Tiger ST⬤RE

Tiger Store 2.9.2
Administration Guide

August 3, 2022

Title:	Tiger Store Administration Guide
Software version:	Tiger Store 2.9.2
Date:	August 3, 2022

Manual Revision and Control

Revision Record

Date	Description	Page	Version
19 Nov. 2017	Initial Draft		2.8
29 Jan. 2018	Steps for enabling Tiger Bridge data replication on S3/S3-compatible object storage updated with step for specifying the object storage provider.		2.8.1
08 June 2018	Steps for activating a Tiger Store license using a software-protection dongle added.	28	2.8.1
02 Nov. 2018	High-availability add-on requirements updated with requirement for cluster nodes' name.	16	2.8.1

Revision Record

Date	Description	Page	Version
27 Mar. 2019	Tiger Bridge Integration chapter updated with steps about installing and using the Tiger Bridge Configuration and Tiger Bridge Tape Management from a remote computer and steps about resolving conflicts in the Tiger Bridge configuration on high-availability cluster.		2.9
27 Mar. 2019	Added support for Microsoft Server 2019.	15	2.9
06 June 2019	A storage server running Microsoft Windows® 7/Server 2008 R2, Windows® 8/Server 2012 must run Windows PowerShell 4.0 or above and the respective .NET framework supporting it.	15	2.9
13 Sept. 2019	View statistics about connected and disconnected client computers.	74	2.9.1
15 Jan. 2020	Installing Tiger Client on macOS Catalina best practices topic added.	111	2.9.2
22 Nov. 2021	Digital certificate requirements added.	17	2.9.2

Table of Contents

Table of Contents

Introducing Tiger Store

Congratulations on your purchase of Tiger Store, Tiger Technology's metadata controller for scale-out NAS and SAN platforms.

This manual will guide you in the process of setting up your Tiger Store metadata controller, administering the access to it and the volumes it manages. This guide is intended for administrators of Tiger Store.

You can find the most up-to-date version of this manual at the following address: https//www.tiger-technology.com/software/tiger-store/docs

The Tiger Store Workflow

With the help of Tiger Store you can achieve a true SAN workflow, providing multiple Windows, Apple Mac and Linux computers with concurrent access to NTFS shared volumes. For the purpose, the computer running Tiger Store must be connected directly or through a switch to the shared storage through 8/16G FC (for FC storage), 1/10GbE (for iSCSI storage) or using SAS connection.

Regardless of their connection Tiger Clients gain block-level access to each shared volumes. Tiger Clients can mount the shared volumes as:

• SAN clients - using FC or GbE connection to the storage.

• LAN clients - using GbE connection to the storage server.

To prevent data corruption when multiple computers access the same file system, Tiger Store acts as a metadata controller that processes requests, coming from Tiger Clients through the LAN connection. Computers that do not have the Tiger Client driver cannot mount volumes managed by Tiger Store, although they might be connected to them. These computers can only mount the volumes that Tiger Store has specified that it does not manage and protect.

If your Tiger Store is part of an Active Directory domain, requests for access to the shared volumes are authenticated against the domain controller. If Tiger Store is deployed in workgroup environment every user has full access to all data on the shared volumes.

Besides acting as a metadata controller on your SAN, Tiger Store also provides you with automatic defragmentation of the shared storage volumes, storage usage and connectivity monitoring tools, etc. You can also greatly optimize your shared storage workflow using the following add-ons:

• pooling of shared volumes and presenting them as one virtual file system.

• data lifecycle management services (data replication and archiving, space reclaiming, geo synchronization) provided by Tiger Bridge.

• failover between Tiger Store server nodes for high availability.

Using the web interface you can also reformat existing volumes and create new volumes.

Concepts Used Throughout the Guide

Storage Server — the computer running Tiger Store software, which acts as a SAN manager and controls access to the volumes it sees and can manage. When the high-availability add-on is activated, the storage server is comprised of two server nodes.

Primary node — when the high availability add-on is activated, this is the server node that is currently processing requests from Tiger Clients and is managing the volumes. The primary/secondary node division is only nominal and depends solely on which server node takes over the leading role first.

Secondary node — when the high availability add-on is enabled, this the server node that is currently in standby mode. In case the primary node fails or is shut down for maintenance, the secondary node takes over its role and starts processing requests for access to the shared volumes i.e. becomes primary node. The primary/secondary division node is only nominal and depends solely on which server node takes over the leading role first.

Failover — the process of transferring the metadata controller role from one server node to the other. As long as the high availability add-on is activated and set up, the failover between server nodes is automatic and ensures constant access to the shared volumes. In most cases the failover is transparent - the second server node takes over the metadata controller role absolutely transparently to all running applications and they can continue working with any open files after the failover takes place. During the failover process requests for access to the shared volume(s) coming from Tiger Clients are not rejected but just delayed till the other server node takes over the metadata controller role.

Tiger Client — each computer running the Tiger Client software, which can mount the shared volume(s). You can install the Tiger Client software on as many computers as you like. Each Tiger Client computer can share the volumes it has mounted or folders on them to LAN clients on the network as SMB/CIFS shares.

SAN Client — a Tiger Client computer that is connected to the shared storage directly or through a switch using FC, network connection (for iSCSI storage) or using a SAS connection.

LAN client — a Tiger Client computer that mounts the shared volumes using LAN connection to the storage server. In contrast to computers on the LAN that do not have the Tiger Client software installed and access only LAN shares of the shared storage, LAN clients mount the volumes and gain block-level access to them.

Shared volume — a volume managed by Tiger Store, which all connected Tiger Clients can mount and work with, in contrast to computers that have access to the volume but do not have the Tiger Client software installed.

Private volume — a volume managed by Tiger Store, which is accessible only to the storage server, usually for performing maintenance operations. Tiger Clients and computers without the Tiger Client software installed cannot mount and work with private volumes.

Offline volume — a volume that is not managed and protected by Tiger Store and that can be mounted by any computer that has access to it. Tiger Store cannot prevent data corruption on offline volumes, when more than one computer accesses them.

SAN to LAN failover — In case there is a failure of the FC HBA or FC cable (or a network port or cable for iSCSI SAN) on a Tiger Client, the SAN to LAN failover mechanism lets this computer reconnect to the shared volumes over the Ethernet and thus it can continue working with the volumes although with decreased performance. For the purpose the Tiger Client computer should disconnect from the storage server and then reconnect again. Once the problem is fixed, the Tiger Client should again disconnect and reconnect to the Tiger Store in order to mount the volume(s) over the SAN connection.

Cluster view — when the high availability add-on is activated, this is the web interface through which your Tiger Store network is administered. It represents the settings valid for the high-availability cluster, regardless of the server node currently playing the role of metadata controller. As long as both server nodes are available, changes introduced in cluster view are synchronized automatically among them.

Node view — when the high availability add-on is activated, this is the web interface, showing the settings valid just for a selected server node. The purpose of the node view is to allow you to resolve conflicting settings of server nodes that cannot be automatically synchronized in cluster view. You can also use it to view and control node specific settings (like Tiger Store activation, firmware version if Tiger Store runs on an appliance, etc.). Changing settings in node view must be done with caution in order not to create conflicts between the settings of both node.

Tiger Store Administrator — the user account with which any user can log on to Tiger Store's web interface and administer the Tiger Store network. The web interface of Tiger Store is accessible to any device with a web browser that is on the same network as the storage server.

Data on the Shared Volumes

By default, data on the shared storage is accessible to anyone seeing the shared volumes. By adding Tiger Store in an Active Directory domain, you can utilize 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.*

Tiger Store doesn't support Windows Recycle Bin on its volumes and any soft-deleted file is permanently deleted. Mac OS X Trash is supported on the shared volumes, allowing Mac OS X 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 Mac OS X clients may move their soft-deleted files to the same Trash folder and empty the Trash containing the files of other users with the same ID.

Storage Server System Requirements

Note: *Tiger Store appliances come with Tiger Store software pre-installed.*

To be able to play the role of a metadata controller, the computer on which you install the Tiger Store software must meet the following minimum system requirements:

• PC with 1.8-GHz 64-bit (x64) processor.

• 64-bit Microsoft Windows® 7/Server 2008 R2, Windows® 8/Server 2012/Server 2012 R2, Windows® 10/Server 2016/Server 2019.

Important: *Microsoft Windows® 7/Server 2008 R2 computers must run at least Service Pack 1 and have the KB3033929 security update installed. Additionally, Microsoft Windows® 7/Server 2008 R2, Windows® 8/Server 2012 computers must run Windows PowerShell 4.0 or above and the respective .NET framework supporting it (for PowerShell 4.0 this is version 4.5.1).*

• 4 GB of physical RAM at least.

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

• Network LAN connection (1 Gb at least).

• 4Gb/8Gb/16Gb FC, 1GbE/ 10GbE or SAS adapter for connection to the storage.

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

• The following TCP ports - 80, 3000, 3001, 8555, 9120, 9121, 9122, 9123, 9124, 9125, 9126, 9127 - must not be blocked by a firewall, if any, and must not in use by any other service or application.

Note: *By default, TCP port 80 is used for access to the web interface of Tiger Store. To assign another port for the purpose, refer to "Change the TCP Port for Access to the Web Interface" best practices topic in the latest Tiger Store release notes.*

• 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 17.

iSCSI Requirements

Tiger Store is designed to be iSCSI initiator agnostic. As long as the iSCSI initiator on the storage server provides direct access to iSCSI target disks (they are displayed online and healthy in Disk Management of the storage server), the NTFS volume(s) created on these disks can be shared through Tiger Store to Tiger Clients. Each Tiger Client computer having block-level access to the target through its iSCSI initiator will mount the shared volume as a SAN client. Tiger Client computers without iSCSI initiator can access the shared volume as LAN clients only.

High Availability Add-on Requirements

Unless you use a Tiger Store appliance with two server nodes, to deploy Tiger Store with high-availability you must install Tiger Store on two computers, which aside from meeting the above mentioned system requirements, must also be set up in the following way:

• The network LAN connection (1 Gb at least) used for public communication must be named "Public" on both nodes.

• The two nodes must be interconnected through an additional direct network connection (1 Gb at least), named "Admin" on both nodes.

• Both server nodes must have an exact IP address for the "Admin" network connection:

  • Node A - IP address: 1.2.3.4 with subnet mask 255.255.255.0

  • Node B - IP address: 1.2.3.5 with subnet mask 255.255.255.0

• Both server nodes must have identical names differing only in the suffix at the end of each node's name:

  • [cluster_name]-A

  • [cluster_name]-B

For example, if you want the high-availability cluster to use the name "SANSRV", in Windows rename one node to "SANSRV-A" and the other to "SANSRV-B".

Note: *The suffix you must add to the name of each computer is not related to the role the respective node plays in the high-availability cluster - primary or secondary node.*

Digital Certificate Requirements

Tiger Store uses a digital certificate issued by GlobalSign certification authority. For the digital certificate to be verified upon installing Tiger Store, GlobalSign's currently used root certificate must be installed in the Trusted Root Certification Authorities of the Certificate Manager on the computer. Additionally, the root certificate's "Code Signing" purpose must not be disabled.

On computers operating in less restrictive environments, this is done automatically during installation of Tiger Store. If the computer, on which you want to install Tiger Store 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 Tiger Store. In addition, you must ensure that the "Code Signing" purpose of the root certificate is enabled.

Storage Requirements

Tiger Store supports any simple or striped NTFS-formatted volume to which the storage server has Read & Write access. You can connect the computer/appliance to the shared storage via Fibre Channel (directly or using a FC switch), using SAS connection or using network connection to iSCSI storage. The storage server can also share its own internal disks, letting any computer on the same LAN gain block-level access to them.

Important: *If you want to use a Tiger Store appliance with iSCSI storage, you should contact the Tiger Technology support team for assistance on setting up the iSCSI initiator on the appliance for work with the storage.*

Introducing Tiger Store

Getting Started with Tiger Store

Install Tiger Store

Note: *Tiger Store comes pre-installed on all Tiger Store appliances. For steps about performing a firmware update of the appliance, refer to "Firmware Update of the Appliance" on page 98.*

You should install the Tiger Store software on the computer that will play the role of metadata controller on your Tiger Store network. Once you install the software and activate Tiger Store on the computer, all supported storage devices that the computer sees and that meet the storage requirements can be shared to Tiger Clients, preventing computers that don't run the Tiger Client software from mounting them.

Additionally, to allow client computers to download the Tiger Client software from the home page of Tiger Store's web UI, you should also install the client bundle, containing the Tiger Client installation for all supported platforms.

Note: *The Tiger Store installation creates the* tbox_db *user account to run maintenance tasks scheduled for it in the Tasks Scheduler of the metadata controller computer. It is important not to delete or disable neither the user account nor the tasks set to it.*

Should you decide to change the metadata controller on your Tiger Store network, you should uninstall and deactivate the Tiger Store software from the current storage server and install and activate it on the new computer that will play the role of metadata controller. For steps about uninstalling and deactivating Tiger Store, refer to "Tiger Store Activation" on page 25.

To install Tiger Store and the client bundle on the storage server:

Important: *Before you install Tiger Store on the storage server, make sure that any other SAN management software is uninstalled from the system.*

1. On the selected computer, log on using an account with administrative privileges.

2. Browse for and double-click the Tiger Store installation file.

    The installation begins.
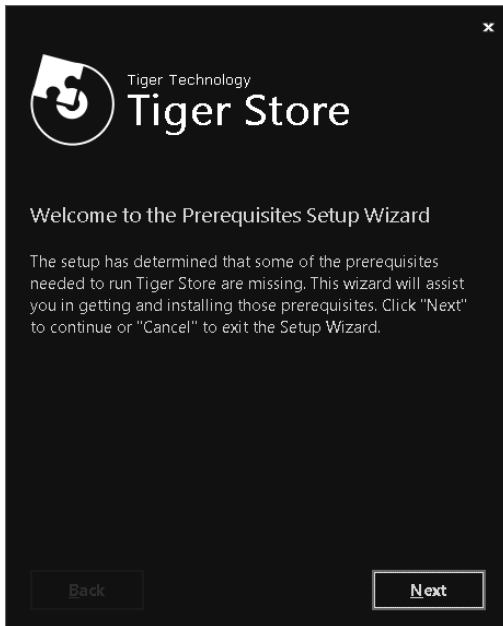
3. Click Next.

4. If the wizard suggests the installation of additional prerequisites, accept and click Next.

5. Select where to install the product, accept the terms of the software license agreement and click Install.
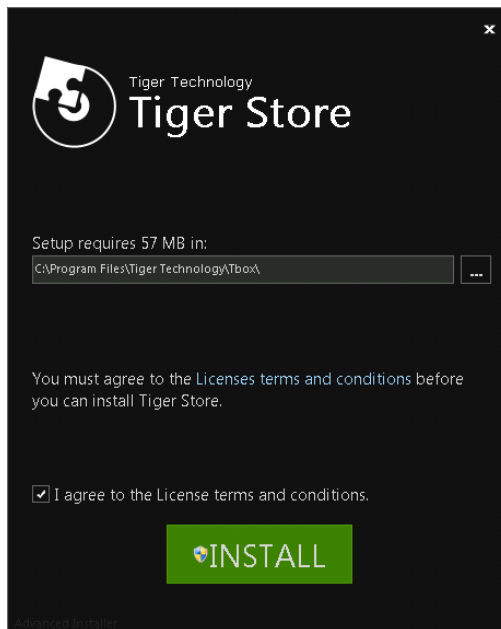
6. When the installation finishes, click Finish and select not to restart the computer, when prompted.

7. Browse for and double-click the Tiger Store clients bundle installation file.

8. When the installation starts, click Next.

9. Select where to install the clients bundle, accept the terms of the software license agreement and click Install.
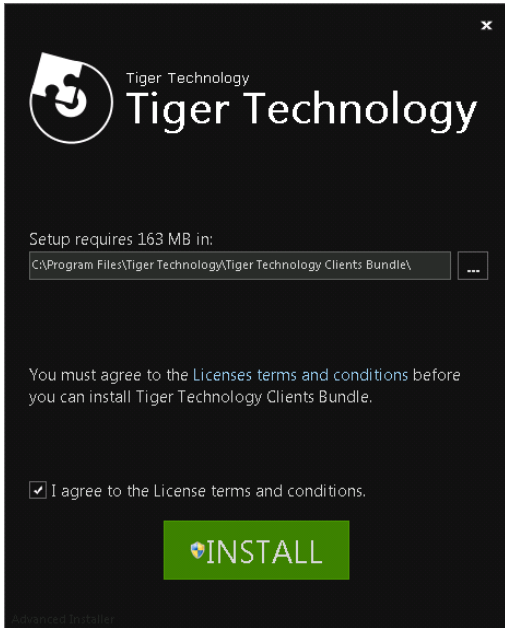
10. When the installation finishes, restart the computer.

Access the Web Interface of Tiger Store

Note: *By default, TCP port 80 is used for access to the web interface of Tiger Store. To assign another port for the purpose, refer to "Change the TCP Port for Access to the Web Interface" best practices topic in the latest Tiger Store release notes.*

Tiger Store can be administered through its web interface, which is accessible to every device with a web browser that is on the same network as the storage server. To access it, in a web browser enter the IP address of the storage server's network port, to which your computer is connected.

By default, the web interface uses a predefined password:
admin

23

It is advisable to set new password for the web interface in order to prevent unauthorized access to the Tiger Store network administration. See "Change the Password for the Web Interface" on page 25.

Note: *Tiger Store's web interface is accessible with most web browsers as long as JavaScript is enabled. If you experience any problems with Tiger Store's web interface, please, contact Tiger Technology support.*

To access the web interface from a network computer:
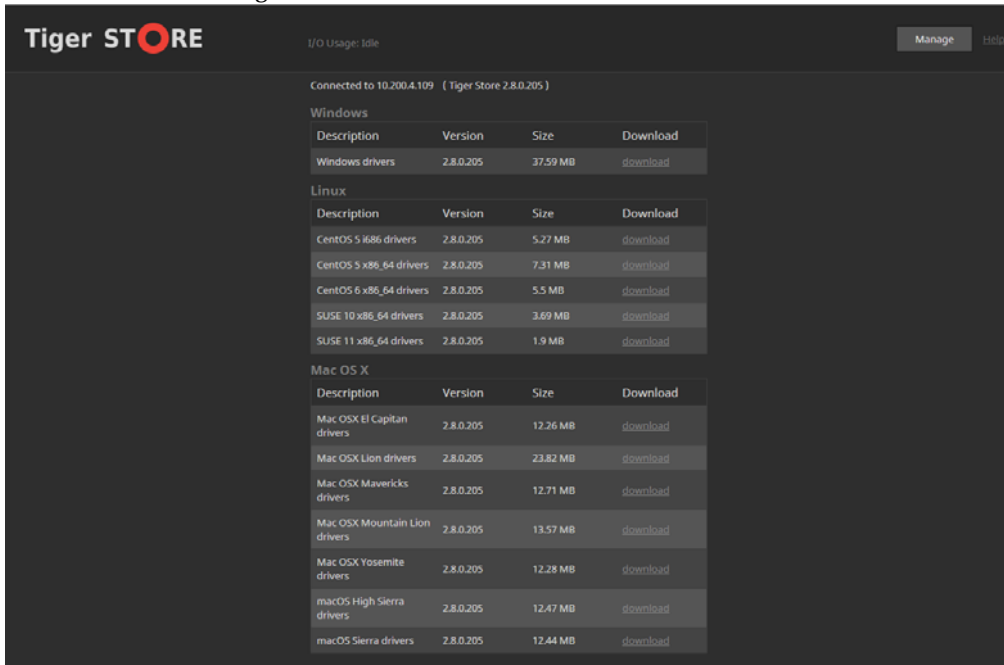
1. In a web browser, do one of the following:

   • type the IP address of the storage server;

   • type the domain name of the storage server;

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

2. Press Enter.

   The web interface of Tiger Store loads.

3. Click Manage and type the password for the web interface.

Change the Password for the Web Interface

Tiger Store's web interface is accessible after supplying a password. By default, the web interface of Tiger Store uses a predefined password:
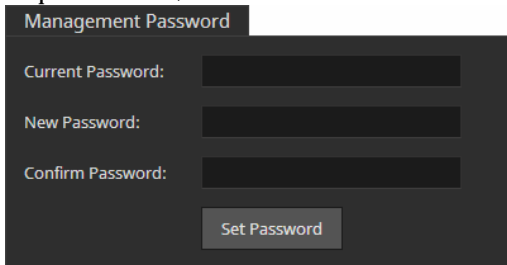
admin

It is advisable to change the predefined password as the web interface is accessible to every computer on the same network. You can change the password for the web interface at any time.

Note: *On Tiger Store appliances with two server nodes, to set identical password on both nodes, either change the password when both nodes are online, or assign the same password to an offline node once you turn it on, following the same steps, but in the node view of this server node.*

To change the web interface password:

1. In the left pane of the web interface, click System and then Settings.

2. In the Management Password field, enter the current password and the new password in the respective fields, and then click Set Password.

Tiger Store Activation

Activate Tiger Store

Note: *Your Tiger Store license can be pre-activated on a Tiger appliance. To view the activation status of Tiger Store, refer to the steps below.*

To benefit from Tiger Store you have to activate the product and any add-on licenses. Until you activate Tiger Store on the storage server, the volumes it is connected to are not protected from data corruption and cannot be shared to Tiger Clients. For activation Tiger Store makes use of a software-protection dongle.

The activation procedure consists of two parts - obtaining an activation key/license file on the licensing server and activating it in the web interface of Tiger Store.

To view the activation status of the storage server:

In the left menu, click System and then About.

