

ATTO Xtend SAN iSCSI Initiator for macOS Installation and Operation Manual



The Power Behind the Storage

155 CrossPoint Parkway
Amherst, NY 14068

P. +1.716.691.1999
atto.com

© 2018 ATTO Technology, Inc. All rights reserved. All brand or product names are trademarks of their respective holders. No part of this manual may be reproduced in any form or by any means without the express written permission of ATTO Technology, Inc.

2/2018

PRMA-0398-000MD

Table of Contents

1	ATTO Xstend SAN Overview	2
2	Installation	3
	Obtain authorization.....	3
	Install Xtend SAN software.....	3
3	Target Discovery	4
	iSNS Discovery	4
	DNS/IP Discovery	5
	Add Targets.....	5
4	Managing Targets	6
	Select a target to manage	6
	Select target ports for connection	6
	Configure Security.....	7
	Configure iSCSI login parameters	8
	Connect to target	9
	Appendix A CLI Provides an ASCII-base Interface.....	10
	CLI error messages	10
	CLI Summary.....	10
	CLI command explanations.....	11
	Commands.....	11
	Shared Common Elements	12
	Options	13
	Appendix B Glossary	15

1 ATTO Xstend SAN Overview

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

ATTO Xstend SAN, the ATTO Technology iSCSI Initiator for macOS, 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 Xstend 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 macOS users who are accustomed to the legendary ease-of-use of macOS, as even non-technical users can set up and manage a server with just a few mouse clicks. ATTO Xstend 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 macOS users have come to expect. The ATTO iSCSI solutions for Apple also enable collaborative workflows with SCSI storage. macOS workstations, including laptops, running ATTO Xstend SAN can 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 macOS 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 error recovery level 1
- Compatible with 64 bit versions of macOS 10.9 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

Exhibit 1 An example of an Xstend SAN Storage Solution setup

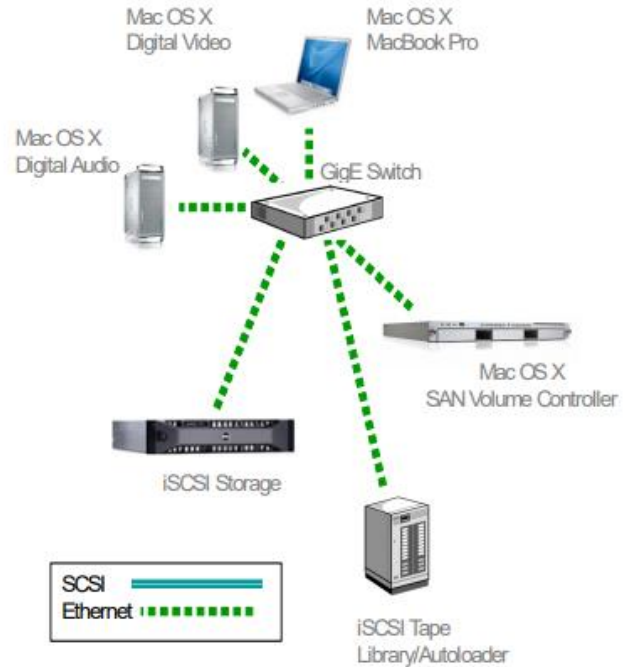
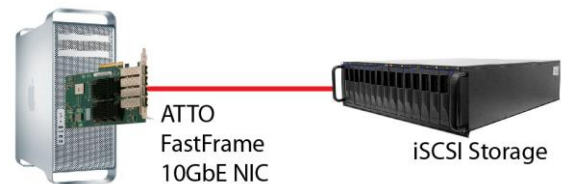


Exhibit 2 Mac workstation directly connected to iSCSI storage



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 macOS 10.9 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 <https://www.attotech.com/support/license>
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 macOS 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 macOS Power Management when running Xtend SAN to avoid losing connections.

9. Double-click the icon to start the application.

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.

