ATTO Xtend SAN® Software Troubleshooting Guide

The Power Behind the Storage

155 CrossPoint Parkway
Amherst, NY 14068

P. +1.716.691.1999
atto.com

04/2021 PRMA-xxxx-000

Table of Contents

Introduction to Xtend SAN

Xtend SAN is an iSCSI software initiator for macOS utilizing the iSCSI protocol to transmit information across Ethernet networks to iSCSI storage. It is a kernel-resident device driver that allows a Mac to function as an iSCSI client by using an existing network card (NIC) and the macOS network stack to emulate SCSI devices.

In General:

- Xtend SAN has no IP address, it is not a Network component.
- Xtend SAN relies on MacOS to provide all Networking functions.
- A valid IP address or DNS from the storage device must be provided to Xtend SAN.
- Xtend SAN is only capable of communicating with a Target IP address or DNS.
- Xtend SAN is unable to locate or detect targets on its own without connecting to an iSNS server or by a user who can manually provide a target IP address.
- Xtend SAN can only create a link through an already viable Network connection. Any failure of the OS, network or target will inhibit Xtend SAN functionality.
- Xtend SAN is not able to verify if a network connection is valid. It will only provide a warning message alerting to a dropped connection. Please be aware that Xtend SAN will fail if this is not corrected.
- Xtend SAN 5 and higher is only compatible and tested under macOS 10.11 or later.
- A PC running Mac OS software (Hackentosh) is not supported.
- Any non-standard install of the Mac OS is not supported. This can include: Boot Camp, Parallel, Virtual Box, Crossover Mac, emulation or even programs such as WINE.

This manual outlines some of the best practices for installing and configuring Xtend SAN as well as troubleshooting steps that can be taken to resolve common problems. Refer to the Xtend SAN Installation and Operations manual for further details.

Troubleshooting Techniques

Troubleshooting Techniques Intro

There are a few categories that failures can be placed in:

- **Hardware**: A component completely or intermittently fails.
- **Interoperability**: One or more devices in the system interpret the protocol specification different than the others resulting in undesirable behavior.
- **Design**: There is an error in the implementation of the software or firmware that prevents or limits functionality.
- **User Error**: The system is unable to achieve expected behavior due to improper installation or configuration or the desired behavior is simply not achievable due to unrealistic expectations.

Troubleshooting steps need to be taken to isolate hardware failures and user errors, which can easily be remedied by replacing a piece of hardware or changing a settings or parameters, whereas interoperability or design errors could require code changes and take considerable time to resolve.

Some of the following techniques may seem simplistic or overly obvious but these are the ones that are commonly overlooked and can take several hours of frustration to locate. It is important to try only one technique at a time. While changing multiple variables may seem to be a time saver, it usually complicates the troubleshooting process because if the problem goes away, there is no sure way of knowing what actually resolved it. Additionally, if the problem does re-occur, you may have actually fixed it with one change, but another change may have caused a similar symptom. The goal is to observe the issue and systematically isolate it to identify the least common factors that causes the issue to occur.

Observations

Take a step back and think about what is being observed. Ask the following questions. Note your answers as this can be very useful information for ATTO Tech support if you need to contact support.

- **What is the observed behavior compared to the expected behavior?**
  - Observe and report the overall "high level" problem as well as the details. For example, an overall problem may be that drives disappear during heavy I/O. The details would include any reported or logged any error when the problem occurred. Note time of day when the problem occurred as this can be useful in reviewing the time stamped logs.
- **Has the configuration been working and all of a sudden now fails?** If you can absolutely ensure that nothing has changed, the issue is most likely due to a hardware failure. However, there are some very subtle changes that could have been made that could affect overall system behavior. This often happens when more than one person has access to the system. Therefore, look very closely to see if you can find even the most minor change:
  - **Has the switch or storage firmware been upgraded?**
  - **Has the operating system been upgraded (is it setup for automatic updates)?**
  - **Has something been added or taken away? USB drive, HBA/NIC, video adapter, disk storage?**
  - **Has any software been installed, uninstalled, or updated?**
- **Is the problem repeatable? If yes, can it be repeated on a non-production test system?**
  - Collecting information such as system error logs is often needed. Since production systems are not generally set up to collect this information in normal operation, it is important to be able to configure the system to collect data and recreate the problem on a non-production test system.
- **What do the status LEDs indicate?** Note the behavior of NIC, switch, and storage LEDs as they are usually a good source of information towards identifying root cause. Refer to the appropriate product manuals to gain an understanding of what the LEDs indicate.

