Tiger Client 2.9.3
User's Guide

September 29, 2023

Title:	Tiger Store Client User’s Guide
Software version:	Tiger Store Client 2.9.3
Date:	September 29, 2023

This guide provides you with instructions for installing and setting up the Tiger Client software on your computer in order to mount and work with volumes managed by a Tiger Store storage server on the same network.

Once you install the Tiger Client software, you can use the Tiger Client tray application (Windows), the menulet (Apple Mac) or command-line interface (Linux) to:

• create a list of the Tiger Store storage servers on your network (see "Create a List of Tiger Store Storage Servers" on page 10).

• connect to and disconnect from storage servers on your list and mount/dismount the volumes they share (see "Connect/Disconnect from Tiger Store" on page 12).

• overwrite the volume mount location on Windows Tiger Client (see "Overwrite The Volume Mount Location (Windows)" on page 15).

• view connection status (see "View Connection Status" on page 17).

• easily access Tiger Store's web interface (see "Access the Tiger Store Web Interface" on page 14).

Install and Uninstall the Tiger Client Software

Minimum System Requirements

Each system that you want to connect to Tiger Store as a Tiger Client must meet the following minimum system requirements:

Apple Mac:

• Apple Mac computer with 1.33-GHz CPU.

• Mac OS X El Capitan (64-bit), macOS Sierra (64-bit), macOS High Sierra (64-bit), macOS Mojave (64-bit), macOS Catalina (64-bit), macOS Big Sur (64-bit Intel and ARM); macOS Monterey (64-bit Intel and ARM); macOS Ventura (64-bit Intel and ARM);

> **Note:** *No support for Mac OS X versions below 10.11.*
>
> **Important:** *To be able to install and run the Tiger Client software on an ARM-based macOS, you must first allow the user management of kernel extensions, following the steps in "Allow the User Management of Kernel Extensions on Apple Silicon macOS" on page 21.*

• 2 GB of physical RAM at least.

• 25 MB of available hard-disk space for Tiger Client software installation.

• 4Gb/8Gb FC, 10GbE and/or 1GbE adapter for connection to the storage.

• Network LAN connection (1Gb at least) for public communication.

• The following TCP ports - 3000, 3001, 8555, 9120, 9121, 9122, 9123, 9124, 9125, 9126, 9127 - should not be blocked by a firewall if any.

Windows:

• PC with 1.33-GHz processor.

• Windows® 8/Server 2012/Server 2012 R2, Windows® 10/Server 2016/Server 2019, Windows® 11/Server 2022.

• 2 GB of physical RAM at least.

• 25 MB of available hard-disk space for Tiger Client software installation.

• 4Gb/8Gb FC, 10GbE and/or 1GbE adapter for connection to the storage.

• Network LAN connection (1Gb at least) for public communication.

• The following TCP ports - 3000, 3001, 8555, 9120, 9121, 9122, 9123, 9124, 9125, 9126, 9127 - should not be blocked by a firewall if any.

• The GlobalSign certification authority's currently used root certificate must be installed on the computer and its "Code Signing" purpose must not be disabled. For more information, refer to "Digital Certificate Requirements" on page 6.

Linux:

• PC with 1.33-GHz Intel processor.

• Red Hat Enterprise Linux 7.x and derivatives:

  • 3.10.0-327.el7.x86_64

  • 3.10.0-327.36.3.el7.x86_64

  • 3.10.0-514.el7.x86_64

  • 3.10.0-514.16.1.el7.x86_64

  • 3.10.0-514.26.2.el7.x86_64

  • 3.10.0-693.el7.x86_64

  • 3.10.0-693.11.6.el7.x86_64

  • 3.10.0-862.3.2.el7.x86_64

  • 3.10.0-862.9.1.el7.x86_64

  • 3.10.0-957.el7.x86_64

  • 3.10.0-957.27.2.el7.x86_64

- 3.10.0-1062.el7.x86_64
- 3.10.0-1062.7.1.el7.x86_64
- 3.10.0-1127.el7.x86_64
- 3.10.0-1127.10.1.el7.x86_64
- 3.10.0-1127.19.1.el7.x86_64
- 3.10.0-1160.el7.x86_64
- 3.10.0-1160.2.1.el7.x86_64
- 3.10.0-1160.81.1.el7.x86_64

Important: *To ensure against kernel panic on RHEL 7.5 and above, before installing the Tiger Client driver disable the hardened usercopy checks for the boot. For sample steps refer to* *"Disable Hardened Usercopy Checks on Red Hat Enterprise Linux and Derivatives" on page 19.*

- Red Hat Enterprise Linux 6.x and derivatives:
  - 2.6.32-220.el6 (64-bit)
  - 2.6.32-220.23.1.el6 (64-bit)
  - 2.6.32-279.el6 (64-bit)
  - 2.6.32-358.el6 (64-bit)
  - 2.6.32-358.23.2.el6 (64-bit)
  - 2.6.32-431.el6 (64-bit)
  - 2.6.32-431.3.1.el6 (64-bit)
  - 2.6.32-573.3.1.el6 (64-bit)
  - 2.6.32-573.7.1.el6 (64-bit)
  - 2.6.32-642.1.1.el6 (64-bit)
  - 2.6.32-642.3.1.el6 (64-bit)
  - 2.6.32-642.15.1.el6 (64-bit)
  - 2.6.32-696.6.3.el6 (64-bit)
  - 2.6.32-220.27.1.el6.x86_64 (64-bit)
- SUSE Linux 11 and derivatives:
  - 2.6.32.12-0.7-default (64-bit)
  - 3.0.80-0.7-default (64-bit)

- 3.0.13-0.27-default (64-bit)
- 3.0.76-0.11-default (64-bit)

Important: *Changing any of the default kernel setting may prevent Tiger Client from operating properly.*

Tip: *To check the exact version of the kernel used by your system, in command-line execute the following:* `uname -a`

Note: *Both uni and multiprocessor versions of the kernels are supported.*

• SELinux should be disabled prior to installing the Tiger Client software.

• 2 GB of physical RAM at least.

• 25 MB of available hard-disk space for installation.

• 4Gb/8Gb FC, 10GbE and/or 1GbE adapter for connection to the storage.

• Network LAN connection (1Gb at least) for public communication.

• The following TCP ports - 3000, 3001, 8555, 9120, 9121, 9122, 9123, 9124, 9125, 9126, 9127- should not be blocked by a firewall if any.