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.*

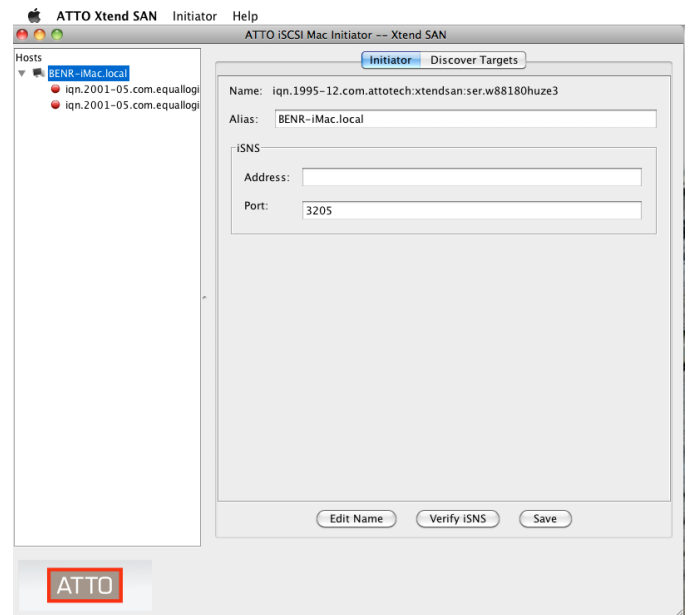
You must have an iSNS server available from the system where the iSCSI Initiator is installed.

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**.
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.

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.

7. Click on the **Discover Targets** tab.
8. Click on **Discover by iSNS**.
9. The discovered targets are listed in the central panel. Continue to [Add targets](#)



DNS/IP Discovery

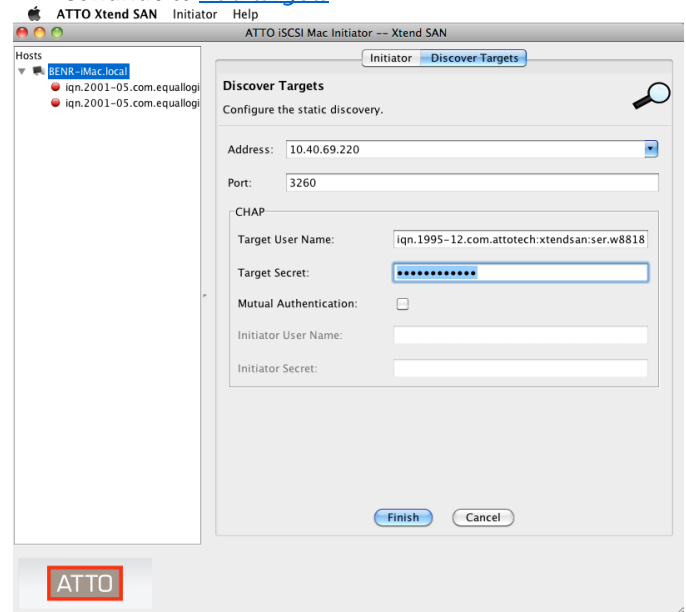
DNS/IP discovery is a mechanism that directly contacts an iSCSI target device. The initiator queries the iSCSI target to determine what targets are available to the initiator. You can select all or some of these available targets and the ATTO iSCSI Initiator creates connections to these targets.

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**.
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](#)

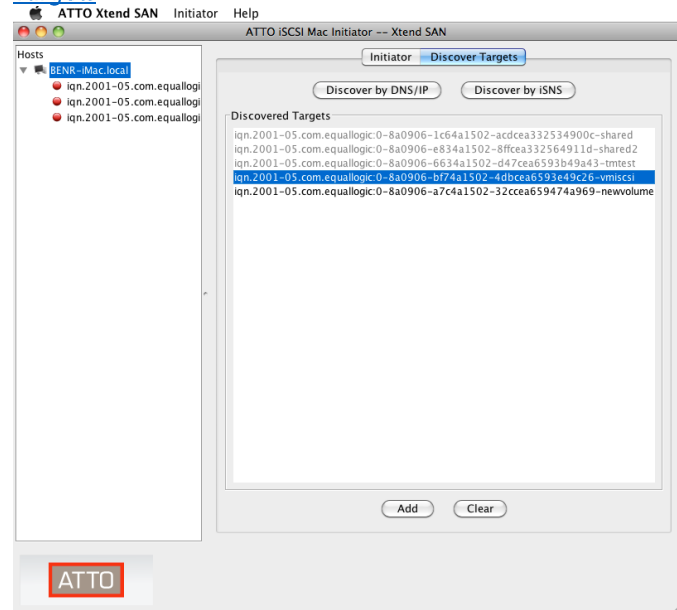


Add Targets

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

1. Targets are listed under **Discovered Targets** in the central panel. 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](#) or [DNS/IP discovery](#)

If you want to manage targets, continue to [Managing Targets](#)



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:

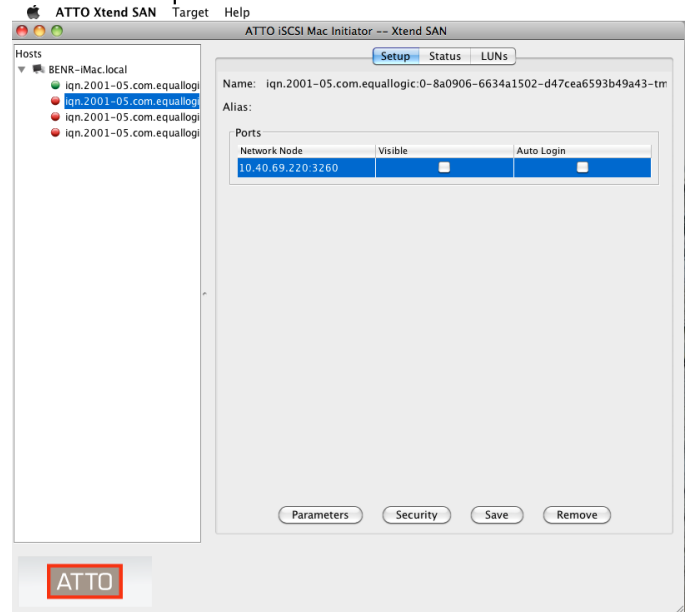
- Select target ports for connection.
- Specify automatic login at boot time.
- Connect to targets.
- Remove targets.
- Configure security for each target.
- View the iSCSI login parameters established during a connection.
- Configure iSCSI login parameters for each connection.
- View a list of LUNs 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**. Use the following instructions for the task you

wish to accomplish.



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.
 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.

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](#) 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.

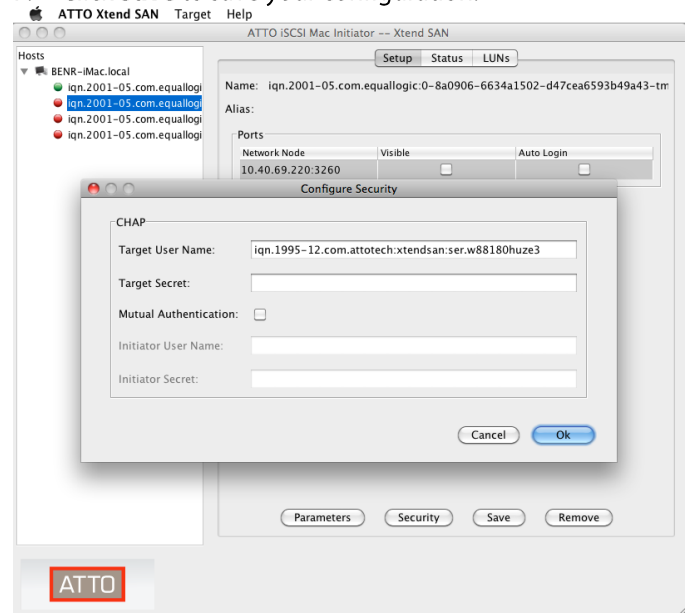
Be sure to have the secrets when configuring security. The ATTO iSCSI Initiator does not impose rules for formatting CHAP secrets. However, many iSCSI targets have formatting rules which determine the format of the ATTO iSCSI CHAP secrets. In general, secrets should follow these guidelines:

- 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.

5. Continue to manage additional targets or continue to Connect to targets.

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.



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.

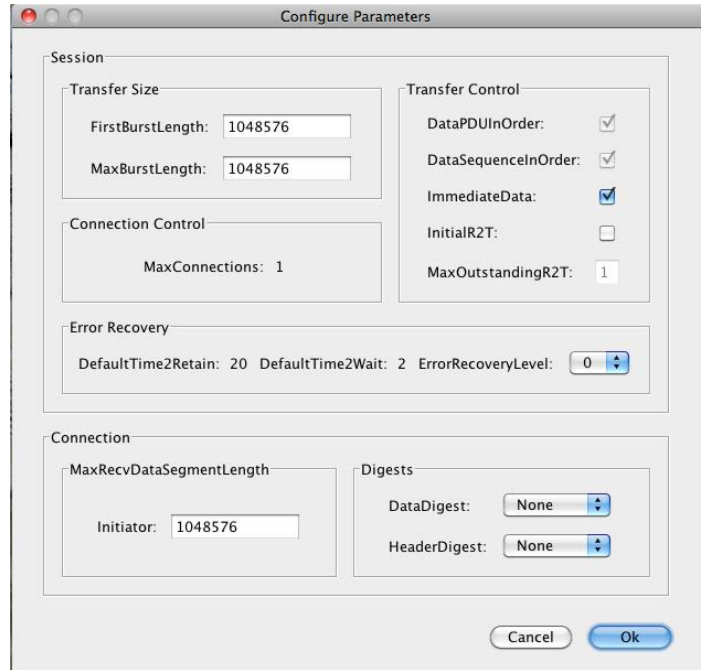
CAUTION Do not change any iSCSI negotiation parameters without extensive knowledge of the default values or specific instructions from ATTO Technology tech support.