Frequently Asked Questions

1. **Is there a trial version of Xtend SAN?** There is no trial version of Xtend SAN.
2. **I purchased one license. How many installs can I do?** One install on one Mac.
3. **Where does Xtend SAN list it's Serial Number?** For security reasons there is no way to observe the Serial Number within the program.
4. **How do I mount with Xtend SAN?** There are no mounting features within Xtend SAN and the iSCSI protocol. The iSCSI LUN(s) will get mounted by MacOS once you format the drives.
5. **Is Xtend SAN compatible with my ISCSI storage or network switch?** Xtend SAN has been rigorously tested against products from leading iSCSI manufacturers. ATTO maintains a list of compatible products at: https://www.atto.com/support/interoperability/. Most other third party products are likely to work as well as long as they adhere to the iSCSI specifications. They just have not yet been tested by ATTO.
6. **Is Xtend SAN backwards compatible?** Supported OS's for versions of Xtend SAN are listed on the download page on the ATTO website.

1 Troubleshooting

Troubleshooting Xtend SAN application issues

1. Xtend SAN will not install. Refer to Appendix A Xtend SAN Installation Best Practices
2. Xtend SAN is successfully installed but will not open and I receive the following error: ***Unable to connect to daemon: connection refused. Nested exception: connection refused**,* and the application will not start.
    a. Reboot the Mac and try again.
    b. If a reboot does not work, try manually starting the daemon. Open ***Terminal*** and issue the following command:

    ```
    sudo launchctl load /Library/LaunchDaemons/com.attotech.iscsid.plist
    ```

    c. You can check to see if the daemon is running using this command in ***Terminal:***

    ```
    sudo ps aux | grep iscsid
    ```

    d. Reinstall Xtend SAN
    e. In the Xtend SAN directory in ***Applications*** use uninstall script to uninstall Xtend SAN
    f. Reboot
    g. Install Xtend SAN
    h. Reboot
3. If using MacOS Big Sur and the Xtend SAN application will not operate after installation, refer to Appendix B - Installing Xtend SAN in Big Sur

Contact ATTO Tech Support if you encounter any other Xtend SAN application issues.

Troubleshooting target connection issues

Cannot ping target

See Appendix C – Ping Test for ping procedure details

1. Verify the physical connections of the Network Adapter, Switches, cables, and target are all secure. Verify link LEDs are "on" where applicable.
2. Verify that you are using the correct IP address and subnetmask on the initiator and the target. Each device must have its own unique IP address. Duplicate IP addresses on the same network is not allowed and can cause many network wide issues. Verify both the target port and the client port are on the same subnet. The following is an example of an "incorrect" IP address configuration scheme followed by an example of a "correct" IP address scheme.

    Example 1:

    Target = 192.168.2.11

    Client = 192.168.3.50

Note that the target is on the ".2" subnet and the client is on ".3" subnet. In this case, the ping test will fail.

Example 2:

Target = 192.168.2.11

Client = 192.168.2.50

In this example, both target and client are on the ".2" subnet and therefore ,the ping test should pass.

3. Check switch/router settings.
    a. If possible, direct attach the target to the client. If the ping is successful, then there is a configuration issue with the switch.
    b. If you cannot remove the switch from the configuration, then set the switch ports to default "basic" settings.
4. If VLANs are configured on the network, verify proper configuration.
5. Disable the MacOS Firewall to see if that is blocking ping requests. Refer to Appendix D – MacOS Firewall
6. Confirm that all nodes (client, target, and switch ports) are using the same Ethernet frame size (MTU). Standard MTU = 1514 while many iSCSI targets use Jumbo MTU = 9000.
7. If you are still having issues with the ping test and discovery, then note any errors observed and include them when contacting ATTO support.