Digital Certificate Requirements

The Windows Tiger Client driver uses a digital certificate issued by GlobalSign certification authority. For the digital certificate to be verified upon installing the Tiger Client driver, the following certificates must be installed in the Trusted Root Certification Authorities of the Certificate Manager on the computer and their "Code Signing" purpose must not be disabled:

• R3 GlobalSign Root Certificate from GlobalSign

• R6 GlobalSign Root Certificate from GlobalSign

• DigiCert Assured ID Root CA from DigiCert

On computers operating in less restrictive environments, this is done automatically during installation of the Windows Tiger Client driver. If the computer, on which you want to install the Tiger Client driver operates in a more restrictive domain environment or is not connected to the Internet, you must manually download the currently used R3 GlobalSign Root Certificate from GlobalSign and install it yourself, before installing the Tiger Client driver. In addition, you must ensure that the "Code Signing" purpose of the root certificate is enabled.

Install the Tiger Client Driver

Important: *It is advisable to remove any other SAN management or device filter software prior to installing the Tiger Client driver. All Tiger Client computers must run the same version of the software as the Tiger Store storage server.*

To download and install the Tiger Client software (Apple Mac and Windows):

1. In a web browser, do one of the following:

   • type the IP address of the Tiger Store storage server for your network connection;

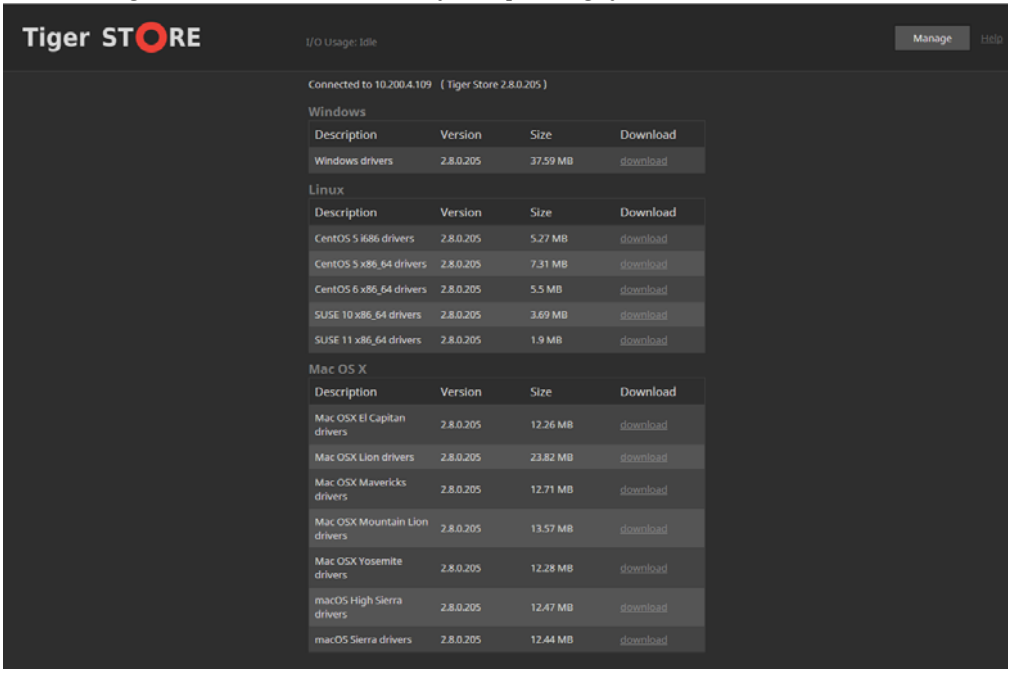
   Note: *If your Tiger Store storage server is comprised of two server nodes, you can type the IP address of any of the server nodes as long as it is online.*

   • type the domain name of the Tiger Store storage server;

   Important: *A DNS server on the network must resolve the IP address of the appliance to its domain name.*

2. Press Enter.

3. Find the Tiger Client installation file for your operating system and click Download.



4. When the installation file downloads to your computer, double-click it to start the installation.

   Note: *On macOS Catalina, to start the Tiger Client installation you may have to control-click it in Finder, choose Open from the menu, and then click Open in the dialog that appears.*

5. Follow the on-screen instructions and when prompted, restart your computer.

Note: *On Apple Mac, if prompted, confirm that you allow the loading of the Tiger Client kernel extensions.*

On Apple Mac and Windows, the Tiger Client icon appears in the Menu Bar/System Tray of your computer.

Important: *On Apple Mac, if the Tiger Client icon does not appear in the Menu bar, you should manually allow the Tiger Client software in the General tab of the Security & Privacy window in System Preferences.*

To download and install the Tiger Client software (Linux):

1. In a web browser, do one of the following:

   • type the IP address of the Tiger Store storage server for your network connection;

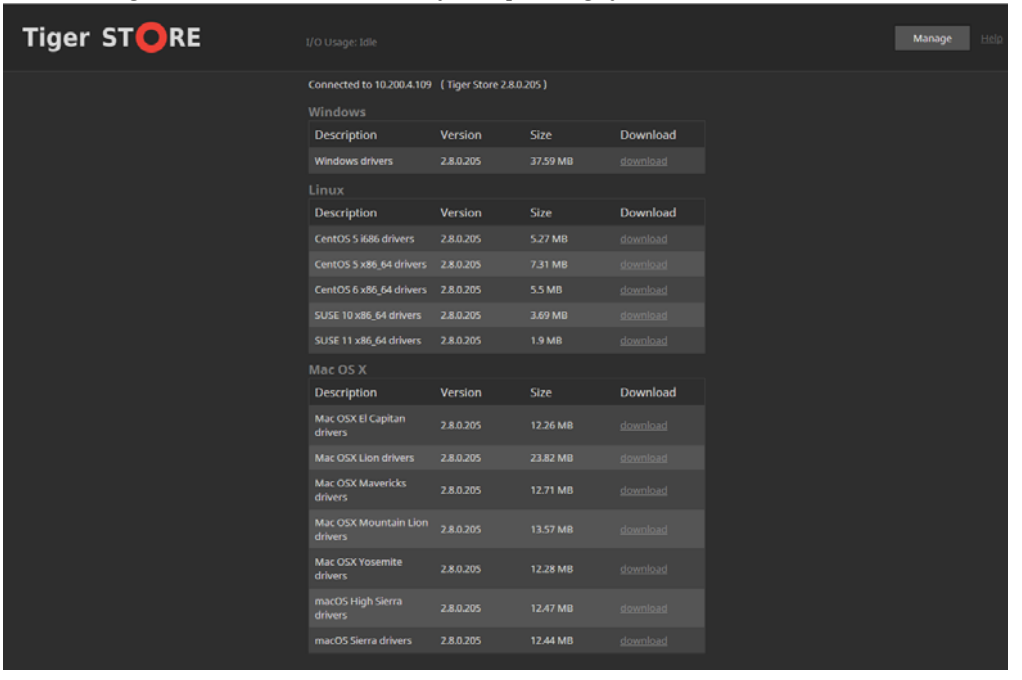
   Note: *If your Tiger Store storage server is comprised of two server nodes, you can type the IP address of any of the server nodes as long as it is online.*

