



Tiger BRIDGE

Tiger Bridge 4.1.11 Administration Guide

April 23, 2021

This publication, or parts thereof, may not be reproduced in any form, by any method, for any purpose.

TIGER TECHNOLOGY MAKES NO WARRANTY, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES, OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, REGARDING THESE MATERIALS AND MAKES SUCH MATERIALS AVAILABLE SOLELY ON AN “AS-IS” BASIS.

IN NO EVENT SHALL TIGER TECHNOLOGY BE LIABLE TO ANYONE FOR SPECIAL, COLLATERAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH OR ARISING OUT OF PURCHASE OR USE OF THESE MATERIALS. THE SOLE AND EXCLUSIVE LIABILITY TO TIGER TECHNOLOGY, REGARDLESS OF THE FORM OF ACTION, SHALL NOT EXCEED THE PURCHASE PRICE OF THE MATERIALS DESCRIBED HEREIN.

Tiger Technology reserves the right to revise and improve its products as it sees fit. This publication describes the state of this product at the time of its publication, and may not reflect the product at all times in the future.

THIRD-PARTY TRADEMARKS

All other brand names, product names, or trademarks belong to their respective holders.

Title: Tiger Bridge Administration Guide
Software version: 4.1.11
Date: April 23, 2021

Manual Revision and Control

Revision Record

Date	Description	Page	Version
07 Feb. 2020	Initial Draft for version 4.0		
16 Sept. 2020	Remote shell extension access functionality added.	11, 26, 134	4.1
16 Sept. 2020	Added support for OpenStack Swift object storage target.	21, 57	4.1
16 Sept. 2020	Check for updates steps added.	27	4.1
16 Sept. 2020	Added option for selecting how to synchronize source with existing data on target when pairing them.	38	4.1

Revision Record

Date	Description	Page	Version
16 Sept. 2020	Enable and configure ransomware protection of replicated data functionality added.	132	4.1
16 Sept. 2020	When undeleting data, you can select the specific files, which to undelete.	160	4.1
16 Sept. 2020	Deleting newer versions of a file functionality added to files and folders versions control.	162	4.1
25 Jan. 2021	Added support for FujiFilm Object Archive target.	22, 78	4.1.8
25 Jan. 2021	Configure offline files rehydration behaviour steps added.	142	4.1.8
19 Feb. 2021	Network share source requirements updated with requirements for NFS shares.	16	4.1.10
19 Feb. 2021	Added support for Hitachi Content Platform (HCP) target.	21, 54	4.1.10
19 Feb. 2021	Added support for Seagate CORTX storage target.	21, 64	4.1.10
20 Apr. 2021	Added support for NFS share as a target.	17, 22	4.1.11
20 Apr. 2021	Added support for LYVE Cloud target.	20, 59	4.1.11
20 Apr. 2021	Added support for RSTOR Space target.	20, 62	4.1.11
20 Apr. 2021	Disabling automatic data replication steps added.	84	4.1.11

toc

Table of Contents

1	Introduction to Tiger Bridge	5
	How It Works	6
	Data Protection	8
	Tiger Bridge Interfaces	9
	Tiger Bridge Configuration	9
	Command-line Interface	10
	Tiger Bridge Shell Extension	10
	Windows Event Viewer	12
	Tiger Bridge Licensing	13
	System Requirements	14
	High Availability Requirements	15
	Storage Requirements	15
	Source Storage Requirements	15
	Target Storage Requirements	16
	Target Storage Prerequisites	17
2	Tiger Bridge Installation	23
	Install Tiger Bridge	24
	Uninstall Tiger Bridge	26
	Update Tiger Bridge	27
3	Get Started with Tiger Bridge Using the Configuration	29
	Activate Tiger Bridge	31
	Add a Source	36
	NAS Source Prerequisites and Setup	36
	Pair Source with a Target	38
	Pair a Source with Microsoft Azure Blob Storage Target	39
	Pair a Source with Amazon S3 Target	42
	Pair a Source with IBM Cloud Object Storage Target	46
	Pair a Source with Backblaze Target	48

Table of Contents

Pair a Source with Wasabi Target	51
Pair a Source with Hitachi Content Platform Target	54
Pair a Source with OpenStack Swift Target	57
Pair a Source with LYVE Cloud Target	59
Pair a Source with RSTOR Space Target	62
Pair a Source with Seagate CORTX Target	64
Pair a Source with S3-compatible Object Storage Target	67
Pair a Source with Google Cloud Target	69
Pair a Source with Google Drive Target	72
Pair a Source with BlackPearl Object Storage Target	74
Pair a Source with Coeus Target	76
Pair a Source with a FujiFilm Object Archive Target	78
Pair a Source with a Network Share Target	80
Pair a Source with a Local Volume Target	82
Configure Automatic Data Replication	83
Refine the List of Automatically Managed Locations	84
Configure Space Reclaiming	86
Configure Data Archiving	91
Configure Active Sync	95
Configure Versioning	99
Configure Operation Mode	100
Pause/Resume Automatic Tiger Bridge Operations	102
Monitor Data Management Statistics	103

4 Get Started with Tiger Bridge Using the Command-line Interface 107

Activate Tiger Bridge	108
Pair Source with a Target.	109
Pair a Source with Microsoft Azure Blob Storage Target	109
Pair a Source with Amazon S3 Target	110
Pair a Source with IBM Cloud Object Storage Target	111
Pair a Source with Backblaze Target	113
Pair a Source with S3-compatible Object Storage Target	114
Pair a Source with BlackPearl Object Storage Target	115
Pair a Source with Coeus Target	116
Pair a Source with a Network Share Target	118
Pair a Source with a Local Volume Target	119
Refine the List of Automatically Managed Locations.	120
Automatic Data Replication	121
Space Reclaiming	122
Automatic Data Archiving.	124
Active Sync	125

Operation Mode Parameters	127
Monitor Data Management Statistics	128
Disable Tiger Bridge	129
5 Manage Advanced Settings	131
General Advanced Settings.	132
Enable and Configure Ransomware Protection	132
Enable/Disable Remote Shell Extension Access	134
Specify Proxy Server Settings	135
Set Startup Scan Wait Time	136
Disable NFS Locking on the Tiger Bridge Computer	137
Advanced Data Replication Settings.	137
Minimum File Size for Replication	138
Enable Partial File Updates	138
Set Number of Parallel Threads during Data Replication	139
Replicate File's Data and Metadata to Different Containers	140
Advanced Space Reclaiming and Data Archiving Settings.	141
Retrieve Nearline Files Behaviour	141
Configure Offline Files Rehydration Behaviour	142
Partial File Retrieve Behaviour	144
Enable Progressive File Retrieval	145
Set File Retrieve Timeout	146
Set Reclaim Space Criteria Parameter	146
Set Stub File Allocation Size Display Option	147
Set Nearline File Head and Tail Sizes	147
Manage Tiger Bridge Logs	148
Manage Tiger Bridge Logs in the Configuration	149
Manage Tiger Bridge Logs in the Registry	150
6 Manually Manage Data	153
Perform Manual Tiger Bridge Operations	154
Manage Data Through the Shell Extension	154
Manage Data Through the Command-line Interface	157
Synchronize Data on the Source and the Target	159
Undelete Data on the Source	160
Manage Files and Folders Versions	162
7 Appendix: Tiger Bridge Logs	173
Information Logs.	173

Table of Contents

Warning Logs	173
Error Logs.	175

1

Introduction to Tiger Bridge

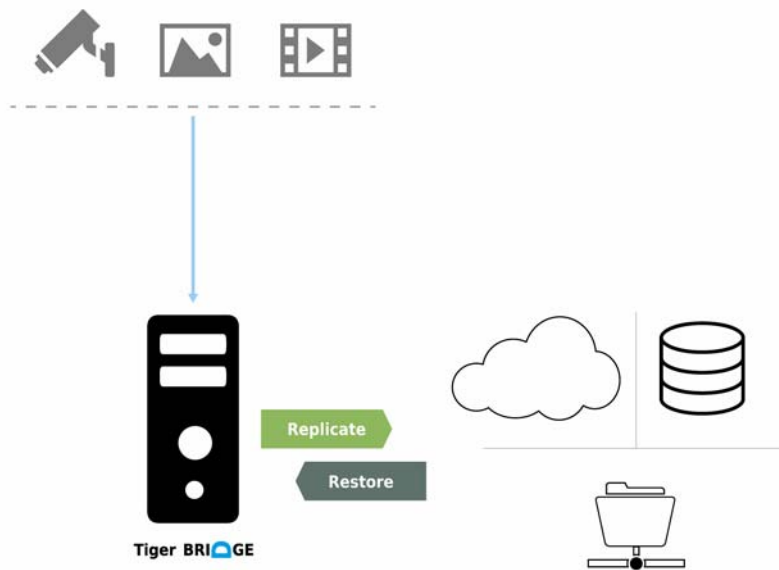
<i>How It Works</i>	6
<i>Tiger Bridge Interfaces</i>	9
<i>Tiger Bridge Licensing</i>	13
<i>System Requirements</i>	14
<i>Storage Requirements</i>	15

Introduction to Tiger Bridge

Congratulations on your purchase of Tiger Bridge, Tiger Technology's data lifecycle manager across heterogeneous storage tiers. It lets you pair a source (locally mounted NTFS volume or an SMB/NFS network share) with a target of your choice (cloud object storage, another local volume or a network share) into a seamless unity. Tiger Bridge takes care to automate the assignment of data to the source or the target tier, based on user-defined policies thus addressing various workflow challenges - from alignment of data with storage costs, transparent data migration and synchronization between storage devices or geographically dispersed places, to extending your primary storage on the cloud and gateway to object storage.

How It Works

As soon as you install and activate Tiger Bridge on the computer, you can create as many pairs consisting of a source and a target storage system as you wish. While in most cases users and applications work directly on the source location, the virtual storage unity displays the contents of both the source and the target, as if it is stored locally. By applying one or more of the following data lifecycle management mechanisms, Tiger Bridge distributes data among the two layers of the virtual unity:



data replication — Tiger Bridge copies a file from the source to the target. Automatic replication is performed based on user defined criteria. You can also manually replicate a file or a whole folder from the source to the target, using Tiger Bridge's command-line interface or the shell

extension. While data replication is indispensable for all other data lifecycle management mechanisms, it can also be used standalone for addressing the simplest scenarios, like data backup and disaster recovery, for example. To learn more, refer to “Configure Automatic Data Replication” on page 83.

space reclaiming — Tiger Bridge frees space on the source by replacing a replicated file with a nearline file. A nearline file is a stub file, which looks exactly like the actual file it replaces, but does not contain any data and does not take up space on your source. A nearline file points to the actual file on the target, which allows its retrieval back on the source. The retrieval from the target is automatic, should a user, an application or a process attempt to access the nearline file, or manual, through Tiger Bridge. Automatic space reclaiming is performed based on user defined criteria. You can also perform manual space reclaiming, using Tiger Bridge’s command-line interface or the shell extension. The most common scenario with space reclaiming is alignment of data with storage costs. To learn more, refer to “Configure Space Reclaiming” on page 86.

Important: *With a NAS source, nearline files are located in the control folder and not on the network share. Still, retrieving a nearline file in the control folder will retrieve it directly on the NAS source. To learn more about space reclaiming on NAS sources, refer to “NAS Source Prerequisites and Setup” on page 36.*

data archiving — Tiger Bridge moves a replicated file from the hot/cool tier of the target to the archival tier and replaces the replicated/nearline file with an offline file. An offline file is a stub file, which looks exactly like the actual file it replaces, but does not contain any data and does not take up space on your source. An offline file points to the actual file on the archival tier of the target, but unlike nearline files it cannot be retrieved on the source automatically (when a user or application attempts to open it) until you make it nearline by rehydrating it to an intermediate tier of the target. You can retrieve an offline file only manually, using the shell extension or the command-line interface. When you retrieve an offline file or folder, it is first rehydrated to an intermediate tier of your target (the Standard or High option of Azure or the temporary storage of S3 Glacier, for example) and from there it can automatically be retrieved on the source. Automatic archiving is performed based on user defined criteria. You can also manually archive, rehydrate or retrieve a file, using Tiger Bridge’s command-line interface or the shell extension. To learn more, refer to “Configure Data Archiving” on page 91.

Note: *On targets, which provide archival tier, but do not support third-party policy for moving data from the hot tier to the archival tier, Tiger Bridge can only verify when a file is moved to the archival tier in accordance with the target’s own archiving policy and update the status of such files on the source to offline. On such targets you cannot manually move data to the archive.*

Important: *With a NAS source, offline files are located in the control folder and not on the network share itself. To rehydrate an offline file, you need to perform the operation on the stub file in control folder. To learn more about data archiving on NAS sources, refer to “NAS Source Prerequisites and Setup” on page 36.*

Introduction to Tiger Bridge

active sync — automatically synchronize the contents of multiple sources, each on a different computer running Tiger Bridge, through a common target. Designed to facilitate geo replication scenarios, this mechanism allows you to select whether to synchronize the contents across all sources paired with the same target or set some sources to update their contents with updates from other sources. To learn more, refer to “Configure Active Sync” on page 95.

data synchronization — Tiger Bridge allows you to manually synchronize the contents of a target with its source. In case Tiger Bridge detects that a file on the target is not available on the source, the synchronization mechanism automatically creates a nearline counterpart for the missing file. Manual data synchronization facilitates scenarios involving data migration from one source to another and disaster recovery of data. For more information, refer to “Synchronize Data on the Source and the Target” on page 159.

By combining the above data management mechanisms with additional functionalities such as management of replicated versions and undeleting data in the cloud, remote shell access, ransomware protection, progressive retrieval of data from the target and others, Tiger Bridge can be deployed for any of the following purposes:

- data backup and disaster recovery
- alignment of data with storage costs
- extending local storage or a file server’s storage capacity on another storage system
- lowering the costs for block storage in the cloud
- interfacing object storage
- geo replication

To see which feature and functionality is included in the available subscription plans, refer to: <https://www.tiger-technology.com/getbridge/>

Data Protection

While Tiger Bridge gains programmatic access to your data at the source location and the target location, it takes care to prevent unauthorized access to it both when at rest and in transit:

- To gain access to any Tiger Bridge functions you need to authenticate yourself as the administrator of the computer on which Tiger Bridge runs. For more information, refer to “Tiger Bridge Interfaces” on page 9.
- The Tiger Bridge workflow supports applying any Windows techniques for controlling access to and protecting data at rest at source level.

- Tiger Bridge does not require maximum privileges of the credentials used for access to the target and adopts the target provider's own mechanisms for ensuring credentials protection is not compromised, like support for AWS access key rotation, for example.
- The credentials for access to the target are stored in the registry of the computer running Tiger Bridge and are encrypted using Advanced Encryption Standard, using Tiger Technology's own 256-bit key.
- Data in transit to cloud targets is protected allowing users to benefit from secure transfer (SSL/TLS) and also relying on the target provider's own mechanism for protecting data in transit, like AWS libraries, for example.

Note: *Tiger Technology encourages you to use any applicable best practices for data protection specified by Microsoft Windows and by the target provider.*

Tiger Bridge Interfaces

Tiger Bridge Configuration

Use the Tiger Bridge Configuration to create pairs of source and target and to configure the automatic data lifecycle management mechanisms valid for all pairs or just for a specific pair.