The About page displays license information:
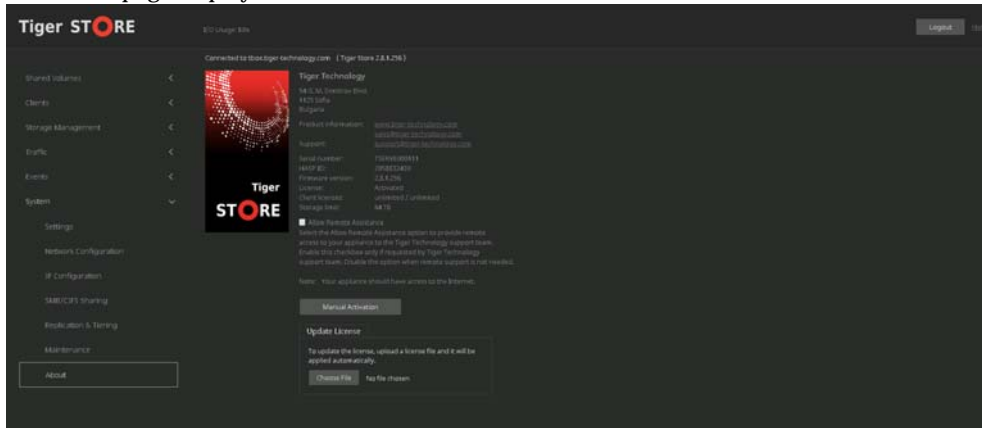
Not present — no license file is found.

Valid till… — displays the date until which the license is valid.

Expired — the license has expired.

Activated — a valid permanent license file is installed.

To activate a Tiger Store license using a software activation key:

1. In the left menu of Tiger Store's web interface, click System and then About.
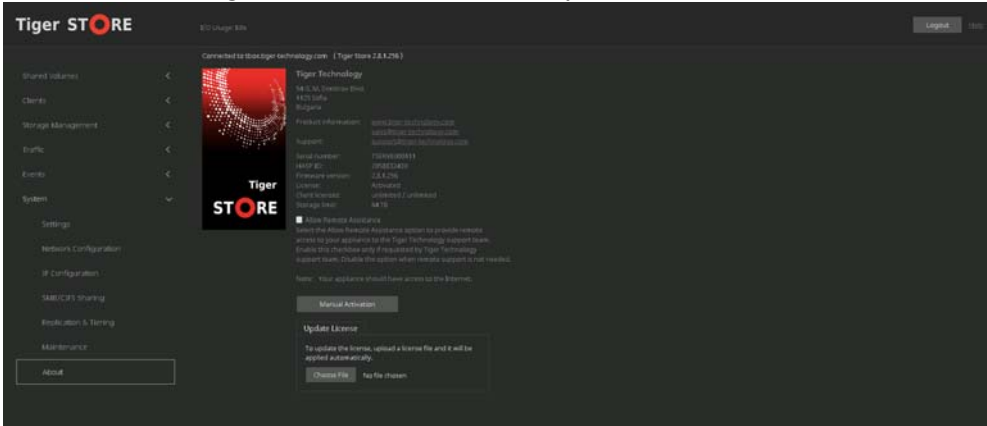
Note: *On a storage server with high availability add-on already activated, you must access the About page of each node in Node view (HA Nodes | Manage Node). Until high availability is activated, Node view is not available in the web interface and the license must be activated on each node following these steps.*

2. Click Manual Activation.

   The License Activation dialog appears.
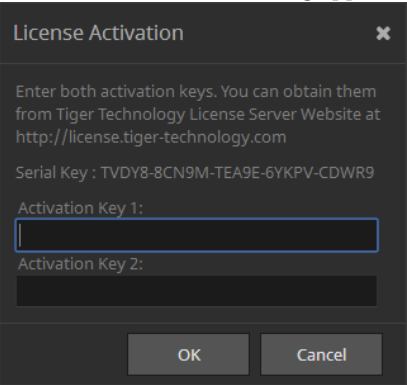
3. Copy the serial number and in a web browser go to:
   https://license.tiger-technology.com

4. In the home page of the licensing server, enter your order name and password in the corresponding fields, and click Log in.

   Note: *If you enter the Tiger Technology licensing site for the first time, you should fill the registration form to continue.*

Important: *The order name and the password are case sensitive.*

The server displays information about your account.

5. In the Licensing Server menu, click Activate License.

6. In Activate License, paste the serial number for your copy of Tiger Store and click Generate Activation Key.

   The licensing server generates two activation keys.

7. In the License Activation dialog in the Tiger Store web interface, paste the keys generated for your copy of Tiger Store, and click OK.

   The About page displays the activation status of the metadata controller and the type of license used.

To activate a Tiger Store license using a software-protection dongle:

1. In a web browser go to
   https://license.tiger-technology.com.

2. In the home page of the licensing server, enter your order name and password in the corresponding fields, and click Log in.

   Note: *If you're entering the Tiger Technology licensing site for the first time, you should fill the registration form to continue.*

   Important: *The order name and the password are case sensitive.*

3. Next to the dongle name in the list, click "Download lic file".

   Tip: *The dongle name is its number, printed on the dongle itself.*

4. In the left menu of Tiger Store's web interface, click System and then About.
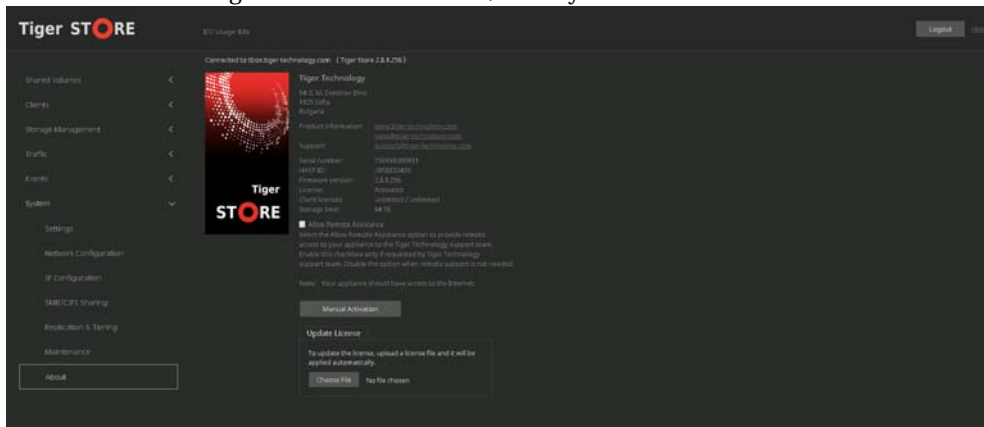
Note: *On a storage server with high availability add-on activated, you must access the About page of each node in Node view (HA Nodes | Manage Node).*

5. Under Update License, click "Choose File".

6. In the dialog, which opens, browse for and double-click the license file downloaded from the Tiger Technology licensing server and then click Continue, when prompted.

Uninstall Tiger Store

Note: *You cannot uninstall the product from a Tiger Store appliance.*

You can uninstall the software-only version of the product from the storage server at any time, keeping in mind that when you install it again on the same computer, you will have to activate it anew.

When you need to assign another computer as a metadata controller, you need to uninstall and deactivate Tiger Store from the current storage server in order to use it on another computer. For steps, refer to "Deactivate Tiger Store" on page 29.

To uninstall Tiger Store:

1. Display the Control Panel.

2. Double-click Programs and Features.

3. Right-click Tiger Store and select Uninstall.

4. Confirm that you want to uninstall Tiger Store.

5. When prompted, restart the computer.

Deactivate Tiger Store

Note: *You cannot deactivate the product from a Tiger Store appliance.*

When you want to transfer your licenses to another machine, you have to obtain new activation key (as the activation key is granted per machine) and return the old one by deactivating your licenses for this computer. After deactivating Tiger Store on the current storage server, you will not be able to activate it again with the same key even if you reinstall Tiger Store.

Currently, Tiger Store doesn't provide interface for deactivating the product. For the purpose, you need to contact Tiger Technology support for assistance on transferring your license to another computer.

Enable File Security in the Tiger Store Network

Note: *When you add a Tiger Store appliance to an Active Directory domain, file security is automatically enabled. Vice versa, when you specify that the appliance operates in workgroup environment, file security is automatically disabled. For information how to add/remove a Tiger*

Store appliance to an Active Directory domain, refer to "Select The Network Environment of Tiger Store" on page 37.

By default, data on the shared storage is accessible to anyone seeing the shared volumes. If your Tiger Store storage server is in an Active Directory domain, you can utilize access permissions for data on the shared volumes. To enable support for file security on the shared volumes, you should create a new string value in the Tiger Store registry on the storage server.

Important: *Note that when the metadata controller is no longer part of an Active Directory domain, you must disable the support for file security on the volumes it shares to Tiger Clients.*

To enable/disable support for file security on the shared volumes:

1. On the Tiger Store computer, start the Registry Editor.

   Tip: *To start Registry Editor, on the Start menu click Run and in the dialog type regedit.*

2. Navigate to:
   HKEY_LOCAL_MACHINE\SOFTWARE\Tiger Technology\tbox\tboxmaster\settings\driver

3. Right-click in the right pane and select New | String Value.

4. Rename the new REG_SZ value to:
   enable_file_security

5. Right-click enable_file_security value and select Modify.

6. Do one of the following:

   • To enable support for file security on the shared volumes, in Value Data enter 1 and click OK.

   • To disable support for file security on the shared volumes, in Value Data enter 0 and click OK.

7. Restart the Tiger Store computer.

Initial Setup of the Appliance

Before you begin work with the product on a Tiger Store appliance, you need to perform its initial setup. The initial setup includes the following procedures:

• Configure the IP address of each network port of the appliance (see "Configure the IP Addresses of the Appliance" on page 32).

• Change the name of the appliance (see "Change the Name of The Appliance" on page 35).

• Specify the time and date settings of the appliance (see "Specify The Time and Date Settings of the Appliance" on page 36).

• Set the environment in which Tiger Store operates - workgroup or Active Directory domain (see "Select The Network Environment of Tiger Store" on page 37).

Important: *If your Tiger Store appliance features two server nodes, in order to synchronize the settings specified during the initial setup between the server nodes, it is advisable both of them to be turned on.*

Once you go through the initial setup, Tiger Store can operate normally without having to change any of its settings. Later on you can change any of the settings that you have specified during the initial setup from any computer that has access to Tiger Store's web interface.

You can perform the initial setup of the appliance in the web interface of Tiger Store.

Configure Appliance Identification and Connectivity

Each Tiger Store appliance is identified in the network by IP address and name (by default, this is the serial number of the appliance).

The appliance must have an IP address for each network port through which it communicates with Tiger Clients (directly or via an Ethernet switch). The IP address of each network port must be on the same LAN as the Tiger Client that will communicate with the appliance through this port. For more information, refer to "Configure the IP Addresses of the Appliance" on page 32.

Tiger Store supports teaming of the ports of each network card. If you choose to team the ports of a network card, all its ports will be accessible through just one IP address. To benefit from ports teaming, you must use an Ethernet switch, which supports Link Aggregation Control Protocol (IEEE 802.1ax, LACP) and is set up for teaming.

Additionally, Tiger Store allows you to assign two or more IP addresses to the same network card, thus making it accessible from networks on different subnets.

Changing the name of the appliance can be useful to more easily identify your appliance on the network or, if you deploy more than one Tiger Store appliances in your organization, to facilitate you in distinguishing them. For more information, refer to "Change the Name of The Appliance" on page 35.

Team/Unteam Network Ports

To facilitate you with assigning IP addresses to the network ports of the appliance, Tiger Store allows you to team the ports of a single network card. This way all ports of a network card will be accessible through a single IP address.

Important: *To benefit from ports teaming, you must use an Ethernet switch, which supports Link Aggregation Control Protocol (IEEE 802.1ax, LACP) and is set up for teaming.*

You can unteam the ports of a network card at any time. When you unteam the ports of a network card, they are automatically assigned the IP addresses they have had before teaming them - either the default ones assigned by the appliance, or the ones you have manually specified. Should you decide to team the ports again, you will have to specify the IP address manually again.

To team/unteam the ports of a network card:

1. In the left pane of Tiger Store's web interface, click System and then Network Configuration.

   The page lists all detected network cards, except the Public port and the Admin port, if such is predefined.

2. In the tile of a network card, do one of the following:

   • Select Use as a team, and then click Apply.
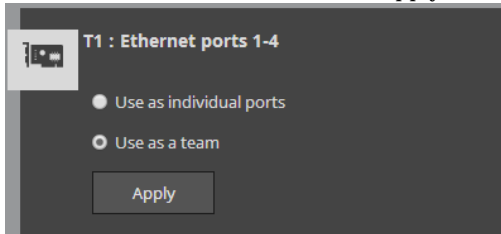
   The teamed ports are listed on the IP Configuration page, where you can assign an IP address to them.

   • Select "Use as individual ports", and then click Apply.
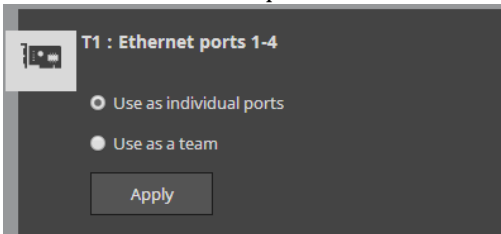
   The ports are listed on the IP Configuration page individually with their previous IP addresses (the ones you have manually specified, or, if none has been specified, the default ones).

Configure the IP Addresses of the Appliance

Your Tiger Store appliance can have any of the following network ports:

Public port — 1GbE port designed to connect the appliance to your corporate network and provide it with access to shared resources and the Internet and also used for metadata exchange between the appliance and Fibre Channel Tiger Clients.

1/10GbE ports — designed to provide for both data and metadata traffic of Tiger Clients connected to the appliance via 10GbE connection.

You must set an IP address for each network port through which the appliance is connected to Tiger Clients (directly or via an Ethernet switch) - the Public port and all other available network ports

or port teams. The IP address you assign to each network port must be on the same subnet as the Tiger Client that will communicate with the appliance through this port. If computers in your facility are already interconnected in a LAN, you can simply assign an IP address to the Public port in the same subnet.

When a LAN client can reach the appliance both through the Public port and another faster port, to ensure that the Tiger Client always mounts the shared volumes over the faster connection, it is advisable to set the IP addresses of the faster ports of both the appliance and the Tiger Client to be on a separate subnet of the LAN used by the Public port. For more information refer to the "Assigning IP Addresses to Network Ports" best practices topic in the latest version of the product release notes.

On Tiger Store appliance with high availability activated, to guarantee the failover between the two server nodes, the network ports/port teams with identical names on both nodes (the Public ports, for example) must be on the same subnet. To facilitate you in this task, Tiger Store attempts to automatically synchronize the IP settings of the two nodes, when you specify these settings in cluster view of the web UI. Thus, when you set an IP address of the Public port, for example, Tiger Store assigns it to the Public port of the current primary node and automatically assigns a consecutive IP address in the same subnet to the Public port of the secondary node. In case the consecutive IP address is already in use or the secondary node is offline, the automatic synchronization fails and you will have to manually specify the IP addresses of the secondary node's network ports in node view. You can ensure that the IP settings of both nodes are synchronized in the HA Nodes page of the web UI. For more information, refer to "Manage High Availability" on page 91.

Important: *Whenever you introduce changes to the IP settings of Tiger Store, on all Tiger Clients you may have to re-add the appliance to the storage servers list, in order to ensure that they can connect to it.*

IP Addresses Limitations

When assigning IP addresses to the network ports of Tiger Store, make sure that you avoid the following IP addresses as they are either link-local addresses or are in use by Tiger Store services:

• Link-local addresses in the range 169.254.0.0 - 169.254.255.255

• IPMI addresses in the range 1.1.1.0 - 1.1.1.255

To assign an IP address to a network port:

1. In the left pane of Tiger Store's web interface, click System and then IP Configuration.

   The IP Configuration page loads. It lists the tiles of the Public port and all individual and/or teamed network ports.

2. In the tile of the respective port or team, enter the IP address and subnet mask.

Note: *As the Public port is also used for connection to the Internet, you can also specify router and DNS server details.*

3. (optional, to assign additional IP address) Click the + button and add an additional IP address and subnet mask for the same network port.

Tip: *You can add as many IP addresses to the same port, by clicking the "+" button. To remove one of the IP addresses, simply click "-" next to it.*

4. Click Apply.

For appliances with two server nodes, as long as the secondary node is also online, Tiger Store attempts to automatically synchronize the IP settings of both nodes and assign consecutive IP addresses to the identical network ports of the secondary node. In case the secondary node is offline or Tiger Store is unable to assign consecutive IP addresses to the ports of the secondary node, to ensure the high availability of the appliance, you must manually configure the IP addresses of one or both nodes in the node view of the respective node.

To assign an IP address to a network port in node view:

Note: *To configure the IP address of a network port, the port adapter must be online.*

1. In the left pane of cluster view, click HA Nodes.

2. In the tile of the server node whose IP settings you want to configure, click Manage Node.

The node view for the selected server node opens in a new tab/window of your web browser.

3. Click Manage and then enter the password for the web interface.

   Tip: *If you have changed the password for the cluster view of the web interface, while this node has been online - enter the new password. In other cases enter the default password - admin.*

4. In the left menu of the node view, click System and then IP Configuration.

5. In the tile of the respective port or team, enter the IP address and subnet mask.

   Note: *As the Public port is also used for connection to the Internet, you can also specify router and DNS server details.*

6. Click Apply.

   Tiger Store applies the new settings only to the selected node.

   Tip: *To make sure that the IP settings of both nodes are synchronized, go to the HA Nodes page of the web UI (see "Manage High Availability" on page 91).*

Change the Name of The Appliance

By default, each Tiger Store appliance is shipped to you with a pre-configured name - the appliance's serial number, printed at the back of the chassis and visible in the About page of the web UI. On appliances with two server nodes, the name of each node is comprised of the name of the appliance plus an automatically added suffix. Tiger Store takes care to automatically synchronize the name setting between the nodes in order to ensure failover can take place. Thus, when you change the name of the appliance on one node, as long as the other node is also online, its name is updated (but with different suffix) as well. When you change the name of the appliance on one node, while the other node is offline (or not available), it is advisable to manually synchronize the name setting across nodes when both of them are online.
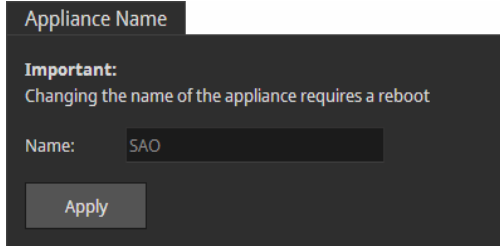
Note: *If you rename a Tiger Store appliance after client computers have already added it to their storage servers list, you may have to manually edit the appliance's name on client computers (refer to the "Tiger Client User's Guide").*

To rename the appliance:

Important: *To rename the appliance you will have to reboot it.*

1. In the left pane of Tiger Store's web interface, click System and then Settings.

2. In Appliance Name, enter a new name of the appliance and click Apply.
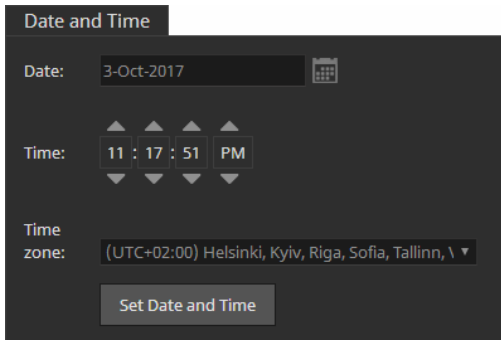
3. Confirm that you want to change the name of the appliance when prompted.

4. In the left pane, select System and then Maintenance.

5. In System Reset drop down box, select "Full system reboot" and then click Full system reboot.

Specify The Time and Date Settings of the Appliance

To ensure the normal work of Tiger Store, you should set the time and date of the appliance as soon as you turn it on. It is advisable to use the same date and time settings on all computers on your Tiger Store network.

To specify the time and date settings of the appliance:

1. In the left pane of the web interface, click System and then Settings.

2. In Date and Time, select the desired date, time zone and specify the exact time.

3. Click Set Date and Time.

Select The Network Environment of Tiger Store

By default, Tiger Store is configured to operate in workgroup environment - the appliance is pre-configured as a member of the WORKGROUP workgroup and any user that can connect to it, has access to all resources on the shared volumes. If your appliance is on the same network as an Active Directory domain controller, you can add the appliance to the domain and benefit from access permissions to files and folders for domain users. For the purpose, you should simply specify the domain name and authenticate as a user that has permissions to join computers to the selected Active Directory domain.

You can switch the network environment in which Tiger Store is deployed from workgroup to domain and vice versa at any time.

Important: *Setting the network environment of Tiger Store requires that you reboot the appliance.*

To set domain environment for Tiger Store:

1. In the left pane of the web interface, click System and then Settings.

2. In Domain Info, click Domain.

3. In the respective fields, enter the domain name and the user name and password of a user that can join computers to the specified Active Directory domain.

4. Click Apply.

5. In the left pane, select System and then Maintenance.

6. In System Reset drop down box, select Full System Reboot and then click Full system reboot.

   When the appliance is online again, accesses to files/folders on the shared volumes are authenticated against the specified Active Directory domain.

To set workgroup environment for Tiger Store:

1. In the left pane of the web interface, click System and then Settings.

2. In Domain Info, click No domain.

The domain controller may require that you authenticate yourself as a user authorized to remove computers from the domain.

3. Click Apply.

4. In the left pane, select System and then Maintenance.

5. In System Reset drop down box, select Full System Reboot and then click Full system reboot.

When the appliance is online again, all users that can mount the shared volumes have unrestricted access to all files/folders on it.

Smart Storage Pooling

Note: *Smart storage pooling is not supported on Linux Tiger Clients and they always mount the individual volumes only.*

The smart storage pooling add-on allows you to unite the volumes shared by the storage server into a single virtual volume - the storage pool - that Windows and Apple Mac Tiger Clients can access through a universal mount point. The pool size equals the sizes of all volumes that comprise it and presents their existing folder structures as one merged folder structure. Volumes can contain data prior to uniting them in a storage pool and it will remain visible in the pool. Similarly, when the pool is disbanded (by disabling smart storage pooling), all data remain on the respective Tiger Store volume and is accessible through the volume itself.