   • type the domain name of the Tiger Store storage server;

   Important: *A DNS server on the network must resolve the IP address of the appliance to its domain name.*

2. Press Enter.

3. Find the Tiger Client installation file for your operating system and click Download.



4. When the installation file downloads to your computer, log on to the Linux system as root.
5. In command-line, type:
   `rpm -i <path to the Tiger Client software .rpm file>`
6. Press Enter.
7. In command-line, execute the following as root:
   `/etc/init.d/tboxd start`

   Important: *On Red Hat Enterprise Linux/CentOS Linux 7 it is advisable to take measures against double mounts, following the steps in "Prevent Double Mounts on Red Hat Enterprise Linux/CentOS Linux 7 Tiger Clients" on page 22.*

Uninstall the Tiger Client Driver

To uninstall the Tiger Client software (Windows):

1. In Control Panel, double-click Programs and Features.
2. Right-click Tiger Client and select Uninstall.

   You are prompted to confirm that you want to remove the Tiger Client software.
3. Click Yes, to confirm.

   Tiger Client uninstallation warns you that you will have to reboot the computer to complete the uninstallation.
4. Click OK.
5. When prompted, restart the computer.

To uninstall the Tiger Client software (Apple Mac):

1. Go to Applications | Tiger Client.
2. Double-click Uninstall.
3. Provide administrator's user name and password.
4. When prompted, confirm that you want to uninstall the Tiger Client software.

To uninstall the Tiger Client software (Linux):

1. Log on to the Linux system as root.
2. In command-line, type:
   `rpm -e Tiger-Client`
3. Press Enter.

Connect and Disconnect to Tiger Store

You should create a list of all available storage servers and then connect/disconnect to any of them in order to mount and work with the volumes they are sharing.

On Tiger Store storage servers with high availability add-on, there's no need to add both server nodes to the storage servers list. Should the node you have added to the list fail, the connection is automatically redirected to the other available Tiger Store node, which takes over sharing and supervising the volumes.

You can manage the Tiger Store storage server(s) on your computer using the Tiger Client application for your operating system:

• the tray application (Windows);

• the menulet (Apple Mac);

• the command-line interface (Linux).

Create a List of Tiger Store Storage Servers

Once you create a list of the available storage servers, you can connect and disconnect to any of them in order to mount/dismount the volumes they manage.

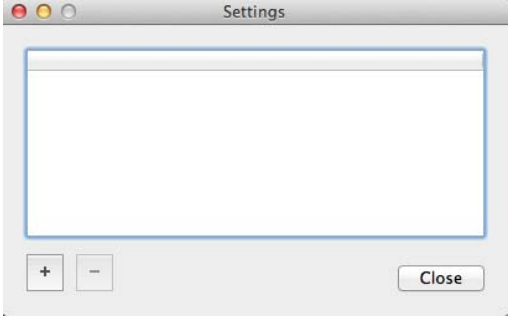
Important: *On LAN clients, always add the Tiger Store storage server to the storage servers list with the IP address set for the faster connection, if there is such.*

Should a Tiger Store administrator change the name or IP address of a Tiger Store appliance on your list, you may have to add anew that storage server to your list, in order to connect to it and mount its volumes. You may also have to re-add a Tiger Store storage server with two server nodes to the list, if at the time of adding it, the IP address of only one of its nodes has been set.

To add a Tiger Store storage server to the list (Apple Mac and Windows):

1. Click the Tiger Client tray/menulet icon and then click Settings.

   The Settings dialog appears. It lists all already added storage servers.

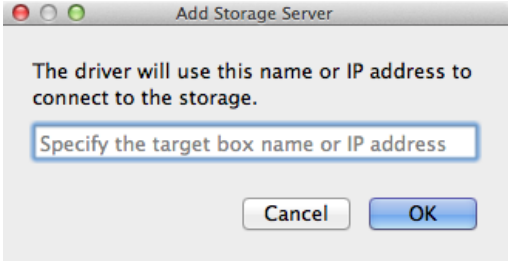


2. Do one of the following:

   • (Windows) Click Add.

   • (Apple Mac) Click the "+" button.

   The Add Storage Server dialog appears.



3. Enter the name or IP address of the Tiger Store storage server.

   Note: *For Tiger Store storage servers with two server nodes, at least one of the nodes must be online.*

4. Click OK.

   The storage server appears in the list.

To add a Tiger Store storage server to the list (Linux):

1. In command-line, type:

   `smct -a [name or IP address]`

   where `[name or IP address]` is the name or IP address of the Tiger Store storage server.

   Note: *For Tiger Store storage servers with two server nodes, at least one of the nodes must be online.*

2. Press Enter.

   If you have successfully added the storage server to the list, the Tiger Client software automatically attempts to mount the volumes it shares on your computer.

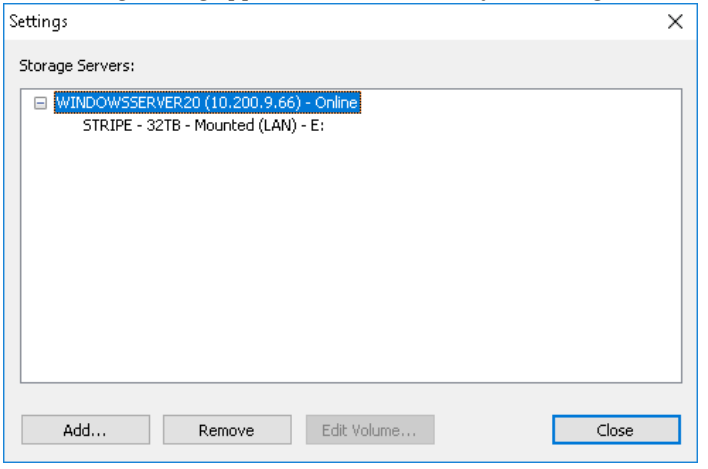
   Tip: *To view all storage servers added to the list on your computer, type* `smct -l` *and press Enter.*

To remove a Tiger Store storage server from the list (Apple Mac and Windows):

Important: *After you remove a Tiger Store storage server from the list, volumes shared by it are automatically dismounted from your computer.*

1. Click the Tiger Client tray/menulet icon and then click Settings.

   The Settings dialog appears. It lists all already added Tiger Store storage servers.



2. Select the storage server you want to remove from the list and do one of the following:

   • (Windows) Click Remove.