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**.

The Configure Parameters screen appears.


- 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
4. Click **OK** when you have completed your choices.
 5. Click **Save** to save your configuration.

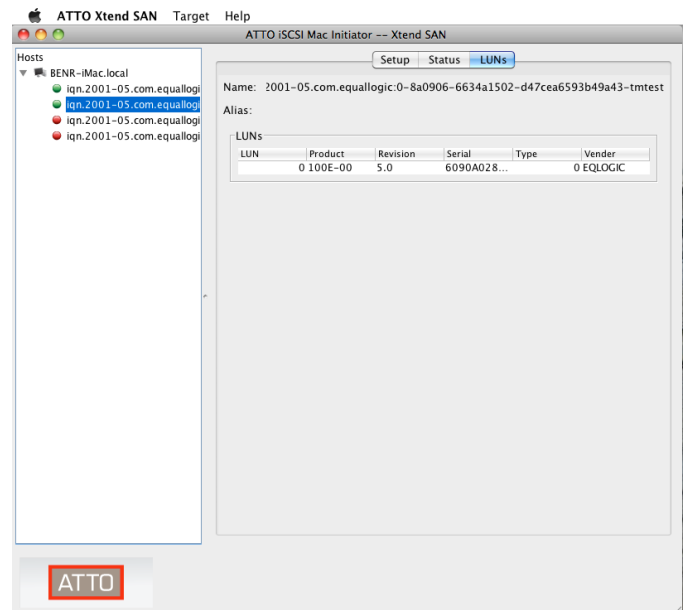
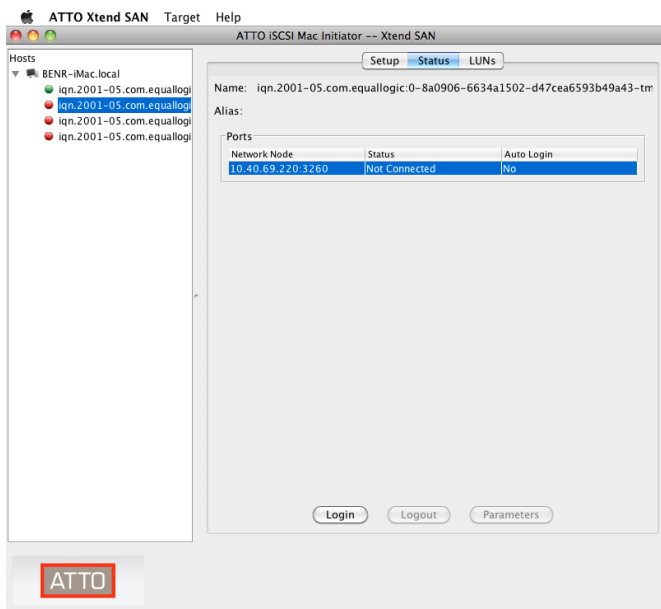
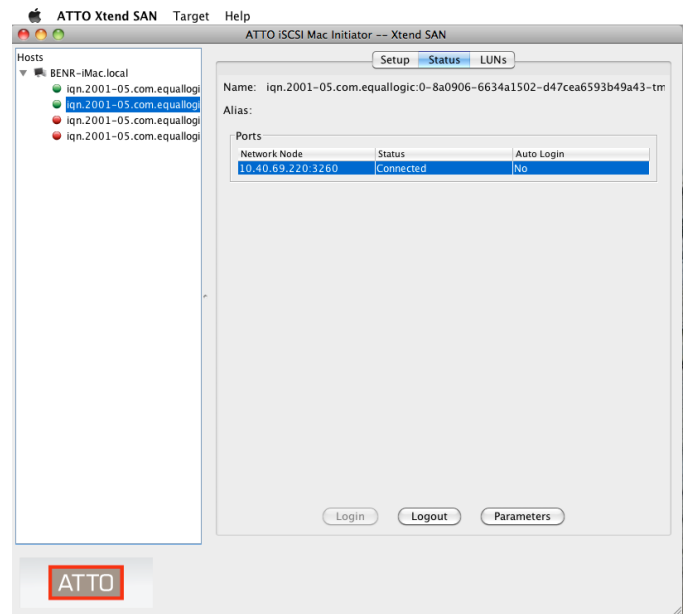


Connect to target

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.
 - 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.