When enabling smart storage pooling on volumes that already contain data, it is possible ambiguity of file objects to occur i.e. files/folders with one and the same name to exist in exactly the same location on two or more volumes in the pool. For more details, refer to "Files and Folders Ambiguity" on page 43.

By default, when writing new data on the pool, Tiger Store tries to store it on the same file system on which the containing folder is stored. In case you write new data on the root of the storage pool, Tiger Store creates it in the root of the shared volume that has more free space. You can change this default behaviour, by applying a data distribution policy. For more details, see "Data Distribution within the Storage Pool" on page 41.

To enable smart storage pooling, there must be at least two shared volumes available. While smart storage pooling is enabled, you can set any volume in the pool to Private or Offline and clients will continue to mount the pool as long as at least one of the volumes in it is shared, but will not be able to access data stored on volumes that are not shared.

You can enable and disable smart storage pooling at any time as long as Tiger Bridge's replication is not currently enabled. You cannot enable smart storage pooling if workspace quotas are enabled in Tiger Spaces. Mac OS X and Windows Tiger Clients will detect that they should mount either the individual volumes or the pool, only on the next attempt to mount the Tiger Store storage.

Options you might want to configure after enabling/disabling smart storage pooling include volume mount location for the pool, Tiger Bridge data replication and space reclaiming.

Enable/Disable Smart Storage Pooling

To enable/disable smart storage pooling:

Note: *You cannot change smart storage pooling settings, while Tiger Bridge data replication is enabled.*

1. In the left pane of the web interface, click Shared Volumes.

2. In Smart Storage Pooling, do one of the following:

> **Smart storage pooling**
>
> Smart storage pooling allows easy and transparent expansion of shared volumes when you connect additional formatted storage. If you enable this feature you do not need to reformat your existing shared volumes to increase the capacity.
>
> Note: Clients should reconnect to detect the change.
>
> ☑ Enable smart storage pooling

• Select the "Enable smart storage pooling" check box, to unite all shared volumes in a pool.

Note: *You cannot enable smart storage pooling if quotas are enabled in Tiger Spaces.*

• Clear the "Enable smart storage pooling" check box, to disband the volume pool and let Tiger Clients access the individual volumes instead.

Data Distribution within the Storage Pool

By default, when writing new data on the pool, Tiger Store tries to store it on the same file system on which the containing folder is stored. In case you write new data in the root of the storage pool, Tiger Store creates it in the root of the volume that has more free space.

You can change this default behaviour for newly created folders, by applying a data distribution policy to a folder (the root of the volume pool or any folder in the pool):

Balance by size — creates the folder on the volume in the storage pool, which has more free space.

Balance by count — creates the folder on the volume in the storage pool, which has the minimal number of folder entries.

Note: *Files are always stored on the volume of their parent folder regardless of the policy you apply.*

To apply one or the other of the above policies, you should create a file with the name of the policy in the root of the storage pool or in any of its subfolders, thus instructing Tiger Store to calculate either the free space or the number of folders on each volume in the pool and only after that to create the new folder on the volume that matches the policy. Should the policy instruct Tiger Store to create the new folder not on the volume containing the parent folder, but on another volume, Tiger Store replicates the entire folder structure from the root of the volume pool to the newly created folder so that the path used to access it would be the same as if accessing it from the parent

folder. For example, if on one shared volume you have a folder "Projects" that contains three subfolders - "May", "June" and "July", and you set the creation behaviour of folder "June" to use the Balance by count policy, when you create a new folder "Drafts" in the "June" folder, and it needs to be stored on another volume, because there are less file objects on it, Tiger Store will create in the root of the other volume, a folder "Projects" containing just the folder "June" with a subfolder "Drafts". The policy is valid just for the folder containing the respective policy file and is not applied recursively to its sub-folders i.e. if you create new folders in the folder "Drafts", which doesn't contain a policy file, the new folders will be stored on the second volume.

If the policy file is missing or both files are stored in the root of the volume pool, Tiger Store assumes that the default behaviour should be used i.e. the folder should be created on the same file system on which the containing folder is stored or, in case this is the root of the volume pool - on the volume that has more free space.

Note: *You can create the policy file from any connected Tiger Client that can mount the pool or the volumes in it.*

To set policy for newly created folders from Windows:

1. In command prompt, navigate to the folder where you want to create the policy file (the root of the volume pool or a subfolder in the pool).

2. Do one of the following:

   • To set balance by size policy, execute the following command:
   ```
   type NUL > .pool_balance_size
   ```

   • To set balance by count policy, execute the following command:
   ```
   type NUL > .pool_balance_count
   ```

   The file is created in the specified location and Tiger Store is instructed to create new folders in this location based on the rules of the selected policy.

To set policy for newly created folders from Mac OS X and Linux:

1. In Terminal/command-line, navigate to the folder where you want to create the policy file (the root of the volume pool or a subfolder in the pool).

   Note: *As smart storage pooling is not supported on Linux, to create the policy file in the root of the volume pool, simply create it in the root of one of the volumes in it, making sure that another policy file doesn't exist in the root of the other volumes in the pool.*

2. Do one of the following:

   • To set balance by size policy, execute the following command:
   ```
   touch .pool_balance_size
   ```

• To set balance by count policy, execute the following command:

```
touch .pool_balance_count
```

The file is created in the specified location and Tiger Store is instructed to create new folders in this location based on the rules of the selected policy.

Files and Folders Ambiguity

As Tiger Store lets you unite in a virtual volume pool volumes that already contain data, it is possible ambiguity of file objects to occur i.e. files/folders with one and the same name to exist in exactly the same location on two or more member volumes. Additionally, Linux Tiger Clients can also contribute to file/folder ambiguity as they always mount the individual volumes and there's no way to prevent them from creating a folder/file with one and the same name in exactly location on more than one of the volumes.

Tiger Store discerns three types of ambiguity:

folder ambiguity — folders with one and the same name existing in exactly the same location on two or more volumes in the pool - for example, a folder "Work" in the root of two shared volumes.

file ambiguity — files with one and the same name existing in exactly the same location on two or more volumes in the pool - for example, a file "Work" in the root of two shared volumes in the pool.

combined ambiguity — a file and a folder with identical names existing in exactly the same location on two or more member volumes in the pool - for example, a folder "Work" and a file "Work" in the root of two volumes in the pool.

Although no data is lost after enabling smart storage pooling, the operating system does not allow two or more files/folders with exactly the same name to coexist in the same location.

When ambiguity occurs with folders, Tiger Store simply displays only one folder in the storage pool and it contains the merged contents of all ambiguous folders with the same name. Still, the displayed folder has the attributes of the ambiguous folder that has been most recently modified. For example, if a folder "Work" with Hidden attributes is stored in the root of volume A and has been most recently modified, and a folder "Work" with Read-only attributes is stored in the root of volume B, the folder "Work" in the root of the storage pool has Hidden attributes. Additionally, if you attempt to delete an ambiguous folder, all folders with the same name are deleted from their volumes.

When ambiguity occurs at file level, Tiger Store displays the ambiguous file with latest modification time stamp and hides the other instances. When performing a file operation on an ambiguous

file in the file browser of your operating system, you can expect the following:

• deleting the ambiguous file that is shown in the storage pool deletes all other ambiguous files as well;

• renaming the ambiguous file that is shown in the pool renames all other ambiguous files as well;

• moving an ambiguous file, moves only the file displayed in the pool and deletes the other ambiguous files with the same name;

In the case of combined ambiguity, Tiger Store always displays the folder and hides the file with the same name. When performing a file operation, Tiger Store performs it only on the folder and ignores the files with the same name in the same location.

Resolve Ambiguities

It is highly advisable to resolve all ambiguities in your pool. You can resolve ambiguities in the file browser of any Tiger Client that has mounted the pool. On Mac OS X and Windows Tiger Clients, you should first disable smart storage pooling and mount the individual volumes. To resolve ambiguities from Linux Tiger Clients, there's no need to disable smart storage pooling. You can resolve ambiguities in the following ways:

• by deleting, renaming or moving the ambiguous file/folder (file ambiguity, folder ambiguity and combined ambiguity);

• by unifying the attributes of the ambiguous folders (folder ambiguity);

Important: *When renaming or moving an ambiguous file, you should take care not to create a new ambiguity.*

To resolve ambiguity in a Tiger Client's file browser:

1. *(if you resolve ambiguities from Mac OS X or Windows)* In the Shared Volumes page, clear the "Enable smart storage pooling" check box, to disband the volume pool and let Tiger Clients access the individual Tiger Store volumes.
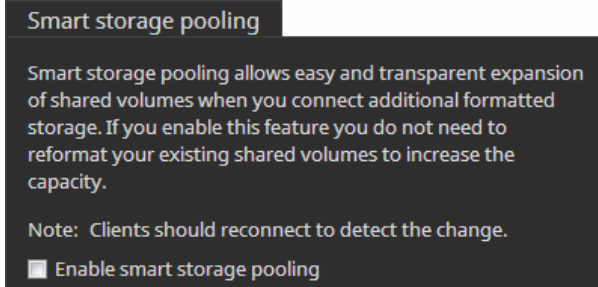
Note: *You cannot change smart storage pooling settings, if Tiger Bridge data replication is enabled.*

2. In the file browser of your operating system, open one of the member volumes to the ambiguous file/folder and do one of the following:

   • delete, rename or move to another location the ambiguous file/folder;

   • change the ambiguous folder's attributes to match the attributes of the other ambiguous folders with the same name;

3. Repeat the above step until all ambiguities in the pool are resolved.

4. *(optional, if you have disabled smart storage pooling)* In the Shared Volumes page, select the "Enable smart storage pooling" check box, to unite the available Tiger Store volumes in a pool.

Smart Storage Pooling

Manage the Tiger Store Storage

For the purposes of the Tiger Store workflow, you can manage the volumes accessible to the storage server in the following ways:

• Share/unshare a volume (see "Share or Unshare Volumes" on page 51).

• Make a volume offline (see "Make a Volume Offline" on page 53).

• Set volume mount location on Windows Tiger Clients (see "Set Volume Mount Location (Windows Only)" on page 53).

Additionally, depending on whether you use the software-only version of the product or a Tiger Store appliance, you can perform some or all of the following operations on volumes, connected to the storage server:

• Rename a volume (see "Rename a Tiger Store Volume" on page 67).

• Create a new volume or create/re-build a RAID on appliances exporting their own storage (see "Create New Volume" on page 55).

• Manage dynamic disks seen by Tiger Store appliances managing external volumes (see "Manage Dynamic Disks Connected to the Appliance" on page 66).

• Perform maintenance operations on a volume:

   • Check and repair the file system of a volume (see "Check and Repair The File System" on page 69).

   • Enable/disable auto-defragmentation of the shared volume(s) (see "Volume Defragmentation" on page 69).

   • Manually defragment a shared volume, when auto-defragmentation is disabled (see "Manually Defragment a Tiger Store Volume" on page 70).

• Export a volume or a folder on it as a SMB/CIFS share to computers that don't have the Tiger Client software installed (see "Share a Volume as a SMB/CIFS Share" on page 71).

Some of the above operations on the shared storage require higher protection. That is why before you perform them, you may have to unshare the volume for Tiger Clients, enter Maintenance mode or even shut down one of the nodes of a Tiger Store storage server with two server nodes. Entering Maintenance mode automatically disconnects all client computers from the shared volumes, that is why it is advisable to make sure that no file operation is being interrupted by entering Maintenance mode. After exiting Maintenance mode client computers are not automatically reconnected to the shared volume and have to manually connect to the storage server in order to mount the volume(s).

Important: *If the storage server is rebooted while in Maintenance mode, any maintenance operation going on at the moment is canceled and clients can reconnect to Tiger Store.*

View Storage Information

View Shared Volumes Details

You can view details about volumes shared to Tiger Clients in the Shared Volumes page of the web interface. If smart storage pooling is disabled for Tiger Store, it displays all shared Tiger Store volumes as separate volume tiles. If smart storage pooling is enabled, it displays the volume tile of the virtual volume. You can view the following details:
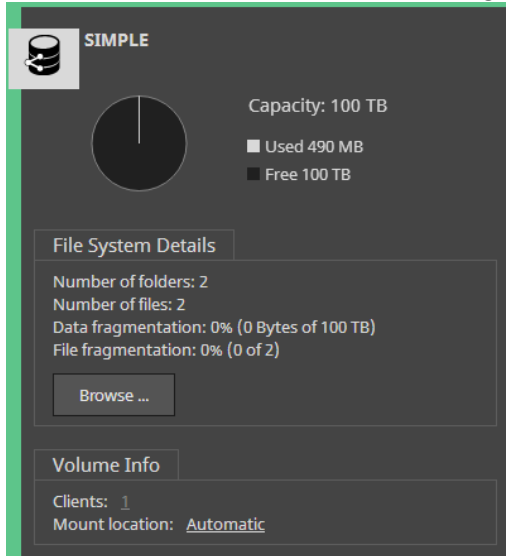
• Volume name.

• Pie chart of the volume capacity with free and used space statistics.

• File system details - number of files and folders on the volume, and fragmentation statistics.

• Number of connected clients.

• Default mount location of the volume on all Windows Tiger Clients.

View All Volumes Details

In the Volumes page (Storage Management | Volumes) each volume seen by Tiger Store is presented with a separate tile, even if smart storage pooling is enabled on Tiger Store. The volume tile in the Volumes page gives you information about the file system, size, partition and disk type,

the capacity of the volume, the free and used space on it as well as the mode of the volume for Tiger Clients (shared, offline or private).
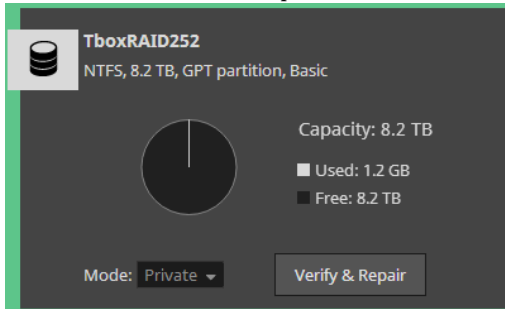
Viewing Disks Details

Note: *This view is available only on Tiger Store appliances, which manage external storage.*

You can view details about the disks accessible to Tiger Store in the Disks page (Storage Management | Disks).

In the Disks page each accessible disk is represented with a separate tile, that gives you information about the disk capacity, status, type and partition(s).
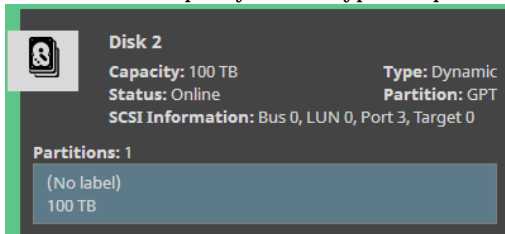
Note: *To view disk details on a storage server with two server nodes, when both of them are turned on, you should view the Disks page in node view of the respective node (HA Nodes | Manage Node).*

View Storage Chassis Details

Note: *This view is available only on Tiger Store appliances, which manage internal storage only.*

In the Chassis page (Storage management | Chassis) each available chassis is represented with a separate tile, that gives you information about the RAID level and status, the number of drives

comprising the RAID, the total capacity of the RAID and the temperature reported by the RAID controller:
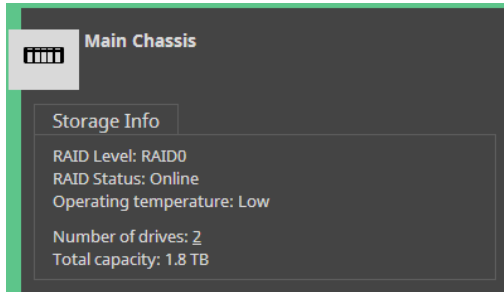
Note: *If the RAID initialization has been halted or interrupted for some reason, a button Resume appears in the chassis' tile, allowing you to resume the RAID initialization process.*

Share or Unshare Volumes

Volumes in the Tiger Store network can have one of the following states:

Shared — the volume can be mounted only on Tiger Clients;

Note: *If smart storage pooling is enabled (see "Smart Storage Pooling" on page 39), the pool mounts on Tiger Clients only if at least one of its volumes is shared.*

Private — the volume is accessible only to the storage server and neither Tiger Clients, nor computers without the Tiger Client software can mount it and work with it;

Offline — the volume is not managed by Tiger Store and can be mounted by any computer that sees it;

Note: *This option is not available on Tiger Store appliances exporting their own disk array to Tiger Clients.*

You can choose which of the volumes managed by the storage server to share to Tiger Clients (by making them shared) and which ones to computers without the Tiger Client software installed (by making them offline). You cannot share a Private volume that is currently used as a replication target by Tiger Bridge. To share such a volume, first disable Tiger Bridge replication on it.

Whenever you perform a maintenance operation like checking and repairing the file system of a volume, instead of disconnecting Tiger Clients from all shared volumes by entering Maintenance mode, you can unshare the volume on which you will perform the respective maintenance operation and after that share it again. You can also set a volume to Private, in order to use it as a replication target for Tiger Bridge. In this case, you cannot share the volume to Tiger Clients until you disable Tiger Bridge replication on it.

To share a volume to Tiger Clients:

Important: *If you share an Offline volume, all non-Tiger Client computers that access it will dismount it and will lose any unsaved data on that volume.*

1. In the left pane of Tiger Store's web interface, click Storage Management and then Volumes.

2. In the Volumes page, find the tile of the private/offline volume, which you want to share and in the drop-down box select Shared.
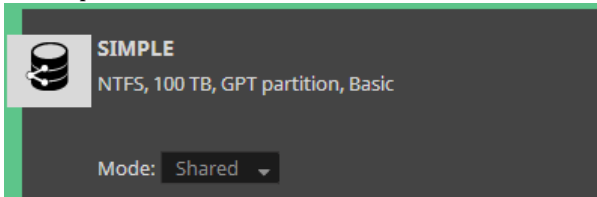
Note: *You cannot share a volume if the product is not activated.*

3. Confirm that you want to share the volume to Tiger Clients.

   The volume is shared to all Tiger Clients that have access to it.

To make a volume Private for the storage server:

Important: *If you make Private an Offline volume, all non-Tiger Client computers that access it will dismount it and will lose any unsaved data on that volume.*

1. In the left pane of Tiger Store's web interface, click Storage Management and then Volumes.

2. In the Volumes page, find the tile of the volume, which you want to unshare and in the drop-down box select Private.
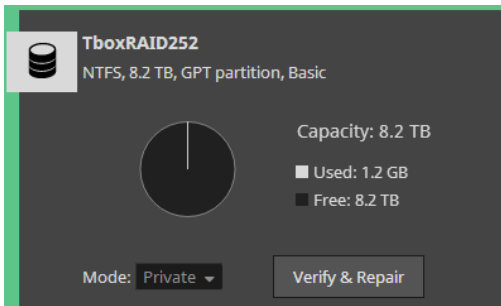
3. Confirm that you want to make the volume Private for the storage server.

   The volume is made Private for the storage server and all computers that had access to it (Tiger Clients or non-Tiger Clients) can no longer mount it.

Make a Volume Offline

Note: *This option is not available on Tiger Store appliances exporting their own disk array to Tiger Clients.*

By default, Tiger Store manages all volumes that the storage server is connected to. Whether or not the storage server shares them to Tiger Clients, these volumes are protected and cannot be mounted by computers that don't run the Tiger Client software, even though they may have access to these volumes. To let non-Tiger Client computers work and mount volumes that Tiger Store sees, you should remove Tiger Store's protection over them. You can do this by making them Offline. An Offline volume is accessible to any computer that sees that volume.

Important: *As offline volumes are not protected by Tiger Store, you should take care not to let more than one computer to mount them at a time in order to prevent data corruption on them.*

To make a volume offline (remove Tiger Store protection):

Important: *If you make a shared volume Offline, all Tiger Clients that access it will dismount it and will lose any unsaved data on that volume.*

1. In the left pane of Tiger Store's web interface, click Storage Management and then Volumes.

2. In the Volumes page, find the tile of the volume, which you want to make offline and in the drop-down box select Offline.
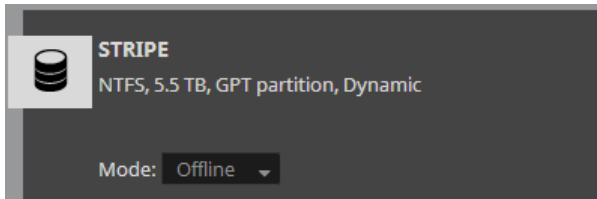
Note: *You cannot set to Offline a volume that is currently used as a replication target by Tiger Bridge. To make the volume Offline for the appliance, you must first disable Tiger Bridge replication on it.*

3. Confirm that you want to make the volume Offline.

   The volume is made Offline and all non-Tiger Client computers that see it can mount it.

Set Volume Mount Location (Windows Only)

By default, each Tiger Store volume uses Automatic mount location on all client computers:

• Windows - the first available drive letter.

• Mac OS X - /Volumes.

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

In the web interface of Tiger Store, you can specify a preferred drive letter as mount location of a Tiger Store volume on all Windows machines. This way, you can make a volume to be mounted in one and the same location on all Windows machines that see it.

Note: *If you specify a drive letter as default mount location, but this drive letter is already in use on a Windows Tiger Client computer, it uses Automatic as mount location setting.*

You can also overwrite this setting for a particular Windows Tiger Client, by specifying different drive letter as default mount point on this computer. For more information, refer to the "Tiger Client User's Guide".