   • (Apple Mac) Click the "-" button.

3. Confirm that you want to remove the storage server from the list.

4. (optional, if clients restriction is enabled on Tiger Store) Enter the Tiger Store administrator's password in the dialog, which shows and then click OK.

   The storage server is removed from the list and its volumes are dismounted from your computer.

To remove a Tiger Store storage server from the list (Linux):

1. In command-line, type:
   `smct -r [name or IP address of the Tiger Store storage server]`

   Tip: *To view all appliances added to the list on your computer, type* `smct -l` *and press Enter.*

2. Press Enter.

3. (optional, if clients restriction is enabled on Tiger Store) Enter the Tiger Store administrator's password when prompted and then press Enter.

Connect/Disconnect from Tiger Store

When you connect to a storage server on your list, you mount the volume(s) it shares to Tiger Clients. Vice versa, when you disconnect from a storage server, you automatically dismount the volumes it shares. Note that when you disconnect from a storage server, you lose all unsaved information on the shared volumes.

To connect to a Tiger Store storage server (Apple Mac and Windows):

1. Click the Tiger Client tray/menulet icon and then click Connect/Disconnect.
2. Click a disconnected storage server (a storage server without a check mark in front of its name/IP address) to connect to it.

   The volumes this storage server shares for your computer are mounted.

   Important: *If a volume with enabled support for Tiger Spaces is set to be hidden in the web interface of Tiger Spaces, this volume will not mount on your computer, when you connect to the storage server.*

To connect to a Tiger Store storage server (Linux):

1. In command-prompt, type:
   `smct -c [number/host/IP address]`

   where `[number/host/IP address]` is the IP address of the storage server or its number in your list of appliances.
2. Press Enter.

   Tip: *To connect to all storage servers on your list, type* `smct -c all` *and press Enter.*

   Important: *If a volume with enabled support for Tiger Spaces is set to be hidden in the web interface of Tiger Spaces, this volume will not mount on your computer, when you connect to the storage server.*

To disconnect from a Tiger Store storage server (Apple Mac and Windows):

1. Click the Tiger Client tray/menulet icon and then click Connect/Disconnect.
2. Click a connected storage server (a storage server with a check mark in front of its name/IP address) to disconnect from it and dismount the volumes it shares.
3. If prompted, confirm that you want to disconnect from the appliance.

   Note: *On Apple Mac, you are asked for confirmation only if a file operation on the shared volume is going on at the moment.*
4. (optional, if clients restriction is enabled on Tiger Store) Enter the Tiger Store administrator's password in the dialog, which shows and then click OK.

   The volumes shared by this storage server for your computer are dismounted.

To disconnect from a Tiger Store storage server (Linux):

1. In command-prompt, type:
   `smct -d [number/host/IP address]`

   where `[number/host/IP address]` is the IP address of the storage server or its number in your list.
2. Press Enter.

Tip: *To disconnect from all appliances on your list, type* `smct -d all` *and press Enter.*

3. (optional, if clients restriction is enabled on Tiger Store) Enter the Tiger Store administrator's password, when prompted and then press Enter.

Access the Tiger Store Web Interface

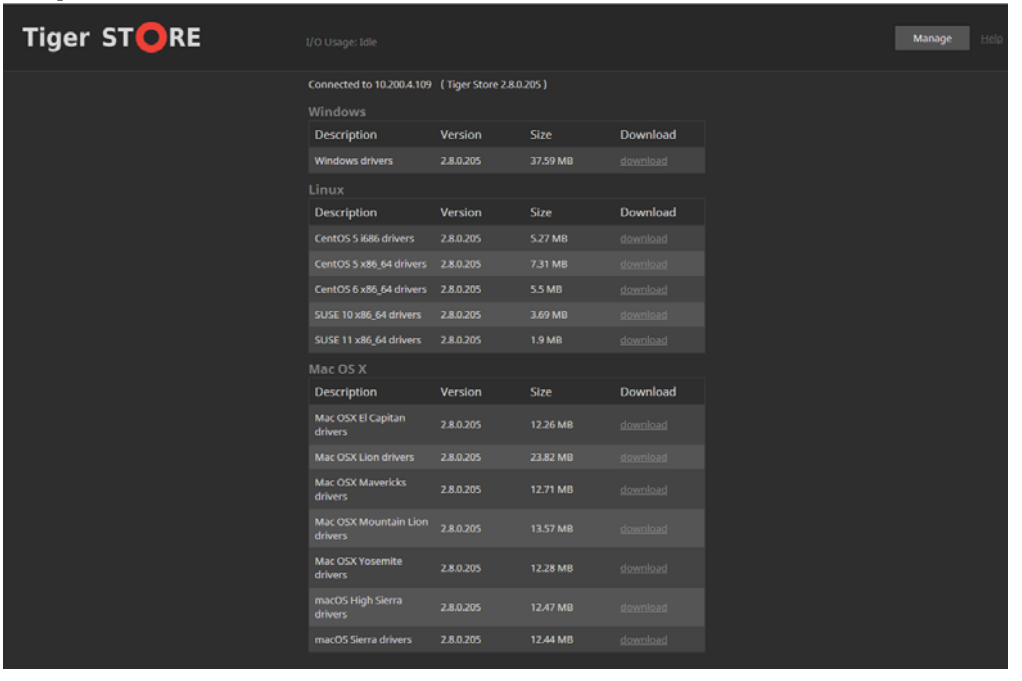
Once Tiger Client computers adds a storage server to their list, they can load the web interface directly through the tray application (Windows), the menulet (Apple Mac), command-line (Linux).

To access the web interface from a Tiger Client (Apple Mac and Windows):

Note: *To connect to the Tiger Store web interface from the tray application/the menulet, the storage server needs to be present in the list of accessible storage servers (see "Connect and Disconnect to Tiger Store" on page 10).*

1. Click the tray application/the menulet.
2. In the menu, click Open Configuration.
3. Click the storage server, whose web interface you want to open.

   The web interface of the selected storage server loads in the default web browser of your computer.