Note: *You need to run the Tiger Bridge Configuration as an administrator in order to apply changes to the product settings.*

To access the Tiger Bridge Configuration:

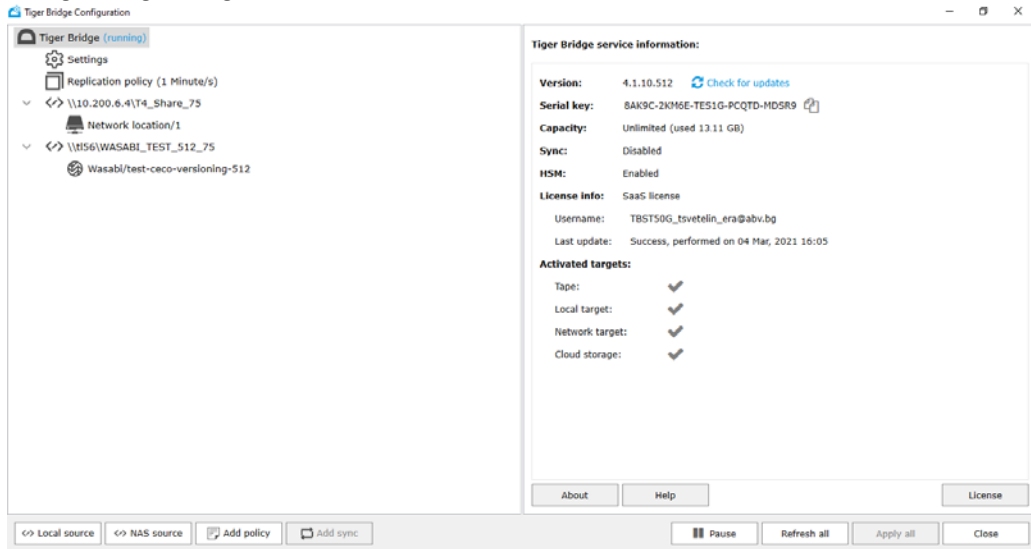
Note: *To access the Tiger Bridge Configuration, you need to run it as administrator.*

Do one of the following:

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

Introduction to Tiger Bridge

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



Command-line Interface

The command-line interface lets you activate and configure the product and perform manual data lifecycle operations. The main advantage of using the command-line interface is that you can automate specific tasks by including the commands in a script.

To access the command-line interface of Tiger Bridge:

Note: To access the Tiger Bridge command-line interface, you need to run command prompt as administrator.

1. In command prompt, execute the following:

```
tiercli
```

Tiger Bridge lists the available commands.

2. To view the command syntax with examples, simply execute a command without providing additional parameters. For example, to view the available commands for specifying data replication policy, execute the following:

```
tiercli config policy replicate
```

Tiger Bridge Shell Extension

The shell extension of Tiger Bridge is integrated with Windows Explorer and displays the status of files and folders on your source - replicated, nearline or offline. The shell extension also allows you

to manually manage data, using the Tiger Bridge menu in the Windows Explorer context menu. For more information, refer to “Manage Data Through the Shell Extension” on page 154.

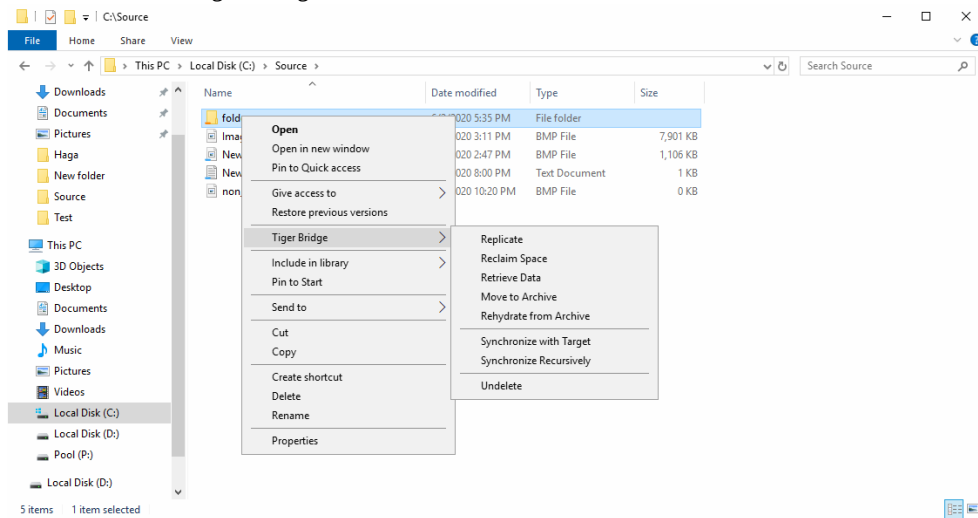
You can use the Tiger Bridge shell extension on the computer running Tiger Bridge as well as on any other remote Windows computer having access to a NAS source or to a local source exported as a network share. For the purpose, a Tiger Bridge administrator must allow remote shell extension access to the sources (for more information, refer to “Enable/Disable Remote Shell Extension Access” on page 134). Only a user with administrative privileges on the remote computer can run the shell extension. Additionally, the user needs to provide the IP address of the Tiger Bridge computer and the full local path to the source on the Tiger Bridge computer.

Note: Use NTFS permissions to control who can manage data at source level through the Tiger Bridge shell extension.

The shell extension can be installed together with Tiger Bridge or as a separate component. For more information, refer to “Install Tiger Bridge” on page 24.

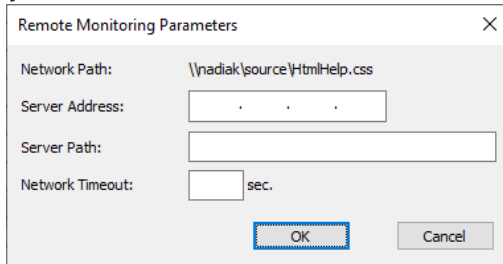
To access the Tiger Bridge shell extension context menu:

1. In Windows Explorer, navigate to a source paired with a target.
2. Right-click the file/folder you want to manage and in the context menu select the respective command under Tiger Bridge.



Introduction to Tiger Bridge

3. On remote computers, before gaining access to the Tiger Bridge shell extension commands, you need to click Remote Monitoring under Tiger Bridge and enter the following details to authorize your access to the source:

A screenshot of a Windows dialog box titled "Remote Monitoring Parameters". It contains four input fields: "Network Path:" with the text "\\nadiak\source\HtmlHelp.css", "Server Address:" with three dots ".", "Server Path:" which is empty, and "Network Timeout:" with a small box containing the number "5" followed by the text "sec.". At the bottom right are "OK" and "Cancel" buttons. The "OK" button is highlighted with a blue dashed border.

- IP address of the computer running Tiger Bridge.
- Full local path to the source on the computer running Tiger Bridge. For example, if you are accessing a local source folder “Source”, which is a sub-folder of folder “Documents” in the root of drive D on the Tiger Bridge computer, enter the following in server path:
D:\Documents\Source
- Specify the timeout after which attempting to perform a shell extension operation should be considered failed, but not delayed. A few seconds are considered normal timeout for receiving response to complete an operation.

Windows Event Viewer

To let you monitor its activity, Tiger Bridge logs all target/source connectivity events in the Windows Event Viewer. You can preview the logs by navigating to Applications and Services Logs | OpenSSH | Tiger Bridge. You can also use a third-party tools to automate the processing of notifications about important events.

Tiger Bridge can be configured to also log an event each time a file is replicated or replaced with a nearline/offline file, when a nearline file is retrieved from the target or when the status of a directory on the source is changed (replicated, nearline, offline), following the steps in “Manage Tiger Bridge Logs” on page 148.

Tiger Bridge logs three types of events in the Windows Event Viewer:

information — logs information about successfully performed operation.

warning — logs an unsuccessful attempt to perform an operation. Warning logs signify a temporary problem and Tiger Bridge attempts to perform the operation again until it either succeeds or reaches the threshold of scheduled attempts, after which it logs an error.

error — logs failure to perform an operation. Error logs signify a problem, which requires that you intervene in order to resolve it.

For a detailed description of each event logged by Tiger Bridge, refer to “Appendix: Tiger Bridge Logs” on page 173.

Tiger Bridge Licensing

You can activate your Tiger Bridge license using a software activation key, a software protection dongle (HASP) or as a software as a service (SaaS). For more information, refer to “Activate Tiger Bridge” on page 31.

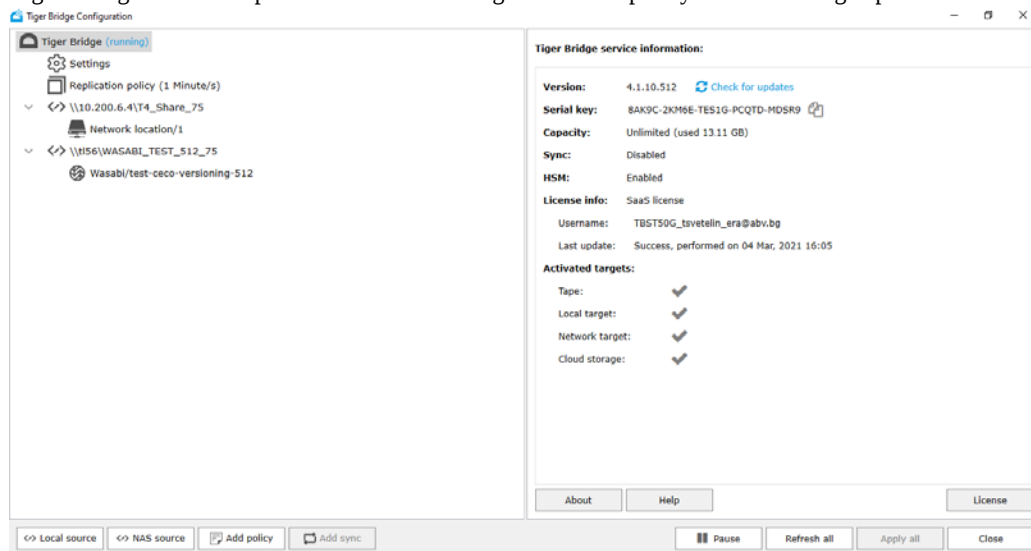
Note: *When provided for evaluation purposes, a license may be valid for a specific amount of time only.*

Regardless of the activation method, Tiger Bridge utilizes capacity-based licensing. With perpetual licenses (software or dongle) the license holds information about the maximum amount of data, which Tiger Bridge manages on all your sources. Once you reach your license’s capacity limit, Tiger Bridge stops replicating any further data, until you either expand the capacity of your license or delete unneeded data from your source. With a SaaS license there is no limit to the amount of data Tiger Bridge manages automatically, but capacity is calculated in order to utilize a consumption-based pricing model.

In both cases capacity is calculated as the sum of all file sizes in each source managed by Tiger Bridge, with the exception of excluded locations (subfolders of your source, which you have specified that Tiger Bridge should not manage automatically). Thus, if you add a source containing 2TB of data, even if only 1TB of its files are currently replicated or replaced by stub files, the overall capacity of this source will be calculated as 2TB.

Introduction to Tiger Bridge

You can keep track of your current capacity usage in the Tiger Bridge Configuration, by clicking Tiger Bridge in the left pane and then checking the used capacity field in the right pane.



Note: To see how to keep track of capacity usage per source, refer to “Monitor Data Management Statistics” on page 103.

System Requirements

You can install Tiger Bridge on a computer that meets these minimum system requirements:

- PC with 64-bit (x64) processor.

Note: Tiger Bridge actively uses the APIs provided by the target provider. These APIs may take significant amount of CPU depending on connection and the amount of data moved. Please, refer to the minimum CPU requirements of your target provider.

- 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 KB976932 and the KB3033929 security updates installed.

- 4 GB of physical RAM at least.
- 30 MB of available hard-disk space for installation.

Note: Tiger Bridge keeps track of the files it manages in a database, stored in the product installation folder. The size of the database grows proportionally to the number of files managed. For example, if Tiger Bridge manages 1 000 000 files, the size of the database is

approximately 100MB. Unless there's enough free space for the database, Tiger Bridge is unable to operate.

- The following TCP ports must not be blocked by the firewall on the Tiger Bridge computer or the computer managing the inbound and outbound traffic on your network:
 - (for communication with object storage target over http connection) **80** - outbound rule only
 - (for SaaS activation and/or communication with object storage target over https) **443** - outbound rule only
 - (for communication with SMB network share target) **445** - outbound rule only
 - **8536** - inbound and outbound rules
 - **8537** - inbound and outbound rules

High Availability Requirements

In order to use Tiger Bridge with high availability, your setup must meet the following requirements:

- Tiger Bridge must be installed on two server nodes, both running Tiger Store also set up for high availability (for more information, refer to the latest Tiger Store Administration Guide).
- All your source locations must be on Tiger Store-managed volumes, accessible with Read & Write permissions by both server nodes.
- Both server nodes must have identical access to all targets.
- The Tiger Bridge configuration must be identical on both server nodes.

Storage Requirements

Source Storage Requirements

Tiger Bridge supports the following sources:

- NTFS or ReFS volume, mounted on the computer running Tiger Bridge as a local volume with Read & Write permissions and on which the System account is granted Full Control.

Note: *You can use as a source the whole volume or just a folder on it. You cannot use as a source a folder whose parent folder is already paired with a target i.e. is set as a source itself.*

- SMB or NFS share accessible on the same network as the computer, running Tiger Bridge:
 - SMB share - you need to provide a dedicated account (Active Directory domain or local account on the NAS appliance), which has Full Control (on Windows) or Read & Write permissions (on Linux) over each share, which will be used as a source.

Introduction to Tiger Bridge

- NFS share - the computer running Tiger Bridge must be allowed to access the NFS share and NFS locking must be disabled on it.

Important: *When adding a network share as a source, Tiger Bridge automatically disables NFS locking on the computer and prompts you to restart the computer for the change to take effect.*

- To use network storage as a source, for each network share you must prepare a control folder located on a locally mounted volume on the Tiger Bridge computer. The control folder is used only for storing stub file copies of the actual files on the network share and facilitates retrieving of data to the network share, should you enable space reclaiming and/or data archiving. For details about configuring a NAS source, refer to “NAS Source Prerequisites and Setup” on page 36.

All sources can contain data prior to pairing them with their respective target. You cannot pair one and the same source with two or more different targets.