To set default mount location on Windows Tiger Clients:

1. In the left pane of Tiger Store's web interface, click Shared Volumes.

2. In the tile of the selected volume, click the link next to Mount Location.
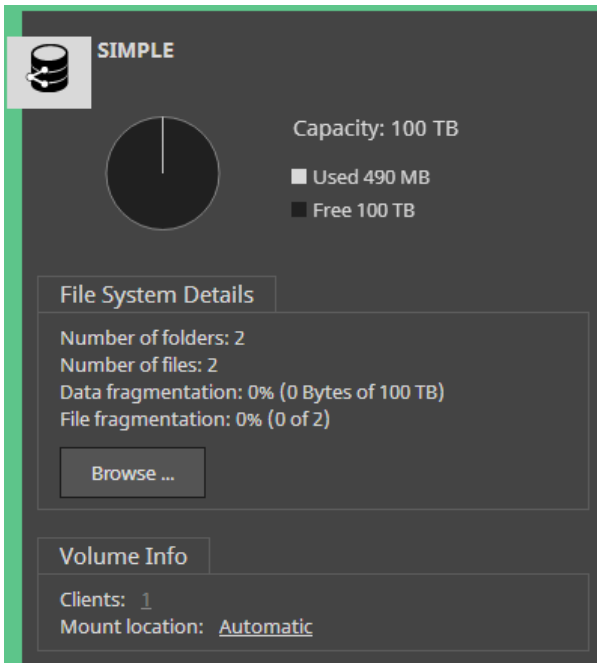
3. In the Mount Location dialog, do one of the following:
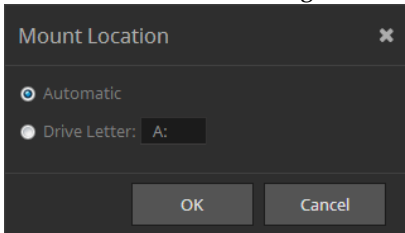
• Select Automatic to let the volume mount on Tiger Clients using the first available drive letter.

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

4. Click OK.

The volume is mounted in the new mount location on Tiger Clients only after they remount it.

Create New Volume

The steps for creating a new volume differ depending on whether your storage server runs a software-only version of Tiger Store or you use a Tiger Store appliance.

On Tiger Store appliances exporting their own disk array to Tiger Clients, you can only create a new RAID on the chassis of the appliance or re-build an existing RAID. See "Manage RAID" on page 62.

Create New Volume (Software-only version)

You can create a new volume on the computer that is storage server after you enter Maintenance Mode. Entering Maintenance mode automatically disconnects all Tiger Clients from the shared storage and stops any file operation going on at the moment.

You can also create a new volume on the disks of a volume seen by the storage server from any non-Tiger Client computer that sees these disks, as long as the volume is made Offline in the Tiger Store interface (see "Make a Volume Offline" on page 53).

To create a new volume:

1. In the left pane of the web interface, click System and then Maintenance.

2. In the Maintenance page, click Enter Maintenance Mode and then confirm that you want to enter Maintenance mode.
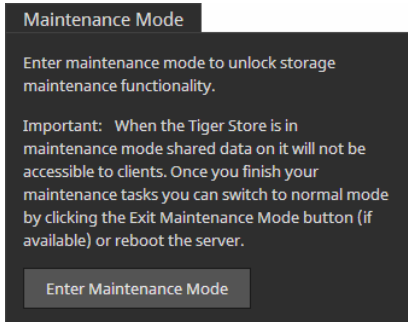
The storage server automatically disconnects all Tiger Clients currently accessing the volumes.

Important: *If you exit Maintenance mode or the storage server is rebooted while in Maintenance mode, any maintenance operation going on at the moment is canceled and clients can re-connect to Tiger Store.*

3. On the storage server, create the new volume, following the steps described in your OS documentation.

4. In the left pane of the web interface, click System and then Maintenance.

5. In the Maintenance page, click Exit Maintenance Mode.
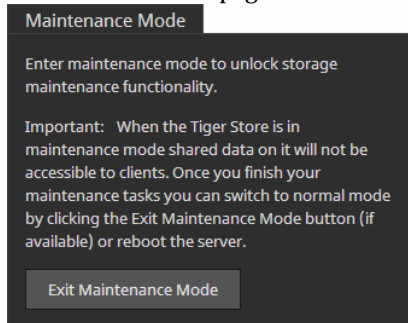
6. In the left pane of the web interface, click Storage Management and then Volumes.

7. Do one of the following:

   • to share the volume to Tiger Clients, in the tile of the newly created volume, click Shared.

   • to let non-Tiger Client computers access the volume, in the tile of the newly created volume, click Offline.

Create New Volume on a Tiger Store Appliance

Note: *On Tiger Store appliances exporting their own disk array to Tiger Clients, you can only create a new RAID on the chassis of the appliance or re-build an existing RAID. See "Manage RAID" on page 63.*

You can create a new volume in the web UI of a Tiger Store appliance managing external storage. You can create either a simple GPT volume (on a single disk) or an NTFS striped volume (on multiple disks). The new volume can be on disks that are not part of any volume or on the disks of an existing volume. When you create a new volume on the disks of an existing volume, you need to clean the disks of their storage type (basic or dynamic). For more information, refer to "Clean Disks" on page 57. When creating an NTFS striped volume, you can set the stripe chunk size of the new volume.

You can also create a new volume on the disks of a volume seen by Tiger Store from any non-Tiger Client computer that sees these disks, as long as the volume is made Offline in the Tiger Store interface (see "Make a Volume Offline" on page 53).

Clean Disks

To create a new volume on the disk(s) of an existing volume, you should first clean the disks of their storage type. By cleaning a disk from its storage type you destroy the existing volume and all data on it. When the disks, on which you want to create a new volume in Tiger Store's web UI, are not part of an existing volume, there's no need to clean them.

On appliances with two server nodes, you can clean a volume's disks or create a new volume in cluster view (the appliance's web UI), but only one of the server nodes must be online. When both server nodes of your appliance are online, before proceeding you should shut down one of the server nodes.

Important: *Cleaning a disk is an operation that requires entering Maintenance mode. Entering Maintenance mode automatically disconnects all client computers from the shared storage and stops any file operation going on at the moment.*

To clean a disk of its storage type:

1. In the left pane of the web interface, click System and then Maintenance.

   Important: *On appliances with two server node, both of which are online, before entering Maintenance mode in cluster view, you must first shut down one or the other server node in node view of the web interface.*

2. In the Maintenance page, click Enter Maintenance mode and confirm then confirm that you want to enter Maintenance mode.

Maintenance Mode

Enter maintenance mode to unlock storage maintenance functionality.

Important: When the Tiger Store is in maintenance mode shared data on it will not be accessible to clients. Once you finish your maintenance tasks you can switch to normal mode by clicking the Exit Maintenance Mode button (if available) or reboot the server.

[Enter Maintenance Mode]

The appliance automatically disconnects all Tiger Clients currently accessing the volumes and the button changes to Exit Maintenance mode.

Note: *If you exit Maintenance mode or the appliance is rebooted while in Maintenance mode, any maintenance operation going on at the moment is canceled and clients can re-connect to Tiger Store.*

3. In the left pane of Tiger Store's web interface, click Storage Management and then Disks.

4. In the Disks page, select the tile of the disk that you want to clean and click Clean Disk in the menu on top of the page.

☑ Disk 2
Capacity: 2.73 TB   Type: Dynamic
Status: Online   Partition: GPT

SCSI Information: Bus 0, LUN 2, Port 1, Target 0

Partitions: 1

(No label)
2.73 TB

Tiger Store cleans the selected disks of their storage type and when the operation finishes updates their tiles with type "Unknown".

Tip: *You can view the operation progress in the band at the top of the page.*

5. Do one of the following:

• Without exiting Maintenance Mode, proceed to create a new volume on the cleaned disk(s).

• Exit Maintenance Mode (go to System | Maintenance, and click Exit Maintenance Mode) to let client computers connect to the shared volumes again.

Create New Basic GPT Volume

Important: *Creating a new volume is an operation that requires entering Maintenance mode. Entering Maintenance mode automatically disconnects all client computers from the shared volumes and stops any file operation going on at the moment.*

To create a new basic GPT volume:

1. In the left pane of the web interface, click System and then Maintenance.

   Important: *On appliances with two server node, both of which are online, before entering Maintenance mode in cluster view, you must first shut down one or the other server node in node view of the web interface.*

2. In the Maintenance page, click Enter Maintenance mode and confirm then confirm that you want to enter Maintenance mode.

   The appliance automatically disconnects all Tiger Clients currently accessing the volumes and the button changes to Exit Maintenance mode.

   Note: *If you exit Maintenance mode or the appliance is rebooted while in Maintenance mode, any maintenance operation going on at the moment is canceled and clients can re-connect to Tiger Store.*

3. In the left pane of Tiger Store's web interface, click Storage Management and then Disks.

4. Select the tile of the disk on which you want to create the new basic GPT volume and click Create Volume.

   Note: *The disk you have selected must be with "Unknown" type, designating it's cleaned of its storage type formatting.*

5. In the Volume dialog, specify the name of the new volume and click OK.
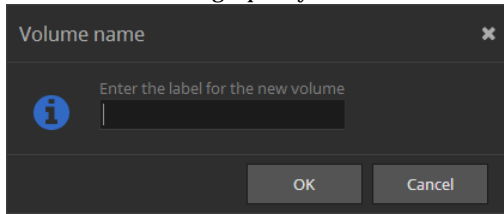
6. Exit Maintenance Mode (in System | Maintenance, click Exit Maintenance Mode) to let Tiger Clients connect to the shared volumes again.

7. Do one of the following:

• to share the volume to Tiger Clients, in the tile of the newly created volume, click Shared.

• to let non-Tiger Client computers access the volume, in the tile of the newly created volume, click Offline.

8. On an appliance with two server node, manually turn on the other server node by clicking its power button on the front panel of the appliance.

Create New Striped GPT Volume

Important: *Creating a new volume is an operation that requires entering Maintenance mode. Entering Maintenance mode automatically disconnects all client computers from the shared volumes and stops any file operation going on at the moment.*
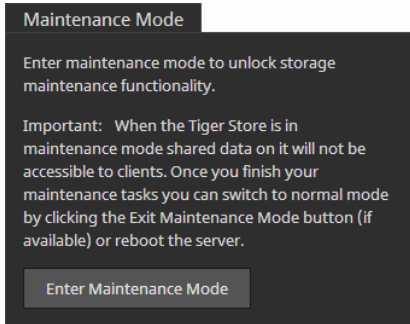
To create a new striped GPT volume:

1. In the left pane of the web interface, click System and then Maintenance.

Important: *On appliances with two server node, both of which are online, before entering Maintenance mode in cluster view, you must first shut down one or the other server node in node view of the web interface.*
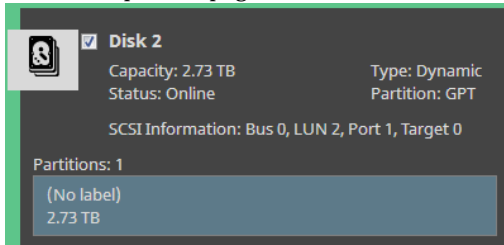
2. In the Maintenance page, click Enter Maintenance mode and confirm then confirm that you want to enter Maintenance mode.

Maintenance Mode

Enter maintenance mode to unlock storage maintenance functionality.

Important: When the Tiger Store is in maintenance mode shared data on it will not be accessible to clients. Once you finish your maintenance tasks you can switch to normal mode by clicking the Exit Maintenance Mode button (if available) or reboot the server.

[Enter Maintenance Mode]

The appliance automatically disconnects all Tiger Clients currently accessing the volumes and the button changes to Exit Maintenance mode.

Important: *If you exit Maintenance mode or the appliance is rebooted while in Maintenance mode, any maintenance operation going on at the moment is canceled and clients can re-connect to Tiger Store.*

3. In the left pane of Tiger Store's web interface, click Storage Management and then Disks.

4. Select the tiles of the disks on which you want to create the new striped volume and click Create Stripe.

Note: *The disks you have selected must be with "Unknown" type, designating they are cleaned of their storage type formatting.*

Disk 2 (Unallocated)
Capacity: 2.73 TB   Type: Unknown
Status: Online   Partition: NA
SCSI Information: Bus 0, LUN 2, Port 1, Target 0

5. In the Volume Name dialog, specify the name of the new volume.

Volume name   ✖

Enter the label for the new volume

Stripe chunk size: 64 ▼

[OK]   [Cancel]

6. (*optional*) In Stripe Chunk Size, select the desired value.

Note: *If you don't make a selection, Tiger Store uses the default stripe chunk size of 64KB.*

7. Click OK.

   Tiger Store creates a new striped volume on the selected disks.

8. Exit Maintenance Mode (in System | Maintenance, click Exit Maintenance Mode) to let Tiger Clients connect to the shared volumes again.

9. Do one of the following:

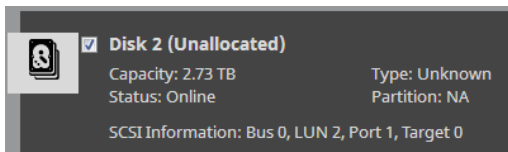   • to share the volume to Tiger Clients, in the tile of the newly created volume, click Shared.

   • to let non-Tiger Client computers access the volume, in the tile of the newly created volume, click Offline.

10. On an appliance with two server node, manually turn on the other server node by clicking its power button on the front panel of the appliance.
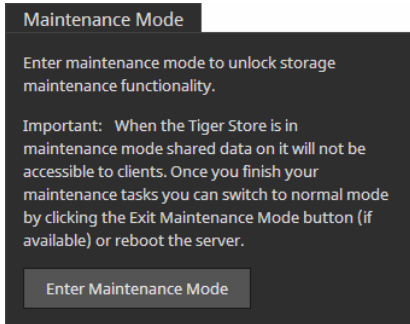
Manage RAID

Note: *You can create a new RAID or re-build an existing RAID through the Tiger Store web interface only on appliances exporting their own storage.*

Create a New RAID

Note: *This option is available only on Tiger Store appliances, exporting their own disk array.*

You can create a new RAID on the disks of the main chassis or the expansion chassis. For the purpose, first you have to destroy the existing RAID (if any) and then create the new RAID, choosing between the following RAID types:

• RAID 5 (default) - provides optimal performance and allows the RAID to operate with one failed drive;

• RAID 6 - provides improved fault tolerance, allows the RAID to operate with up to two failed drives;

• RAID 0 - provides maximum speed;

Important: *All data on the disks will be lost after creating a new RAID. That is why it is advisable to back it up before creating the RAID.*

To create a new RAID:

1. In the left pane of the web interface, click System and then Maintenance.

2. In the Maintenance page, click Enter Maintenance mode and confirm then confirm that you want to enter Maintenance mode.
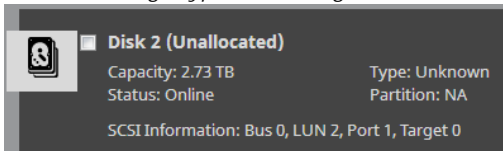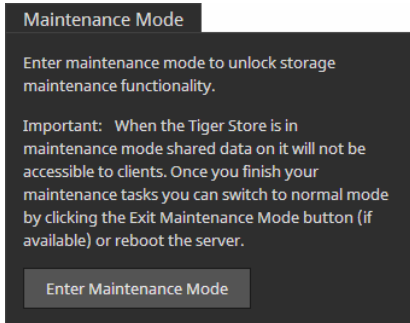

All connected Tiger Clients are automatically disconnected from the storage and any file operation going on at the moment is canceled.
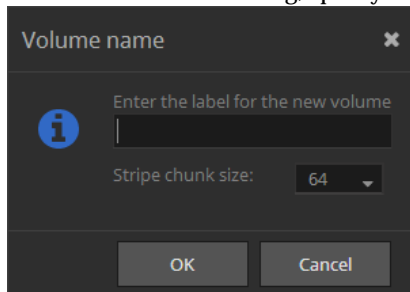
Important: *If you exit Maintenance mode or the appliance is rebooted while in Maintenance mode, any maintenance operation going on at the moment is canceled and clients can re-connect to Tiger Store.*

3. In the left pane of the web interface, click Storage Management and then Chassis.

4. In the Chassis page, find the tile of the chassis whose RAID you want to destroy and click Destroy RAID.
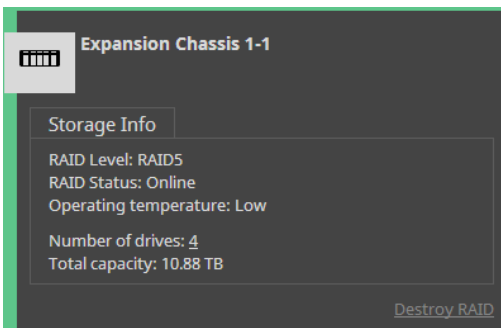
5. Click Continue to confirm that you want to destroy the RAID.

Tiger Store destroys the RAID.

6. In the tile of the chassis, whose RAID you have just destroyed click Create RAID.

Expansion Chassis 1-1

Storage Info

RAID Status: NONE

Number of drives: 4
Total capacity: 10.88 TB
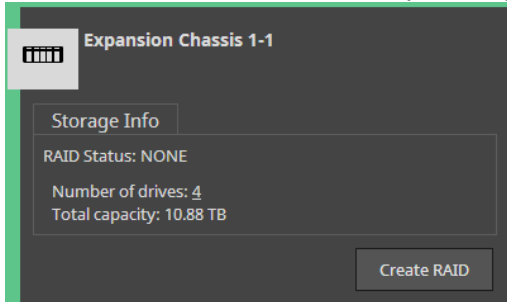
Create RAID

Note: *The Create RAID button is not available if Tiger Store is not operating in Maintenance Mode.*

7. In Create New RAID Options dialog, select the RAID type and click Continue.

Create New RAID Options ✕

Select the RAID type of the new RAID you want to create

◉ RAID 5 (Recommended) for optimal performance

○ RAID 6 for maximum protection

○ RAID 0 (Not recommended) for maximum speed

Continue   Cancel
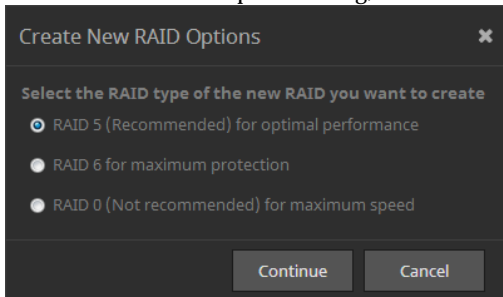
8. When the newly created RAID appears as a volume in the Volumes page, exit Maintenance mode (in System | Maintenance, click Exit Maintenance Mode) and share the new volume to Tiger Clients.

Re-build Existing RAID

The RAID controller of Tiger Store appliance exporting its own storage reports the RAID status in the Volume tile of the respective chassis:

Main Chassis

Storage Info

RAID Level: RAID0
RAID Status: Online
Operating temperature: Low

Number of drives: 2
Total capacity: 1.8 TB
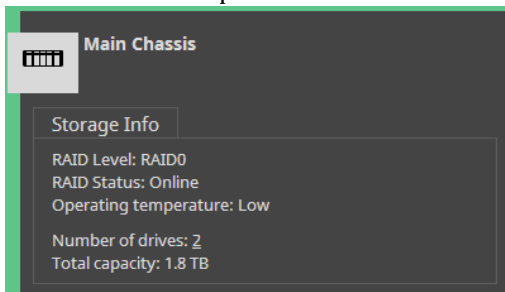
• Online

• Degraded - a drive has failed and the RAID needs to be re-built

• Rebuilding - the RAID is in the process of re-building

> Note: *If the re-building of the RAID has been interrupted, the status displayed is "Degraded (Rebuild - Halted)".*

Depending on how your RAID is configured, you can replace one (RAID5) or two (RAID6) failed hard disks, while the appliance is operating and no data on the RAID will be lost (refer to the appliance Assembly Guide for information about replacing a failed RAID drive). Once you replace the failed drive(s), you must re-build the RAID, following the steps below.

To re-build the RAID:

1. In the left pane of the web interface, click Storage Management and then Chassis.

2. In the tile of a volume with degraded RAID status, click Rebuild.
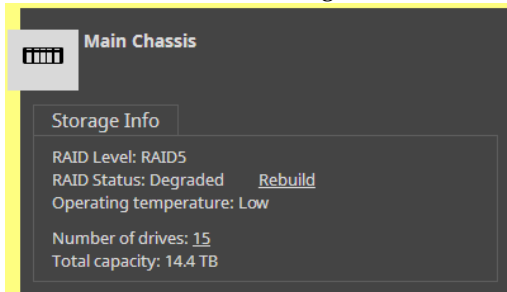
While the RAID is being re-built, it is still available to Tiger Clients although with decreased performance. You can pause the RAID re-building and then resume it again.

Import RAID

> Note: *This option is available only on 3U Tiger Store appliances with hardware version 3.0 exporting their own storage.*

If the RAID controller of your Tiger Store appliance fails to detect its disks (they are reported as Foreign), you can import the RAID, following the steps below.

To import the RAID:

1. In the left pane of the web interface, click Storage Management and then Chassis.

2. In the tile of a volume whose disks are reported as Foreign, click Import RAID.
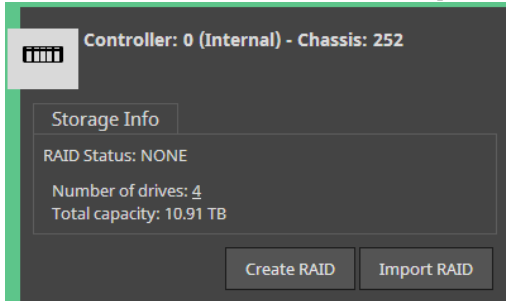
Manage Dynamic Disks Connected to the Appliance

Note: *Tiger Store appliances exporting their own storage cannot have access to dynamic disks.*

When you connect your appliance to an already formatted striped volume, it is possible that Tiger Store doesn't recognize the LDM configuration of the volume's dynamic disks and they appear as Foreign. To be able to manage the striped volume, you should import its disks.

Important: *Once you import the disks on Tiger Store, you may have to import them on each computer that has previously seen the striped volume.*

You may also have to reactivate dynamic disks that are with Offline or Missing status on the appliance, in order to manage them.

