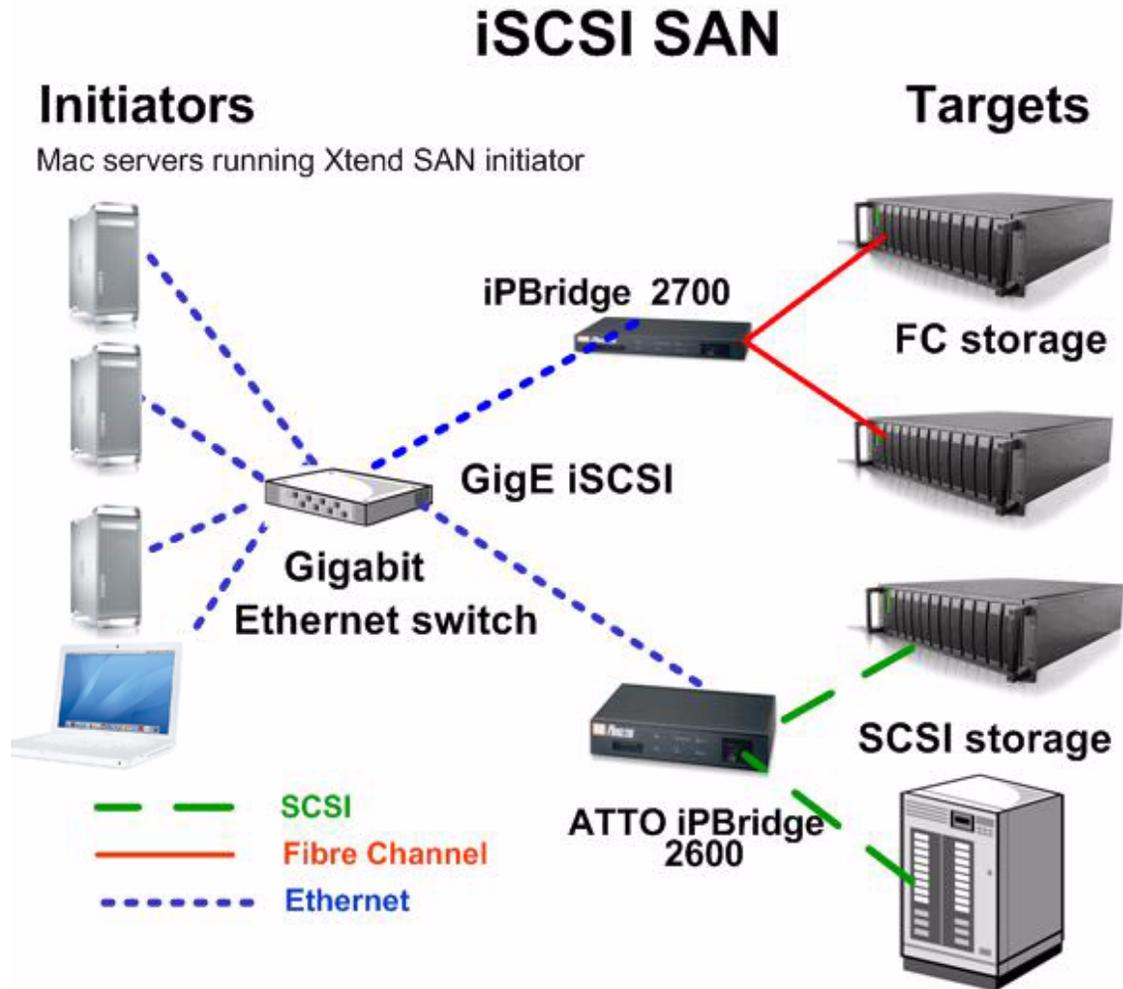
2 Installation

The ATTO Xtend SAN iSCSI Initiator is provided on CD or may be downloaded for purchase at the ATTO Webstore.

The ATTO Xtend SAN Initiator program executes under Macintosh OS X 10.4 or later and Java version 1.5 or later.

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.