Target Storage Requirements

Note: *Refer to “Target Storage Prerequisites” on page 17 for specific requirements about each storage type.*

Currently, Tiger Bridge provides support for the following target types:

- Public cloud storage:
 - Amazon S3 object storage (with support for all available storage classes)
 - Microsoft Azure Blob Storage
 - Google cloud storage
 - IBM Cloud Object Storage
 - Backblaze B2 Cloud Storage
 - Google drive storage
 - LYVE Cloud
 - RSTOR Space
 - Wasabi Hot Cloud Storage
 - S3-compatible object storage (using protocol signature version 2)
 - Seagate CORTX
- On-premises storage:
 - Hitachi Content Platform (HCP)
 - IBM COS

- OpenStack Swift
- S3-compatible object storage (using protocol signature version 2)
- Seagate CORTX
- Spectra BlackPearl Deep Storage Gateway
- Coeus managed digital content library
- FujiFilm Object Archive
- another volume locally mounted NTFS volume
- SMB or NFS network share

Target Storage Prerequisites

Amazon S3 Object Storage

To use Tiger Bridge with Amazon S3 object storage, you need to:

- create a separate bucket for each source configured on the same computer
- provide IAM user credentials to be used by Tiger Bridge

Important: *Never provide your AWS account root user credentials. For best practices on securing your AWS resources, refer to the following recommendations for the AWS Identity and Access Management (IAM) service:*

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

- Tiger Bridge does not require that the IAM user has permissions to list other buckets or even to delete the bucket, which will be paired with the source. You can ensure that Tiger Bridge operates normally, if you grant the IAM user full permissions over objects in the bucket. Still, if the security policies of your organization are more restrictive, you can use the following bucket policy as a sample for granting the minimum required permissions for a bucket "bucket-name" to user "bridge_user":

```
{
  "Version": "2012-10-17",
  "Id": "S3AllActionsOnTigerBucket",
  "Statement": [
    {
      "Sid": "AllowAllActionOnS3ToTigerUsers",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::your_aws_subscription:user/bridge_user"
      },
      "Action": [
        "s3:GetAccelerateConfiguration",
```

Introduction to Tiger Bridge

```
"s3:GetBucketLocation",
"s3:GetBucketVersioning",
"s3:ListBucket",
"s3:ListBucketVersions",
"s3:ListBucketMultipartUploads",
"s3:PutLifecycleConfiguration"
],
"Resource": "arn:aws:s3:::bucket-name"
},
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::your_aws_subscription:user/bridge_user"
  },
  "Action": [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:ListMultipartUploadParts",
    "s3:PutObject",
    "s3:RestoreObject"
  ],
  "Resource": "arn:aws:s3:::bucket-name/*"
}
]
```

Tip: You can find instructions about creating buckets and managing the permissions in the *Amazon S3 Console User Guide*:

<https://docs.aws.amazon.com/AmazonS3/latest/user-guide/what-is-s3.html>

- to benefit from the versioning and undelete Tiger Bridge functionalities, you must enable versioning on the target, following these instructions:
<https://docs.aws.amazon.com/AmazonS3/latest/user-guide/enable-versioning.html>
- Amazon S3 Object Lock is supported under the following conditions:
 - versioning is enabled on each bucket with Object Lock enabled.
 - Tiger Bridge is configured to replicate files' data and metadata to different buckets, following the steps in "Replicate File's Data and Metadata to Different Containers" on page 140.
 - if you use Governance mode, the account Tiger Bridge uses for access to the bucket(s) is not an account, which has special permissions to alter the retention settings or delete the objects.

Microsoft Azure Blob Storage

To use Tiger Bridge with Microsoft Azure blob storage, you need to:

- provide account name and key for access to the Azure Blob storage
- a separate empty container for each source you intend to pair with the target, to which the account you have provided has at least write access

Google Cloud Storage

To use Tiger Bridge with Google cloud storage, you need to:

- provide the email and private JSON key of a Google Cloud service account

Note: For more information about creating and managing service account keys, refer to the Google Cloud documentation at:

<https://cloud.google.com/iam/docs/creating-managing-service-account-keys>

- for each source you want to pair with the Google Cloud storage target, create a separate empty bucket, for which the service account has IAM role with at least Storage Admin permissions

Note: For more information about creating and managing service account keys, refer to the Google Cloud documentation at:

<https://cloud.google.com/iam/docs/creating-managing-service-account-keys>

- to benefit from the Tiger Bridge versioning functionality, you must enable object versioning on the bucket(s) used as a source.

Note: You can enable object versioning using the Google Cloud SDK. For more information, see:

<https://cloud.google.com/storage/docs/using-object-versioning>

Important: Tiger Bridge replicates data directly to the storage class specified for the Google Cloud bucket - Standard, Nearline or Archive.

IBM Cloud Object Storage

To use Tiger Bridge with IBM cloud object storage, you need to:

- provide an access key ID and secret access key
- create a separate empty bucket for each source you want to pair with the target, to which the account has at least write access

IBM COS

To use Tiger Bridge with IBM COS on-premises storage, you need to:

- create a separate empty bucket for each source you want to pair with the target
- provide the access key ID and secret access key, which provide at least write access to the respective bucket

Backblaze B2 Cloud Storage

To use Tiger Bridge with Backblaze B2 cloud storage, you need to:

- provide a Backblaze application key and keyID for access to the Backblaze B2 cloud storage
- create a separate empty bucket for each source you want to pair with the target

Google Drive

To use Tiger Bridge with Google Drive storage, you need to:

- provide the credentials for access to your Google Drive account
- create a separate folder on your Google Drive for each source you pair with Google Drive
- make sure Tiger Bridge is authorized to preview, edit, create and delete files in your Google Drive

LYVE Cloud

To use Tiger Bridge with LYVE Cloud storage, you need to:

- create a separate empty bucket for each source you want to pair with the LYVE Cloud target
- provide the access key ID and secret access key, which provide at least write access to the respective bucket

RSTOR Space

To use Tiger Bridge with RSTOR Space storage, you need to:

- create a separate empty bucket for each source you want to pair with the RSTOR Space target
- provide the access key ID and secret access key, which provide at least write access to the respective bucket

S3-compatible Object Storage

To use Tiger Bridge with S3-compatible object storage, you need to:

- provide access key ID and secret access key of an S3-compatible object storage account
- create a separate empty bucket for each source you want to pair with the S3-compatible object storage target, to which the account has at least write access

Wasabi Cloud Object Storage

To use Tiger Bridge with Wasabi cloud object storage, you need to:

- provide access and secret keys of a Wasabi cloud object storage account
- create a separate empty bucket for each source you want to pair with Wasabi to which the Wasabi account has at least write access

Note: *Region specific target URL may be required.*

Hitachi Content Platform (HCP)

To use Tiger Bridge with HCP storage, you need to:

- provide access key ID and secret access key of an HCP object storage account
- create a separate empty bucket for each source you want to pair with the HCP object storage target, to which the account has at least write access

OpenStack Swift Object Storage

To use Tiger Bridge with Swift storage, you need to:

- provide access key ID and secret access key of an OpenStack Swift object storage account
- create a separate empty bucket for each source you want to pair with the Swift object storage target, to which the account has at least write access

Seagate CORTX

To use Tiger Bridge with Seagate CORTX storage, you need to:

- provide access key ID and secret access key of an CORTX object storage account
- create a separate empty bucket for each source you want to pair with the CORTX object storage target, to which the account has at least write access

BlackPearl Object Storage

To use Tiger Bridge with BlackPearl object storage, you need to:

- provide access key ID and secret access key for access to the BlackPearl object storage
- create a separate bucket for each source you want to pair with the BlackPearl object storage

Coeus Managed Digital Content Library

To use Tiger Bridge with Coeus managed digital content library, you need to:

- create a separate Coeus account for each source paired with the Coeus managed digital content library
- provide the names of the watch and archive folders associated with the Coeus account
- provide user name and password for access to the Coeus share path.
- provide the Coeus address, port through which it is accessible from the computer running Tiger Bridge and API key.

FujiFilm Object Archive

To use Tiger Bridge with FujiFilm Object Archive, you need to:

- provide access key and secret key of a FujiFilm Object Archive storage account
- create a separate empty bucket for each source you want to pair with the FujiFilm Object Archive storage target, to which the account has at least write access

Local NTFS Volume

To use Tiger Bridge with another local NTFS volume as a target, you need to:

- make sure the volume is mounted as a local volume with Read & Write permissions on the Tiger Bridge computer
- provide a unique path on the volume (the root of the volume or a subfolder) for each source you want to pair with the local volume

Important: *The root of the volume or the subfolder must not contain any other data.*

Network Share

To use Tiger Bridge with a network share as a target, you need to:

- create an empty folder on the network share for each source you want to pair with the network share
- SMB share - you need to provide a dedicated account (Active Directory domain or local account on the NAS appliance), which has Full Control (on Windows) or Read & Write permissions (on Linux) over each share, which will be used as a source.
- NFS share - the computer running Tiger Bridge must be allowed to access the NFS share and NFS locking must be disabled on it. You can find sample steps about disabling NFS locking on the Tiger Bridge server on page 137.



Tiger Bridge Installation

<i>Install Tiger Bridge</i>	<i>24</i>
<i>Uninstall Tiger Bridge</i>	<i>26</i>

Install Tiger Bridge

During Tiger Bridge installation, you can select to install the following components:

- Tiger Bridge - installs the product, the graphic and command-line interfaces for configuring the product.
- Shell Extension - provides integration with Windows Explorer, allowing you to view the status of files and folders on your source (replicated, nearline or offline), and to manually manage data through the Windows Explorer context menu.

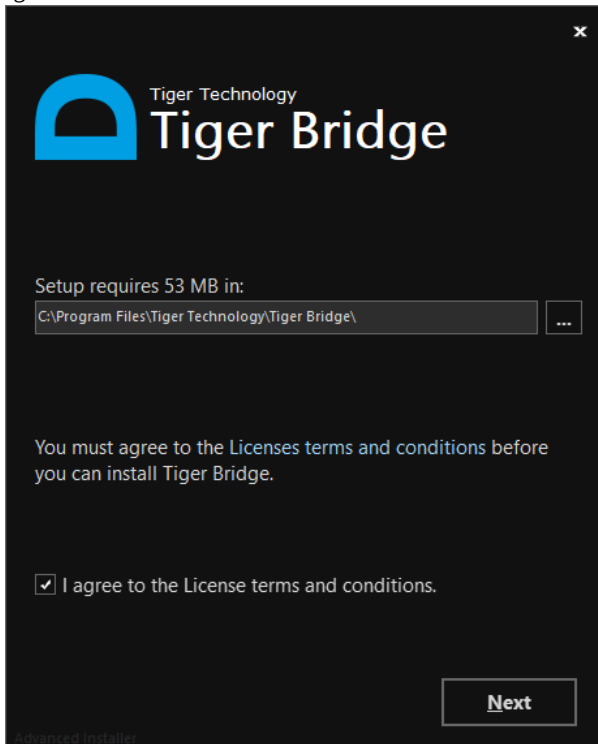
Note: To use the Tiger Bridge from a remote computer, you must install it as a standalone component, using its own installation file.

To install Tiger Bridge and additional components:

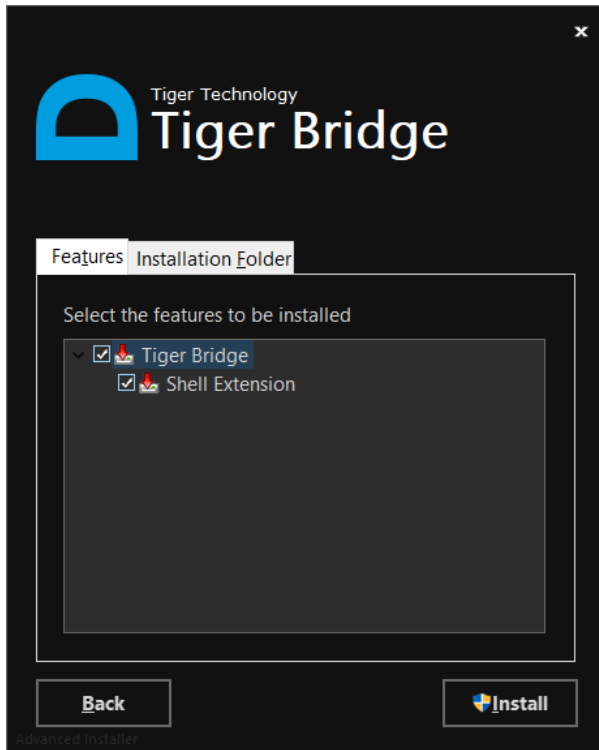
1. Double-click the Tiger Bridge installation file.

Note: If the setup wizard detects that prerequisites needed to run Tiger Bridge are not installed on the computer, click next to install them.

2. Select the folder where to install Tiger Bridge, accept the terms of the software license agreement and click Next.



3. Make sure the check boxes of the Tiger Bridge components you want to install are selected and then click Install.



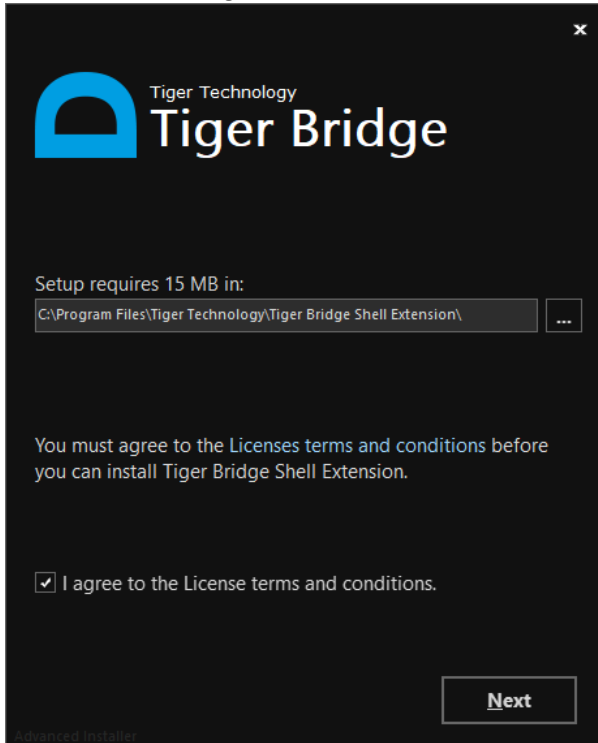
Note: If you clear the check box of a component, you can install it later, following the same installation steps.

4. When the installation is complete, click Finish.

Tiger Bridge Installation

To install the Tiger Bridge shell extension:

1. Double-click the Tiger Bridge shell extension installation file.
2. Select the folder where to install the Tiger Bridge shell extension, accept the terms of the software license agreement and click Next.



3. Make sure the check box of the Tiger Bridge shell extension is selected and click Install.
4. When the installation is complete, click Finish.

Note: For instructions how to use the shell extension from a remote computer, refer to “Tiger Bridge Shell Extension” on page 10.

Uninstall Tiger Bridge

You can uninstall Tiger Bridge and/or any of the additional components at any time. After you uninstall Tiger Bridge, you will not be able to retrieve any replicated file, which has a copy only on the target, except by manually accessing the target. Tiger Bridge preserves the link between files on the source and the target, and should you decide to install it again, you will be able to retrieve all your files from the target.

To uninstall Tiger Bridge or any of its components:

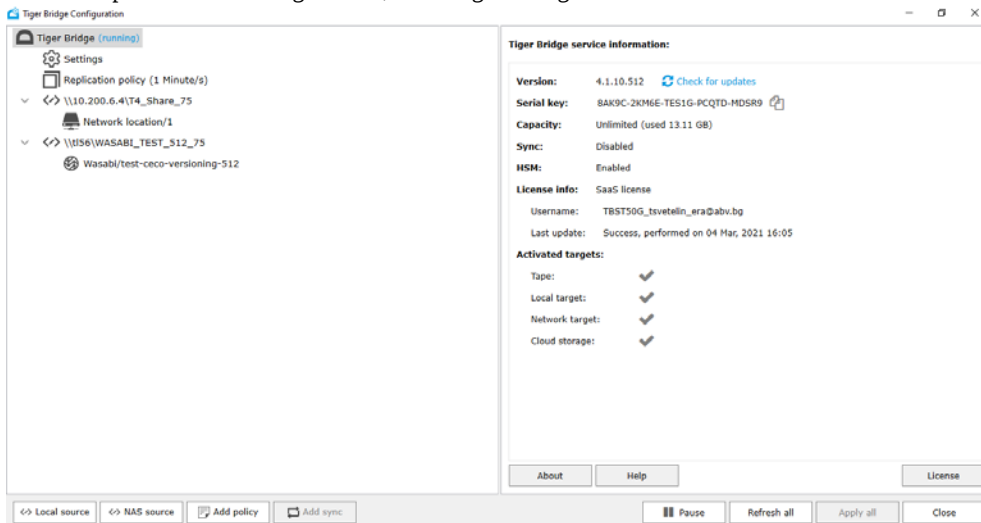
1. In Control Panel, go to Programs and Features.
2. Right-click Tiger Bridge or any of its components and select Uninstall.
3. When prompted to confirm that you want to remove Tiger Bridge or any of its components from the computer, click Yes.