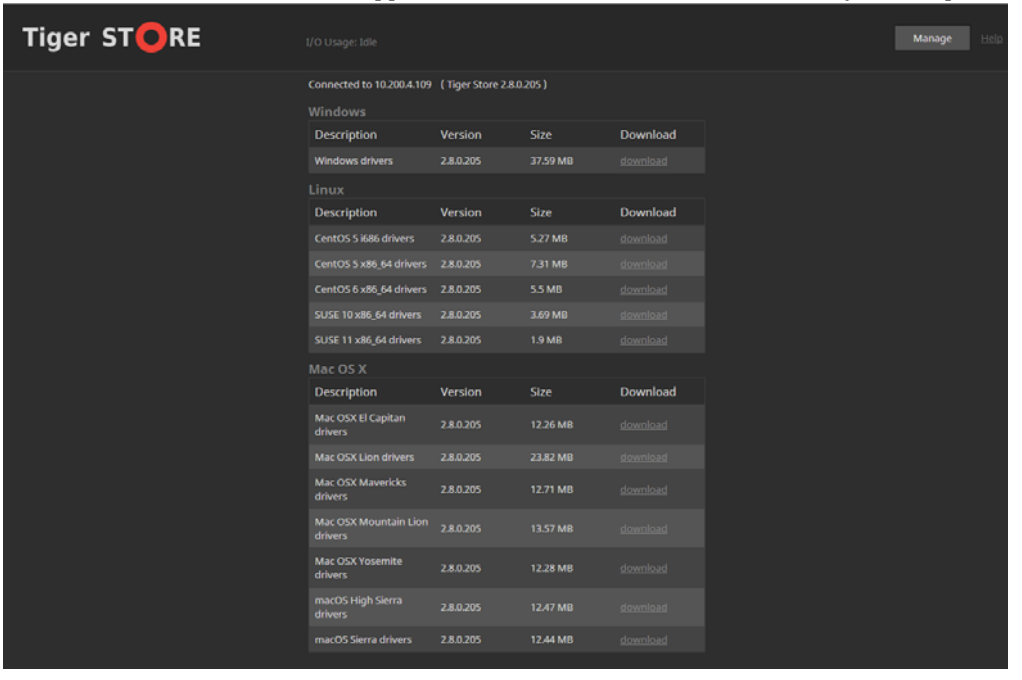


To access the web interface from a Tiger Client (Linux):

Note: *To connect to the Tiger Store web interface from a Linux Tiger Client, the storage server needs to be present in your list of accessible storage servers (see "Connect and Disconnect to Tiger Store" on page 10).*

Tip: *Instead of executing command-line commands, in a web browser you can simply type the IP address of the appliance, whose interface you want to access.*

1. In command-line, type this:
   `smct -config [number/host/IP address]`
   where `[number/host/IP address]` is the IP address of the storage server or its number in your list.
2. Press Enter.
   The web interface of the selected appliance loads in the default web browser of your computer.



Overwrite The Volume Mount Location (Windows)

By default, each volume shared by Tiger Store uses Automatic mount location on all Tiger Clients:

• Windows - the first available drive letter.

• Apple Mac - `/Volumes`.

• Linux - `/mnt` directory with an automatically created symbolic link /Volumes, which points to the /mnt directory.

In the web interface of Tiger Store, a Tiger Store administrator can specify a preferred drive letter as mount location of a Tiger Store volume on all Windows Tiger Clients. This way, a volume can be mounted in one and the same location on all Windows Tiger Clients that see it. Using the Tiger Client tray application, you can overwrite this setting on your Windows Tiger Client computer and specify a different drive letter as default mount point on this computer.

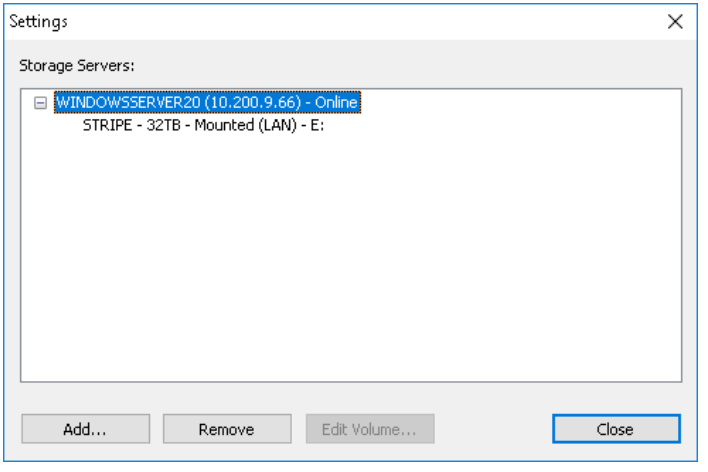
To overwrite the default volume mount location on your computer:

Note: *To overwrite the mount location of a volume, it must be disconnected from your computer.*

1. Click the Tiger Store tray application and then click Settings.

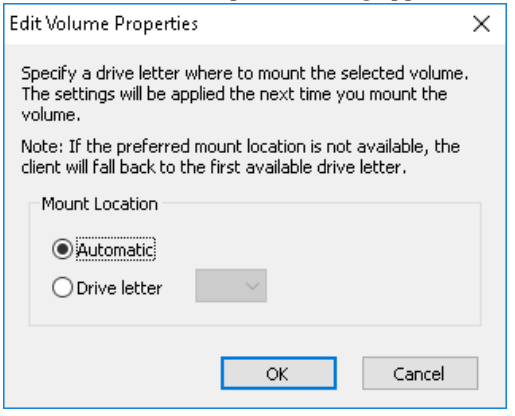
   The Settings dialog appears. It lists all already added Tiger Store storage servers.

2. Expand a disconnected storage server and select the volume whose mount location you want to overwrite.



3. Click Edit Volume.

   The Edit Volume Properties dialog appears.



4. Do one of the following:

   • Select Automatic to let the volume mount on your computer using the first available drive letter.

   • Select Drive Letter and in the drop-down box select a drive letter.

   Note: *Tiger Store does not allow you to select a drive letter that is already in use on your computer.*

5. Click OK.

   The volume will be mounted in the new mount location on your computer the next time you mount it.

View Connection Status

The Tiger Client tray application/menulet icon on your computer shows the connectivity status of your computer:

• Windows:

  •  - connected as SAN client to all storage servers in the list;

  •  - connected as LAN client to all storage servers in the list;

  •  - there's problem with the connection between your computer and one or more storage servers in the list;

• Apple Mac:

  •  - connected to all storage servers in the list;

•  - there's problem with the connection between your computer and one or more storage servers in list;

Note: *On Apple Mac, you can check the type of connection by the icon of each Tiger Store volume mounted on your computer:*

 *- volume is mounted over Fibre Channel;*

 *- volume is mounted over the Ethernet;*

On Linux, to view the connectivity status of your computer for each storage servers on the list, type:
`smct -l`
and then press Enter:

• Online - the storage server is online, but you are not connected to it;

• Mounted (LAN) - your computer is connected as a LAN client to all storage servers on the list;

• Mounted (Fibre) - your computer is connected as a SAN client to all storage servers on the list;

• Offline - there's problem with the connection between your computer and one or more storage servers on the list;

Data on the Shared Volumes

By default, data on the shared storage is accessible to anyone seeing the shared volumes. When Tiger Store operates in an Active Directory domain, it utilizes access permissions for data on the shared volumes. When Tiger Store is set up to operate in domain environment, the permissions that are already set on the file system are respected. You can manage the permissions from any Windows Tiger Client computer, which can mount the shared volume(s). For more details, refer to the documentation of the Windows Domain Server that controls permissions on your network.