Obtain authorization

1   On the Internet, go to software registration www.attotech.com/license.html

2   Select **Xtend SAN** and the current version number.

3   Type in your Email address, company name and the serial number found on the Xtend SAN CD case.

> **Note**
>
> *Your authorization file is sent to you in an Email message. Please contact ATTO Technology Tech Support if you do not receive the authorization file.*

Install Xtend SAN software

1   Insert the Installation CD.

2   After it mounts, open the Xtend SAN volume.

3   Double click on the installer.

4   Enter the OS X administrator password when asked.

> **Note**
>
> ***You must have administrator access to install the program.***

5   Follow the installation instructions, clicking on **Next** to continue from page to page.

6   Enter the authorization code when prompted to do so.You can drag and drop the authorization file into the registration file text box in the dialog box.

7   Reboot the system.

8   Locate the application icon in the folder you created during installation.

> **CAUTION**
>
> **Disable OS X Power Management when running Xtend SAN to avoid losing connections.**

9   Double-click the icon to start the application.

ATTO Technology Inc.

3   Target Discovery

You must first identify a target in order to access and manage it.

The ATTO iSCSI Initiator connects to targets (storage devices) identified during the Target Discovery process.

The ATTO iSCSI Initiator provides two mechanisms to discover iSCSI targets: iSNS discovery and DNS/IP discovery.

The ATTO iSCSI Initiator presents all discovered targets in a list. You must select the targets to be accessed from the list and add them to the ATTO iSCSI Initiator target list.

iSNS discovery

iSNS server provides a centralized system to manage access to targets that are registered with the iSNS server.

Note

Detailed explanation of the iSNS protocol is outside the scope of the manual.

You must have an iSNS server available from the system where the iSCSI Initiator is installed.

The ATTO iSCSI Initiator requires the DNS or IP address for the iSNS server. Please have this information available before proceeding.

1   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**. See Exhibit 3-1 on page 5.

3   Click the **Initiator** tab.

4   Type in the iSNS server IP address or hostname.

5   The default **Port Number** is **3205**. Edit the port number if the port number for your iSNS server is different.

6   Click **Verify iSNS** to verify the IP information to the iSNS server.

7   Click on the **Discover Targets** tab.

8   Click on **Discover by iSNS.**

9   The discovered targets are listed in the central panel. See Exhibit 3-3 on page 7. Continue to Add targets on page 7.
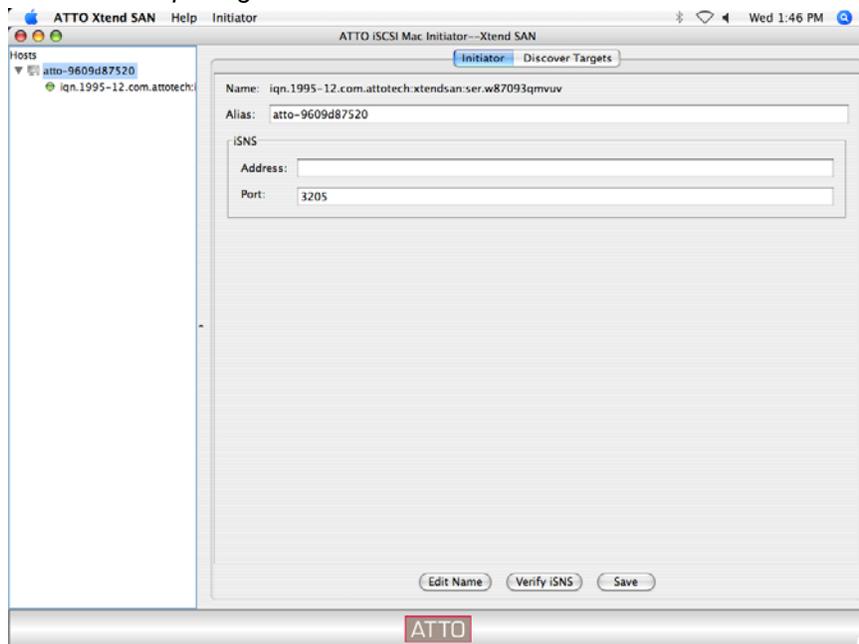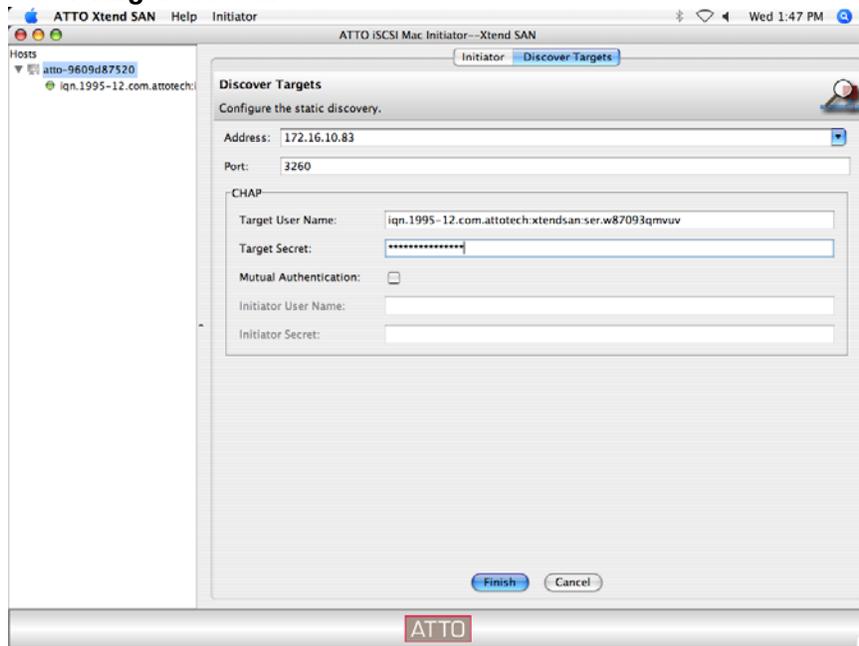
Exhibit 3-1   The Xtend SAN opening screen.