Cannot discover iSCSI target

1. Verify the Target is configured correctly.
    a. Make sure that the target is setup so that any client can discover it.
    b. Some targets provide Access Control Lists (ACLs) to prevent unwanted clients from discovering the targets. You will either need to disable the ACLs on the target or add the client PC to the ACL list on the target. Check with your target vendor on how to configure ACLs.
    c. Check to see if the target has "Discovery CHAP" enabled. If so, then you need either need to disable discovery CHAP on the target, or you need to configure discovery CHAP in Xtend SAN. Refer to your target's user manual for details on discovery CHAP. You will need the target's discovery CHAP secret to provide to Xtend SAN. Refer to Section 3 – Target Discovery in the Xtend SAN user manual.
2. If you are using an iSNS server for discovery of iSCSI devices on your network, then make sure iSNS is enabled in Xtend SAN. Refer to Section 3 – Target Discovery in the Xtend SAN user manual.
3. If you have a 2nd Mac running Xtend SAN on your network, try to see if the 2nd client can discover the iSCSI target. If so, then compare the "working" Mac to the "failing" Mac and note the differences.
4. Check NIC and iSCSI target requirements for MacOS Firewall and implement any required settings. Refer to Appendix D – MacOS Firewall

Login Errors

LUN 0 error

When attempting to Login in, the following message occurs:

Login failed: Driver failed login (0x5000001)

MacOS requires that the 1st iSCSI target is configured at LUN 0, otherwise login will fail with this error. Therefore, make sure the 1st iSCSI target LUN presented by your iSCSI target is set to LUN 0. Contact your target manufacturer on how to set LUN values in their application. The target LUN can be an actual disk target, or a target processor device.

Authentication error

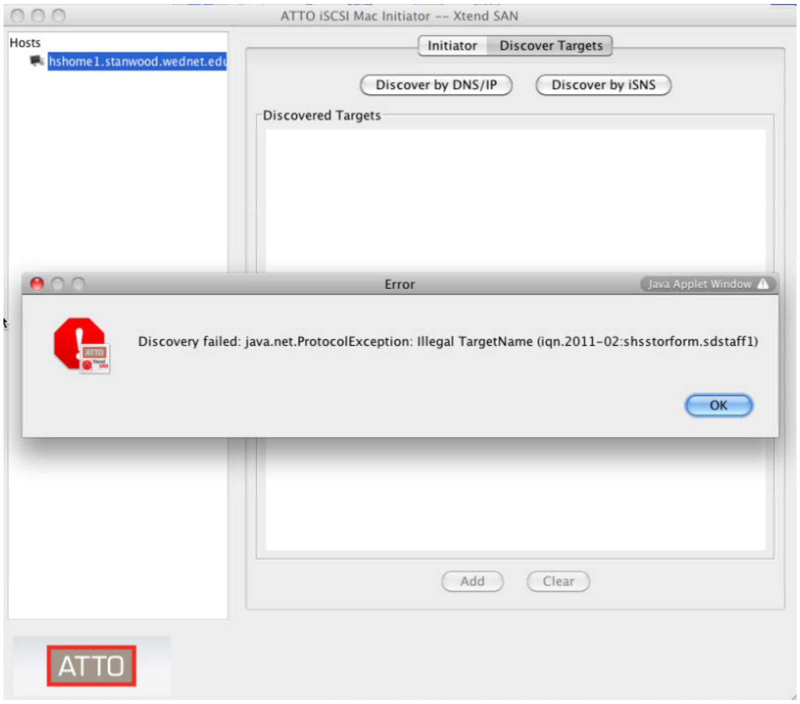
These types of errors typically mean that the target is requiring authentication to access the iSCSI target. Authentication is managed either through ACLs or using CHAP (Challenge Authentication Protocol).