Important: *Whether or not the volumes are accessed in domain environment, the SYSTEM account must always have full control.*

Deleted Data

Tiger Store does not support Windows Recycle Bin on its volumes and any soft-deleted file is permanently deleted. Apple Mac Trash is supported on the shared volumes, allowing Apple Mac clients to soft-delete files and later restore them or permanently delete them by emptying the Trash.

When Tiger Store operates in Active Directory domain environment, each domain user moves their soft-deleted files to their own Trash folder. In workgroup environment, as the Trash folder is created per user ID and two or more different users on different Apple Mac clients may move their

soft-deleted files to the same Trash folder and respectively - empty the Trash containing the files of other users with the same ID.

Data Managed by Tiger Bridge

When a shared volume is subject to Tiger Bridge's data lifecycle management mechanisms, data on it can have the following status:

Normal — a file that does not have a copy on the replication target or a file that has been modified after its last replication (i.e. is subject to replication again);

Replicated — a file that is replicated and exists on both the Tiger Store volume and the replication target;

Nearline — a stub file pointing to the actual file, which exists only on the target. A nearline file can be retrieved on the source through the Volume Browser.

Offline — a stub file pointing to the actual file, which exists only on the archival tier of the target.

To view the Tiger Bridge status of a file, you must open the Volume Browser in the web interface of Tiger Store. For more details refer to the latest version of the Tiger Store Administration Guide.

Tiger Client Best Practices

Disable Hardened Usercopy Checks on Red Hat Enterprise Linux and Derivatives

On Red Hat Enterprise Linux and derivatives, the hardened usercopy checks are enabled by default for the boot. Installing the Tiger Client driver when the hardened usercopy checks are enabled may lead to kernel panic. That is why it is advisable to disable the checks by editing the kernel boot parameters in the GRUB configuration file.

If you have already installed the Tiger Client without disabling the option, first disable it for the current boot and only after that proceed with changing the default boot option. You can disable hardened usercopy for the current boot following these steps:

1. When the computer starts, press the E key on your keyboard while loading the GRUB.
2. Using the keyboard arrows navigate within the boot parameters to the end of the "`linux`" line.
3. Add the following entry at the end of the "`linux`" line, separating it with a space from the previous entry:
   `hardened_usercopy=off`

4. Press CTRL+X to continue booting with the changed parameters.

Important: *Before proceeding with the steps below, back up the GRUB configuration files as a precaution.*

To back up the GRUB configuration files on an MBR (BIOS-based) system:

In Terminal, execute the following:

```
sudo cp /etc/default/grub /etc/default/grub-backup
sudo cp /boot/grub2/grub.cfg /boot/grub2/grub.cfg-backup
```

To back up the GRUB configuration files on a GPT (UEFI-based) system:

In Terminal, execute the following:

```
sudo cp /etc/default/grub /etc/default/grub-backup
sudo cp /boot/efi/EFI/redhat/grub.cfg /boot/efi/EFI/redhat/grub.cfg-backup
```

To disable hardened usercopy checks in the GRUB file:

1. In Terminal, open the /etc/default/grub file for editing by executing the following:
   `sudo vi /etc/default/grub`
2. Enter Insert mode, by pressing the "i" key on your keyboard.
3. In the /etc/default/grub configuration file, find the `GRUB_CMDLINE_LINUX` option line and add the following entry preceded by a space:
   `hardened_usercopy=off`

   A sample `GRUB_CMDLINE_LINUX` line in the GRUB configuration file may look like this:
   ```
   GRUB_CMDLINE_LINUX="console=ttyS0,115200 console=tty0
   vconsole.font=latarcyrheb-sun16 crashkernel=auto  vconsole.keymap=us
   hardened_usercopy=off"
   ```
4. Exit Insert mode, by pressing the ESC key on your keyboard.
5. Save your changes and exit the configuration by executing the following:
   `:wq`
6. Regenerate the GRUB configuration file with your changes, by executing one of the following:

   • For an MBR (BIOS-based) system:
   `sudo grub2-mkconfig -o /boot/grub2/grub.cfg`

   • For a GPT (UEFI-based) system:
   `sudo grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg`
7. Reboot the system to apply the changes, by executing the following:
   `sudo systemctl reboot`

8. Verify that the hardened usercopy is indeed disabled, by executing the following command:
   `cat /proc/cmdline`

   The output must contain the following entry "`hardened_usercopy=off`". A sample output may look like this:

```
BOOT_IMAG=/vmlinuz-3.10.0-1160.90.1.el7.x86_64 root=/dev/mapper/
centos-root ro crashkernel=auto hardened_usercopy=off
rd.lvm.lv=centos/root rd.lvm.lv=centos/swap rhgb quiet
```

Allow the User Management of Kernel Extensions on Apple Silicon macOS

The Tiger Client software utilizes macOS kernel extensions, notarized by Apple in accordance with the OS security requirements, which need to be manually allowed in the General tab of the Security & Privacy window in System Preferences, in order for the client software to run.

On macOS client workstations that are based on the Apple Silicon architecture, managing kernel extensions is disabled by default, thus an additional mandatory prerequisite is to enable the setting named "Allow user management of kernel extensions from identified developers" via the Startup Security Utility in the Recovery Console.

Before you can install and run the Tiger Client software on an ARM-based macOS computer, you must enable the aforementioned setting, following the sample steps below:

1. Reboot the macOS Apple Silicon client system into Recovery mode.
2. In the Utilities menu, select Startup Security Utility.
3. In Startup Security Utility, click Security Policy.
4. In Security Policy, do the following:
   - Select Reduced Security.
   - Select the “Allow user management of kernel extensions from identified developers” check box.
   - Click OK.
5. Restart the computer.
6. Allow the blocked Tiger Client kernel extensions.

   Note: *For most up-to-date steps about allowing the user management of kernel extensions on ARM-based computers, refer to the Apple documentation at: https://support.apple.com/guide/mac-help/change-security-settings-startup-disk-a-mac-mchl768f7291/mac*

Enable Searching Shared Volumes in the Finder of macOS Tiger Clients

Version 2.9.3 and above allows macOS Tiger Clients to search the contents of shared volumes in the Finder. For this to work you must delete the `.metadata_never_index` file in the root of each volume and then remount the volume again on the storage server.