*Exhibit 3-2* **Discover Targets** *screen.*

DNS/IP 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   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**. See Exhibit 3-1 on page 5.

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. See Exhibit 3-2 on page 6.

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.

    c.   Type in the **Initiator User Name** and the **Initiator Secret**.

8   Click on **Finish**.

9   The discovered targets are listed in the central panel. See Exhibit 3-3 on page 7. Continue to Add targets.

Exhibit 3-3   Discovered targets.
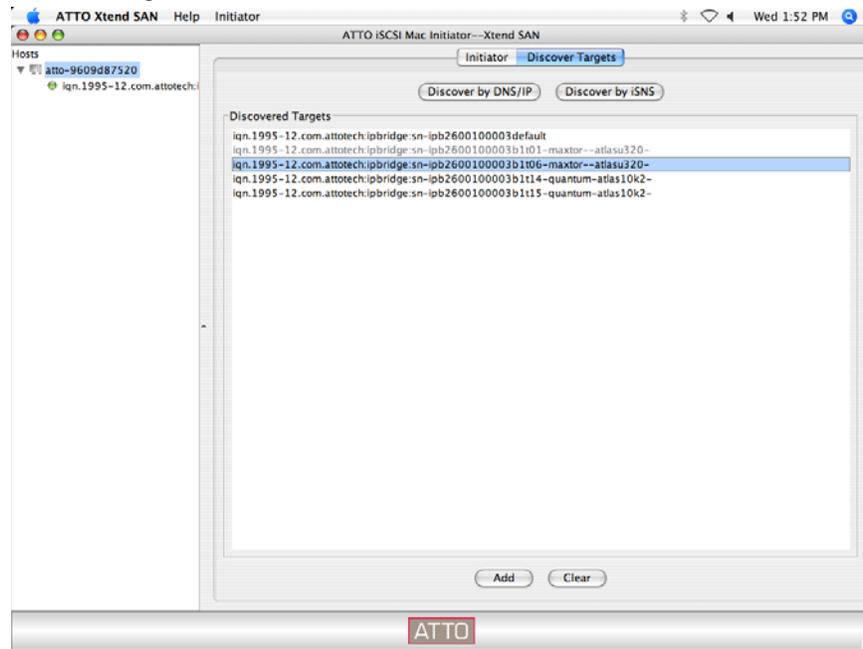
Add targets

The ATTO iSCSI Initiator maintains a list of added targets that have been discovered. The ATTO iSCSI Initiator verifies the path to these targets after a system boot and after the network interface is re-established. You do not have to rediscover a target once it has been added to the ATTO iSCSI Initiator list of targets.