a. **ACLs -** Some targets provide Access Control Lists (ACLs) to control what clients can access the iSCSI targets. You will either need to disable the ACLs or add the client PC to the ACL list in the target. Check with your target vendor on how to configure ACLs.

b. **CHAP -** Check to see if the target has CHAP enabled for target login. If so, then you either need to disable CHAP on the target (refer to iSCSI user manual), or you need to configure CHAP in Xtend SAN. Refer to your target's user manual for details on setting up CHAP. Refer to Section 4 – Managing Targets – Configure Security in the Xtend SAN user manual.

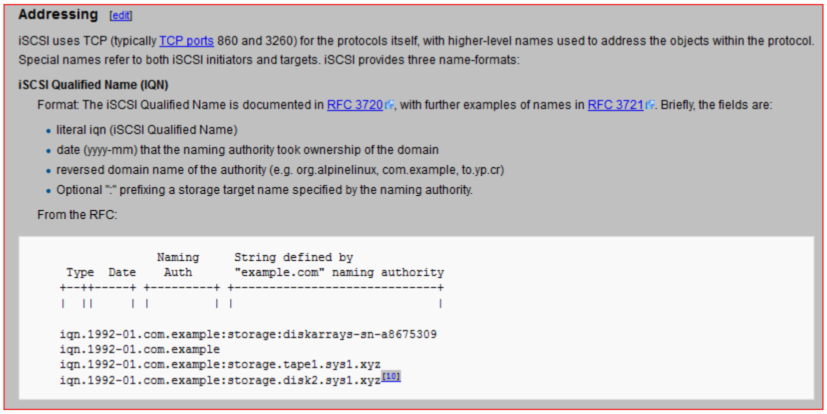
IQN Naming error

The error would look like the following:



Discovery failed: java.net.ProtocolException: Illegal TargetName (iqn.2011-02:shsstorform.sdstaff1)

An IQN name error is an incorrectly setup iSCSI qualified name string. The IQN name is a unique identifier to each iSCSI node whether it be the client (Xtend SAN) or the iSCSI target. If you receive this error, your target is presenting an invalid IQN address. You will need to contact your target manufacturer to see if there is a way to modify the target's qualified name string. The format of the IQN name is shown below taken from the iSCSI wiki.



Addressing [edit]

iSCSI uses TCP (typically TCP ports 860 and 3260) for the protocols itself, with higher-level names used to address the objects within the protocol. Special names refer to both iSCSI initiators and targets. iSCSI provides three name-formats:

iSCSI Qualified Name (IQN)

Format: The iSCSI Qualified Name is documented in RFC 3720, with further examples of names in RFC 3721. Briefly, the fields are:

- literal iqn (iSCSI Qualified Name)
- date (yyyy-mm) that the naming authority took ownership of the domain
- reversed domain name of the authority (e.g. org.alpinelinux, com.example, to.yp.cr)
- Optional ":" prefixing a storage target name specified by the naming authority.

From the RFC:

```
                Naming     String defined by
 Type  Date      Auth       "example.com" naming authority
+--++-----+ +---------+ +-----------------------------+
|  ||     | |         | |                             |

iqn.1992-01.com.example:storage:diskarrays-sn-a8675309
iqn.1992-01.com.example
iqn.1992-01.com.example:storage.tape1.sys1.xyz
iqn.1992-01.com.example:storage.disk2.sys1.xyz[10]
```

Auto login fails

In Xtend SAN, you can setup your target so that it will automatically login and mount the volume(s) on system reboot. If this fails, most likely the MacOS network stack is taking longer than expected to become ready. Xtend SAN does have a boot delay option that will allow you to change how long the Xtend SAN daemon will wait before loading. The boot delay option can only be set via the Xtend SAN CLI tool. If you did a "complete install" of Xtend SAN, then you should have an application called "Xtend SANcli" located in "/usr/local/libexec". If you do not see Xtend SANcli in that location, you will have to run the Xtend SAN installer and reinstall Xtend SAN using the "Complete Install" option.