To import foreign disks:

1. In the left pane of the web interface, click Storage Management and then Disks.

2. In the tile of a Foreign disk, click "Import this disk".
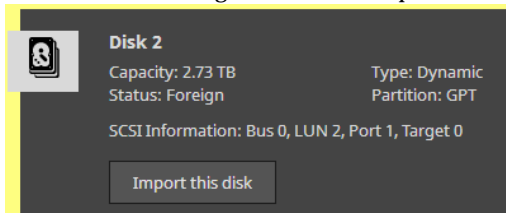
3. Confirm that you want to import the selected disk on Tiger Store.

   Tiger Store imports all dynamic disks comprising the striped volume.

Note: *To let Windows SAN Tiger Clients access the striped volume, you should import its disks in Windows Disk Management on each Windows SAN Tiger Client too.*

To reactivate dynamic disks:

1. In the left pane of the web interface, click Storage Management and then Disks.

2. In the tile of a disk with Offline/Missing status, click "Reactivate this disk".
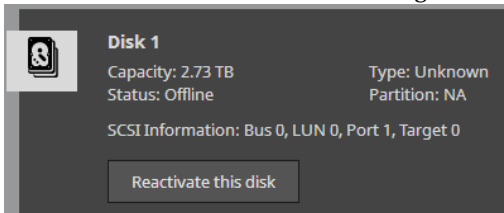
Tiger Store reactivates all disks with Offline/Missing status in the same group.

Rename a Tiger Store Volume

The name of each volume, managed by Tiger Store, is used as its label on client computers. You can change the name of a shared volume at any time. Computers that have mounted a shared volume with its old name can see it with its new name only after reconnecting to the storage server.

Note: *When smart storage pooling is enabled on the appliance, the name of the pool is used as a label of the virtual volume (by default this is "Pool"). You cannot rename a storage pool.*

To rename a Tiger Store volume:

1. In the left pane of the web interface, click Shared Volumes.

2. Click the name of the volume/pool in the tile of a shared volume.
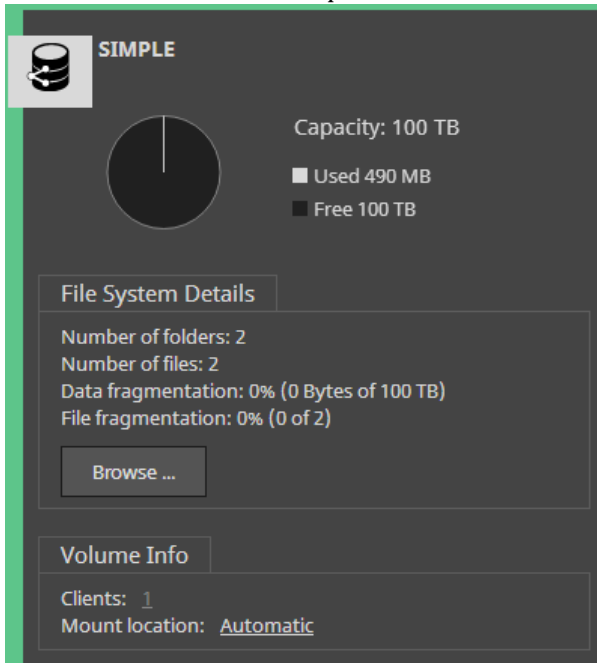
3. In the Rename dialog, enter a new name of the volume/pool and click OK.
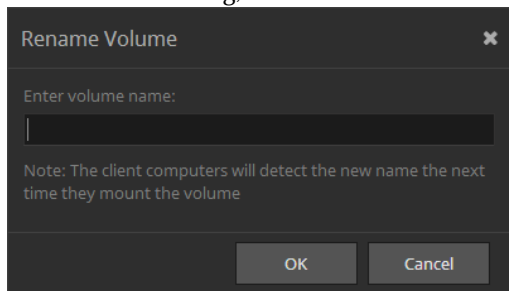
Note: *In case you need to immediately rename the volume again, wait for the web interface to refresh automatically with the latest volume name, before assigning a new one. Otherwise it is possible Tiger Store to revert to the last saved name.*

The new volume name is displayed on client computers only after they remount the volume.

Storage Maintenance

Check and Repair The File System

Note: *On Tiger Store appliances, request assistance from the Tiger Technology support for checking and repairing the file system of a volume.*

It is advisable to use the operating system tools, like chkdsk, for checking and repairing the file system of a volume. Before you proceed, make sure that Tiger Clients do not have access to the volume, by making it Private for the storage server. Once the file system of a volume is repaired, you can share it to Tiger Clients again.

Note that checking and repairing the file system of a Private volume, which is currently used as a Tiger Bridge replication target, pauses Tiger Bridge's replication & tiering until this maintenance operation finishes.

Volume Defragmentation

Tiger Store's defragmentation engine is designed not only to reduce the fragmentation of the file system, but also to optimize the processing of file sequences on the shared volumes. By default, Tiger Store's auto-defragmentation is enabled. It defragments data on the shared volume(s) only when the system is in idle state (overall traffic to the shared storage doesn't exceed 10MB/s for at least 30 minutes) and automatically pauses, when traffic above this threshold is detected. You can disable auto-defragmentation and run defragmentation manually from the web interface instead.

Note: *You cannot run defragmentation (automatic or manual) on a private volume (volume that is not shared to Tiger Clients).*

To enable/disable auto-defragmentation:

1. In the left pane of the web interface, click Shared Volumes.

2. In the Auto-defragmentation field, do one of the following:
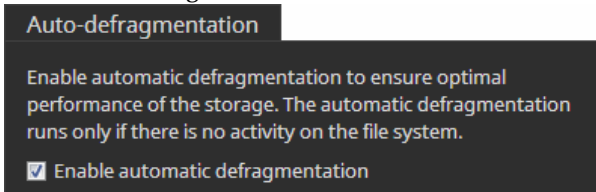
   • Select the "Enable automatic defragmentation" check box, to enable auto-defragmentation of the volume.

   • Clear the "Enable automatic defragmentation" check box, to disable auto-defragmentation of the volume.

3. Click Continue to Confirm the selected option.

Manually Defragment a Tiger Store Volume

If you have disabled Tiger Store's automatic defragmentation (see "Volume Defragmentation" on page 69), it is advisable that you perform manual defragmentation of the volume(s) when needed. You can keep track of the fragmentation of each Tiger Store volume in the Volume tile - it displays information about both data fragmentation and file fragmentation. Both values show the fragmentation level of data on the disk, but using different measuring systems. Data fragmentation lists the amount of fragmented data in bytes, while file fragmentation lists the number of fragmented files. Manual defragmentation can be stopped at any time.

To manually defragment a Tiger Store volume:

1. In the left pane of the web interface, click Shared Volumes.

2. In the tile of a selected volume, click Defragment.
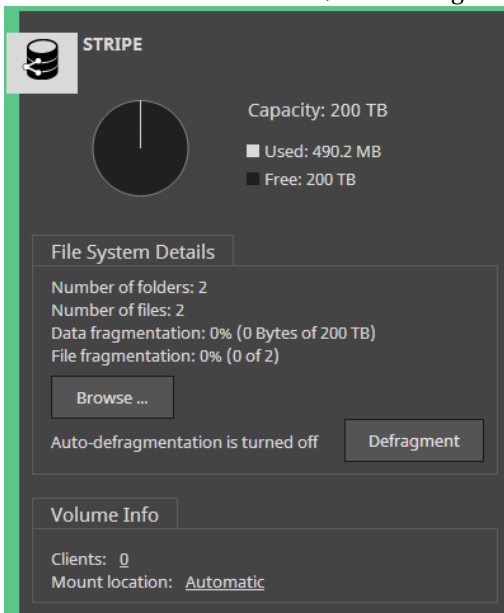
Important: *When smart storage pooling is enabled, to manually defragment the volumes comprising the pool, you must first disable smart storage pooling (see "Enable/Disable Smart Storage Pooling" on page 40).*

While the process is running, the Volume tile displays the defragmentation progress percentage and allows you to stop the defragmentation by clicking Stop Defrag.

Share a Volume as a SMB/CIFS Share
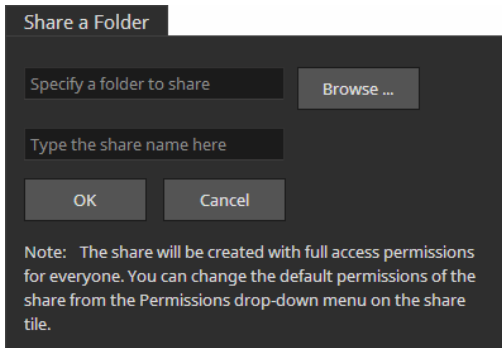
The web interface of Tiger Store on appliances allow you to export a shared volume (or a folder on it) as a SMB/CIFS share to computers on the network that don't have the Tiger Client software installed. You can export as many shares as you like or remove any one of them at any time. The exported shares are accessible to all computers on the same LAN segment, by typing the name/IP address of the appliance in the file explorer of the operating system.

By default, the newly created SMB/CIFS share is accessible with "Full access" permissions to everyone. You can change the access permissions to the share for Everyone (domain or workgroup users) in the web interface of Tiger Store.

Note: *To change the name of a share, you should first remove it then re-create it with its new name.*

To create a SMB/CIFS share on a Tiger Store volume:

1. In the left pane of the web interface, go to System | SMB/CIFS Sharing and click Share a Folder.

2. In Share a Folder, click Browse and browse to the desired volume and select the folder on it.

Tip: *To share a whole volume, select the root of the volume.*

3. Enter a name of the share and click OK.

Note: *If you do not specify a name of the share, it automatically takes the name of the folder.*

The share appears in the list of shares. By default, it is accessible to everyone with "Full access" permissions. To change the share permissions, refer to page 72.

To remove a SMB/CIFS share of a Tiger Store volume:

1. In the left pane of Tiger Store's web interface, click System and then SMB/CIFS Sharing.

2. Find the tile of the share that you want to remove and click Stop Sharing.

> **SIMPLE**
> Path: /
>
> Permissions: Full ▾   Stop Sharing...
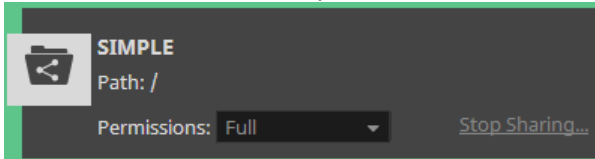
> **Important**: *All LAN clients that are currently accessing the SMB/CIFS share through Tiger Store lose connection to it and any file operation going on at the moment may fail.*

3. Confirm that you want to remove the share.

   The share is removed from the list of shares.

To set permissions of a SMB/CIFS share on a Tiger Store volume:

1. In the left pane of Tiger Store's web interface, click System and then SMB/CIFS Sharing.

2. Find the tile of the share whose permissions you want to set.

> **SIMPLE**
> Path: /
>
> Permissions: Full ▾   Stop Sharing...
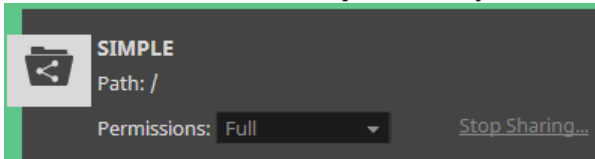
3. In the drop-down box, select the respective permissions for Everyone.

   The permissions are applied on the next re-mount of the share on non-Tiger Client computers.

Manage Tiger Clients

As a Tiger Store administrator you can manage Tiger Client computers in the following ways:

• view connected Tiger Clients and their connection status.

• connect/disconnect a Tiger Client computer from the storage server.

• restrict Tiger Clients from disconnecting from the storage server.

• specify the volumes, which each Tiger Client can mount.

• view traffic information for Tiger Clients (see "View Traffic Information" on page 77).

View Tiger Clients Information and Connection Status

The Clients page of the web interface lists all computers on the same network, which run the Tiger Client driver and are connected to the Tiger Store storage server.

The Clients Information field gives you information about the number of connected SAN and LAN client computers as well as the number of all disconnected client computers:
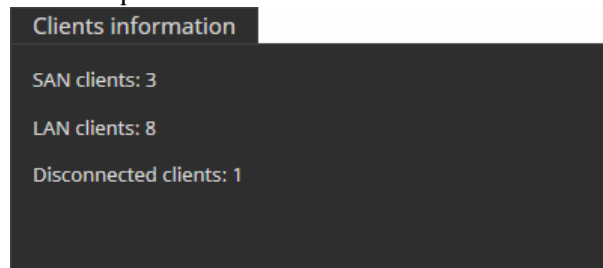
Additionally, each Tiger Client is represented by a tile, which gives you information about the name, IP address, operating system of the computer and the version of the Tiger Client driver it is

running. The tile of a Tiger Client also gives you information about the computer's connectivity to the storage server:
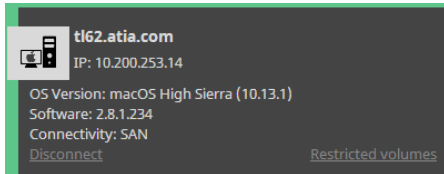
tl62.atia.com IP: 10.200.253.14 OS Version: macOS High Sierra (10.13.1) Software: 2.8.1.234 Connectivity: SAN Disconnect Restricted volumes	The computer is connected as a SAN client.
TL55 IP: 10.200.4.43 OS Version: Microsoft Professional (build 9200), 64-bit Software: 2.8.1.234 Connectivity: LAN Disconnect Restricted volumes	The computer is connected as a LAN client.
DESKTOP-HON99M0 IP: 10.200.9.240 OS Version: Microsoft Professional (build 9200), 64-bit Software: 2.8.1.234 Connectivity: None Connect Remove Restricted volumes	The computer is not connected to the storage server or is offline.
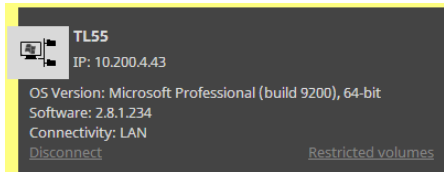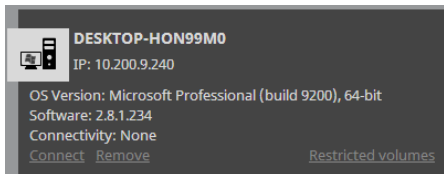
You can remove the tile of a disconnected Tiger Client computer from the list, when the computer no longer runs the Tiger Client driver, for example. If the Tiger Client computer you have removed from the list is online, the Tiger Store computer/appliance is automatically removed from the client computer's list of storage servers.

To make a removed Tiger Client appear again on the Clients page, on the client computer you must add the storage server to the list of storage servers and manually connect to it. If the client computer is offline, when you remove it from the Clients page, to make it appear on the Clients page, once it is turned on again manually connect it to the storage server.

To remove a Tiger Client's tile from the list of client computers:

1. In the left pane of Tiger Store's web interface, click Clients.

2. In the tile of a disconnected client computer, click Remove.

   The Tiger Client tile is removed from the list.

Connect/Disconnect a Tiger Client

In the tile of a Tiger Client in the Clients page, you can force disconnect a selected Tiger Client from the shared volumes it sees. Vice versa, you can force connect a disconnected Tiger Client computer as long as it is currently online.

Note: *Disconnected Tiger Clients can manually connect to the appliance following the steps in the "Tiger Client User's Guide".*

To force disconnect a selected client computer:

Important: *When you disconnect a Tiger Client from a shared volume, any file operation performed from that computer on the shared volume will be canceled.*

1. In the left pane of Tiger Store's web interface, click Clients.

2. In the tile of the computer that you want to disconnect, click Disconnect.

   Note: *The Disconnect button is not present, if the Tiger Client computer has not mounted any volume.*

   Tiger Store disconnects the selected Tiger Client from all shared volumes it has mounted.

To force connect a selected client computer:

1. In the left pane of Tiger Store's web interface, click Clients.

2. In the tile of the computer that you want to connect, click Connect.

   The selected Tiger Client computer mounts all volumes it is allowed to mount.

Specify the Allowed Volumes per Tiger Client

By default, each Tiger Client can mount all volumes shared by the storage server. You can restrict the mounting of certain volumes on a specific Tiger Client computer.

To restrict the mounting of a shared volume on Tiger Client computer:

1. In the left pane of Tiger Store's web interface, click Clients.

2. In the tile of a Tiger Client computer, click Restricted volumes.

3. In the Restricted Volumes dialog, do one of the following:

   • Select the check box of a shared volume, to restrict the selected Tiger Client from mounting it.

   • Clear the check box of a shared volume, to allow the selected Tiger Client to mount it.

4. Click OK.

Restrict Tiger Clients from Manually Disconnecting

To ensure that a Tiger Client computer remains connected to the storage server no matter what user is currently logged on to it, you can set Tiger Store to require an administrators password each time a user attempts to disconnect its computer from Tiger Store. By default, this option is disabled.

To restrict Tiger Clients from manually disconnecting from the storage server:

1. In the left pane of Tiger Store's web interface, click Clients.

2. In Clients Restriction, do one of the following:

• Select the "Restrict client actions" check box, to require a Tiger Store administrator's password when manually disconnecting from the storage server.

• Clear the "Restrict client actions" check box, to allow require a Tiger Clients to manually disconnect from the storage server.

> The option you have selected is applied on each Tiger Client computer once it reconnects to the storage server.

View Traffic Information

To facilitate you in monitoring the workload of the shared storage and the connectivity with currently connected Tiger Clients, Tiger Store's web interface offers you the Traffic monitoring tool. You can view data and metadata traffic statistics between the shared volumes and all currently connected computers for a selected period.

To view traffic information:

1. In the left pane of Tiger Store's web interface, click Traffic.
   The Traffic page appears.

2. In the drop-down box above the graph, select the type of metric:
   - Volume I/O in MB/s;
   - Volume I/O in requests/s;
   - Network I/O in MB/s;
   - Network packets/s;
   - Number of open operations;

3. In the drop-down box below the graph, select the time interval for which you want statistics.

   The Traffic page displays a graph showing you the statistics for the parameters you've chosen in the respective drop-down boxes.

   Tip: *Instead of refreshing the web page to update the results displayed, make sure the "Update automatically" check box is selected, this way allowing the web interface to automatically update the information displayed.*

Tiger Bridge Integration

Tiger Bridge provides data lifecycle management to your shared storage. With its help you can automatically or manually replicate and/or archive data, as well as reclaim space on your shared storage volumes.

To benefit from Tiger Bridge, you have to install and activate it on your shared storage server. On a storage server running the software version of Tiger Store, you can install and configure Tiger Bridge following the steps in the latest version of the Tiger Bridge Administration Guide. Unless Tiger Bridge is already installed on your Tiger Store appliance, you can install it as a firmware update. Contact Tiger Technology support team for assistance on installing and activating Tiger Bridge on your Tiger Store appliance.

To configure Tiger Bridge on a Tiger Store appliance, you can use the Tiger Bridge Configuration application, which provides remote access to Tiger Bridge from any computer on the same network as the storage server. For more details about downloading and installing the Tiger Bridge Configuration application, see "Download and Install Tiger Bridge Configuration" on page 80.

Additionally, if you are using a tape library as a target, on Tiger Store appliances you can download and install on a remote computer the Tiger Bridge Tape Management application, which lets you manage drives, tapes and the contents on them. For more information, refer to "Download and Install Tiger Bridge Tape Management" on page 82.

Regardless of your storage server type, you can perform manual Tiger Bridge operations on data on your shared storage using the Volume Browser. For more information, refer to "Manage Data in The Volume Browser" on page 84.

Download and Install Tiger Bridge Configuration

The Tiger Bridge Configuration application provides graphic user interface for activating and configuring Tiger Bridge from a remote computer on the same network as the storage server.

To download and install the Tiger Bridge Configuration application:

1. In the web interface of your storage server, click Manage and type the password for the web interface.

2. Click the Tiger Store logo to load the Downloads page.

3. Find the Tiger Bridge Configuration installation file and click Download.
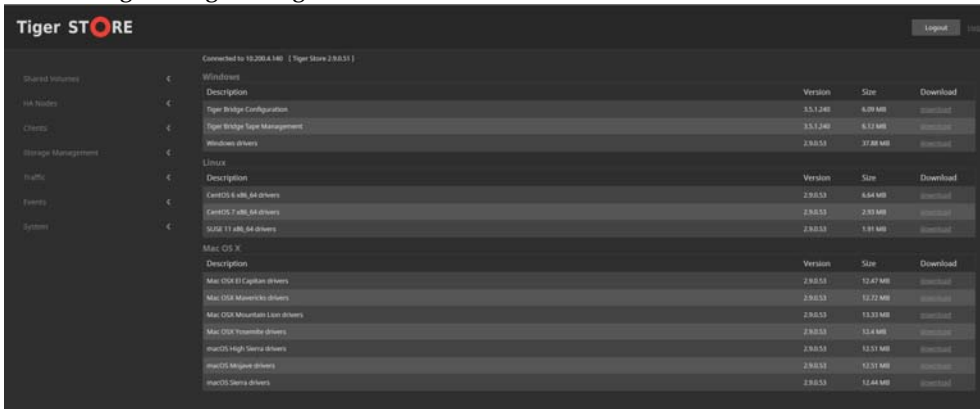
4. When the installation file downloads to your computer, double-click it to start the installation and follow the on-screen instructions.

To run the Tiger Bridge Configuration:

Note: *To work with the Tiger Bridge Configuration, you need to run it as administrator.*

1. To start the Tiger Bridge Configuration, do one of the following:

• Double-click the Tiger Bridge Configuration shortcut on the desktop.