1   Targets are listed under **Discovered Targets** in the central panel. See Exhibit 3-3. Targets that have been previously added appear as light grey.

Highlight the target(s) to be added. Multiple targets may be highlighted at one time.

2   Click on **Add**.

3   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 iSNS discovery on page 5 or DNS/IP discovery on page 6.

- If you want to manage targets, continue to Managing Targets on page 9.

ATTO Technology Inc.

ATTO Xtend SAN Installation and Operation Manual

4   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.

Select a target to manage

You must first select targets in order to manage them.

1   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.

2   Click on the target you wish to manage.

3   The central panel contains tabs for **Setup**, **Status** and **LUNs**. See Exhibit 4-1.

Use the following instructions for the task you wish to accomplish.

Exhibit 4-1   ***Setup, Status** and **LUNs** tabs.*

ATTO Technology Inc.
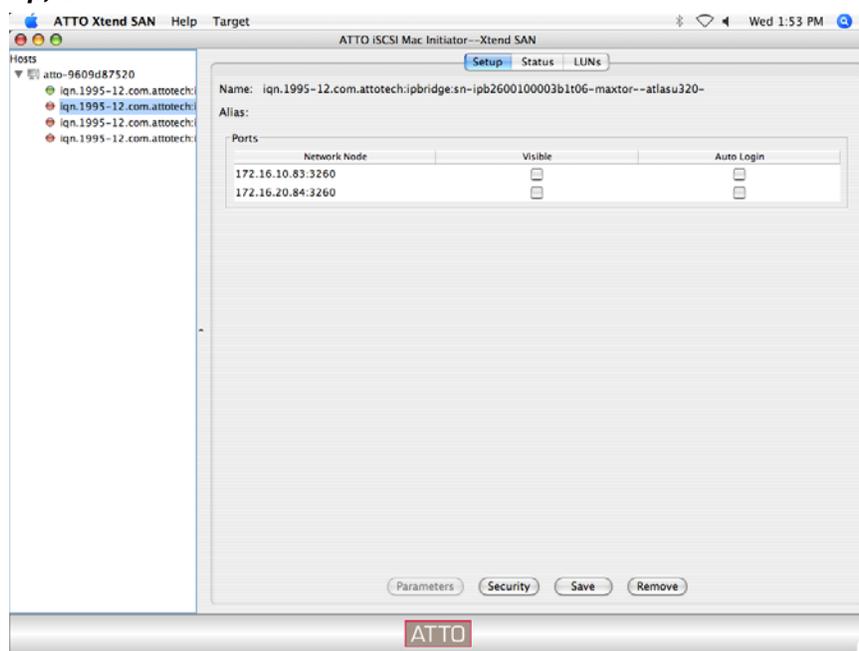
Select target ports for connection

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. See Exhibit 4-1.
2   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.

3   Set up the remaining ports by highlighting each port and selecting the options listed in Step 2.
4   When you have set up all the ports, click on **Save** to save the configuration.
5   Continue to manage additional targets or continue to Connect to targets on page 12.

Configure security

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). Refer to Glossary on page i of the Appendix for a definition of CHAP terms.