To set the boot delay:

1. Open terminal and change to the following directory:
   cd /usr/local/libexec
2. Execute the following command. Note that "setBootDelay" is case sensitive so you must use upper case "B" and "D" and the reset is lower case.
   ./Xtend SANcli setBootDelay 10
3. Reboot and see if that resolves the auto login problem. If not, repeat these steps and increase the delay to 15, then 20, then 25, and so on until you find the best delay time.
   a. If you encounter any other errors during iSCSI target login, note the error and contact ATTO Technical support.

Appendix A – Xtend SAN Installation Best Practices

Most issues with Xtend SAN occur during software installation or when trying to connect to the iSCSI targets. The following tips will help guide you through the process especially with newer versions of macOS that use Gatekeeper.

Note: You cannot install Xtend SAN remotely. Gatekeeper will cause problems if this is attempted.

Prepare Xtend SAN program

1. Download Xtend SAN. Use only the most recent from the ATTO Website
2. Using the serial number provided, activate your Xtend SAN license here
3. Remember to keep track of the license, the tmp file, or the original e-mail from ATTO in case you need to reinstall the application at a later date.

Prepare macOS

1. It is highly recommended to disable any OS Power Management, Hibernation, Energy Saver, Computer Sleep, or Hard Disk Sleep function.
2. Newer versions of the macOS can be a little sensitive when installing new drivers. To reduce potential install issues with Xtend SAN, it is strongly recommended to disconnect or disable any unnecessary hardware or applications.
3. It is recommended to temporarily disable your Mac's WiFi until after installation is complete.

Install Xtend SAN

Note
If installing on MacOS Big Sur, go to Appendix B – Installing Xtend SAN in Big Sur

1. Open the osx_app_Xtend SAN_xxx.dmg (where xxx is the version number). A finder window should open with the Xtend SAN installer (***Xtend SAN_xxx***) and the ***Xtend SAN Manual.pdf***
2. Run ***Xtend SAN_xxx***

   a. Enter your macOS admin password when prompted.
   b. If prompted, allow the installer to run.
   c. Choose type of installation
      a) ***Typical*** = Application only
      b) ***Complete*** = Application + CLI tools (Recommended)
   d. Enter the Authorization Code.
      a) either by dragging & dropping *attolicensexyz123*.tmp
      b) or by manually entering the requested information

Note
You must manually enter the data for macOS 10.15 or later

   e. Finish by clicking "Next".

3. Open ***System Preferences*** then click ***Security & Privacy***. Click the ***General*** tab. If you see a message stating that an ATTO driver is trying to be loaded and you see a greyed out ***Allow*** button, then click the ***Lock*** icon at the bottom left

and enter the admin password. The ***Allow*** button should become active so click the button. Note that if the ***Allow*** button is not shown continue to step 4, then try step 3 after the reboot.

4. Reboot the system.

⚠ CAUTION *Refrain from opening Xtend SAN until you have done a reboot after installation. The Xtend SAN daemon may not automatically start after installation.*

After reboot

1. If the **Allow** option was not available before reboot, repeat step 3 in the procedure above.
2. Locate Xtend SAN in the Applications director and launch the program.
3. Once Xtend SAN is successfully opened, reattach any 3rd Party devices.

Suggested actions if installation fails or if *Allow* command icon is not available

1. Perform a second power cycle and try again. Sometimes the first time does not catch.
2. Perform a hard power cycle as follows if any install complications or failures occur.

    a. Shutdown Mac normally using Apple > Shutdown option. Do not use the power button or any other method to Force Quit.
    b. Wait 20 – 30 seconds.
    c. Remove Power Cord from the Mac and keep it removed for at least 2 minutes. (NOTE: This step will only work on Mac systems that do not run on a battery).
    d. Reattach power and boot system.