Update Tiger Bridge

There is no need to uninstall Tiger Bridge, when you want to upgrade it to a newer version. Simply run the new installation file on the computer running Tiger Bridge, following the steps in “Install Tiger Bridge” on page 24. All configuration settings will be preserved after the upgrade.

You can use the Tiger Bridge Configuration to check for availability of a newer version:

1. In the left pane of the Configuration, click Tiger Bridge.



2. In the right pane, click Check for updates.

Tiger Bridge either redirects you to a web page from which to download the newer version or displays a message that no newer version is available.

Tiger Bridge Installation



Get Started with Tiger Bridge Using the Configuration

<i>Activate Tiger Bridge</i>	<i>31</i>
<i>Add a Source</i>	<i>36</i>
<i>Pair Source with a Target</i>	<i>38</i>
<i>Configure Automatic Data Replication</i>	<i>83</i>
<i>Configure Space Reclaiming</i>	<i>86</i>
<i>Configure Data Archiving</i>	<i>91</i>
<i>Configure Active Sync</i>	<i>95</i>
<i>Configure Versioning</i>	<i>99</i>
<i>Configure Operation Mode</i>	<i>100</i>
<i>Pause/Resume Automatic Tiger Bridge Operations</i>	<i>102</i>
<i>Monitor Data Management Statistics</i>	<i>103</i>

Get Started with Tiger Bridge Using the Configuration

To get started with Tiger Bridge using the Configuration, you need to:

- Activate Tiger Bridge. For more details, refer to “Activate Tiger Bridge” on page 31.
- Pair a source with a target. For more details, refer to “Add a Source” on page 36.
- Configure automatic data replication - specify what files are automatically replicated to the target. As data replication is indispensable for any Tiger Bridge workflow, a global replication policy governing all pairs of source and target is configured by default. The global replication cannot be deleted and you can only change its settings. You can overwrite the global replication policy for any pair of source and target. For more details about managing replication policies, refer to “Configure Automatic Data Replication” on page 83.
- Configure space reclaiming - specify which replicated files to be replaced with nearline files on the source. You can configure global space reclaiming policy, valid for all pairs of sources and targets. You can also overwrite the global space reclaiming policy for any pair of source and target. For more details about managing space reclaiming policies, refer to “Configure Space Reclaiming” on page 86.
- Configure automatic data archiving - on targets like Microsoft Azure and Amazon S3 Glacier, the policy defines which files on the source should be moved to the archival tier on the target and replaced by an offline file on your local storage. On targets like IBM Cloud Object Storage Archive and some S3-compatible object storage providers, which have their own policy for moving files from the hot or cool tier to the archival tier, you can specify at what interval Tiger Bridge should check for file moved to the archival tier and change their status on the source accordingly. As the data archiving policies differ from target to target, you cannot configure a global archiving policy, valid for all pairs of source and target. You can only specify archiving policy for a specific pair of source and target. For more details about managing archiving policies, refer to “Configure Data Archiving” on page 91.
- Configure active sync (geo replication) - specify when a source on one computer sends a notification to sources on other computers that new data is replicated on the same target and also when a source updates its contents with files replicated on the same target from other sources. You can configure global active sync policy, valid for all sources. You can also overwrite the global active sync policy for any source. For more details about configuring active sync policies, refer to “Configure Active Sync” on page 95.
- Configure versioning - specify whether modifications of the file on the source should be kept each as a separate version on the target or the latest modifications should overwrite the previous one. For more information, refer to “Configure Versioning” on page 99.
- Configure operation mode - whether Tiger Bridge should keep the copy on the target, when a nearline file is retrieved back on the source and also whether to keep the replicated file on the target, when its counterpart on the source is deleted. For more details, see “Configure Operation Mode” on page 100.

- Pause/resume all automatic Tiger Bridge operations. For more details, see “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Activate Tiger Bridge

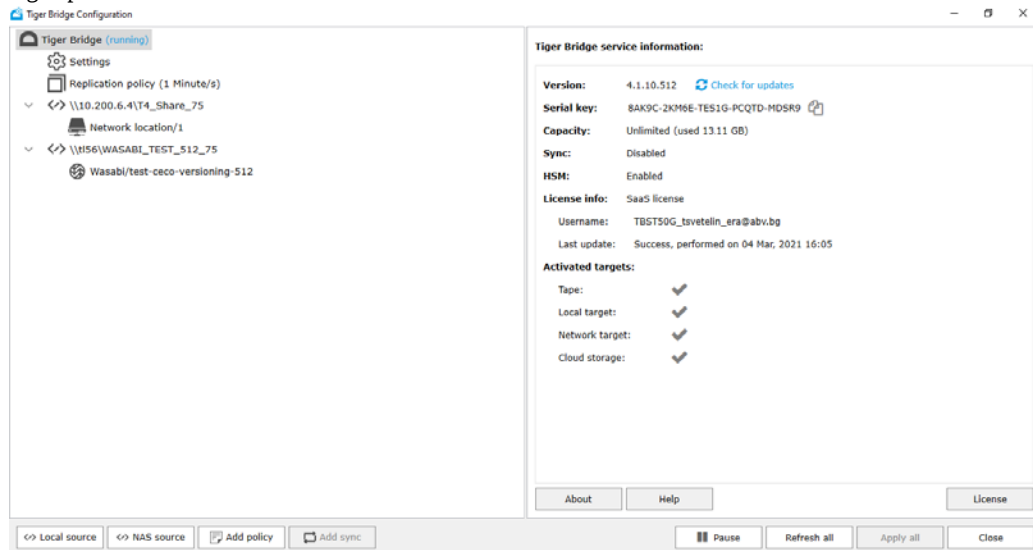
You can activate Tiger Bridge using one of the following:

- software activation key;
- software protection dongle, if such is detected;
- Software as a service (SaaS) license;

Note: To see how to activate Tiger Bridge using the command-line interface, refer to “Activate Tiger Bridge” on page 108.

To view the activation status of Tiger Bridge on your computer:

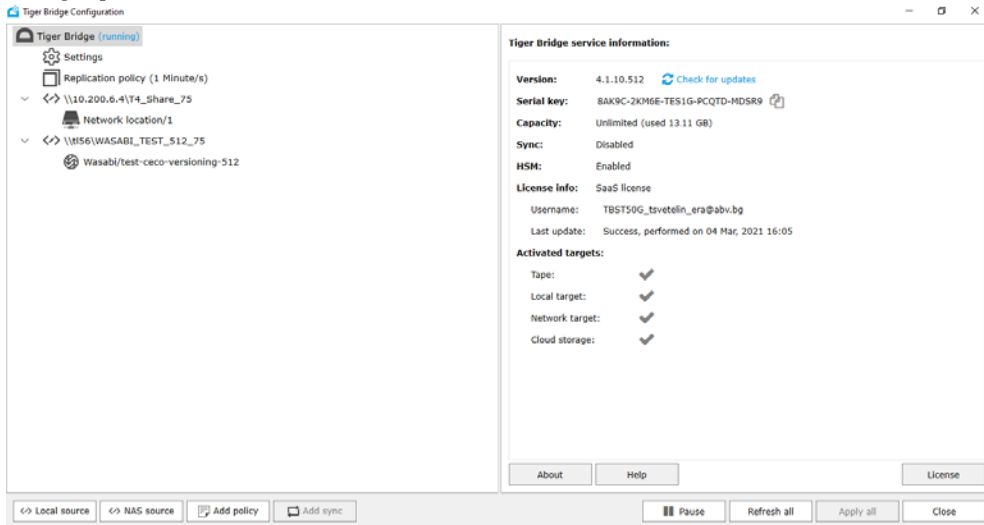
Click Tiger Bridge in the left pane and check the Tiger Bridge service information displayed in the right pane.



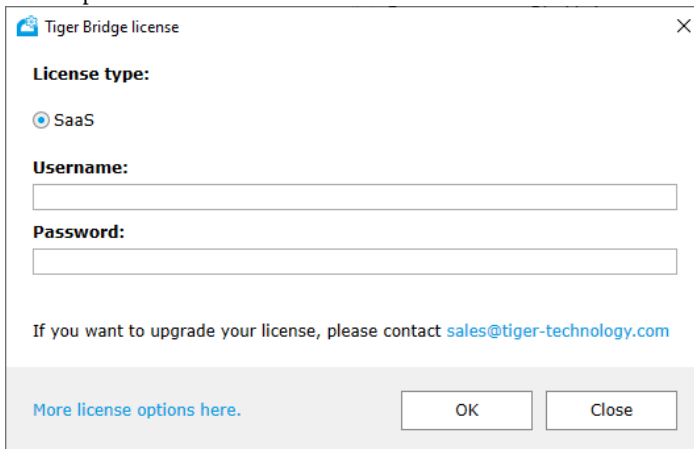
Get Started with Tiger Bridge Using the Configuration

To activate a Tiger Bridge SaaS license:

1. In the Tiger Bridge Configuration, click Tiger Bridge in the left pane and then click License in the right pane.

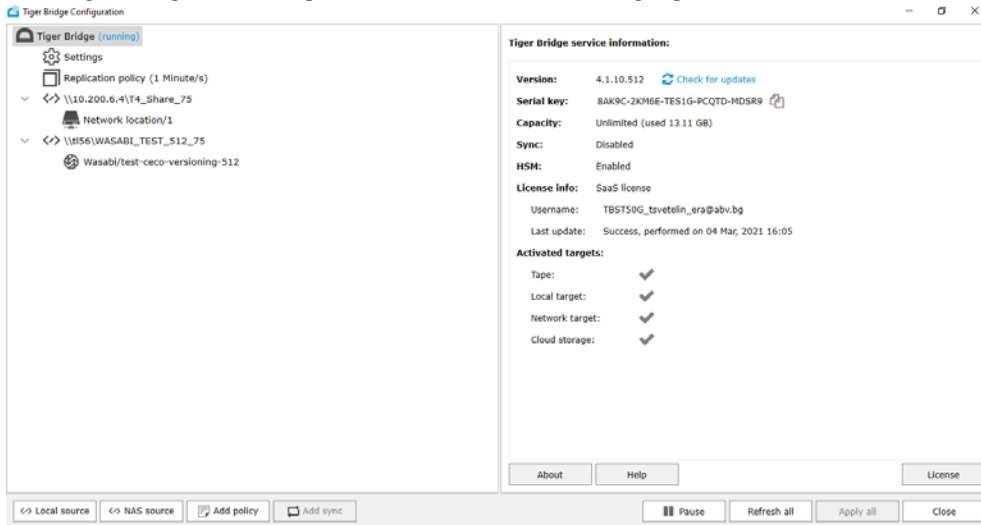


2. In the Tiger Bridge License dialog, enter the username and password for your software subscription and then click OK.

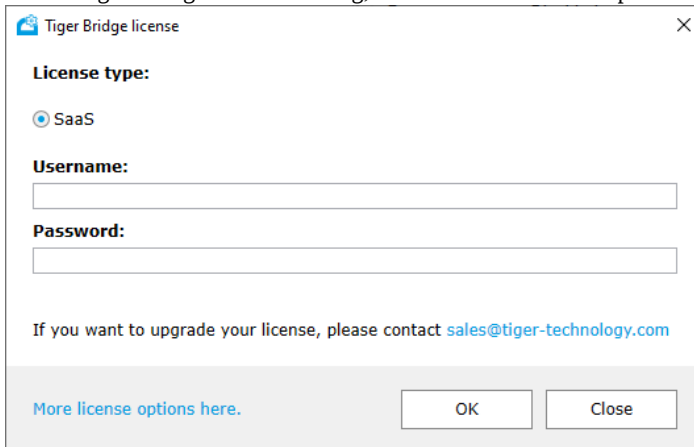


To activate Tiger Bridge with a software activation key:

1. Click Tiger Bridge in the left pane and click License in the right pane.

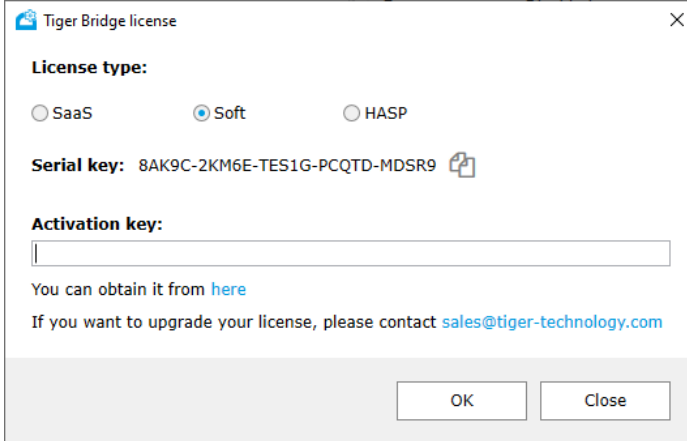


2. In the Tiger Bridge License dialog, click on More license options here.



Get Started with Tiger Bridge Using the Configuration

3. Select Soft and then copy the product serial key, by clicking the Copy button .

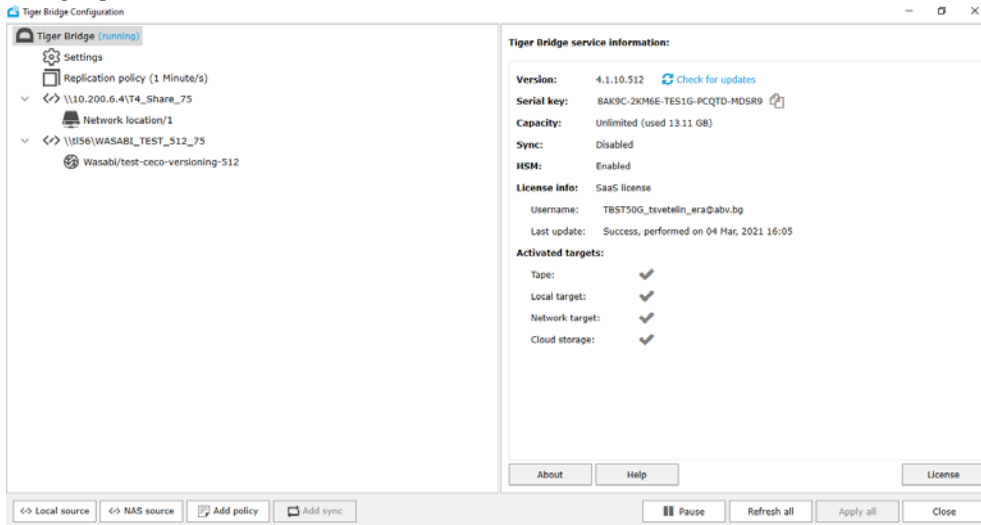


4. In a web browser go to <https://license.tiger-technology.com>
Tip: Click the link below the Activation key field, to automatically load the URL in your default web browser.
5. In the home page of the licensing server, enter your order name and password in the corresponding fields, and click Log in.
Important: The order name and the password are case sensitive.
6. In the Licensing Server menu, click Activate License.
7. Paste the serial number and click Generate Activation Key.
8. Copy the activation key generated for your license.
9. In the Tiger Bridge License dialog, paste the activation key and click OK.