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 the **Security**.
3   The **Configure Security** screen appears. See Exhibit 4-2 on page 11.
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 4-2   The **Configure Security** screen.*
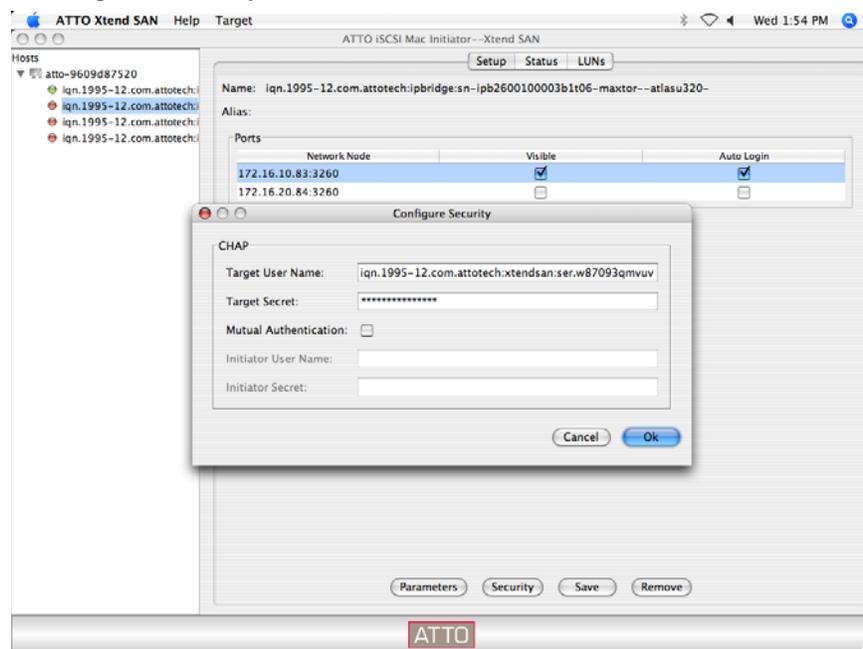
Configure iSCSI login parameters

iSCSI negotiation parameters are presented to each target port during a login by the iSCSI Initiator. The ATTO iSCSI Initiator defaults are appropriate for most iSCSI targets. However, you may need to change the parameters for a specific target.

⚠ **CAUTION**

Do not change any iSCSI negotiation parameters without extensive knowledge of the default values or specific instructions from ATTO Technology tech support.

1   Click on the **Setup** tab. A list of one or more ports is displayed. You must set up each port separately.
2   Highlight one of the target's ports.
3   Click on **Parameters**.
4   The **Configure Parameters** screen appears. See **Exhibit 4-3**.
    • Transfer size
        • FirstBurstLength
        • MaxBurstLength

• Connection Control
    • MaxConnections (for information only)
• Transfer Control
    • DataPDUInOrder (information only)
    • DataSequenceInOrder (information only)
    • ImmediateData
    • InitialR2T
    • MaxOutstandingR2T (information only)
• Error Recovery
    • DefaultTime2Retain (information only)
    • DefaultTime2Wait (information only)
    • ErrorRecoveryLevel
• Connection
    • MaxRecvDataSegmentLength
• Digests
    • HeaderDigest
    • DataDigest
5   Click **OK** when you have completed your choices.
6   Click **Save** to save your configuration.

ATTO Technology Inc.

*Exhibit 4-3   The **Configure Parameters** screen.*
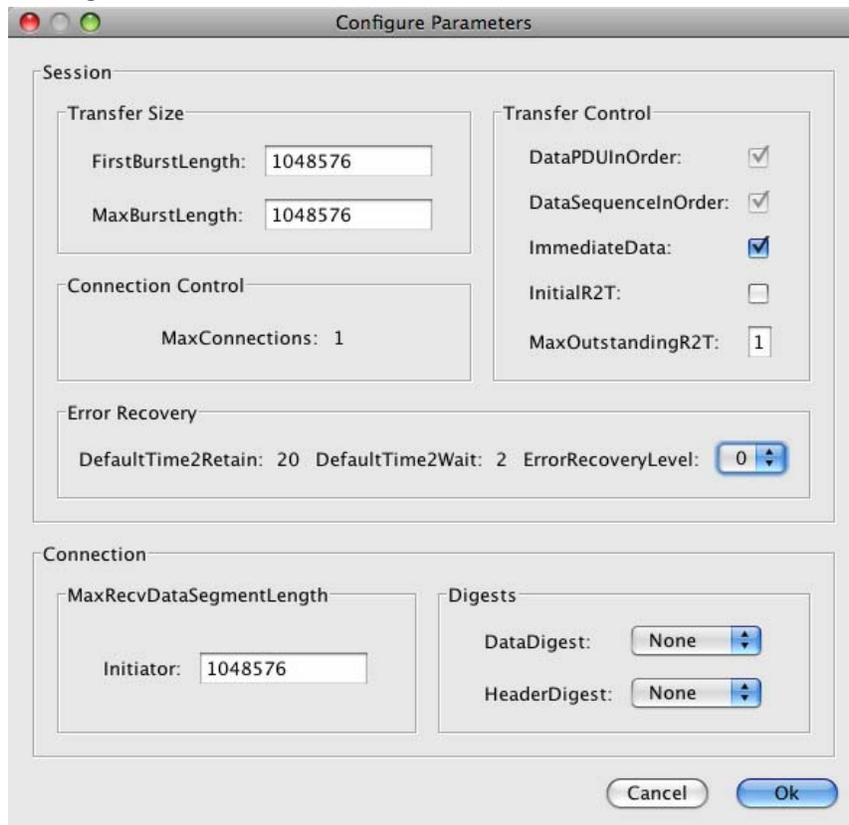
Connect to targets