• Navigate to the installation folder of the Tiger Bridge Configuration and double-click TigerBridgeConfiguration.exe

2. Enter the IP address of the storage server, on which Tiger Bridge is installed and click Connect.
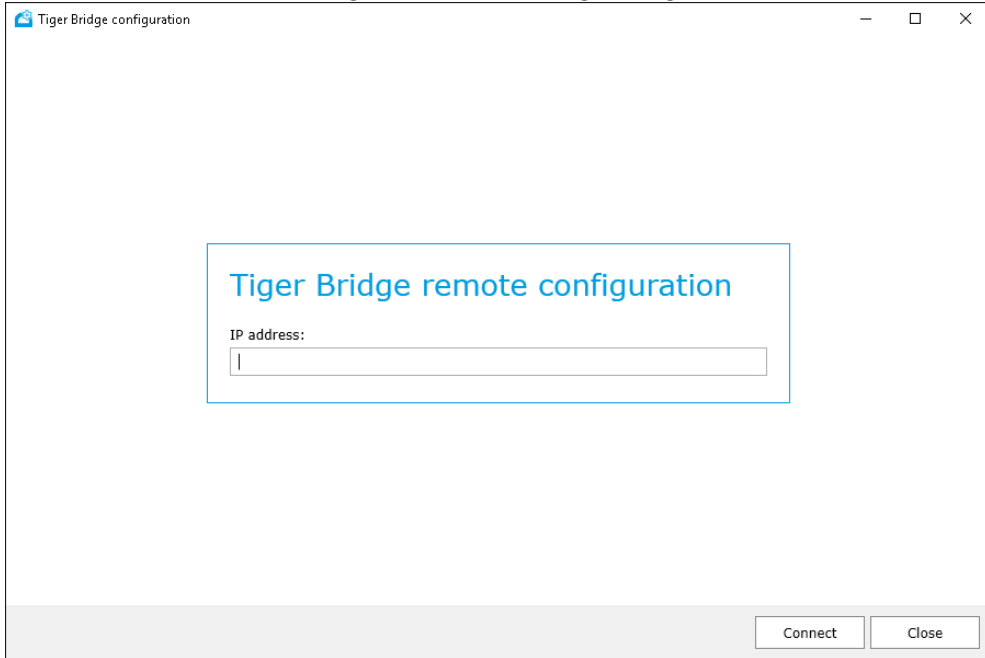
> **Important**: *If your storage server is deployed with high availability, you must enter the IP address of the current primary node.*

> **Note**: *The dialog for establishing remote connection to the Tiger Bridge server is not available, if Tiger Bridge is installed on the computer from which you run the Tiger Bridge Configuration.*

3. Refer to the Tiger Bridge Administration Guide for detailed steps on using the application.

Download and Install Tiger Bridge Tape Management

Tiger Technology's Tape Management application is designed to work in conjunction with Tiger Bridge in order to facilitate you in performing the following task:

• prepare your tape libraries for work with Tiger Bridge.

• manage and monitor tapes and drives in your libraries.

• explore, manage and download data stored by Tiger Bridge on your tape libraries.

To use the Tiger Bridge Tape Management application on a Tiger Store appliance, you need to install it on a computer, which is on the same network as the storage server and configure it to access the storage server remotely, following the procedures described below.

To download and install the Tiger Bridge Tape Management application:

1. In the web interface of your storage server, click Manage and type the password for the web interface.

2. Click the Tiger Store logo to load the Downloads page.

3. Find the Tiger Bridge Tape Management installation file and click Download.
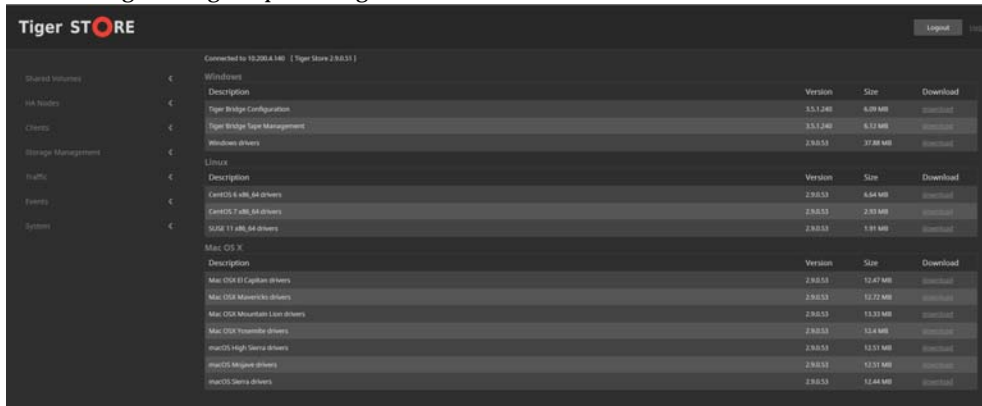
4. When the installation file downloads to your computer, double-click it to start the installation and follow the on-screen instructions.

To run the Tiger Bridge Tape Management application:

1. To start the Tiger Bridge Configuration, do one of the following:

   • Double-click the Tiger Bridge Tape Management shortcut on the desktop.

   • Navigate to the installation folder of the Tiger Bridge Tape Management and double-click TigerBridgeTapeManagement.exe

2. Enter the IP address of the storage server, on which Tiger Bridge is installed and click Connect.
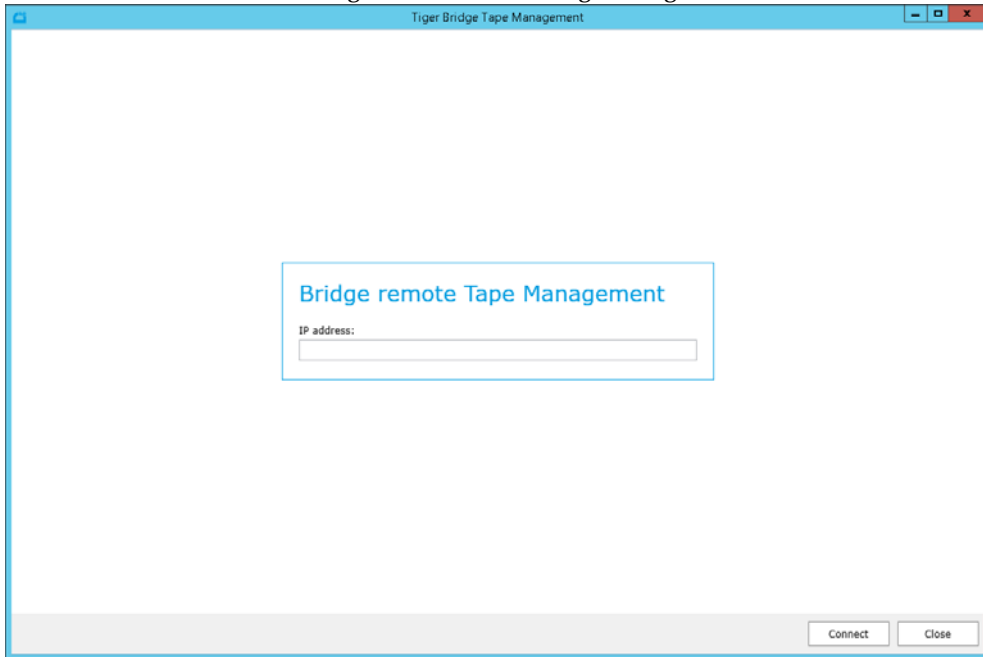
Important: *If your storage server is deployed with high availability, you must enter the IP address of the current primary node.*

Note: *The dialog for establishing remote connection to the Tiger Bridge server is not available, if Tiger Bridge is installed on the computer from which you run the Tiger Bridge Tape Management.*

3. Refer to the Tiger Bridge Tape Management User's Guide for detailed steps on using the application.

Manage Data in The Volume Browser

Note: *On a storage server running the software version of Tiger Store, you can also manually manage data in Windows Explorer, using the Tiger Bridge shell extension. For more details, refer to the Tiger Bridge Administration Guide.*

The Volume Browser is the place where you can explore data on the shared Tiger Store volumes and manually perform Tiger Bridge operations on it:

• replicate a file or a whole folder.

• reclaim space on the shared storage volumes by replacing a replicated file with a nearline file (a stub file linking to the copy of the file on the target).

• retrieve a nearline file or all nearline files in a folder from the target.

• delete a file or a whole folder from both the source and the target.

> **Important**: *Depending on the mode in which Tiger Bridge operates, executing this command either deletes the file just from the source, or both from the source and the target. For more information, refer to the Tiger Bridge Administration Guide.*

• synchronize the contents of the source and the target by rescanning it.

Initiating a task in the Volume Browser always takes precedence over the automatically scheduled Tiger Bridge tasks. That means that if you choose to manually replicate files through the Volume Browser, the execution of the operation will begin immediately and will probably pause the automatic replication queue that is being processed at the moment.

Note: *The Volume Browser hides system files such as files associated with the Recycle bin, volume icons, etc.*

To access the Volume Browser:

In the Shared Volumes page of the web interface, click Browse in the tile of a volume.
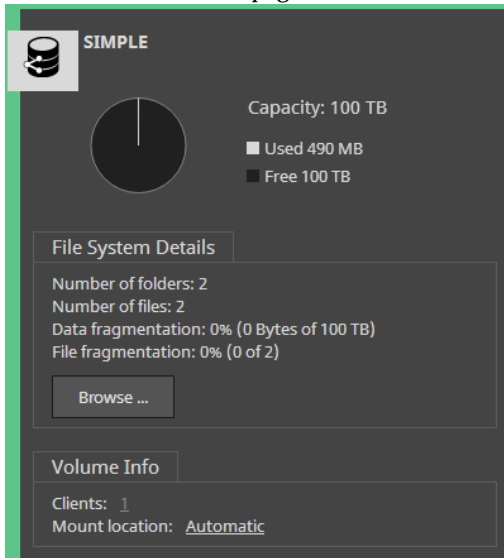
The Volume Browser opens.
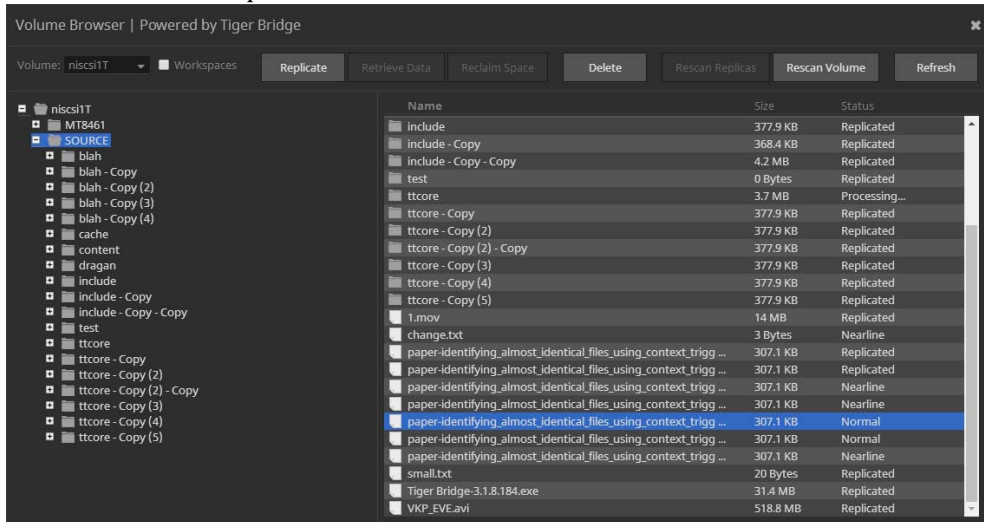
The left pane allows you to navigate the tree structure of the contents of the volume selected in the drop-down box.

Note: *To explore or manage Tiger Spaces data on the selected volume, select the "Workspaces" check box next to the Volume drop-down box. To switch the view back to other contents of the volume, clear the "Workspaces" check box.*

By expanding the node of a folder, you can view its hierarchical structure. Clicking an item in the tree view, displays its contents in the right panel.

The file operations you can perform in the Volume Browser depend on the status of the selected file:

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.

Processing — Tiger Bridge is currently performing a data lifecycle management operation on the file/folder.

To perform a manual Tiger Bridge operation on a file/folder, simply select it in the right pane and then click the respective button in the Volume Browser taskbar. When performing a Tiger Bridge operation on a folder, you are performing it on all matching files in that folder i.e. for example, clicking Retrieve for a selected folder will retrieve from the target all nearline files in that folder.

Note: *When a manual Tiger Bridge operation is not applicable for a selected file/folder in the Volume Browser, its button in the taskbar is inactive. For example, the button Replicate is inactive when you have selected a replicated file in the Volume Browser.*

Re-scanning Replicated Data

There are some situations in which a replicated file on the target can have no counterpart on the Tiger Store volume. To allow you to create a nearline file for each file existing on the target, Tiger Bridge provides you with a mechanism for re-scanning the replicated data. Thus, when Tiger Bridge detects a replicated file on the target, which does not have a counterpart (a replicated or nearline file) on the Tiger Store volume, Tiger Bridge automatically creates a nearline file in the source folder.

Note: *You can re-scan a whole shared volume or just a folder on it.*

To re-scan replicated data:

In the taskbar of the Volume Browser, do one of the following:
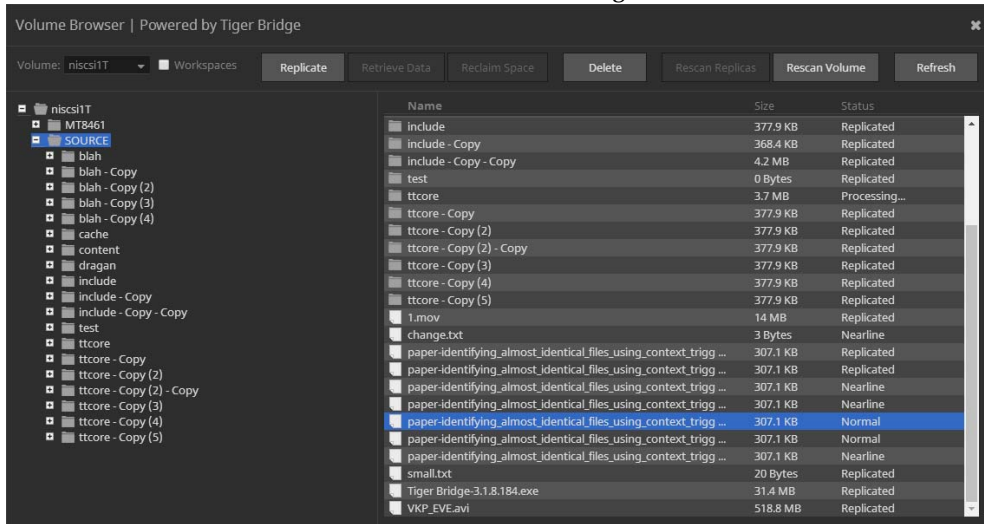
• Click Rescan Volume, to re-scan the whole volume that is selected in the drop-down box of the Volume Browser.

• Browse to and select the folder, whose contents you want to re-scan and then click Rescan Replicas.

Tiger Bridge on a Storage Server with High Availability

When your storage server is deployed with high availability, both its server nodes must have identical settings in order to provide failover capability. Thus, in order to consistently manage data lifecycle in case of failover, Tiger Bridge must have identical configuration on both server nodes. When there are conflicts in the configuration of Tiger Bridge on the two nodes, the HA Nodes page of the web interface displays a warning sign ⚠ in the Tiger Bridge field of the node settings comparison table.

You can resolve these conflicts either by accessing the Tiger Bridge Configuration of one or the other node, or directly in the HA Nodes page of the web interface. When you select to resolve the conflicts in the HA Nodes page, Tiger Store automatically overwrites the Tiger Bridge configuration on the standby node with the settings of the current primary node.

To resolve conflicting Tiger Bridge settings in the HA Nodes page:

1. In the left pane of the web interface, click HA Nodes.

2. Next to Tiger Bridge in the node settings comparison table, click Sync.
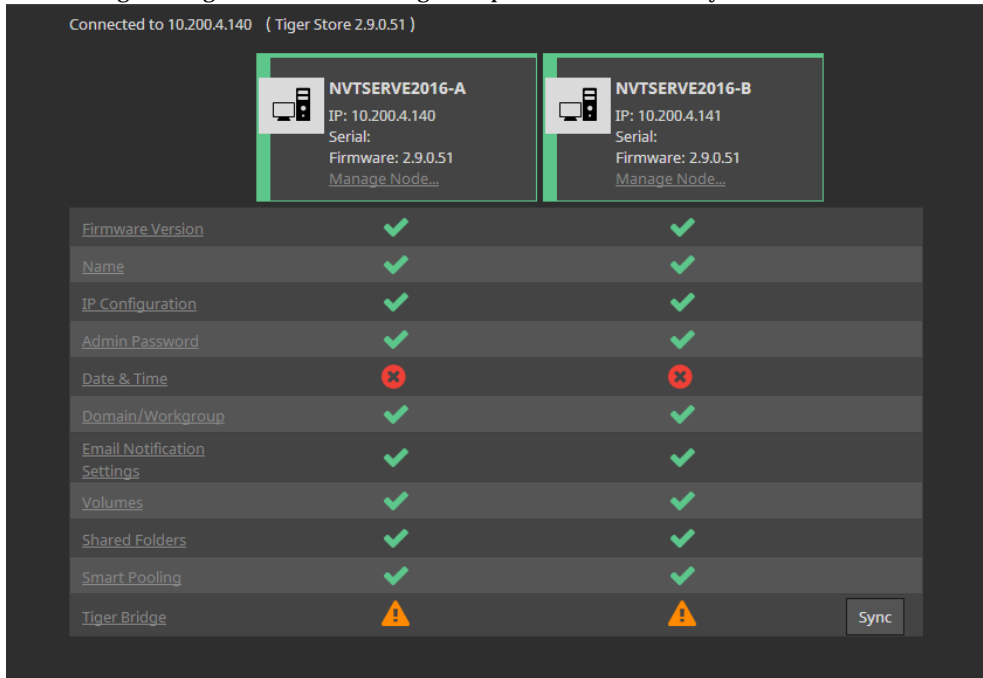
When Tiger Store overwrites the Tiger Bridge configuration on the standby node with the settings of the current primary node, the field displays the synchronized settings icon ✔.

Tiger Bridge Integration

Manage High Availability

To be able to provide constant availability to the shared storage, the two server nodes of your Tiger Store storage server (be it an appliance with two server nodes or two computers acting as a high-availability cluster) must be online and have identical settings.
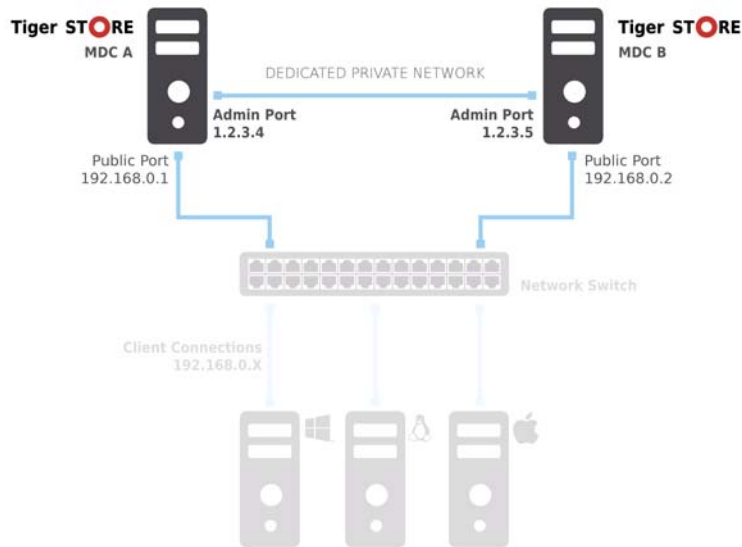
Tiger Store is designed in such a way that changes introduced in the cluster view of the web interface are automatically synchronized among the server nodes as long as both of them are online. While you can rely on the automatic synchronization of settings between server nodes for most settings, some settings (like firmware version and Tiger Store activation, for example) cannot be automatically synchronized on both server nodes. Additionally, should you add a second server node after all the settings have already been configured, you may have to synchronize the secondary node's settings manually.

Monitor Server Nodes Synchronization

The HA Nodes page in the web interface allows you to monitor the settings synchronization among nodes.

It displays the tiles of the available server nodes and a table comparing their settings:

✔ - settings are synchronized;

⚠ - conflicting settings of the two server nodes, but failover can take place;

✖ - critical conflict in settings, which does not allow failover to take place;

To resolve conflicting settings, you will have to access the node view of one or the other nodes and manually change the conflicting setting of the selected node.

Resolve Conflicting Settings in Node View

Note: *You can resolve conflicts in the configuration of Tiger Bridge, following the steps in "Tiger Bridge on a Storage Server with High Availability" on page 88.*

To apply changes on a specific server node only, you should access the node view of the web UI, which displays just the information valid for the node, but not for the cluster. The purpose of the node view is to allow you to resolve conflicts in those settings of the two nodes that cannot be synchronized automatically in cluster view (like Tiger Store activation, firmware version, etc.).

Important: *When accessing the node view of the web interface, make sure you don't introduce changes that may lead to conflicts between the two server nodes.*

To access the node view of the web UI:

1. In the left pane of the web interface, click HA Nodes.

2. In the tile of the server node, whose web UI you want to access, click Manage Node.
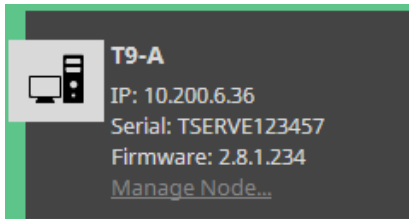
The node view for the selected server node opens in a new tab/window of your web browser.

3. Click Manage and then enter the password for the web interface.

Tip: *If you have changed the password for the cluster view of the web interface, while this node has been online - enter the new password. In other cases enter the default password -* admin*.*

System Maintenance

The following options facilitate you in maintaining and monitoring the Tiger Store system:

• Tiger Store reboot options.

• enabling remote access to a Tiger Store appliance.

• Tiger Store appliance firmware update.

• backing up and restoring the Tiger Store configuration of an appliance.

• e-mail notifications for problems.

• viewing events reports.

Tiger Store Reboot Options

To facilitate you in performing certain tasks and in order not to obstruct users work with the appliance, Tiger Store offers you several reboot options.

You can issue the following commands:

• Restart add-on services - restarts all add-on services, installed on the storage server (like auto defragmentaion, Tiger Bridge, etc.).

• Restart all services - restarts all Tiger Store services and starts them in the correct order, clients are disconnected from the storage server.