Appendix A CLI Provides an ASCII-base Interface

Use CLI to automate access to multiple iSCSI targets.



Note *In order to use the Xtend SAN CLI functionality, a complete install is required to install the CLI. CLI is accessed in a normal OS X terminal window by typing `/usr/local/libexec/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.*

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.

Command	Example
addTargets	<code>xtendsancli addTargets 192.168.0.1 All</code>
discoverTargets	<code>xtendsancli discoverTargets -address 192.168.0.1</code>
getInitiatorName	<code>getInitiatorName</code>
getBootDelay	<code>getBootDelay</code>
Help	
listTargetsSetup	<code>xtendsancli listTargetsSetup -address 192.168.0.1 All</code>
listTargetsStatus	<code>xtendsancli listTargetsStatus -address 192.168.0.1 All</code>
loginTargets	<code>xtendsancli loginTargets -address 192.168.0.1 All</code>

logoutTargets	xtendsancli logoutTargets -address 192.168.0.1 All
removeTargets	xtendsancli removeTargets -address 192.168.0.1 All
setBootDelay	setBootDelay 30
setInitiatorName	setInitiatorName attofast
version	

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.*

Commands

addTargets[Options] -address <address> Target(s) Adds targets found at the address to the configuration. The targets' port that match the address will be visible after addition. The target must have been previously discovered. If a target has been previously added, an error message will be printed and the offending target will be omitted from the target addition process.

Options:

-autoLogin Controls whether an auto login occurs. If not specified, the default value is 'No'

-connection Overridden connection parameters

-session Overridden session parameters

-security The security parameters to use when logging into a target

-discoverySecurity The security parameters to use during discovery of the targets. Do not specify to use the same security parameters as when logging into a target. Specify NONE for the algorithm to specify security parameters when logging in only. Specify a security algorithm and parameters to use separate security parameters for logging into a target versus performing the discovery beforehand.

discoverTargets [OptionsOptions] -address <address>
Lists all of the iSCSI targets available at the specified address.

Options:

-isns Address parameter specifies an iSNS server

-security The security parameters if the address is NOT an iSNS server

-verbose Prints more detailed discovered target information

getInitiatorName [Options] Gets the initiator name for the host.

Options:

-verbose Prints more detailed initiator name information

getBootDelay Gets the number of seconds the daemon will wait before starting.



Note *This command should not be used unless otherwise directed to do so by ATTO Technical Support.*

help Writes the usage information to standard output.

listTargetsSetup [Options] Target(s) Writes the target setup information to standard output. The list will include only those targets that have been previously added to the iSCSI configuration whose target name(s) match the input target name(s).

Options:

-address Specifies a socket address to filter the target(s) by

-verbose Prints more detailed target setup information

Output Format (Non-Verbose): <Target Name><PortGroupTag> <Address:Port> <AutoLogin>

***** Name:
<Target Name> Port Group Tag: <Port Group Tag>
Address: <Address> Auto Login: <Auto Login>

Additional Notes:

- For non-verbose output, the spaces in-between the values will be tabs, unless a target has multiple connections, in which case the spaces in between the values may be a combination of spaces and tabs.
- Please see the command element specification for more detailed information about specifying specific targets.

listTargetsStatus [Options] Target(s) Writes the target status information to standard output. The status that is displayed will reflect the current connection status for the supplied target(s) whose name(s) match the input target name(s). The target information will be retrieved from the iSCSI configuration, unless a socket address is supplied. In this case, the target information will be obtained directly from the target.

Options:

-address Specifies a socket address to obtain target information from

-discoverySecurity specifies any security parameters required if they are required to perform a discovery to the target at the target address

-verbose Prints more detailed target status information

Output Format (Non-Verbose): <Target Name><PortGroupTag><Address:Port> <Connection Status>

Output Format (Verbose):
***** Name:

<Target Name> Port Group Tag: <Port Group Tag>
Address: <Address> Connection Status:
<Connection Status>

Additional Notes:


- For non-verbose output, the spaces in between the values will be tabs, unless a target has multiple connections, in which case the spaces in between the values may be a combination of spaces and tabs.
- A value of "true" for the <Connection Status> signifies that the initiator is connected to the target via the specified socket address.
- Please see the command element specification for more detailed information about specifying specific targets.

loginTargets -address <address> Target(s) Connects to a configured target.

logoutTargets -address <address> Target(s) Disconnects from a configured target.

removeTargets -address <address> Target(s) Removes the configuration for the target(s) that use the specified address. The target(s) must already be added before performing this command. If the input address is a saved address for the target(s), then all traces of the target(s) are removed from the configuration file.

setBootDelay <seconds> Sets the number of seconds the daemon will wait before starting. A value of 0 specifies a normal startup sequence.