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. See Exhibit 4-4 on page 13.
2   Select the target port.

3   Click **Login** at the bottom of the tab.
    The highlighted target status changes to **connected**. See Exhibit 4-5 on page 13.
4   Continue selecting other ports or view the iSCSI parameters established for each port during login.
    a.   Highlight the target's port.
    b.   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. See Exhibit 4-6 on page 14.
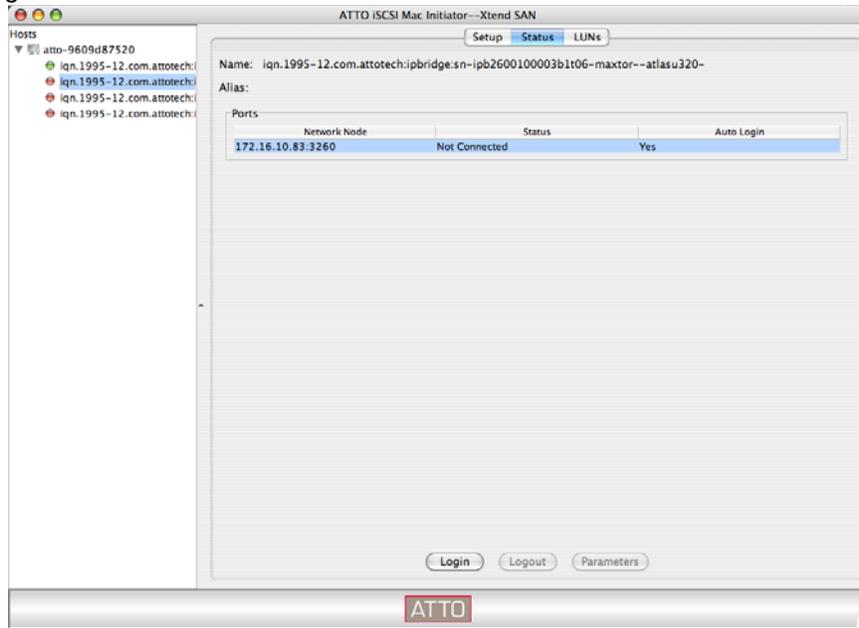
*Exhibit 4-4   Target **Status:** not connected.*