• Full System reboot - Tiger Store automatically disconnects any connected client computer and shuts down, then starts again. Once the system is up again, the web interface is automatically refreshed.

Note: *After restarting the appliance, client computers are not automatically reconnected to it.*

• Shutdown - Tiger Store automatically disconnects any connected client computer from the storage server and shuts it down.

Note: *On Tiger Store with high-availability add-on activated, when the respective reboot option is issued in cluster view of the web interface, it applies to both server nodes, and when you issue the command in node view, it applies to the selected server node only.*

Whenever you need to restart or shut down a Tiger Store appliance, it is advisable to do it from the web interface, instead of pressing the Power or Reset buttons on the back of the appliance.

Important: *Some of the Shut down and Reboot commands are not available when maintenance operations such as Firmware Update are going on at the moment.*

To issue a reboot option command:

1. In the left pane of the web interface, click System and then Maintenance.

2. In System Reset, select the desired option in the drop down box and then click the button below to issue the selected command.

```
System Reset

Reset mode:    Restart add-on services    ▾

Description:  This command will restart all
backend services which you are running. They may
include Tiering and replication, Automatic
defragmentation, Hardware monitoring and
others. This command will not interfere with any
file systems activity and will not unmount any
clients.

      Restart add-on services
```
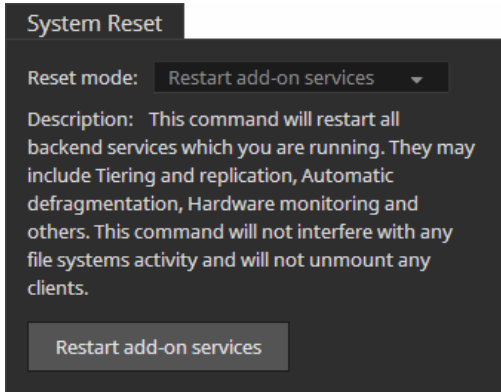
Tip: *The button below the drop down box changes according to the selected command.*

Enable/Disable Remote Access to the Appliance

For some maintenance operations you may need the assistance of the Tiger Technology support team. To facilitate them in diagnosing the problem and resolving it, you may have to provide remote access to the appliance. This is done by enabling the pre-installed software for remote assistance.

Enable remote access to the appliance only if requested by Tiger Technology support team. Disable the setting once remote support is no longer needed.

To disable/enable remote access to the appliance:

1. In the left pane of the web interface, click System and then About.

2. Do one of the following:

   • Select the "Allow remote assistance" check box, to enable remote access to the appliance.

```
☑ Allow Remote Assistance
Select the Allow Remote Assistance option to provide remote
access to your appliance to the Tiger Technology support team.
Enable this checkbox only if requested by Tiger Technology
support team. Disable the option when remote support is not needed.

Note:  Your appliance should have access to the Internet.
```
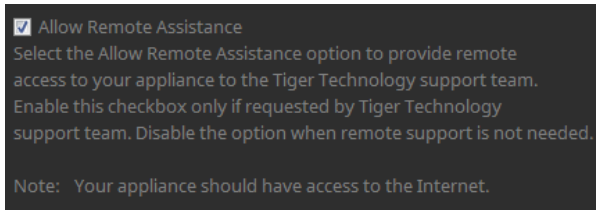
> **Note:** *Remember to disable this option once your remote session with Tiger Technology support finishes.*

• Clear the "Allow remote assistance" check box, to disable remote access to the appliance.
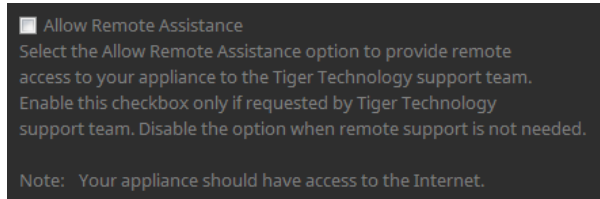
Firmware Update of the Appliance

You can use the web interface of Tiger Store to update the appliance firmware. You can check the current firmware version in the About page of the web interface.

Note: *On appliances with two server nodes, you should check the current firmware version of each node in Node view.*

Once you receive a firmware update, it is advisable to upload it on your appliance to guarantee its good functionality. The procedures for performing a firmware update on your appliance differ depending on whether it features two server nodes or just one. Both server nodes should run the same firmware version in order to act as a high-availability cluster.

Some firmware updates require that the Tiger Client software also be updated on client computers.

You can update the firmware, when no client computer is connected to the appliance and no other maintenance operation is going on at the moment. That is why before updating the firmware you should enter Maintenance mode, which disconnects all client computers.

To upload a firmware update on an appliance with one server node:

Important: *The process of firmware update cannot be interrupted or paused. Do not shut down or restart the appliance after a firmware update has begun.*

1. In the left pane of the web interface, click System and then Maintenance.

2. Click Enter Maintenance mode and then confirm that you want to enter Maintenance mode.

   Maintenance Mode

   Enter maintenance mode to unlock storage maintenance functionality.

   Important: When the Tiger Store is in maintenance mode shared data on it will not be accessible to clients. Once you finish your maintenance tasks you can switch to normal mode by clicking the Exit Maintenance Mode button (if available) or reboot the server.

   [Enter Maintenance Mode]
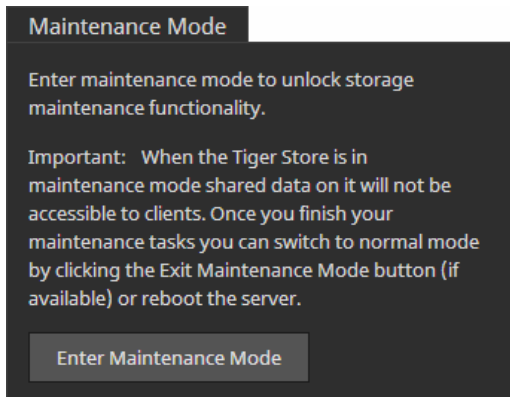
   Important: *All connected Tiger Clients will be automatically disconnected from the shared volumes and any file operation going on at the moment will be canceled.*

3. In Firmware Update, click Browse/Choose File and then browse for and select the file containing the firmware update to upload.

   Firmware Update

   To update the firmware, Tiger Store must be in maintenance mode. Browse to the firmware binary and upload it to Tiger Store. Once the firmware is uploaded successfully, the firmware will be installed automatically and Tiger Store will reboot.

   [Choose File] No file chosen

   Current firmware version: 2.8.1.234
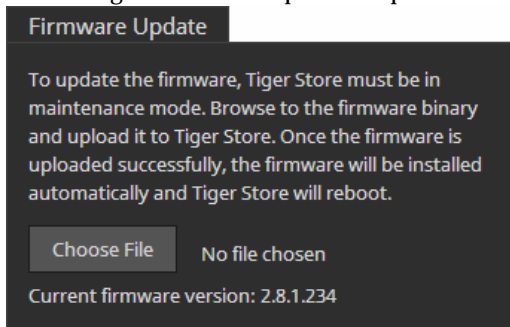
4. Click Continue to confirm that you want to perform firmware update.

   Tiger Store uploads the firmware on the system hard drive, unpacks it and applies the firmware update. When the firmware update finishes, the system automatically restarts.

To upload a firmware update on an appliance with two server nodes:

1. In the left pane of the web interface, click System and then Maintenance.

2. Click Enter Maintenance mode and then confirm that you want to enter Maintenance mode.

Maintenance Mode

Enter maintenance mode to unlock storage maintenance functionality.

Important: When the Tiger Store is in maintenance mode shared data on it will not be accessible to clients. Once you finish your maintenance tasks you can switch to normal mode by clicking the Exit Maintenance Mode button (if available) or reboot the server.

Enter Maintenance Mode

Important: *All connected Tiger Clients will be automatically disconnected from the shared volumes and any file operation going on at the moment will be canceled.*

3. In the left pane, go to HA Nodes and in the tile of each server node, click Manage Node.

   The node view of each server node opens in a new tab/window of your web browser.

4. In the node view of the first server node, go to System | Maintenance.

5. In Firmware Update, click Browse/Choose file and then browse for and select the file containing the firmware update to upload.

Firmware Update

To update the firmware, Tiger Store must be in maintenance mode. Browse to the firmware binary and upload it to Tiger Store. Once the firmware is uploaded successfully, the firmware will be installed automatically and Tiger Store will reboot.

Choose File   No file chosen

Current firmware version: 2.8.1.234
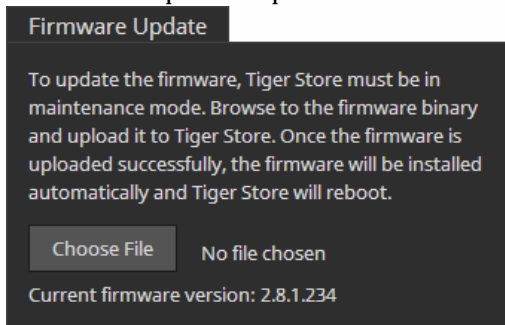
6. Click Continue to confirm that you want to perform firmware update.

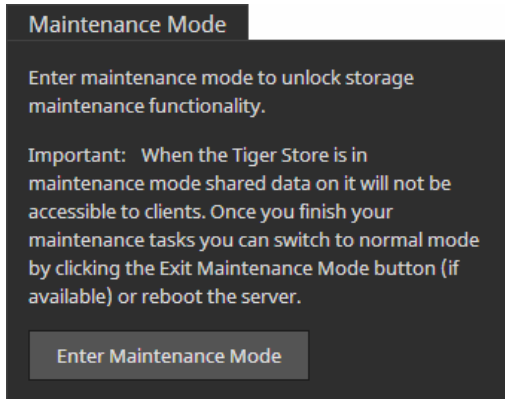7. In the node view of the second server node, go to System | Maintenance.

8. In Firmware Update, click Browse/Choose file and then browse for and select the file containing the firmware update to upload.
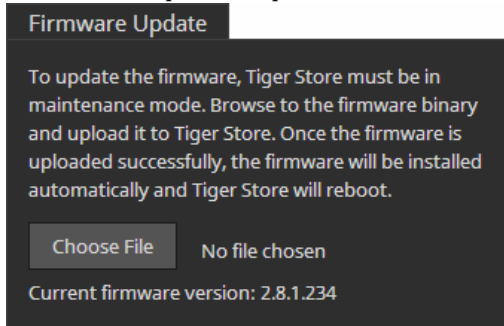
9. Click Continue to confirm that you want to perform firmware update.

When the firmware update finishes, both server nodes automatically restart.

Back Up/Restore the Tiger Store Configuration

To facilitate you when upgrading your Tiger Store appliance, Tiger Store allows you to back up and then restore all settings configured in the web interface, thus sparing you the effort to configure them again. When you restore a previously backed up configuration, you restore all settings for appliance name, shared, offline and private volumes (identified by volume GUID), default volume mount point on Windows Tiger Clients, auto-defragmentation, smart storage pooling, domain settings, Tiger Bridge settings, IP configuration, except the names of the volumes seen by the storage server.

Note: *Tiger Store doesn't back up and restore the password for the web interface, but keeps the last used password.*

On Tiger Store appliances with high-availability add-on activated, to ensure the consistency of the backup file, Tiger Store allows you to back up and restore the settings configuration only if both server nodes are online. This way, when you restore a backed up configuration, there's no need to restore it on each node - Tiger Store takes care to restore and synchronize the settings on both nodes.

By default, the file with the backed up configuration is saved with the following name: [storage server name]_[time]_[date]_backup.json. You can create as many backups as you want and change their name to make it easier for you to discern between one another as long as you keep their extension (.json). To provide protection of sensitive information in the configuration backup file, Tiger Store encrypts it. Additionally, you can ensure that no unauthorized user restores a backed up configuration file by protecting the backup file with a password.

Important: *Restoring a backed up settings configuration automatically disconnects all Tiger Clients and restarts the storage server computer.*

To back up the Tiger Store settings configuration:

1. In the left pane of the web interface, click System and then Maintenance.

2. In Back Up System Settings, click Back Up.

> **Back Up System Settings**
>
> Download a backup of this Tiger Store settings.
>
> You can use the backup file to restore the settings after firmware restore.
>
> **Back Up**
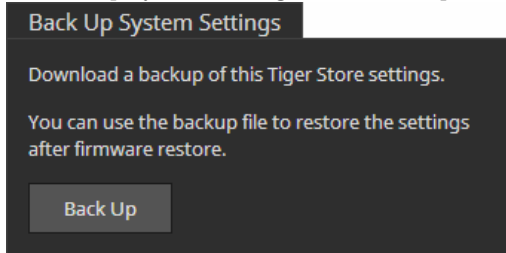
3. Do one of the following:

   • Leave the password field empty and click OK, to be able to restore the settings configuration without providing password.

   • Enter a password and click OK, to allow restoring the settings configuration only after providing a password.

4. Select the location where to save the file and click Save.

To restore a Tiger Store settings configuration:

1. In the left pane of the web interface, click System and then Maintenance.

2. In Restore System Settings, click Choose File.

> **Restore System Settings**
>
> Restore backed up settings to this Tiger Store.
>
> Important: Restoring settings will disconnect clients and restart Tiger Store.
>
> **Choose File**   No file chosen
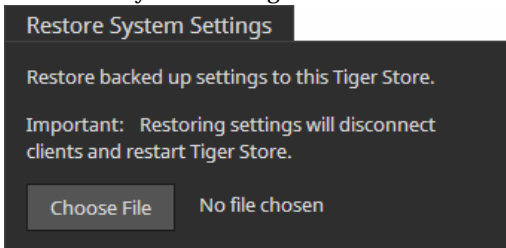
3. Select the file and click Open.

4. Do one of the following:

   • Leave the password field empty and click OK, to restore a settings configuration, which isn't password protected.

   • Enter a password and click OK, to restore a settings configuration protected with a password.

5. Tiger Store automatically disconnects all Tiger Clients and after importing the selected backup file restarts.
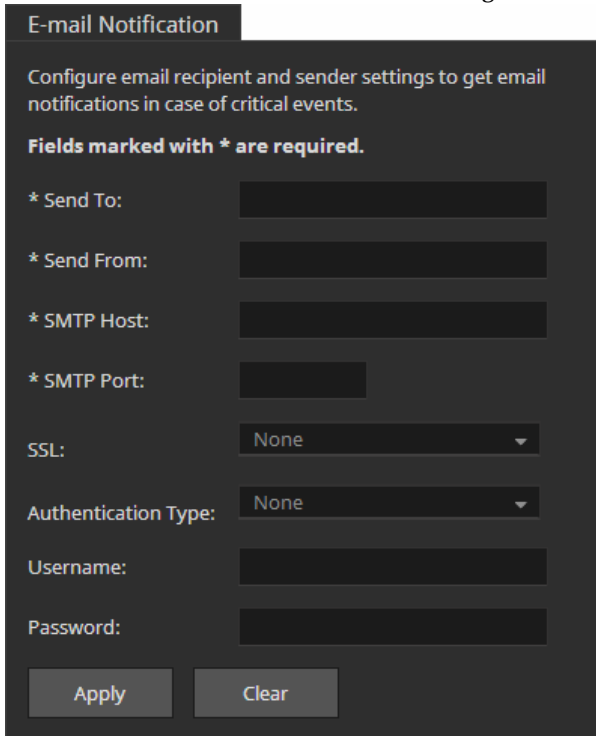
Configure E-mail Notifications

Tiger Store offers you the opportunity to receive e-mail notifications each time there's a problem with the shared volumes. The notifications give you detailed information about the storage status and the exact disk that has failed. To benefit from the e-mail notifications, besides specifying the e-mail account(s) to which the notifications to be sent, you must also specify an e-mail account from which these notifications to be sent. This account must be managed by a mail server to which Tiger Store is connected via the Public port or another Ethernet port. It is advisable to let the system administrator set the notification settings as you will also need the password, SMTP host, SMTP port, SSL and authentication type details of the account from which the notifications will be send. Your system administrator can create a new e-mail account specifically for the purposes of sending e-mail notifications from Tiger Store.

You can enable/disable e-mail notifications at any time, keeping in mind that each time you disable them, you lose all e-mail notification settings you have specified.

To enable/disable e-mail notifications:

1. In the left pane of the web interface, click Settings.

2. In E-mail Notification, do one of the following:

• To enable e-mail notifications or edit the e-mail notifications settings, enter the needed information in the respective fields and click Apply.

Note: *In case you want to set more than one e-mail account to receive notifications, in the Send To field enter the respective e-mail accounts separated by commas.*

Tip: *To verify that you have correctly specified the e-mail notification settings, click Send Test Message and check the Inbox of the e-mail account for the test message.*

• To disable e-mail notifications, click Clear and then Apply.

View Event Reports

In the web interface you can view detailed reports about events regarding the shared volumes, a Tiger Client or all Tiger Clients within a selected time period. You can filter the events by three categories - informations, warning and errors.

Note: *You can generate Event reports, only if you are currently connected to the storage server for which you generate the report.*

To generate an event report:

1. In the left pane of the web interface, click Events.

   Tip: *On Tiger Store with high-availability add-on activated, to view events report for a specific server node only, open its node view in the web UI.*

   The Events page appears.
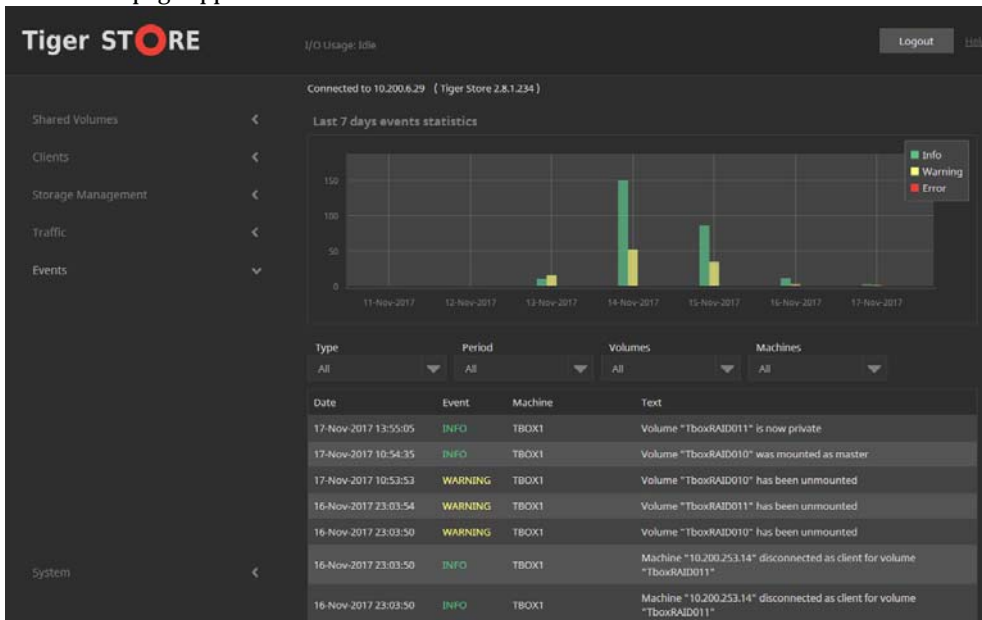
2. In the Type drop-down box, select whether to generate a report about all events or filter it to specific type only.

3. In the Period drop-down box, select the time period for which to generate the report.

4. In the Volumes drop-down box, select whether to generate report for a selected volume only or for all volumes.

5. In the Machines drop-down box, select whether to generate a report about all machines or filter it to a specific computer only.

   The Events page displays graphs with the event types by date and below lists all events in descending order.

System Maintenance

Best Practices

Storage Server Best Practices

Change the TCP Port for Access to the Web Interface

By default, TCP port 80 is designated for access to the web interface of Tiger Store. If this port is already in use by another service or you simply want to access the Tiger Store's web interface through another port, you can assign a different port for the purpose. To do this, you should create a new string value in the Tiger Store registry on the storage server. On a storage server running the software-only installation of Tiger Store, follow the steps below. On Tiger Store appliances, contact Tiger Technology support for assistance.

Once you assign a different TCP port for access to the web interface of Tiger Store, each time you want to access it in your web browser, aside from providing the IP address/domain name of the storage server, you must also provide the number of the new TCP port as well. For example, if your storage server uses IP address 10.200.6.33 and you have assigned TCP port 8380 to be used instead of the default port 80, to access the web interface of Tiger Store you must enter the following in the address bar of the web browser:

10.200.6.33:8380

Important: *Even if you assign a new TCP port for access to the web interface of Tiger Technology, accessing the web interface from Tiger Client computers using the tray application (Windows) or the menulet (Mac OS X) will always redirect the request through TCP port 80.*

To assign new TCP port for access to Tiger Store's web interface:

1. On the storage server, start the Registry Editor.

   Tip: *To start Registry Editor, on the Start menu click Run and in the dialog type regedit.*

2. Navigate to:
   HKEY_LOCAL_MACHINE\SOFTWARE\Tiger Technology\tbox\tboxmaster\settings\

3. Right-click in the right pane and select New | String Value.

4. Rename the new REG_SZ value to:
   webui_port

5. Right-click the webui_port value and select Modify.

6. In Value Data enter the number of the TCP port to be used for access to Tiger Store's web interface and then click OK.

7. Restart the storage server.

8. Make sure the new TCP port is not blocked by the firewall on the storage server.

Installing Tiger Spaces after Tiger Store

In case you want to install Tiger Spaces on your storage server, to ensure the normal functionality of both products, you must first install Tiger Store software and only after that Tiger Spaces.

Configure a DNS Reverse Lookup Zone to use Active Directory in Heterogeneous Environment

When Tiger Store operates in cross-platform environment (with Mac Tiger Clients), to benefit from Active Directory support, DNS reverse lookup zone must be configured on the domain controller. Otherwise, the domain permissions will not be respected by the Mac Tiger Client.

For information about configuring DNS reverse lookup zone, refer to your Active Directory domain controller documentation.