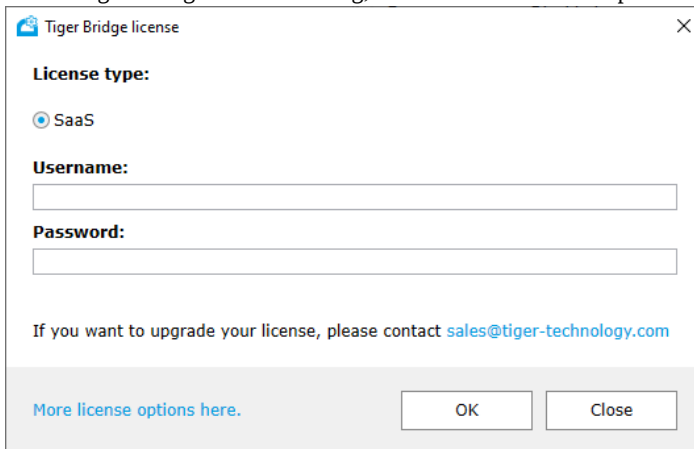
To activate Tiger Bridge using a software protection dongle:

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.
Important: The order name and the password are case sensitive.
3. Next to the dongle name in the list, click “Download lic file”.
Note: The dongle name is its number, printed on the dongle itself.

4. In the Tiger Bridge Configuration, click Tiger Bridge in the left pane and then click License in the right pane.

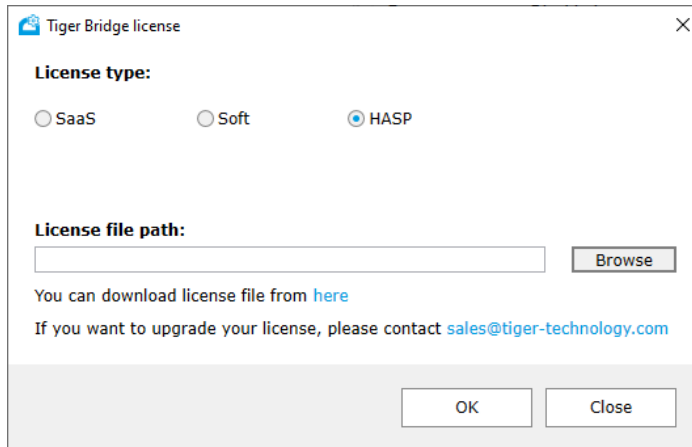


5. In the Tiger Bridge License dialog, click on More license options here.



Get Started with Tiger Bridge Using the Configuration

6. Select HASP and then click Browse.



7. Browse to and double-click the downloaded license file, and then click OK.

Add a Source

You can use as a source a locally mounted NTFS/ReFS volume, an SMB/NFS network share or just a folder on the volume/share. Specifying a folder as source allows you to pair folders on one and the same volume/share with different targets, and thus define different criteria for data replication, space reclaiming, data archiving, etc. You cannot use as a source a folder whose parent folder is already paired with a target i.e. is set as a source itself.

You can add as many sources as you wish.

NAS Source Prerequisites and Setup

For each network share you want to use as a source, you must assign an empty folder on a locally mounted volume on the Tiger Bridge computer. This folder is used as a control location and contains a copy of each file on the NAS source in the form of a stub file. The control folder acts as a gateway between the NAS source and the target.

While with data replication there is no difference from local volume source, when the Tiger Bridge space reclaiming or data archiving mechanism needs to replace the actual file on the NAS source with a stub file, it actually creates the stub file only in the control folder, but creates a placeholder file with .reclaimed extension on the NAS source, to let you identify that the stub counterpart is in the control folder. If you want to retrieve a nearline file or rehydrate an offline file manually, you need to perform the operation on the stub file located in the control folder. The same goes for the active sync mechanism, unless you have configured the mechanism to automatically retrieve on the source synchronized data from other sources. When you need to synchronize the contents of source

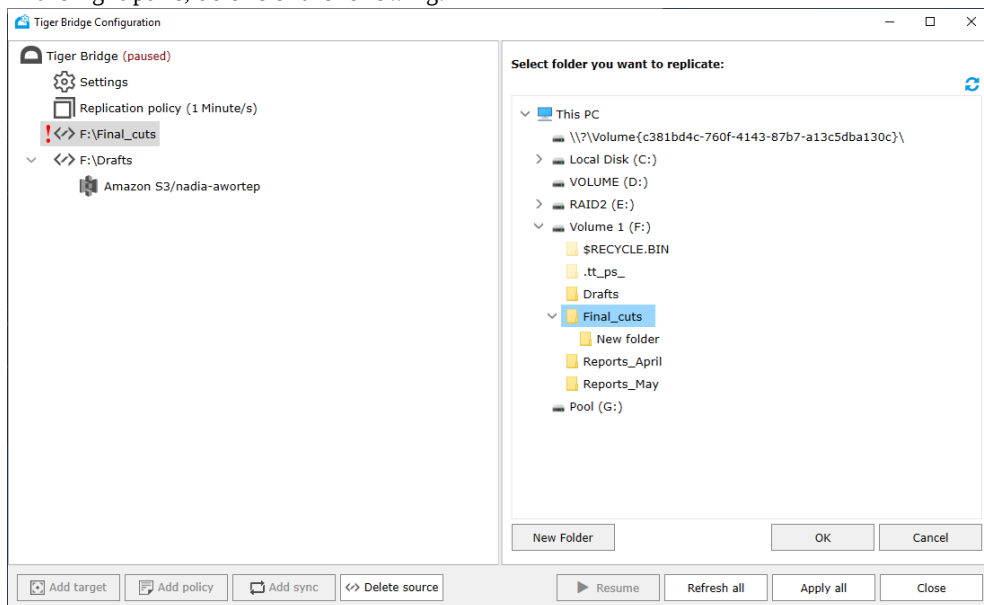
and target, you need to perform the operation on the control folder and all restored data will appear there in the form of stub files in the control folder and placeholder files on the NAS source itself. You can then manually retrieve the stub files on the NAS source.

As stub files are actually located only in the control folder, to allow retrieving them on demand, you must export the control folder as a SMB/NFS share on your network. When a user or an application attempts to open a nearline file on the exported control folder, Tiger Bridge will automatically retrieve it directly on the NAS source.

As a general rule the capacity of the control folder must be at least 15% of the capacity of the NAS source itself.

To add a local volume source:

1. In the Tiger Bridge Configuration, click Tiger Bridge in the left pane and then click Local Source.
2. In the right pane, do one of the following:

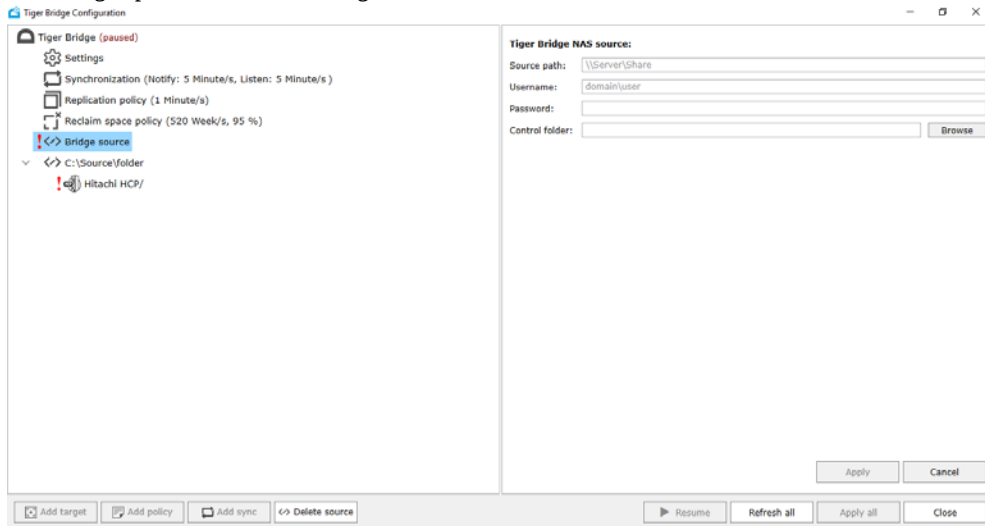


- To add a whole volume as a source, select the root of the volume and click OK.
- To add an existing folder as a source, browse to and select the folder and click OK.
- To create a new folder as a source, browse to the location where you want to create it, click New Folder, enter a name of the new folder and then click OK.

Get Started with Tiger Bridge Using the Configuration

To add a NAS source:

1. In the Tiger Bridge Configuration, click Tiger Bridge in the left pane and then click NAS Source.
2. In the right pane, do the following:



- In Share path, enter the full path to the network share you want to use as a source.
- (SMB shares only) Enter username and password of a user with Full Control over the network share in the respective fields.

Important: You must enter the username in the following format [NAS server domain name or IP address]\[username]. For example, if the IP address of your NAS server is 10.200.0.65 and the name of the user, whose credentials you are providing is “test”, enter the following in the Username field:

10.200.0.65\test

- In Control folder, browse to and select a folder on a locally mounted volume, which to use as a control folder.
- Click Apply.

Pair Source with a Target

Once you add a source, you can pair it with one of the supported targets. For prerequisites about each target, refer to “Target Storage Prerequisites” on page 17.

Important: You cannot pair one and the same source with two or more different targets.

When pairing the source with an object storage target, Tiger Bridge allows you to select what to do with already existing data in the container/bucket. You can choose between the following options:

No action — no data will be imported on your source. You can import it later on, following the steps in “Synchronize Data on the Source and the Target” on page 159.

Import on demand — Tiger Bridge creates a stub file (nearline or offline file, depending on your target) for each file from the target, only when you browse the containing folder on your source. For example, if on the target there are two files (“one.xml” and “two.xml”) and a folder “Target folder” containing a file “three.xml”, should you choose to import them on demand, once you browse the root of your source, Tiger Bridge will create stub files “one.xml” and “two.xml” and “Target folder”. “Target folder” will remain empty until you open it on your source and Tiger Bridge will then create a stub file “three.xml”.

Import all metadata — your source will be populated with all folders and files from the target, but the files will be represented by stub files (nearline or offline files, depending on your target), which you can retrieve either on demand (by attempting to open them) or manually, through Tiger Bridge.

Restore all data — Tiger Bridge retrieves on your source all files and folders from the target, keeping their hierarchical structure. All retrieved files will be with replicated status.

Important: *The operation may take time and the free space on your source must be enough to accommodate all data found only on the target.*

Link existing data — all files with matching metadata (name and size) found both on your source and the target are linked and represented as replicated. Any file for which no match is found on your source is imported as a stub file (a nearline or offline file depending on your target).

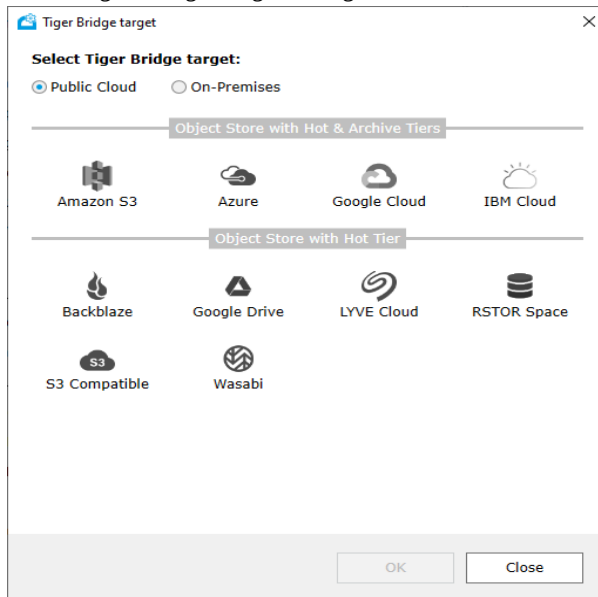
Pair a Source with Microsoft Azure Blob Storage Target

Note: *To see how to pair a source with Microsoft Azure using the command-line interface of Tiger Bridge, refer to “Pair a Source with Microsoft Azure Blob Storage Target” on page 109.*

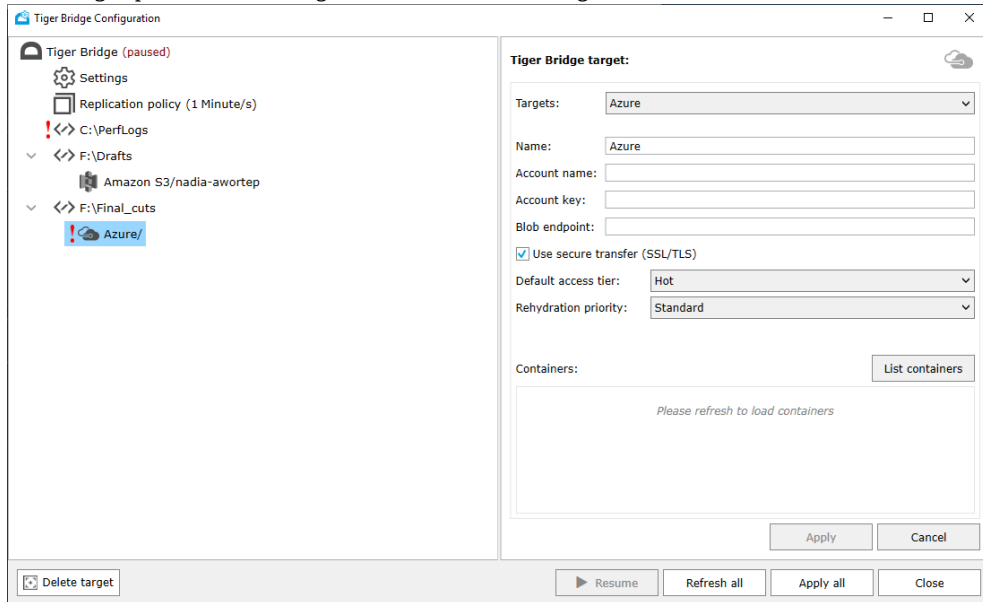
Get Started with Tiger Bridge Using the Configuration

To pair a source with Microsoft Azure target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select Public Cloud, then select Azure and click OK.



3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

- Enter the account name and key, and the Blob endpoint in the respective fields.
- Choose whether to access the target using secure transfer (SSL/TLS) by selecting or clearing the check box.
- In Default access tier, select whether to use the Hot, Cool or Archive tier of Azure as default tier for Tiger Bridge replication.
- In Rehydration priority, select whether offline files should be rehydrated using the Standard or the High option.
- Click List containers to display the list of containers available for the account you have specified and then select the container on the target, which to be paired with the selected source.

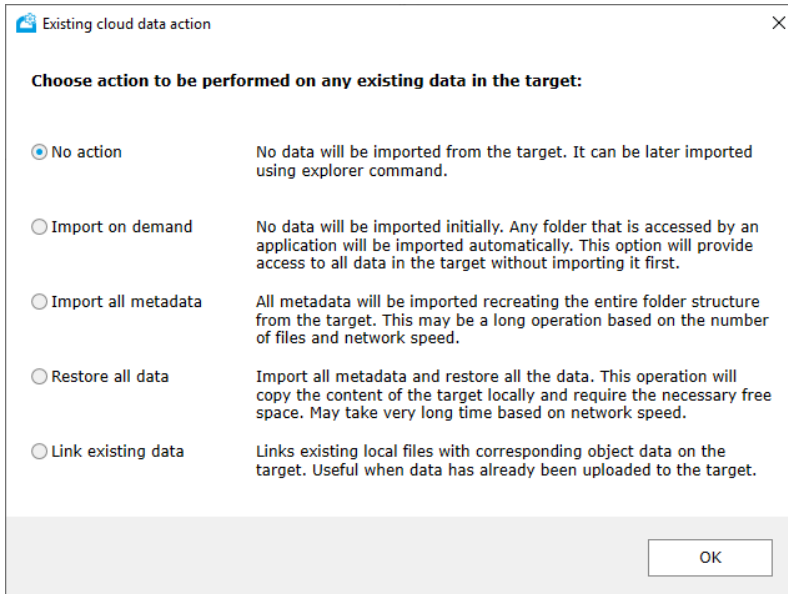
Note: If the user whose credentials you have provided, does not have sufficient permissions to list all containers, Tiger Bridge displays a text box for you to manually enter the name of the container, which will be paired with the source.