*Exhibit 4-5   Target **Status**: connected.*
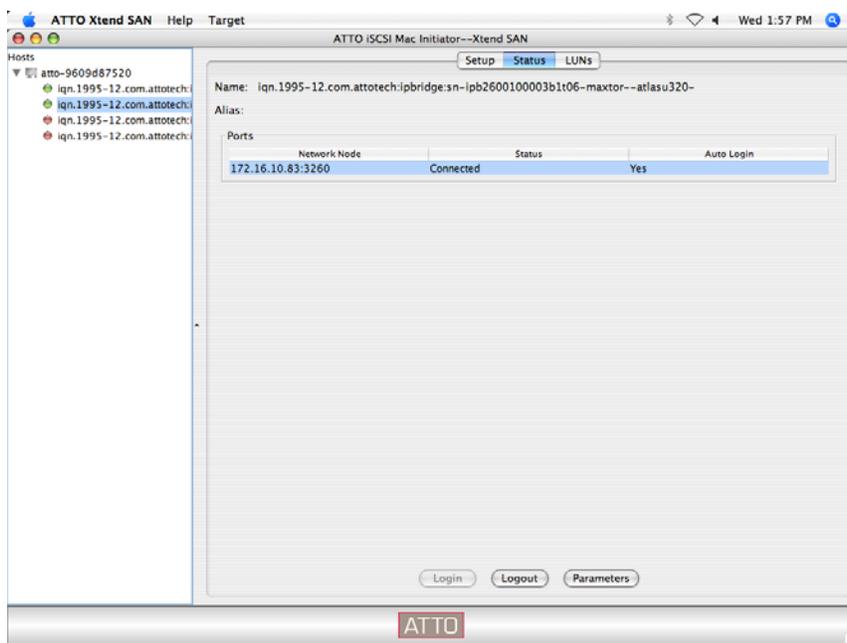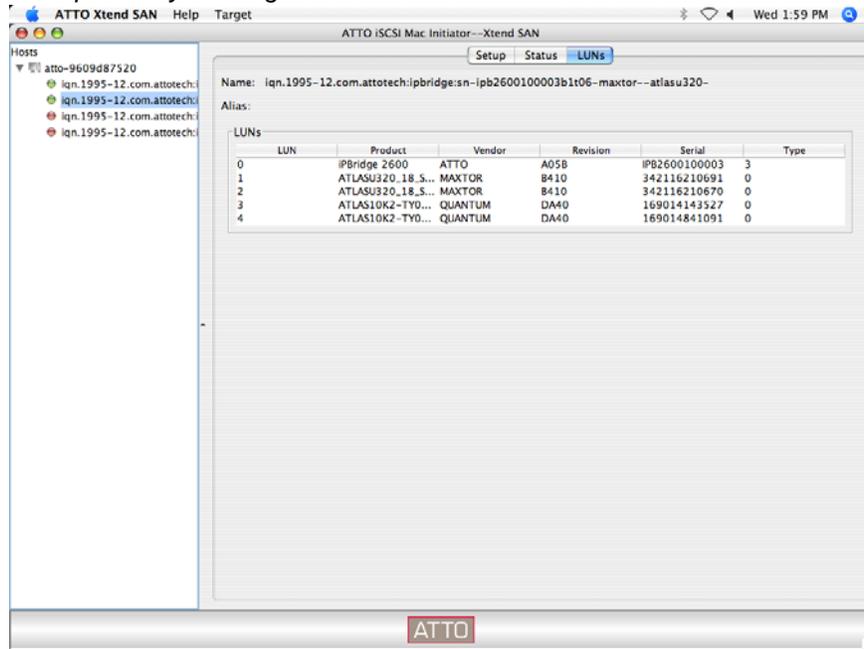
ATTO Technology Inc.

Exhibit 4-6   LUNs exposed by the target.

ATTO Xtend SAN Installation and Operation Manual

Appendix A   CLI Provides an ASCII-based Interface

Use CLI to automate access to multiple iSCSI targets.

Note
In order to use the Xtend SAN CLI Functionality you must choose to install CLI when you install Xtend SAN. CLI is accessed in a normal OS X terminal window by typing xtendsancli and then the appropriate CLI command

⚠ CAUTION
Changing parameters may disrupt access to iSCSI targets.

The Xtend SAN Graphic User Interface (GUI) is the preferred method to operate and manage the ATTO iSCSI initiator.

The command line interface (CLI) is a set of ASCII-based commands which perform configuration and diagnostic tasks.

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

`Command [Parameter1|Parameter2]`

followed by the **return** or **enter** key.

- CLI commands are case sensitive: you must type all characters as they appear on the help screen.

Note
The Command Line Interface cannot be used while the Xtend SAN application is open.

Exhibit A-1   Symbols, typefaces and abbreviations used to indicate functions and elements of the command line interface used in this manual.

Symbol/Abbreviation	Indicates
-	A range (6 – 9 = 6, 7, 8, 9)
...	Indicates optional repetition of the preceding item
< >	Required entry
|	Pick one of
[ ]	Optional entry

CLI error messages

The following error messages may be returned by the Command line Interface:

```
ERROR. "user" is already logged in from /127.0.0.1
ERROR. The daemon process does not appear to be running
ERROR. The daemon process is temporarily unavailable
ERROR. The "All" target names option cannot be used with other target names.
```

CLI summary

The following chart summarizes the Command Line Interface commands, their defaults, and an example of how to enter the commands. Commands which have no default values have a blank entry in that column of the table.