Note that this file is present in the root of the volume only if it has been created using version 2.9.2 or below or if you create a new RAID in the web interface of Tiger Store 2.9.3 or above on a Tiger appliance.

Installing Tiger Client on macOS Catalina and Above

If macOS Catalina and above does not allow you to open the Tiger Client installation file by double-clicking it, because Apple cannot check it for malicious software, you must control-click it in Finder, choose Open from the menu, and then click Open in the dialog that appears.

Mounting Volumes on macOS Catalina and Above as a SAN Client

In order a Tiger Client running macOS Catalina or above to mount shared volumes as a SAN client, you must manually allow Full Disk Access of the Tiger Client daemon to each LUN the computer is physically connected to, following these steps:

1. In the System Preferences of the macOS computer go to Security & Privacy.
2. In the Privacy tab, select Full Disk Access in the left pane and then select the check box of "tboxd" in the right pane.
3. Click Apply.

Prevent Double Mounts on Red Hat Enterprise Linux / CentOS Linux 7 Tiger Clients

Once the Tiger Client driver is installed on your Red Hat Enterprise Linux/CentOS Linux 7 computer, it parses the available devices and creates a device node file in the /dev directory for each detected partition. As the operating system itself creates a device node files in the same directory, a partition can be exposed to and eventually mounted by the operating system twice - using the device node file created by the operating system and the one created by the Tiger Client driver.

To prevent possible double mounts, it is advisable to either set the Tiger Client driver to mount all volume partitions over the LAN or to limit the partitions parsed and managed by Tiger Client to a specific HBA on your computer. Both workarounds require editing the Tiger Client daemon startup script. Perform one or the other workaround following the steps below or contact the Tiger Technology support team for assistance.

To set all available volume partitions to mount over the LAN:

1. Open for editing the Tiger Client daemon startup script, located in:
   `/etc/init.d/tboxd`
2. In the script, find the following line:
   `insmod /lib/modules/${KERNEL_VERSION}/tbox/sanevda.o >/dev/null 2>/dev/null`
3. Change it to the following:
   `insmod /lib/modules/${KERNEL_VERSION}/tbox/sanevda.o nopscan=1 >/dev/null 2>/dev/null`
4. Save your changes to the script.
5. Restart the computer.

Note: *To disable mounting of all partitions over the LAN connection, either change the* nopscan= *value to zero (*nopscan=0*), or simply delete "*nopscan=1*" and save the script.*

To limit the partitions managed by the Tiger Client driver to a specific HBA:

Note: *You can set the Tiger Client to mount as a SAN client only the partitions accessible through one HBA. All partitions accessible through other HBAs on your computer will be mounted by the operating system itself or, if they are public SAN volumes, over the LAN connection.*

1. To list all HBAs on your computer, in Terminal execute the following:
   `dmesg | grep sanevda`
2. Find the HBA, through which you want to mount disk partitions as a SAN client and copy its name.
3. Open for editing the Tiger Client daemon startup script, located in:
   `/etc/init.d/tboxd`
4. In the script, find the following line:
   `insmod /lib/modules/${KERNEL_VERSION}/tbox/sanevda.o >/dev/null 2>/dev/null`
5. Change it to the following:
   `insmod /lib/modules/${KERNEL_VERSION}/tbox/sanevda.o hba_restrict='[HBA name URL-encoded]' >/dev/null 2>/dev/null`

   where `[HBA name URL-encoded]` is the URL-encoded name of the HBA (spaces in the name are replaced with "%20".

   For example if the HBA you want to use for mounting partitions as SAN client is named 'ATTO Celerity 16Gb/32Gb Fibre Channel Adapter', change the line to:
   `insmod /lib/modules/${KERNEL_VERSION}/tbox/sanevda.o hba_restrict='ATTO%20Celerity%2016Gb%2F32Gb%20Fibre%20Channel%20Adapter' >/dev/null 2>/dev/null`

6. Save your changes to the script.
7. Restart the computer.

Avoid Frame Corruption with Baselight Software

To avoid frame corruptions when using Baselight colour grading and editing software on Tiger Store-managed volumes, it is advisable to contact FilmLight's support team for assistance on setting up Baselight to use the cache for I/O operations (nodirect=1 setting).

Setting Up the SAN Policy on Windows Tiger Clients

By default, on Tiger Client computers running Windows operating system all shared disks visible to the computer are delivered as offline and read-only. You can bring these disks to online mode in Disk Management, still, there's a possibility on the next boot of the system the disks to be offline again. To change this behaviour, you should make sure that the SAN policy of the operating system is set to "Online All". To view and set the SAN policy of your computer you can use diskpart.exe command-line utility that is stored in the system drive of your computer.

To view and change the SAN policy of your computer:

1. Run command prompt as administrator.
2. In command prompt, start diskpart utility by typing:
   `diskpart`
3. To view the current SAN policy, type this followed by return:
   `SAN`

   The utility displays one of the following:

   • Offline Shared - all newly discovered disks that do not reside on a shared bus are brought online and made read-write.

   • Offline - all newly discovered disks remain offline and read-only.

   • Online All - all newly discovered disks are brought online and made read-write.
4. Do one of the following:

   • If the SAN policy of your computer is “Online All”, exit diskpart utility and command prompt.

   • If the SAN policy of your computer is not “Online All”, proceed with the steps below.
5. Run command prompt as administrator.
6. In command prompt, start diskpart utility by typing:
   `diskpart`

7. Execute the following:
   ```
   san policy=OnlineAll
   ```

Using Identical Time and Date Settings

It is advisable to use identical settings for time and date on all computers on your Tiger Store network (the storage server and all client computers). Using different time and date settings may hamper communication with the storage server and the Traffic and Events reports may display incorrect information.

Disable Mac OS X Time Machine for Shared Volumes

It is highly advisable to exclude all volumes shared by Tiger Store from the list of locations Time Machine is set to back up on your Mac OS X. Keeping this feature turned on for shared volumes may hamper performance.

To exclude a shared volume from Time Machine's backup:

1. In Time Machine preferences, click the Options button.
2. In the sheet with locations, select a shared Tiger Store volume and click the "-" button.
3. Repeat the above step for each shared Tiger Store volume.
4. Click Save.

Calculating Folder Size (Mac OS X)

Use the Calculate Sizes option, available in List view of the Finder, to calculate sizes per folder and per window. Activate this option only for folders on your local disks. Do not enable it for folders on the shared storage volumes, as this will temporarily slow down performance. If you enable this option on a shared volume, network computers that see the volume will be unable to work on it.

For details about managing the “Calculate Sizes” option, refer to your Mac OS X® documentation.