Important: Do not use the same container for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active

Get Started with Tiger Bridge Using the Configuration

Sync” on page 95). Do not change the name of the container as this may prevent Tiger Bridge replication from operating.

4. In the Existing cloud data action dialog, select what to do with data already existing in the container and then click OK.



5. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

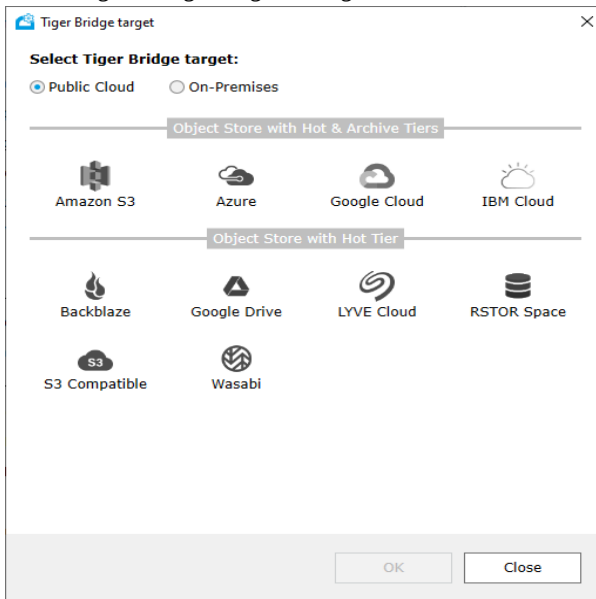
Pair a Source with Amazon S3 Target

Note: To see how to pair a source with Amazon S3 target using the command-line interface of Tiger Bridge, refer to “Pair a Source with Amazon S3 Target” on page 110.

When you pair a source with an S3 target, you can also select the Amazon storage class, to which Tiger Bridge to replicate data directly, omitting any intermediate tiers, in case you do not want to use the default storage class (S3 Standard-IA). You can also specify Amazon archive retrieval option, in case you do not want to use the default archive retrieval option (Standard). For more information about Amazon storage classes and archive retrieval options, refer to the Amazon S3 documentation.

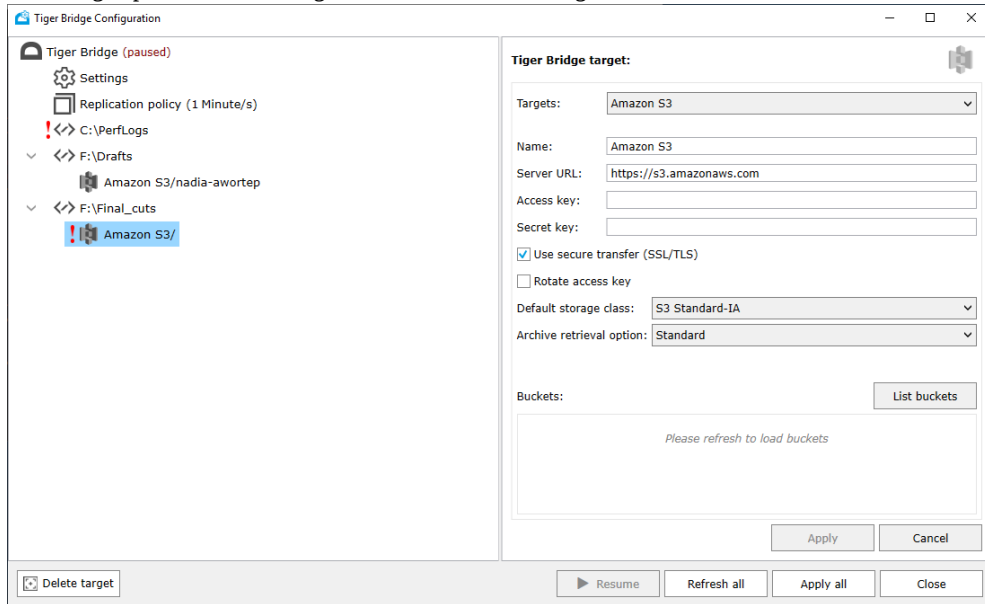
To pair a source with Amazon S3 object storage target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select Public Cloud, then select Amazon S3 and click OK.



Get Started with Tiger Bridge Using the Configuration

3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

- Enter the server URL, access and secret keys of the S3 target.

Important: To use Tiger Bridge with an acceleration-enabled buckets, include “accelerate” in the server URL as described in the Amazon documentation.

- Choose whether to access the target using secure transfer (SSL/TLS) by selecting or clearing the check box.

- To benefit from Amazon’s access key rotation, select the “Rotate access key” check box to let Tiger Bridge update the access key of the IAM user once a week.

Note: Before enabling access key rotation in Tiger Bridge, make sure you have created an Amazon S3 policy that allows IAM users to rotate their own access keys, signing certificates, service specific credentials, and passwords.

Important: If you deploy Tiger Bridge for geo replication, to allow successful access key rotation on each computer running Tiger Bridge you must specify a different IAM account for access to the same bucket(s).

- In Default storage class, select the storage class to which Tiger Bridge to replicate data directly, omitting any intermediate tiers.

Note: If you do not select a specific storage class, Tiger Bridge uses S3 Standard-IA.

- In Archive retrieval option, select the method for retrieving data from the archival tier of your S3 object storage.

Note: If you do not select a specific archive retrieval option, Tiger Bridge uses Standard as default.

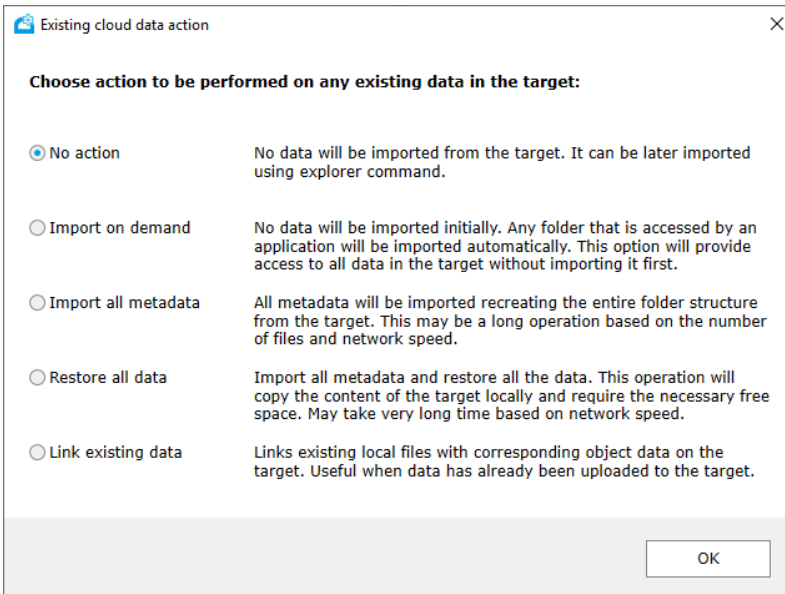
Important: If at the time of data retrieval there is insufficient capacity to process an Expedited request, Tiger Bridge automatically switches to Standard. Expedited retrieval option is not available for S3 Glacier Deep Archive storage class. Make sure you are acquainted with the Amazon pricing model, before changing your archive retrieval option, in order to avoid incurred costs.

- Click List buckets, to display the list of buckets available for the account you have specified and select the bucket on the target, which to be paired with the selected source.

Note: If the user whose credentials you have provided, does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not use the same bucket for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active Sync” on page 95). Do not change the name of the bucket on the S3 object storage as this may prevent Tiger Bridge replication from operating.

4. In the Existing cloud data action dialog, select what to do with data already existing in the bucket and then click OK.



The dialog box is titled "Existing cloud data action" and contains a close button (X) in the top right corner. Below the title bar, the text "Choose action to be performed on any existing data in the target:" is displayed. There are five radio button options, each with a corresponding description:

- ☒ **No action**: No data will be imported from the target. It can be later imported using explorer command.
- ☐ **Import on demand**: No data will be imported initially. Any folder that is accessed by an application will be imported automatically. This option will provide access to all data in the target without importing it first.
- ☐ **Import all metadata**: All metadata will be imported recreating the entire folder structure from the target. This may be a long operation based on the number of files and network speed.
- ☐ **Restore all data**: Import all metadata and restore all the data. This operation will copy the content of the target locally and require the necessary free space. May take very long time based on network speed.
- ☐ **Link existing data**: Links existing local files with corresponding object data on the target. Useful when data has already been uploaded to the target.

An "OK" button is located at the bottom right of the dialog box.

5. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

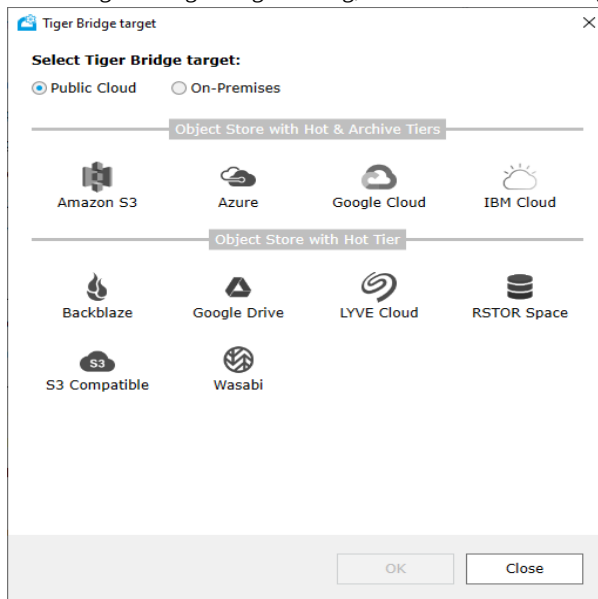
Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Pair a Source with IBM Cloud Object Storage Target

Note: To see how to pair a source with IBM cloud object storage target using the command-line interface of Tiger Bridge, refer to “Pair a Source with IBM Cloud Object Storage Target” on page 111.

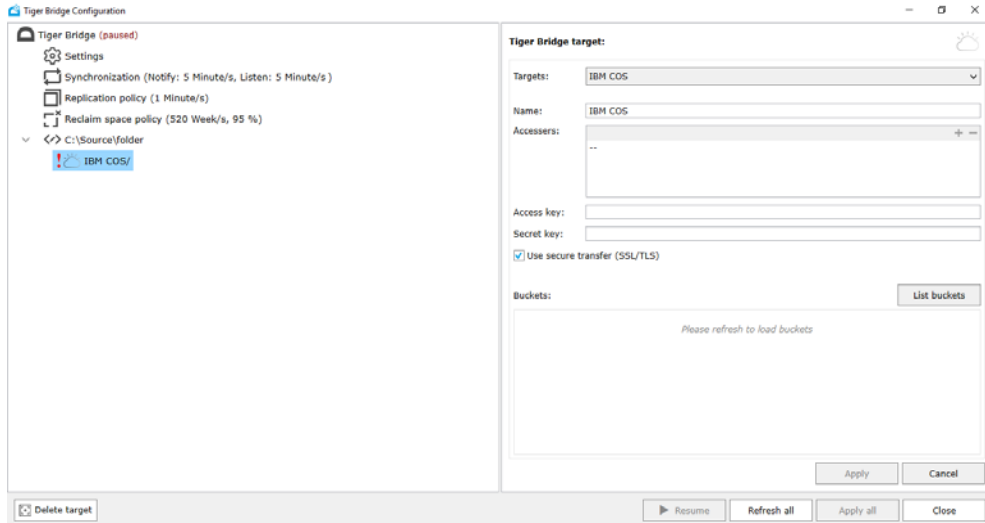
To pair a source with IBM cloud object storage target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, do one of the following:



- if you are configuring the public IBM cloud object storage as a target, select “Public Cloud” and then select IBM Cloud and click OK.
- if you are configuring an on-premises IBM cloud object storage target, select “On-premises” and then select IBM COS and click OK.

3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

- (public IBM Cloud) In Server URL, enter the URL for access to the public IBM cloud.
- (on-premises IBM cloud object storage) Under Accessers, enter IP address of the IBM cloud object storage server and click the “+” button to save it.

Tip: You can specify alternative IP address through which you can access the server providing access to your account for the IBM cloud object storage. For the purpose in the Accessers field click the “+” button, keeping in mind that the main IP address for access to it must be specified first.

- Enter the access ID and secret access keys in the respective fields.
- Choose whether to access the target using secure transfer (SSL/TLS) by selecting or clearing the check box.
- Click List buckets, to display the list of buckets available for the account you have specified and select the bucket, which to pair with the source.

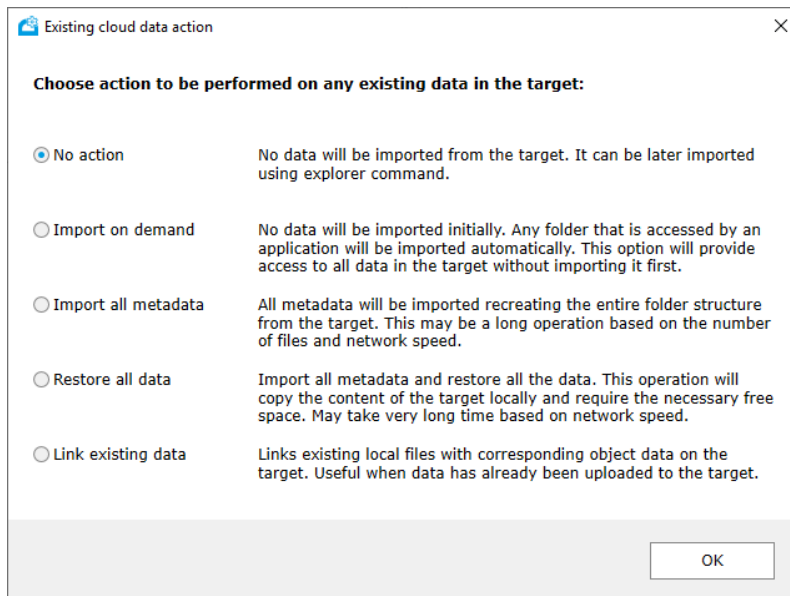
Note: If the user whose credentials you have provided, does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not use the same bucket for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active

Get Started with Tiger Bridge Using the Configuration

Sync” on page 95). Do not change the name of the bucket on the IBM cloud object storage as this may prevent Tiger Bridge replication from operating.

4. In the Existing cloud data action dialog, select what to do with data already existing in the bucket and then click OK.



5. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

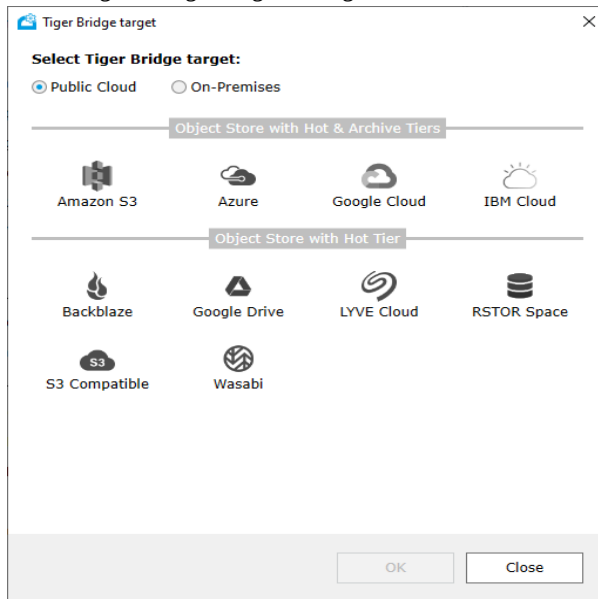
Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Pair a Source with Backblaze Target

Note: To see how to pair a source with Backblaze target using the command-line interface of Tiger Bridge, refer to “Pair a Source with Backblaze Target” on page 113.