3. We have observed rare but occasional issues with installing Xtend SAN under the following conditions. Try to eliminate these variables if issues continue to occur.

    a. Disconnect any targets attached during install.
    b. Disconnect any transmitters of any kind (i.e. mice transmitters, Bluetooth Headset, USB Firestick, etc.)
    c. Connect monitors directly to the Mac. Do not connect the monitor via KVM's.

Appendix B - Installing Xtend SAN in MacOS Big Sur

With the release of macOS Big Sur, Apple has deprecated the socket we use to plug the ATTO Xtend SAN virtual SCSI driver into their kernel. In the past, Apple allows the user to "allow" the use of the driver but this option is not available in Big Sur.

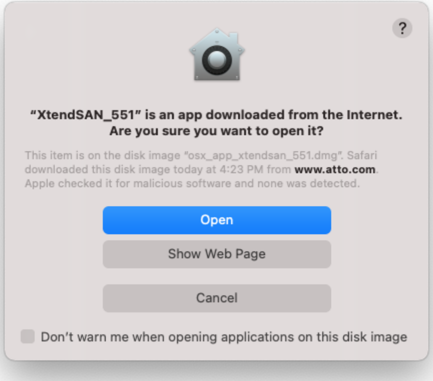
In order to support our customers who want to use Xtend SAN in Big Sur, we have found a work around which will allow the Xtend SAN driver to load. After running the Xtend SAN installer, perform the following procedure.

Note ***You may need a wired USB Keyboard for this procedure***

Note ***If this is a fresh install of Big Sur, then you do not need to pre-install Xtend SAN prior to running this procedure. Perform the initial install in step 6.***

1. Fully power off your Mac.
2. Enter recovery mode **-** Power on the Mac and immediately press and hold the ***Command (⌘)*** + ***R*** keys until you see the Apple logo, spinning globe, or other startup screen.
3. Click the ***Utilities*** menu and select ***Terminal***.
4. Enter the following commands in ***Terminal***
5. spctl kext-consent add FC94733TZD
6. Reboot the Mac
7. Install/Reinstall Xtend SAN. The file can be redownloaded here

If you downloaded Xtend SAN from the ATTO website, you will see the following prompt. Click ***Open***.

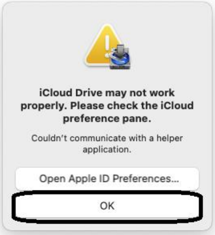


"XtendSAN_551" is an app downloaded from the Internet.
Are you sure you want to open it?

This item is on the disk image "osx_app_xtendsan_551.dmg". Safari downloaded this disk image today at 4:23 PM from **www.atto.com**. Apple checked it for malicious software and none was detected.

?
Open
Show Web Page
Cancel
□ Don't warn me when opening applications on this disk image

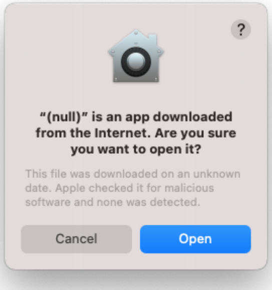
When you start the Xtend SAN installer, macOS will prompt you with the following warning. Select ***OK*** to proceed with the install.



iCloud Drive may not work properly. Please check the iCloud preference pane.

Couldn't communicate with a helper application.

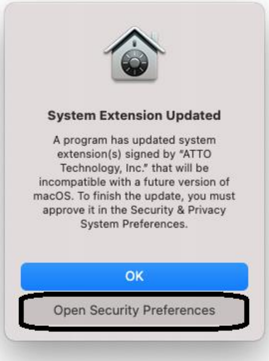
MacOS may also prompt you with the following warning. Select ***Open*** to proceed with the install.



"(null)" is an app downloaded from the Internet. Are you sure you want to open it?

This file was downloaded on an unknown date. Apple checked it for malicious software and none was detected.