ATTO Technology Inc.

Command	Example
addTargets	xtendsancli addTargets 192.168.0.1 All
help	
listTargetsSetup	xtendsancli listTargetsSetup -address 192.168.0.1 All
listTargetsStatus	xtendsancli listTargetsStatus -address 192.168.0.1 All
loginTargets	xtendsancli loginTargets -address 192.168.0.1 All
logoutTargets	xtendsancli logoutTargets -address 192.168.0.1 All
removeTargets	xtendsancli removeTargets -address 192.168.0.1 All
version	

ATTO Xtend SAN Installation and Operation Manual

CLI command explanations

Command Line Interface commands are listed alphabetically with explanations of what they are used for, their defaults and syntax.

⚠️ **CAUTION**

Using CLI without contacting an ATTO technician is not recommended because changing parameters may cause loss of data and/or disruption to performance and reliability of Xtend SAN.

AddTargets
Adds targets found at the address to the configuration.

[-autoLogin <Yes | No>] [-connection options] [-security options] [-sesion options] <address> <All | targetName[...] >

-autoLogin Specifies target should auto login on system boot
address The addres of the targets in the form < hostName [:port] > | ip [:port] >
All | targetName[...]Specifies the targets to be processed

Help
Display the usage text.

ListTargetsSetup
Writes a list of target setups to standart out. The list will only include targets that have been previously added to the configuration.

[-address address] <All | targetName[...] >

All | targetName[...]Specifies the targets to be processed

ListTargetsStatus
Writes a list of target statuses to standard out. The list will only include targets that have been previously added to the configuration.

[-address address] <All | targetName[...] >

All | targetName [...] Specifies the targets to be processed

LoginTargets
Logs into the configured targets with ports that match the addresss.

[-address address] <All | targetName[...] >

All | targetName [...] Specifies the targets to be processed

LogoutTargets
Logs out of the configured targets with ports that match the addresss.

[-address address] <All | targetName[...] >

All | targetName [...] Specifies the targets to be processed

RemoveTargets
Removes the target session configurations with ports that match the address.

[-address address] <All | targetName[...] >

All | targetName [...] Specifies the targets to be processed

Version
Displays the version.

ATTO Technology Inc.

Appendix A   Glossary

Term	Definition
CHAP	Challenge Handshake Authentication Protocol. A mechanism for authenticating the device at the other end of a network link. The authentication is successful when the challenged device knows the CHAP secret of the challenging device.
CLI	Command Line Interface. For advanced users and automation of commands within the ATTO iSCSI Initiator
Discovery Domain	A concept of the iSNS Server that allows iSCSI initiators and targets to be segregated into management groups called domains. All initiators in a domain can discover all the targets in the domain. Initiators cannot discover targets in a Discovery Domain in which they are not a member. A device can be a member of one or more domains.
Initiator Challenge	A CHAP authentication request that is sent from the initiator device to the target device. The target device must know the Initiator Secret in order to complete the challenge successfully. An Initiator Challenge is only performed during Mutual Authentication.
Initiator Secret	The CHAP secret held by the initiator used as the basis for challenging the target during the Initiator Challenge. The target must know this secret to build the proper response when challenged.
IP / DNS Discovery	The method used to discover an iSCSI target by specifying the IP address or the DNS name for the target device.
iSCSI Digests	Header and Data Digests which are negotiated during iSCSI logon to ensure data integrity
iSNS Discovery	The method used to discover all of the iSCSI targets in the same Discovery Domain(s) as the initiator.
Mutual Authentication	CHAP procedure in which a Target Challenge is performed and, if that is successful, then an Initiator Challenge is performed.
Target Challenge	A CHAP authentication request that is sent from the target device to the initiator device. The initiator device must know the Target Secret in order to complete the challenge successfully.
Target Connection	The procedure to establish a connection between an initiator and a target. The procedure includes parameter negotiation and may include authentication.