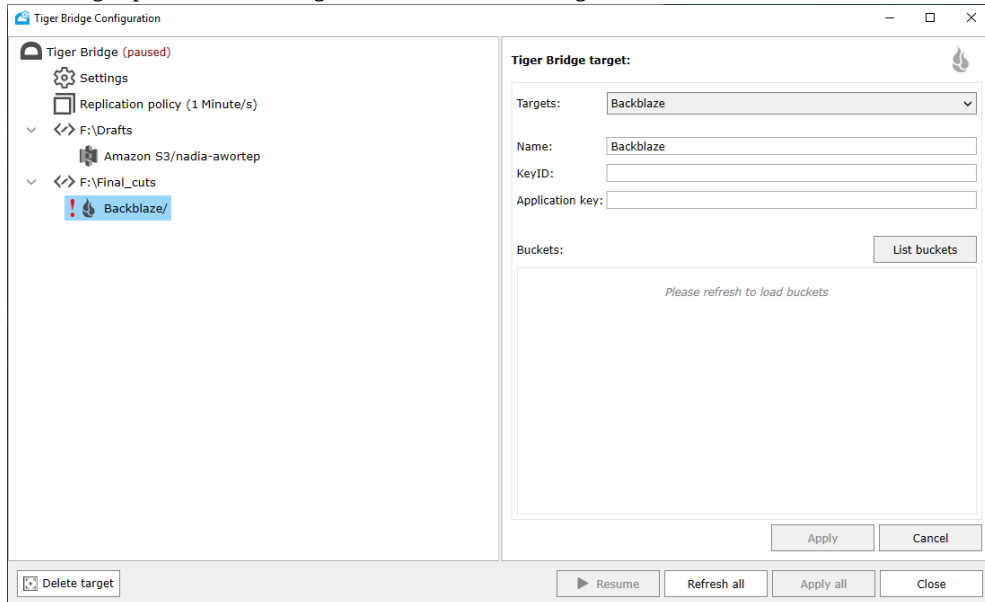
To pair a source with Backblaze B2 cloud storage target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select Public Cloud, then select Backblaze and click OK.



Get Started with Tiger Bridge Using the Configuration

3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

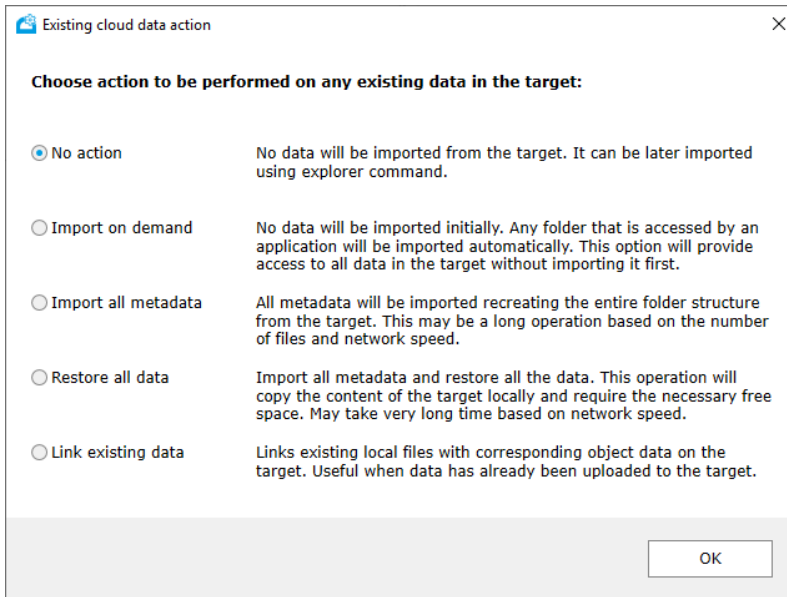
Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

- Enter the keyID and the application key for access to the Backblaze B2 cloud.
- Click List buckets, to display the list of buckets available for the account you have specified and then select the bucket, which to pair with the source.

Note: If the user whose credentials you have provided, does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not use the same bucket for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active Sync” on page 95). Do not change the name of the bucket on the Backblaze cloud storage as this may prevent Tiger Bridge replication from operating.

4. In the Existing cloud data action dialog, select what to do with data already existing in the bucket and then click OK.



5. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

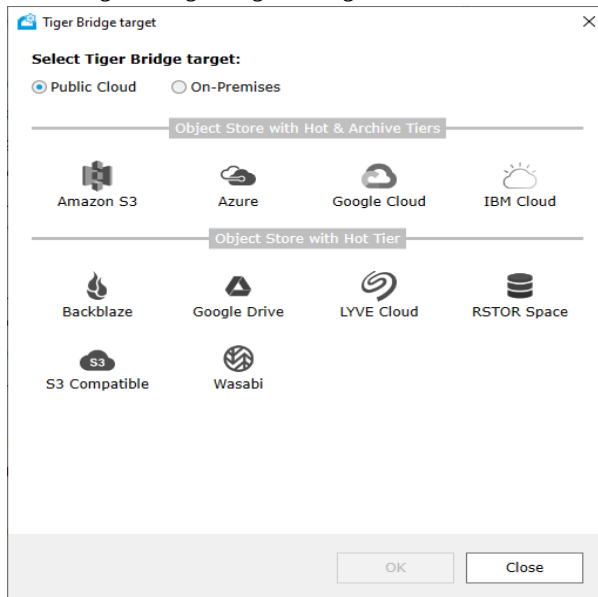
Pair a Source with Wasabi Target

Note: To see how to pair a source with Wasabi target using the command-line interface of Tiger Bridge, refer to “Pair a Source with S3-compatible Object Storage Target” on page 114.

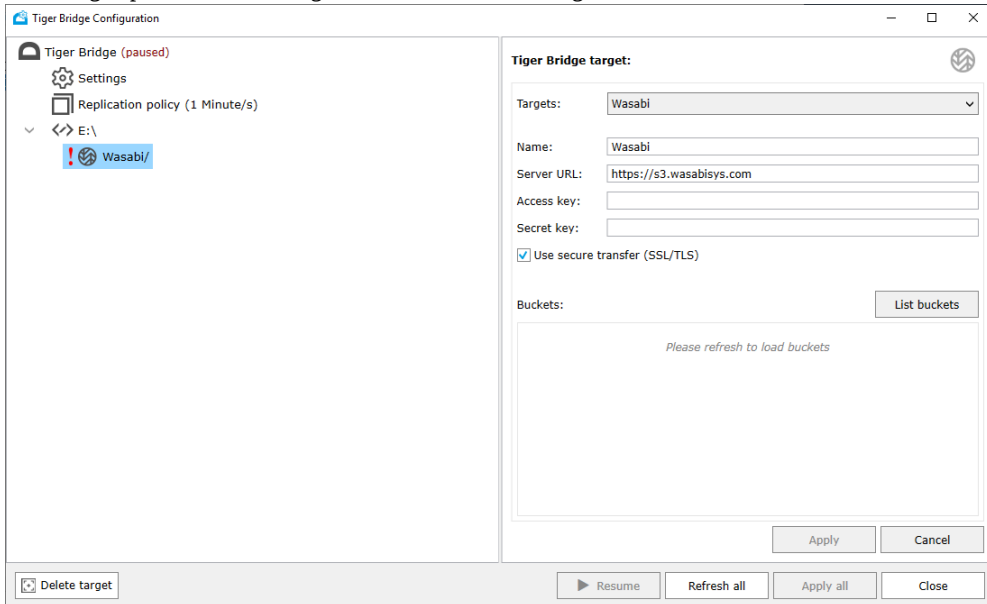
Get Started with Tiger Bridge Using the Configuration

To pair a source with Wasabi cloud storage target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select Public Cloud, then select Wasabi and click OK.



3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

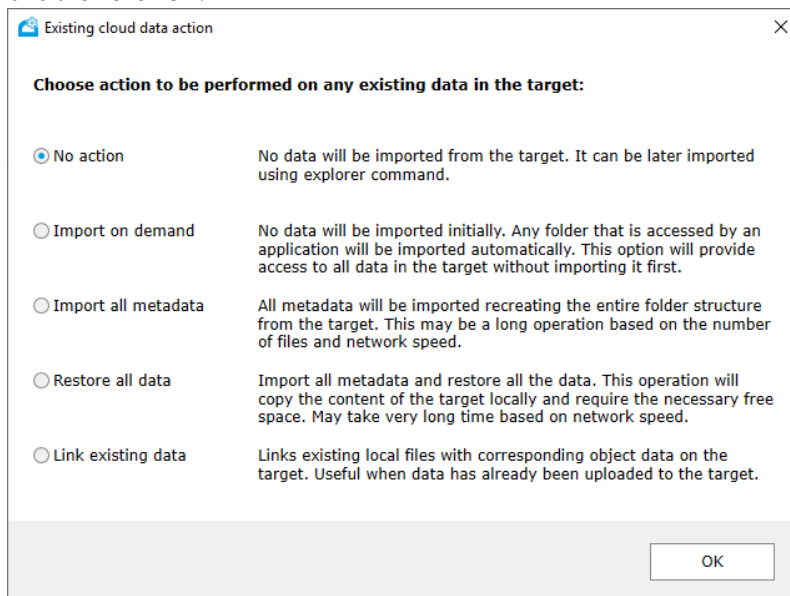
- Enter the server URL, access and secret keys of the Wasabi target.
- Choose whether to access the target using secure transfer (SSL/TLS) by selecting or clearing the check box.
- Click List buckets, to display the list of buckets available for the account you have specified and then select the bucket, which to pair with the source.

Note: If the user whose credentials you have provided, does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not use the same bucket for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, only when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active Sync” on page 95). Do not change the name of the bucket on the Wasabi cloud storage as this may prevent Tiger Bridge replication from operating.

Get Started with Tiger Bridge Using the Configuration

4. In the Existing cloud data action dialog, select what to do with data already existing in the bucket and then click OK.



5. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

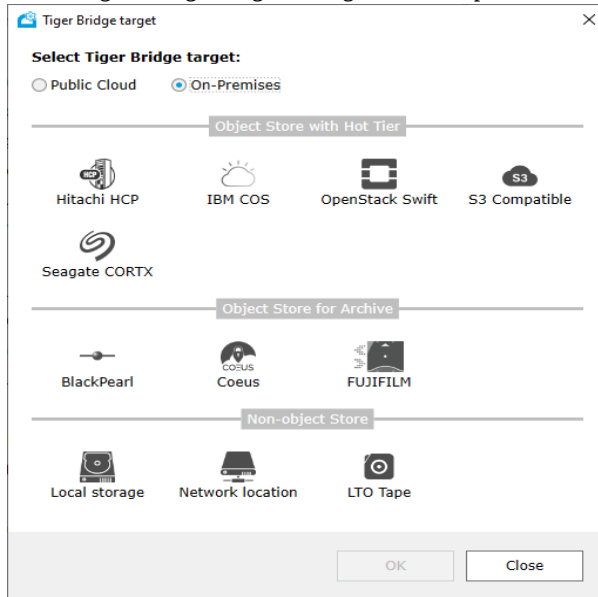
Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Pair a Source with Hitachi Content Platform Target

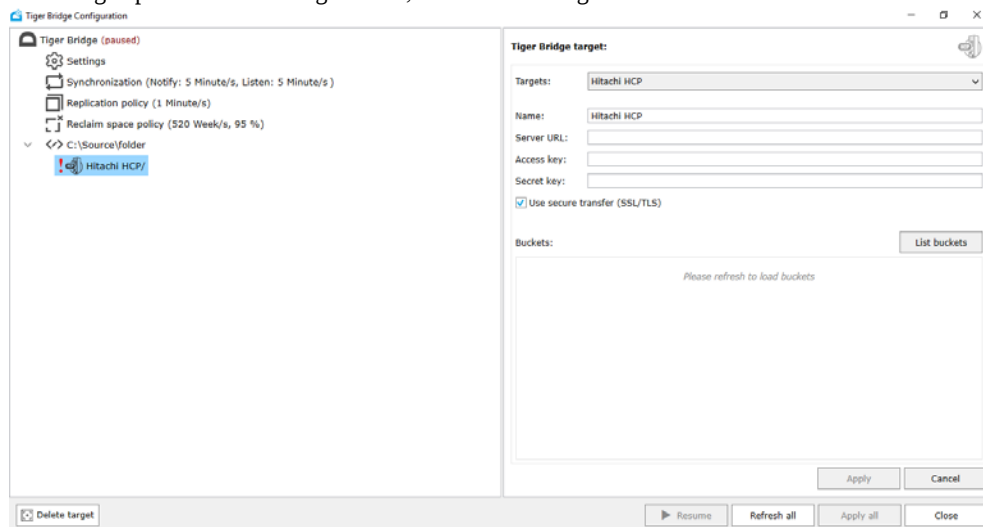
Note: Currently, you can pair a source with an HCP target only in the Tiger Bridge Configuration.

To pair a source volume with Hitachi HCP target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select On-premises, then select Hitachi HCP and click OK.



3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

Get Started with Tiger Bridge Using the Configuration

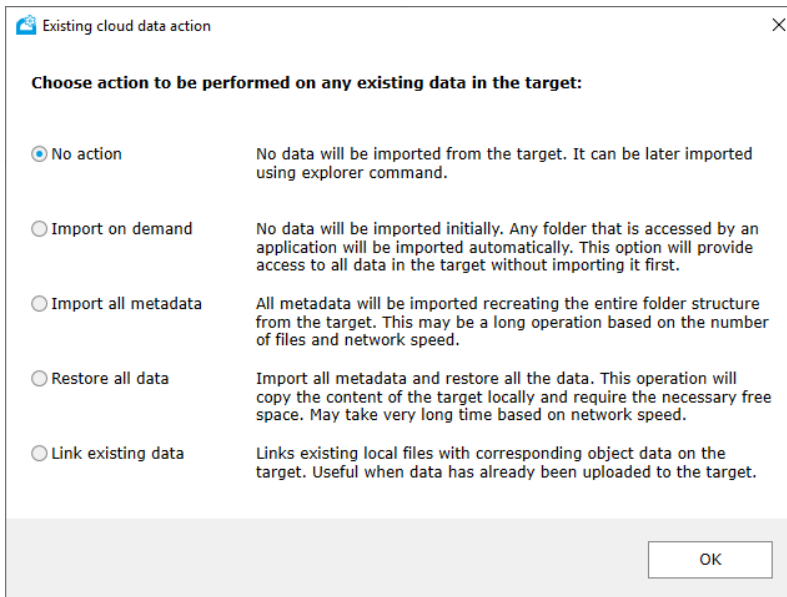
Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

- Enter the server URL, access and secret keys of the Hitachi HCP target.
- Choose whether to access the target using secure transfer (SSL/TLS) by selecting or clearing the check box.
- Click List buckets, to display the list of buckets available for the account you have specified and then select the bucket, which to pair with the source.

Note: If the user whose credentials you have provided, does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not use the same bucket for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, only when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active Sync” on page 95). Do not change the name of the bucket on the Hitachi HCP target as this may prevent Tiger Bridge replication from operating.

4. In the Existing cloud data action dialog, select what to do with data already existing in the bucket and then click OK.