Avoid Backing Up the Settings Configuration in Maintenance Mode

Tiger Store cannot ensure the consistency of the settings configuration backup, when you save it while in Maintenance mode. To avoid possible problems, it is advisable to always back up and restore the settings configuration when the appliance is not running in Maintenance mode.

Granting Full Control to the System Account

In Windows, the built-in System account, used by the operating system and by services, by default has Full Control to all files on an NTFS volume. To provide for the normal operation of Tiger Store, it is advisable not to change the Full Control permissions of this account.

For details about displaying the System account when setting permissions and granting Full Control to it, refer to your Windows documentation.

Assigning IP Addresses to Network Ports

IP Addresses Limitations

When assigning IP addresses to the network ports of Tiger Store, make sure that you avoid the following IP addresses as they are either link-local addresses or are in use by Tiger Store services:

• Link-local addresses in the range 169.254.0.0 - 169.254.255.255

• IPMI addresses in the range 1.1.1.0 - 1.1.1.255

IP Addresses on Tiger Store with High-Availability

It is sometimes possible a request from a LAN Tiger Client to be redirected through the 1GbE port instead of a faster connection (through a 10GbE port, for example). The problem can be observed

with Tiger Store storage servers with high-availability and is reproducible when the node you have added to your storage servers list tries to redirect you to the other server node, which is currently playing the role of a primary node. To avoid the problem, it is highly advisable to set the IP addresses of the ports on the faster network connection between the storage server and the LAN Tiger Client to be on a separate LAN or on a subnet of the LAN used by the Public port.

For example, if the Public port uses IP address 172.16.1.1 (with subnet mask 255.255.255.0), set the IP address of the first 10GbE port to 172.16.2.1 (with subnet mask 255.255.255.0) and change the IP address of the Tiger Client 10GbE port to be on the same subnet. For the next 10GbE port of the storage server, set IP address 172.16.3.1 (with subnet mask 255.255.255.0) and respectively change the IP address of the 10GbE port of a Tiger Client to be on the same subnet.

Another important thing is to add Tiger Store to the storage servers list on each LAN Tiger Client using the IP address set for the faster network connection and not the Public port.

Synchronization of IP Settings Between High-Availability Nodes

To guarantee the failover between the two server nodes of a storage server with high-availability, the network ports with identical names on both nodes (the Public ports, for example) must use consecutive IP addresses and identical settings for subnet, router and DNS server. In case you cannot meet these requirements, the failover between server nodes cannot take place. When you configure the IP settings of one node, as long as the other node is also online, Tiger Store attempts to automatically synchronize the IP settings and assigns the same settings for subnet, router and DNS server and a consecutive IP address of the port with the same name on the other server node. If the consecutive IP address on the network is already taken, Tiger Store will assign a random IP address to the identical port of the other server node and failover between the two nodes will not be possible.

When one of the nodes is offline while you change the IP configuration settings of the other node, you must synchronize the IP settings of the two nodes manually, in order not to obstruct failover between server nodes. You can do this in the Node view of the respective server node.

Using a DHCP Server on Your Tiger Store Network

A Dynamic Host Configuration Protocol (DHCP) server automatically assigns and leases IP addresses to computers as they are added to a network. While you can allow run-time configuring of IP addresses of both the Tiger Store server and the Tiger Clients, to ensure the proper cross-network communication, there should be a DNS server on the network that resolves the IP address of each connected computer to its domain name. Additionally, each Tiger Client should add the Tiger Store server to its storage servers' list using its domain name instead of the IP address with which it is currently identified.

In case there isn't a DNS server on the network, you should configure your DHCP server to use static allocation of IP addresses to the Tiger Store server and Tiger Clients.

Note: *Non Tiger Client computers can still benefit from dynamic allocation of IP addresses by the DHCP server.*

Restarting A Server Node While in Maintenance Mode

When you enter Maintenance mode, Tiger Clients are automatically disconnected from both server nodes of your Tiger Store appliance, until you exit Maintenance mode in the web UI or restart the appliance. It is advisable not to restart just one server node (in node view) as it will exit Maintenance mode and will attempt to supervise the volumes managed by Tiger Store, while the other node is in Maintenance mode and performs a maintenance operation.

Tiger Client Best Practices

Installing Tiger Client on macOS Catalina

If macOS Catalina 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.

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%20Adapt
er' >/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.

Shared Storage Best Practices

Avid File System Emulation and Avid Versions Without Bin Locking

Tiger Store's Avid file system emulation allows you to mount one and the same Avid project with Read & Write permissions on multiple Tiger Client computers simultaneously, letting Avid restrict accesses to the bins that are currently in use.

Still, when you use an Avid version, which does not provide bin locking (like Avid Media Composer | First, for example) even though Avid file system emulation may be enabled on the volumes, Tiger Store cannot prevent users on different computers from accessing the same bin and from overwriting each other's changes.

Extending Volumes Managed by Tiger Store

Unlike most disk management operations that can be executed while in Maintenance mode, extending a volume is a rather complex task that functions on low level and may not be cleanly performed while the Tiger Store drivers are loaded, even if the storage server operates in Maintenance mode.

With this in mind, the recommended procedure for extending a SAN volume managed by Tiger Store is to first change the volume's status to Offline and then uninstall Tiger Store from the storage server. Once the storage server is rebooted and the volume can be mounted and accessed as a private NTFS volume, you can perform the extend operation.

Detaching Shared Volumes from Tiger Store for Use on Another Computer

To protect volumes from data corruption that could occur when multiple computers have access to them simultaneously, Tiger Store marks the volumes it manages. To be able to mount a volume without Tiger Store, this volume needs to be unmarked. Tiger Store automatically unmarks all volumes with Offline status. If you intend to physically disconnect a volume for use on another computer, you must first change the status of this volume to Offline. If you fail to set the volume to Offline, you need to contact Tiger Technology support for assistance on unmarking the volume.

Using Antivirus on the SAN

It is advisable to use an antivirus software (like ESET NOD32, for example) on your shared storage only when needed or if inevitable for your workflow. Additionally, to avoid decreased performance, it is advisable to run the checks only from the storage server computer.

Data on the Shared Storage Best Practices

File Systems Behaviour and Files Compatibility

The three operating systems (Windows, Mac OS X and Linux) on which you can install the Tiger Client software differ in the way they manage files. On Windows, files can have many streams, in contrast to Mac OS X (only 2 streams - data fork and resource fork), and Linux (only data stream). In addition, files created by Mac OS X also have extended attributes (such as the Finder Info, for example) that are not available on the other two platforms.

These peculiarities of the file systems lead to partial loss of information when transferring a file created on one platform through a machine running on another platform.

For instance, when on Mac OS X you copy a file with 50 streams created by Windows, all file streams' information is lost, except the information of the data stream. The result will be the same

when a Linux computer copies a 50-stream Windows file. A Mac OS X file copied by Linux will also lose its resource fork's info.

Streams' information is not lost when copying Mac OS X or Linux files by a Windows computer, but in this case a Mac OS X file will lose the extended attributes information.

There is another problem with files sharing common file format. For example, a movie file created with Final Cut Pro on Mac OS X is playable by QuickTime. If a Windows workstation copies this file, it will not recognize it as QuickTime-playable until adding the *.mov extension to it.

See also "Final Cut Pro X Project Names on the Shared Volumes" on page 116.

Avoiding Long File Names

By default, on Windows the length of file names is limited to 260 characters and on Mac OS X - to 1024 characters. On both Windows and Mac OS X, the full path to the file is also included in the character count. That is why it is possible to receive errors when attempting to create or copy a file with long file name. For this reason it is advisable to avoid long file names in order to ensure that file operations on the shared storage are normally processed.

Final Cut Pro X Project Names on the Shared Volumes

It is advisable that the Final Cut Pro X projects you create on the shared volumes have names that do not exceed 31 symbols.

Migrating Replicated Data

Migrating Replicated Data from One Replication Target to Another

While the Replication & Tiering mechanism of Tiger Bridge does not restrict you about changing the replication target, to avoid problems, you should set a new replication target with caution and after careful planning. If you need to set a new replication target to which files to be copied, you should keep in mind that all already replicated files will be inaccessible from the new replication target. Additionally, nearline and offline files (replicated files that have a copy only on the replication target) cannot be retrieved unless they have a counterpart on the new replication target.

When changing the replication target of your shared storage, it is recommended to migrate all already replicated data from the previous replication target to the new one. The safest workflow to do this is to let Tiger Bridge replicate it again on the new replication target. For the purpose, you have to make sure that:

• all already replicated files are available on the shared storage (note that lack of free space on your shared storage may hamper the process).

• the status of all already replicated files is not "replicated" but "normal" as Tiger Bridge will skip files on the shared storage that are with "replicated" status and will not copy them to the new replication target.

You can achieve this following these steps:

1. To ensure that each replicated file has a nearline/offline counterpart on the shared volume(s), in the drop-down box of the Volume Browser, select a volume with enabled replication and then click Rescan Volume.

2. Repeat the above step for each volume on which replication is enabled.

3. In the left pane of the Volume Browser, select the root of the volume and in the right pane select a folder and click Retrieve Data

   Note: *You have to manually select all nearline files in the root of the volume and click Retrieve Data.*

4. Repeat the above step for each folder on each volume with enabled replication in order to retrieve all replicated files to their original locations.

5. In Tiger Bridge, specify a new replication target.

6. In "Folders excluded from replication" add the root of the source and click Apply.

7. In the left pane of the Volume Browser, select the root of the volume and in the right pane select a folder and click Reclaim Space, to revert all files from "replicated" status to "normal" status.

   Note: *You have to manually select all retrieved files in the root of the volume and click Reclaim Space to revert their status to "normal".*

   Important: *Clicking Reclaim Space transfers the status of replicated files to "normal" only if Tiger Bridge detects that the selected files do not have copies on the replication target. If you issue the command for a file with "replicated" status, which actually has a copy on the replication target, the command will replace the file on the shared storage with a stub file pointing to its copy on the replication target.*

8. Repeat the above step for each folder on each volume with enabled replication.

9. In Tiger Bridge, adjust the replication policy parameters to match your desired workflow with the new replication target and to let Tiger Bridge replicate files to it normally.

Migrating Replicated Data to a New Volume

When you need to reformat a volume from which data has been replicated or to replace it with a volume with bigger capacity, instead of manually moving data between volumes in order to retrieve data on the new volume, you can use the replication & tiering mechanism of Tiger Bridge to automate the process. Following the steps below, you will be able to retrieve all already replicated data from the replication target to the new volume. Data will be retrieved in the form of stub files, which you can make normal in the Volume Browser or on demand (by accessing them) in your file browser.

To ensure that all needed data is copied to the replication target, you may have to manually replicate files or whole folders in the Volume Browser:

1. In the Volume drop-down box of the Volume Browser, select the old volume.

   Note: *If you are migrating Tiger Spaces data, in the Volume Browser select the "Workspaces" check box to display all workspaces folders.*

2. In the right pane, select a file or folder with Normal status and click Replicate.

   Note: *In the Volume Browser a folder is with Normal status if it contains even just one file, which is not yet replicated.*

   When all files/folders you want to migrate to the new volume are with replicated status in the Volume Browser, you are ready to proceed with the migration steps below.

   Important: *If you're using a Private volume as replication target, before you reformat or detach the volume from which data has been replicated, you must get its GUID as well as the GUID of the volume, on which you will restore data. For the purpose you can access the web interface of your storage server through port 9125, typing the following in the address bar of a web browser:*

   ```
   [IP address of the storage server]:9125/volumes
   ```

   The storage server lists information about each shared volume. Search the list for the label of the respective volume and copy its GUID from the "guid" field of the list.

To retrieve replicated data on a new volume:

1. If you are migrating Tiger Spaces data, enable support for Tiger Spaces on the new volume.

2. In Tiger Bridge, enable replication on the new volume, by setting exactly the same replication target as for the old volume (the same private volume, folder on the SMB/CIFS share, bucket, etc.).

3. (for replication on a Private volume only) Pause all Tiger Bridge automatic operations (in the Tiger Bridge window select Tiger Bridge in the left pane and then click Pause in the taskbar) and share the private volume, then in your file browser go to the .tt_rt folder in the root of the volume and rename the folder with the GUID of the old volume with the GUID of the new volume, then enable replication again using the same settings as in the step above.

4. In the Volume drop-down box of the Volume Browser, select the new volume and then click Rescan Volume.

   Tiger Bridge creates a stub file for each replicated file on the replication target, which it cannot find on the volume i.e. all files that have been replicated from the old volume.

5. (for migrated Tiger Spaces data only) Convert all retrieved files from nearline to replicated: in the Volume Browser, select the new volume in the drop-down box and select the "Workspaces" check box, then one by one select each workspace and click Retrieve Data.

6. (Tiger Spaces only) Log on to Tiger Spaces, log on as administrator and rescan each workspace, to regenerate its information such as size, users, application type, number of files, etc. as well as to queue proxy media generation.

7. In Tiger Bridge resume all automatic operations (in the Tiger Bridge window select Tiger Bridge in the left pane and then click Resume in the taskbar).

Best Practices

Known Issues

Shared Storage Known Issues

Automatic Defragmentation Disabled on Storage Servers Running Windows Update 1809

Due to possible problems when automatic volume defragmentation is performed from a storage server running Windows update 1809 or above, this option is disabled. On all storage servers running other than Windows update 1809, you can enable/disable Tiger Store's automatic volume defragmentation.

No Support for Manual Defragmentation

Currently, you cannot perform manual defragmentation of your shared volumes. To keep your volumes defragmented it is advisable to enable the automatic defragmentation.

Volume Status not Preserved after Exiting Maintenance Mode

Note: *This issue cannot be observed on Tiger Store appliances with two server nodes.*

Volumes that have been shared before entering Maintenance mode may become Private after exiting Maintenance mode even though its tile shows Shared status. That is why after exiting Maintenance mode, it is advisable to check the status of all volumes seen by the storage server and manually change it. If the status of the volume is Shared, but it cannot be mounted on Tiger Clients, first set it to Private and then set it to Shared to let client computers mount 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 Software Mirrored Volumes

Currently, Tiger Store does not provide support for software mirrored volumes. You can use hardware mirrored volumes as part of your shared storage.

No Support for Spotlight Indexing

Currently, Spotlight Indexing is not supported on Mac OS X clients. To index and search through shared volumes from Tiger Clients running Mac OS X, 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 Mac OS X

You can change the appearance of a shared volume's icon on a Mac OS X 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.

Importing Offline Dynamic Disks in Maintenance Mode

Offline dynamic disks cannot be imported when your Tiger Store appliance operates in Maintenance mode. To import offline disks, you have to exit Maintenance mode.

Storage Server Known Issues

Teaming Network Ports Known Issues

After enabling/disabling the setting for teaming of network ports, the web interface may display error, whereas the setting is actually applied. Additionally, on a Tiger Store appliance with 2 server nodes, the default IP address assigned to the team is identical on both server nodes. Note that

manually assigning an IP address to the team in cluster view, synchronizes the setting on both server nodes if they are online and there's no need to assign it in node view.

Renaming a Volume

You may have to rename a volume twice in the web interface of Tiger Store in order to permanently change its name.

Volume Disappears from Web UI during Check and Repair Procedure

While you perform the Check & Repair procedure on a Tiger Store volume, it is not listed in the web UI. Once the procedure finishes, you can manage the volume in the web interface again.

Exporting a SMB Share in Domain Environment

To ensure that Tiger Store can export a SMB share to computers without the Tiger Client software, when your appliance is deployed in an Active Directory domain, the domain account "Everyone" must have at least Read Only access to the root of the volume from which the share is exported.

Applying New Network Environment Settings

It is possible when changing the settings for network environment (domain or workgroup) of your appliance after clicking the Apply button in the Settings page an error to be displayed, when in fact the changes have been applied. It is advisable to refresh the web UI of Tiger Store in order to verify whether the new settings have been applied.

Renaming the Appliance

Should you rename your Tiger Store appliance after it has been added to an Active Directory domain, Tiger Clients may fail to browse the volumes it shares even if they re-add it to their storage servers list. It is advisable before renaming the appliance, to set the network environment to workgroup and manually delete the records about the appliance from the domain controller. It is advisable to do this each time you switch the network environment of your Tiger Store from domain to workgroup.

Alternatively, you can manually change the DNS record for the Tiger Store appliance in the respective DNS Zones in your domain so they can match the new name of the appliance. For details about configuring DNS services, refer to your Windows documentation.

Errors When Entering/Exiting Maintenance Mode

When entering/exiting Maintenance mode, the web UI of Tiger Store may display errors, when in fact the operation has succeeded. To verify that you have entered/exited Maintenance mode, refresh the browser. If on exiting Maintenance mode the error persists, restart the storage server.

No Authorization Required When Removing Tiger Store from the Domain

If you decide to switch your Tiger Store from domain to workgroup environment, the domain controller does not require that you authenticate yourself as a user authorized to remove computers from the domain.

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 File Security in the Tiger Store Network" on page 29 for steps about enabling/disabling file security.

Note: *File security is automatically enabled on a Tiger Store appliance once it is added to an Active Directory domain. For assistance on disabling file security, contact Tiger Technology support.*

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.

Mac Clients Mounting NTFS Stripe Partitions over the LAN

Currently, Apple Mac client computers can mount just the first partition of a striped NTFS volume over the Fibre Channel and all other partitions are mounted over the Ethernet.

Label of SAN Disks Missing in Windows Explorer of Windows Tiger Clients

On some Windows Tiger Clients, the label of shared volumes mounted over the Fibre Channel may be missing in Windows Explorer.

To attempt to resolve the problem restart the Tiger Client computer or disconnect and then reconnect to Tiger Store:

1. Click the Tiger Client tray application and then click Connect/Disconnect.

2. In the list of all storage servers, click the Tiger Store appliance to disconnect from it.

3. Again click Connect/Disconnect and click the Tiger Store appliance in the list to connect to it.

It is possible the above workaround to be inapplicable on Windows 10 Tiger Clients. If this is the case, you can still identify volumes in Windows Explorer by their drive letter or use command-line to list their labels (using diskpart utility, for example).

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 Mac OS X

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 Mac OS X:

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.

High Availability Known Issues

Activating the High-availability Add-on

After activating the high-availability add-on on your storage server, you need to restart the storage server to be able to view the HA Nodes page in the web interface.

Connecting to a Newly Added Secondary Node from Tiger Clients

In case you have added a Tiger Store appliance to your storage servers list when only one of its nodes has been online, when the other server node is also online and an IP address is assigned to it, you may have to remove the appliance from the list and add it anew, in order to ensure that in case of failover you can connect to it.

Incorrect LAN Traffic Statistics

If you monitor the LAN traffic statistics of Tiger Store with high-availability add-on activated, by accessing its web interface through the secondary node (the server node that is in standby mode), the graph will display no LAN traffic. To view the actual statistics, open the web interface using the IP address of the current primary node.

Smart Storage Pooling Known Issues

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).

Specifying Name and Preferred Mount Location of a Volume Pool

You cannot rename a smart storage pool or set preferred mount location on Windows Tiger Clients.

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).

Tiger Bridge Known Issues

Prevent Replicated Data Loss After Upgrading to Tiger Bridge

Due to incompatibility between version 2.7.3 and below of Tiger Store's replication & tiering mechanism and Tiger Bridge, it is possible after upgrading to Tiger Bridge to lose data from the replication target. To avoid this problem, before upgrading to Tiger Bridge you must contact the Tiger Technology support team for assistance on converting the attributes of replicated and nearline files, which will prevent data loss.

Duplicated Files on Spectra Logic BlackPearl

When the Tiger Bridge add-on is set to replicate on a Spectra Logic BlackPearl appliance, it is possible duplication of files to occur on both the target and the shared volume(s). As the BlackPearl appliance cannot tell that an already replicated file is moved to another directory on the shared volume, it perceives it as a new file to replicate and keeps both its copy in its previous location and the new one. Similarly, should you attempt to retrieve a replicated file that has been moved, the

mechanism will restore two copies of the file - one in its original location and another in the location to which it has been moved.

Retrieving Deleted Tiger Spaces Workspace from the Target

When you delete a replicated workspace in the Tiger Spaces web interface, Tiger Spaces automatically moves it to a temporary Trash folder in the workspaces depot. Should Tiger Bridge happen to replicate the Trash folder before Tiger Spaces deletes it, the deleted workspace is automatically moved to a Trash folder on your target.

Note: *Currently the replication on Spectra Logic BlackPearl does not support paths synchronization when renaming the containing folder and the deleted workspace will be present in both the depot and the Trash folder on the target. Thus, you will be able to retrieve the deleted folder directly from the depot.*

To retrieve the workspace in the depot on your main storage from the Trash folder on a Private volume, SMB/CIFS network share or cloud storage target, you should:

• (SMB/CIFS network share) Manually move the workspace from the Trash folder to the Workspaces folder and then rescan the Volume in order to re-generate the deleted files as stub files, which you can then retrieve.

• (Private volume) Disable Tiger Bridge on the Private volume and share it to Tiger Clients, then unhide the .tt_rt folder in the root of the volume and manually move the deleted workspace from the Trash folder to the Workspaces folder. Make the volume Private again and enable Tiger Bridge, then rescan the shared volume in the Volume Browser in order to re-generate the deleted files as stub files, which you can then retrieve.

• (cloud storage) Rescan the volume and regenerate the deleted data as stub files and then contact Tiger Technology support for assistance on moving the data from the hidden Trash folder to the Workspaces folder.

Regardless of the target you use, the final step to allow Tiger Spaces to detect and let you work with the workspace in Tiger Spaces is to restart the add-on services in the Maintenance page of Tiger Store.

Moving Replicated or Nearline Files/Folders

If you move a replicated or nearline file/folder from its original location to a folder that is not subject to Tiger Bridge's replication on the shared storage, this folder will also appear on the replication target, but will contain just the files/folders that are subject to replication. For example, if you move a nearline file "Report" from its original folder "April" to folder "Drafts" that is not subject to replication and contains other files as well, the replication and tiering mechanism of Tiger Store will create on the replication target a folder "Drafts", but containing just the file "Report".

Index