Tiger Client Known Issues

No Support for File Security on Linux Tiger Clients

To allow Linux Tiger Clients to connect to the storage server and work with shared volumes, you must disable file security on your Tiger Store network. Once you disable file security, domain access permissions to files and folders will not be applicable, even if your storage server operates in Active Directory domain and all users will have full access to all resources on your shared storage.

Refer to "Enable/Disable File Security in the Tiger Store Network" in the Tiger Store Administration Guide for steps about enabling/disabling file security.

Disconnecting Tiger Clients from the Storage Server

When the "Restrict client actions" check box is enabled, Apple Mac and Linux clients may fail to manually disconnect from the storage server (through the menulet or the command-line interface, respectively) as the field for providing an administrator's password may not appear.

LAN Clients Taking Up SAN Client Licenses

When a Tiger Client sends a request to Tiger Store for connection to the shared volumes, the storage server checks the number of currently available licenses for this type of connection (SAN or LAN) and if a license is available, lets the Tiger Client computer mount the volumes. If all connections for this type are already in use, the storage server lets the Tiger Client mount the volume(s) using another type of connection as long as such is available. While this lets Fibre Channel clients mount the volumes over the Ethernet when there's a problem with the FC HBA or port, or all SAN connections are already in use, it is possible a LAN client to take up a SAN connection and thus prevent a SAN computer from mounting the volumes, because all SAN connections are already taken up. A workaround to this problem is to manually free the connection, by disconnecting the LAN computer in the Clients page of the web interface.

Incorrect Connection Status on Mac Tiger Clients

The Tiger Client software on Apple Mac may sometimes fail to correctly display the connection status to the Tiger Store appliance. For example, the Settings dialog of the Tiger Client menulet may display that the Tiger Store is online, when it is actually offline. Another example is when the Tiger Client loses its Fibre Channel connection to the appliance and mounts the volume(s) over the LAN, while the volume icons in the Finder and on the desktop are not of volumes mounted over the Ethernet. Additionally, in this case Tiger Clients running Apple Mac may fail to disconnect from the volume(s).

Allowing smct.app and vpd During Tiger Client Installation on Apple Mac

During installation of Tiger Client on Apple Mac, even if you specify that smct.app and the vpd daemon must be added as firewall exceptions, you should manually allow them in the firewall database of your computer. Note that as long as the firewall of your computer is turned on, you will have to add them to the firewall database after each reboot of the computer.

Manually Refreshing the Contents of a Directory

The contents of a directory may not be automatically refreshed on Tiger Clients and some file operations may fail. For instance if a Linux Tiger Client tries to copy a directory that is deleted by a Windows Tiger Client, the Linux computer may not be notified about this, and the copy operation will result in error.

To overcome such problems you may have to manually refresh the contents of the disks/directories you are working with.

Browsing Hard Links Pointing to the Same File from Mac Tiger Client

On NTFS hard links to the same file have identical file IDs. That is why, if a file has two hard links in the same directory, when you browse this directory in the Finder only one of the hard links will be shown.

User Switching Known Issues

Switching between users on a single machine, without quitting applications and logging out, lets users leave their applications running and their files open, when another user needs to log in.

While operations on the shared volumes are not interrupted when you switch users on a Tiger Client computer, the Tiger Client tray application/menulet may not be present when a new user logs on, thus preventing that user from controlling the available Tiger Client commands. A workaround to this problem is to force display the Tiger Client tray icon/menulet by restarting it.

Note: *As users on Linux computers use the command-line interface to manage the Tiger Client driver, you can use fast user switching without problems.*

To restart the Tiger Client tray application on a Windows computer:

1. Run the Task Manager as administrator.
2. In the Processes tab, right-click smct.exe and select End Process.
3. In the Run command (press Windows logo key+R to display it), execute this:

   ```
   C:\Program Files\Tiger Technology\Tbox\smct.exe
   ```

   Note: *Where C: is the drive, on which the Tiger Client driver is installed.*

To restart the Tiger Client menulet application on Apple Mac:

1. Start the Activity Monitor (go to Applications | Utilities | Activity Monitor).
2. In the Disk tab, in the Process name column select smct.
3. Click End Process in the Activity Monitor task bar.

4. Provide an administrator's user name and password.
5. On the drive, on which the operating system is installed, go to /Library/Application Support/embedded/smct and double-click it.

No Support for Sparse Files

Tiger Store does not provide support for sparse files on SAN volumes.

Executing Operation on a Shared Volume from Terminal

When Tiger Store is deployed in an Active Directory domain, you will not be able to execute certain operations on the shared volume(s) from the Terminal of a Mac OS X client computer even if you have logged on as a user that has Full Control. These security mapping issues are not valid for operations performed in the file browser.

No Support for Spotlight Indexing

Currently, Spotlight Indexing is not supported on Apple Mac Tiger Clients. While you can search the contents of a shared volume in the Finder, to index it you must use Spotlight alternatives.

No Support for Indexing Service on Shared Volumes

Currently, Tiger Store does not support the Windows indexing service on shared volumes mounted on Tiger Clients.

Manually Refreshing the Contents of a Directory

The contents of a directory may not be automatically refreshed on Tiger Clients and some file operations may fail. For instance if a Linux Tiger Client tries to copy a directory that is deleted by a Windows Tiger Client, the Linux computer may not be notified about this, and the copy operation will result in error.

To overcome such problems you may have to manually refresh the contents of the disks/directories you are working with.

Changing Volume's Icon on Apple Mac

You can change the appearance of a shared volume's icon on an Apple Mac client computer, but the original icon of the volume will be restored immediately after restarting the storage server and your personal icon will be deleted.

Compressing or Encrypting Folders on Shared Volumes

You will not be able to compress or encrypt any folder on a shared volume. If you try to complete any of these operations, the system displays an error message.

Displaying Volumes Part of a Pool in the Finder of macOS Mojave

When smart storage pooling is enabled, the Finder on macOS Mojave Tiger Client may display both the volume pool and the individual volumes. Still, users on the Tiger Client computer can access only the pool and attempting to access the contents of the individual volumes returns error.

File Moved to Another Volume in the Pool After Modifying It

If you use an application that creates a temporary file when modifying an existing file on the volume pool, after you save the file it might be moved to another volume in the pool (the one on which the distribution policy in the pool creates new files).

Mounting a Storage Pool on Tiger Client in Domain Environment

In case you have deployed Tiger Store in Active Directory domain and smart storage pooling is enabled, Windows Tiger Clients may fail to mount the storage pool unless the group ‘Everyone’ has Read access to the virtual volume.

No Support for Hard Links on Storage Pool

Currently you cannot use hard links on pooled volumes (smart storage pooling).