8. **<u>Allow Xtend SAN driver to load</u>** – When Xtend SAN installation completes, you may see a pop up window similar to the following warning you that the ATTO driver could not load. Click **Open Security Preferences.**

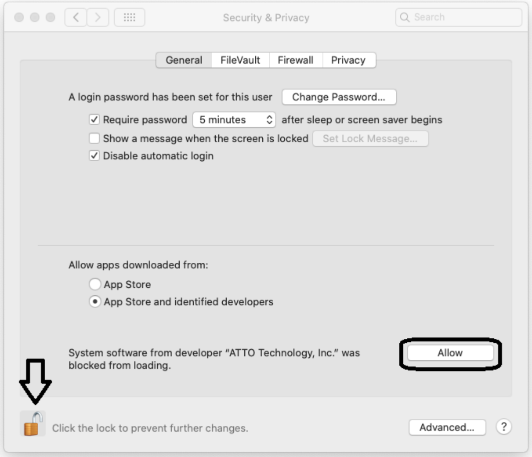


System Extension Updated

A program has updated system extension(s) signed by "ATTO Technology, Inc." that will be incompatible with a future version of macOS. To finish the update, you must approve it in the Security & Privacy System Preferences.

If you do not get the pop up window, you can manually get to this location by opening ***System Preferences*** then click ***Security & Privacy***.

Once you are in ***Security &*** Privacy, click the ***General*** tab and then click the ***Lock*** icon at the bottom left of the page and enter the system admin and password. Once the page is unlocked, the ***Allow*** icon should become active. Click the ***Allow*** icon then reboot the workstation.



A login password has been set for this user

☑ Require password 5 minutes after sleep or screen saver begins

☐ Show a message when the screen is locked

☑ Disable automatic login

Allow apps downloaded from:

○ App Store

● App Store and identified developers

System software from developer "ATTO Technology, Inc." was blocked from loading.

Click the lock to prevent further changes.

9. After the reboot completes, Xtend SAN should operate normally at this point.

Appendix C - Ping Test

Xtend SAN is dependent on a valid Ethernet connection between the initiator and the iSCSI target. A ping is a command that can be manually typed into a terminal window on a host computer to verify a connection to another device.

1. Open a Terminal
2. Enter the Command: ping <IP_Address_of_target_device>

Example of successful ping test

Example: *ping 192.168.25.220*

Response:

```
PING 192.168.25.220 (192.168.25.220): 56 data bytes
64 bytes from 192.168.25.220: icmp_seq=0 ttl=255 time=0.316 ms
64 bytes from 192.168.25.220: icmp_seq=1 ttl=255 time=0.210 ms
64 bytes from 192.168.25.220: icmp_seq=2 ttl=255 time=0.196 ms
64 bytes from 192.168.25.220: icmp_seq=3 ttl=255 time=0.201 ms
64 bytes from 192.168.25.220: icmp_seq=4 ttl=255 time=0.170 ms
^C
- - - 192.168.25.220 ping statistics - - -
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.170/0.219/0.316/0.050 ms
```

Example of a failed ping test

Example: *ping 192.168.25.100*

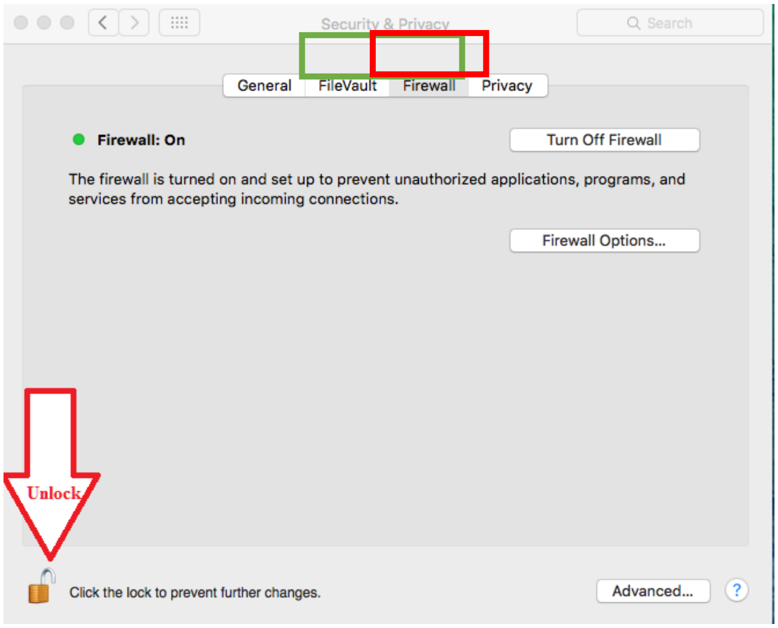
Response:

```
PING 192.168.25.100 (192.168.25.100): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
^C
--- 192.168.25.100 ping statistics ---
11 packets transmitted, 0 packets received, 100.0% packet loss
```