 **Note** *This command should not be used unless otherwise directed to do so by ATTO Technical Support.*

setInitiatorName <name> Sets the initiator name for this host. Note that this operation will only set the suffix on the initiator name, i.e. the part of the initiator name after the 'xtendsan:' portion.

version Writes the version information to standard output.

Shared Common Elements

Target(s) Indicates the name of one or more iSCSI targets. If the special name "All" is specified, then all targets at the target address will be used. If a specific target name is specified, then only that target will be used at the target address. If more than one target name is specified, they are separated by whitespace.

Options

-address <address> Specifies the IP address or hostname to connect to. This may be in either IPv4 for IPv6 format, and a port specification is optional. If no port is specified, the default port of 3260 is used, unless the **-isns** option is also specified (which defaults to 3205).

Examples: IPv4:192.168.10.6
IPv4:192.168.10.6:3260
IPv6:fec0::9427::8d67::b6f3::3576
IPv6:[fec0::9427::8d67::b6f3::3576]:3260

autoLogin <Yes | No> Specifies if the Xtend SAN daemon should auto-matically login to the specified target upon system boot.

Examples: -autoLogin Yes

-connection <Option>,... Specifies the values that should be used when negotiating a connection to a target. Any combination of options are valid.

Options: DataDigest=<None | CRC32C>
HeaderDigest=<None | CRC32C>
MaxRecvDataSegmentLength=<Integer from 512 to 16777215>

Examples: -connection
DataDigest=CRC32C,MaxRecvDataSegmentLength=1024

-isns specifies that the address argument is an iSNS server.

-security <Protocol>,<Option>,... Specifies the security settings to use when connecting to a target.

Available Security Protocols: CHAP

Options: TargetUserName=<UserName>
TargetSecret=<Secret>
InitiatorUserName=<UserName>
InitiatorSecret=<Secret>
MutualAuthentication=<Yes | No>

Valid Option Combinations: [TargetUserName, TargetSecret] [TargetUserName, TargetSecret, InitiatorUserName, InitiatorSecret, MutualAuthentication]

Additional Notes:

- The CHAP parameter string must always be enclosed with the single quote character (') in order to prevent the shell from removing any characters. Please note that if any of the following characters appear in any of the parameter strings: (\), (,) they must be preceded by the escape sequence: (\). For example: 'TargetUserName=Exam\\p\,le' produces "TargetUserName=Exam\p,le"

Example: -security
CHAP,TargetUserName=example,TargetSecret=testSecret

-discoverySecurity <Protocol>,<Option>,... Specifies the security settings to use when performing a discovery to a target.

Available Security Protocols: NONE CHAP

Options: TargetUserName=<UserName>
TargetSecret=<Secret>
InitiatorUserName=<UserName>
InitiatorSecret=<Secret>
MutualAuthentication=<Yes | No>

Valid Option Combinations: [TargetUserName, TargetSecret] [TargetUserName, TargetSecret, InitiatorUserName, InitiatorSecret, MutualAuthentication]

Additional Notes:

- The CHAP parameter string must always be enclosed with the single quote character (') in order to prevent the shell from removing any characters. Please note that if any of the following characters appear in any of the parameter strings: (\), (,) they must be preceded by the escape sequence: (\). For example: 'TargetUserName=Exam\\p\,le' produces "TargetUserName=Exam\p,le".

Example: -security
CHAP,TargetUserName=example,TargetSecret=testSecret

- **session <Option>**,... Specifies the values that should be used when configuring a session for a target. Any combination of options are valid.

Options: ErrorRecoveryLevel=<0 | 1>
FirstBurstLength=<Integer from 512 to 16777215>
ImmediateData=<Yes | No> InitialR2T=<Yes | No>
MaxBurstLength=<Integer from 512 to 16777215>

Example: -session

ErrorRecoveryLevel=0,ImmediateData=Yes,MaxBurstLength=1024

-**verbose** Prints more detailed output to standard output while the command is being executed (if applicable).

Appendix B 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.