Appendix D - MacOS Firewall

To modify MacOS Firewall settings:

1. Open System Preferences
2. Click Security & Privacy
3. Click the Firewall Tab
4. Click the Lock on the bottom left and provide admin password when prompted.
5. Enable/Disable firewall as necessary.



● **Firewall: On**

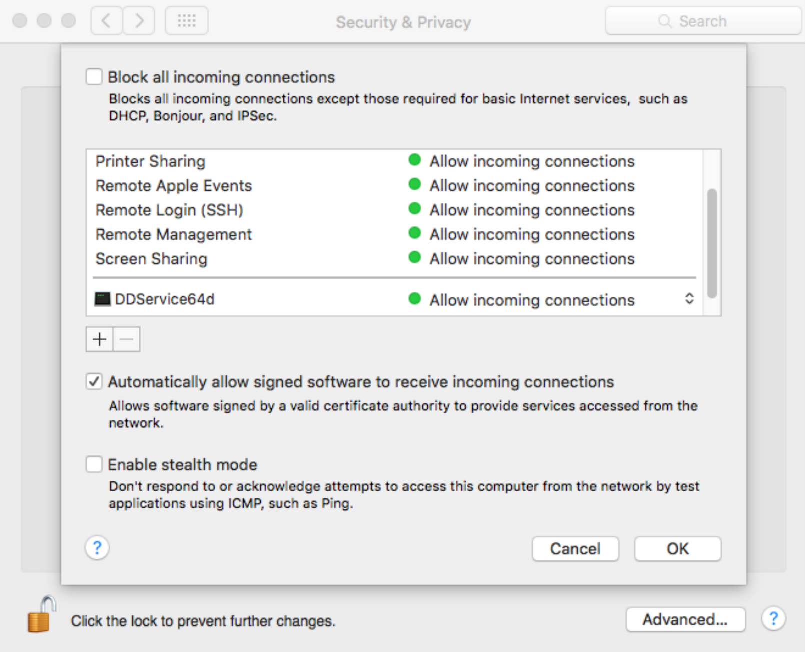
The firewall is turned on and set up to prevent unauthorized applications, programs, and services from accepting incoming connections.

Click the lock to prevent further changes.

In some unique 3rd party hardware cases it is required to actually Turn ON Mac OS Firewall. If this is the case, click **Firewall Options**

6. Modify or add policies per 3rd party hardware requirements. For any assistance, contact the 3rd party hardware vendor.

ATTO does not maintain any 3rd party macOS Firewall settings.



☐ Block all incoming connections
Blocks all incoming connections except those required for basic Internet services, such as DHCP, Bonjour, and IPSec.

Printer Sharing	● Allow incoming connections
Remote Apple Events	● Allow incoming connections
Remote Login (SSH)	● Allow incoming connections
Remote Management	● Allow incoming connections
Screen Sharing	● Allow incoming connections
DDService64d	● Allow incoming connections

☑ Automatically allow signed software to receive incoming connections
Allows software signed by a valid certificate authority to provide services accessed from the network.

☐ Enable stealth mode
Don't respond to or acknowledge attempts to access this computer from the network by test applications using ICMP, such as Ping.

Click the lock to prevent further changes.