The dialog box is titled "Existing cloud data action" and contains a close button (X) in the top right corner. Below the title bar, the text "Choose action to be performed on any existing data in the target:" is displayed. There are five radio button options, each with a description:

Option	Description
☒ No action	No data will be imported from the target. It can be later imported using explorer command.
☐ Import on demand	No data will be imported initially. Any folder that is accessed by an application will be imported automatically. This option will provide access to all data in the target without importing it first.
☐ Import all metadata	All metadata will be imported recreating the entire folder structure from the target. This may be a long operation based on the number of files and network speed.
☐ Restore all data	Import all metadata and restore all the data. This operation will copy the content of the target locally and require the necessary free space. May take very long time based on network speed.
☐ Link existing data	Links existing local files with corresponding object data on the target. Useful when data has already been uploaded to the target.

An "OK" button is located at the bottom right of the dialog box.

5. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global

data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

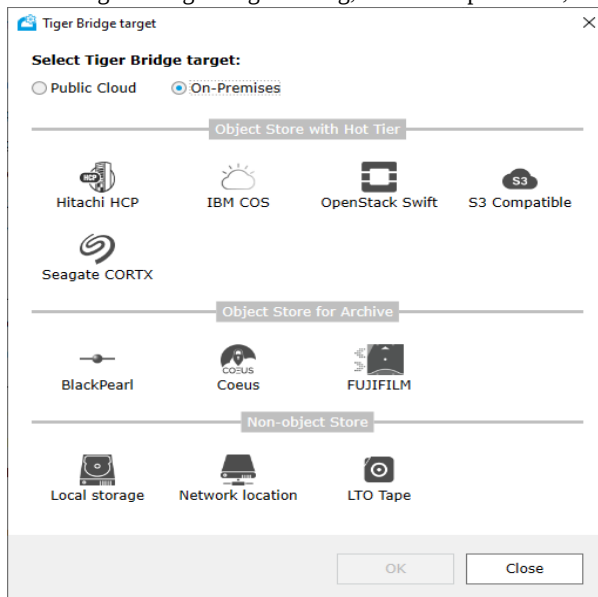
Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Pair a Source with OpenStack Swift Target

Note: Currently, you can pair a source with an OpenStack Swift target only in the Tiger Bridge Configuration.

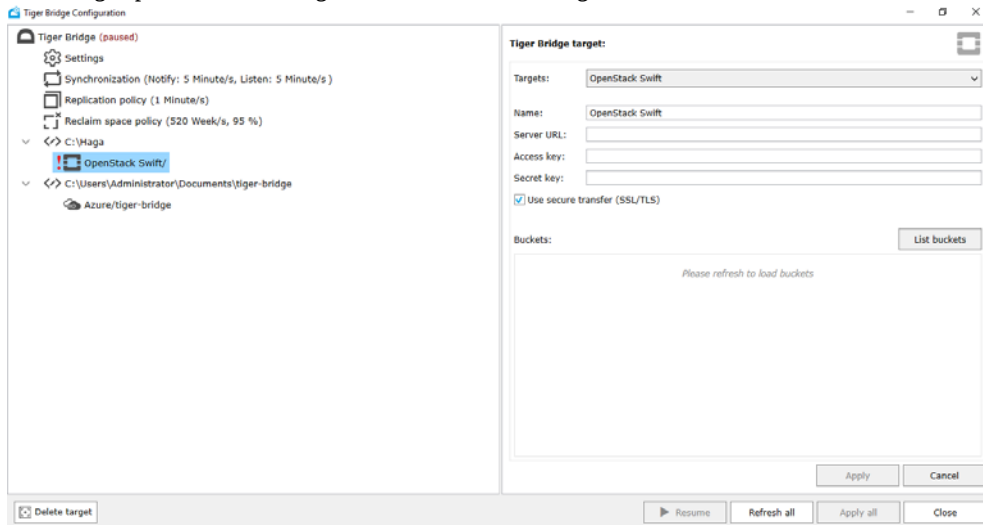
To pair a source with OpenStack Swift target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select On-premises, then select OpenStack Swift and click OK.



Get Started with Tiger Bridge Using the Configuration

3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

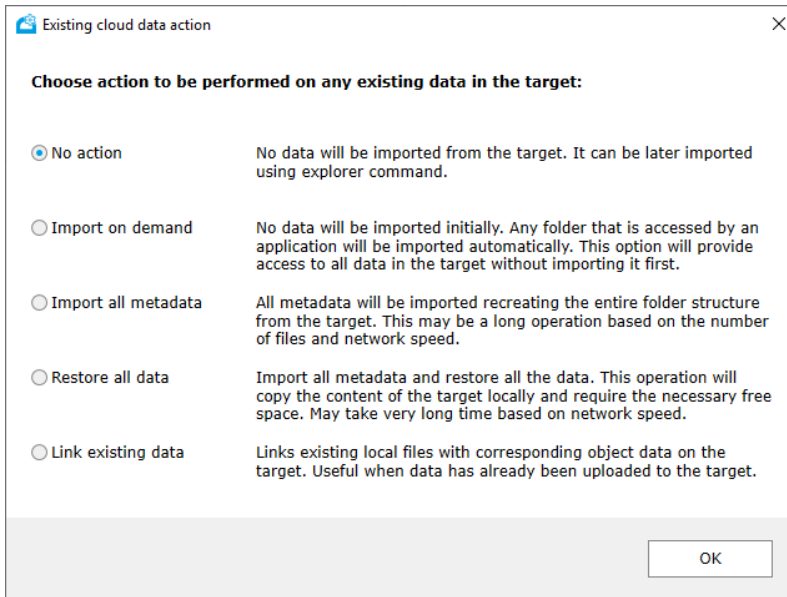
Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

- Enter the server URL, access and secret keys of the OpenStack Swift target.
- Choose whether to access the target using secure transfer (SSL/TLS) by selecting or clearing the check box.
- Click List buckets, to display the list of buckets available for the account you have specified and then select the bucket, which to pair with the source.

Note: If the user whose credentials you have provided, does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not use the same bucket for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, only when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active Sync” on page 95). Do not change the name of the bucket on the OpenStack Swift target as this may prevent Tiger Bridge replication from operating.

4. In the Existing cloud data action dialog, select what to do with data already existing in the bucket and then click OK.



5. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

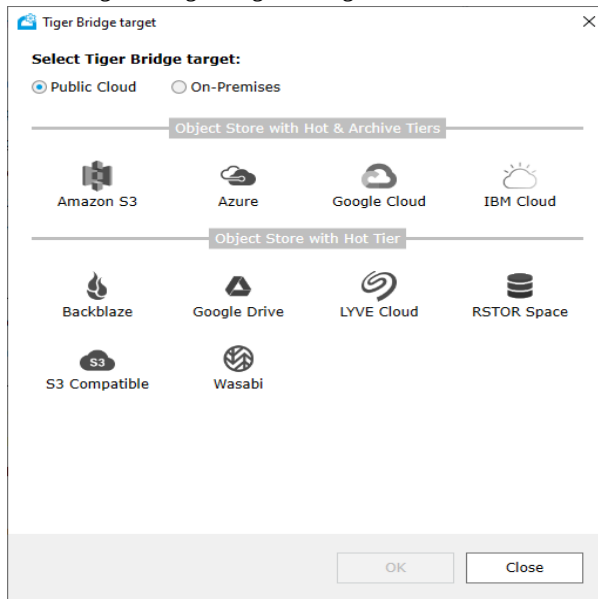
Pair a Source with LYVE Cloud Target

Note: Currently, you can pair a source with a LYVE Cloud target only in the Tiger Bridge Configuration.

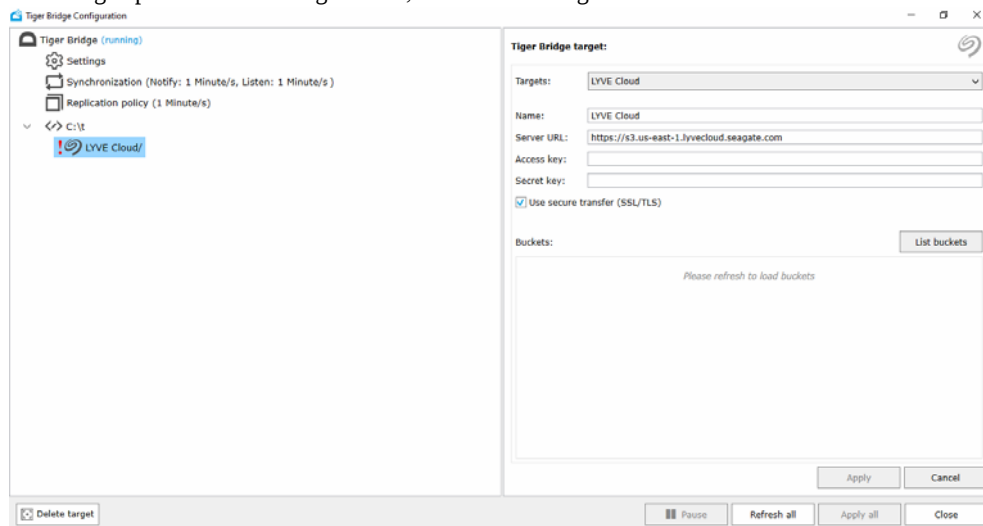
Get Started with Tiger Bridge Using the Configuration

To pair a source volume with LYVE Cloud target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select Public Cloud, then select LYVE Cloud and click OK.



3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

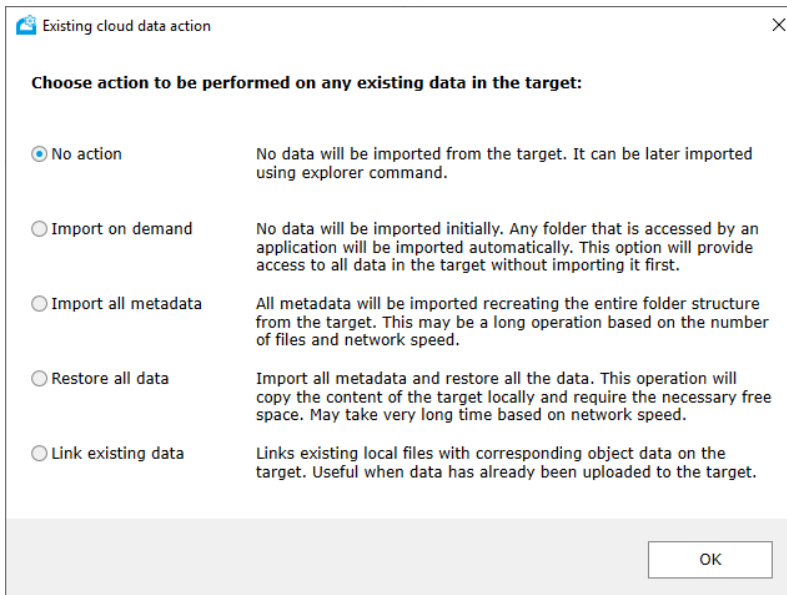
Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

- Enter the server URL, access and secret keys of the LYVE Cloud target.
- Choose whether to access the target using secure transfer (SSL/TLS) by selecting or clearing the check box.
- Click List buckets, to display the list of buckets available for the account you have specified and then select the bucket, which to pair with the source.

Note: If the user whose credentials you have provided, does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not use the same bucket for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, only when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active Sync” on page 95). Do not change the name of the bucket on the LYVE Cloud target as this may prevent Tiger Bridge replication from operating.

4. In the Existing cloud data action dialog, select what to do with data already existing in the bucket and then click OK.



The dialog box is titled "Existing cloud data action" and contains a close button (X) in the top right corner. Below the title bar, the text "Choose action to be performed on any existing data in the target:" is displayed. There are five radio button options, each with a description:

- ☒ **No action**: No data will be imported from the target. It can be later imported using explorer command.
- ☐ **Import on demand**: No data will be imported initially. Any folder that is accessed by an application will be imported automatically. This option will provide access to all data in the target without importing it first.
- ☐ **Import all metadata**: All metadata will be imported recreating the entire folder structure from the target. This may be a long operation based on the number of files and network speed.
- ☐ **Restore all data**: Import all metadata and restore all the data. This operation will copy the content of the target locally and require the necessary free space. May take very long time based on network speed.
- ☐ **Link existing data**: Links existing local files with corresponding object data on the target. Useful when data has already been uploaded to the target.

An "OK" button is located at the bottom right of the dialog box.

5. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global

Get Started with Tiger Bridge Using the Configuration

data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

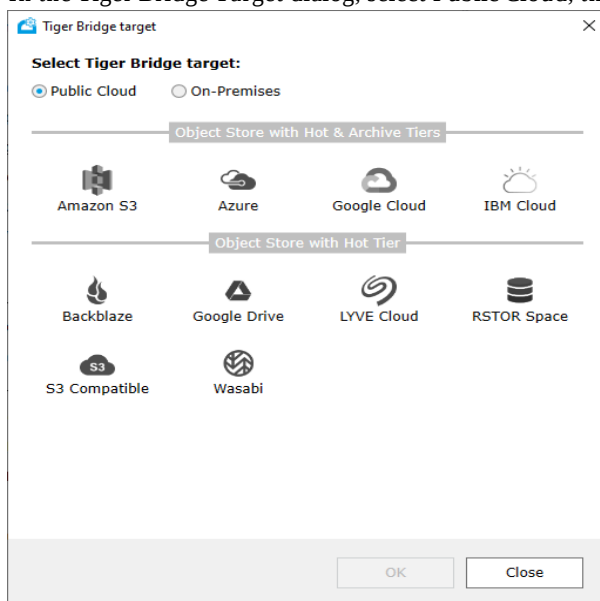
Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Pair a Source with RSTOR Space Target

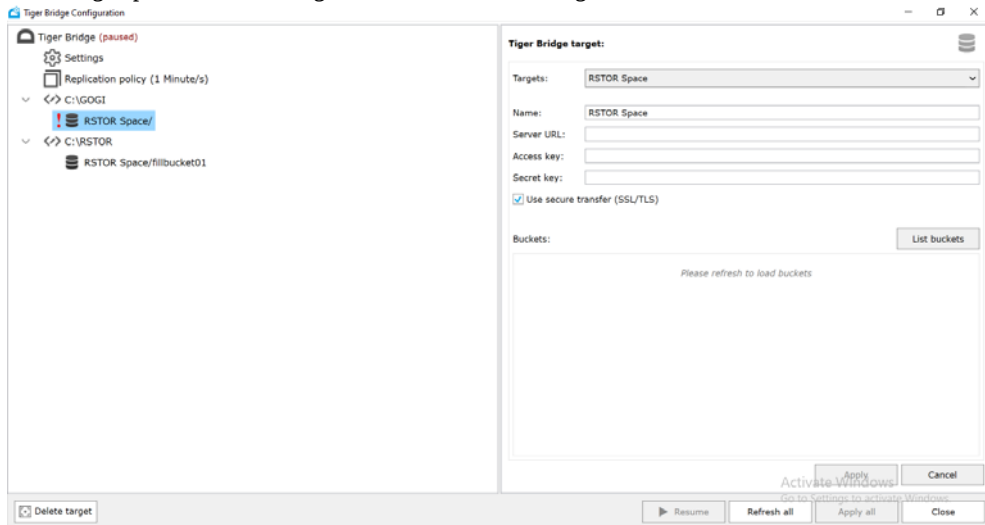
Note: Currently, you can pair a source with a RSTOR Space target only in the Tiger Bridge Configuration.

To pair a source volume with RSTOR Space target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select Public Cloud, then select RSTOR Space and click OK.



3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

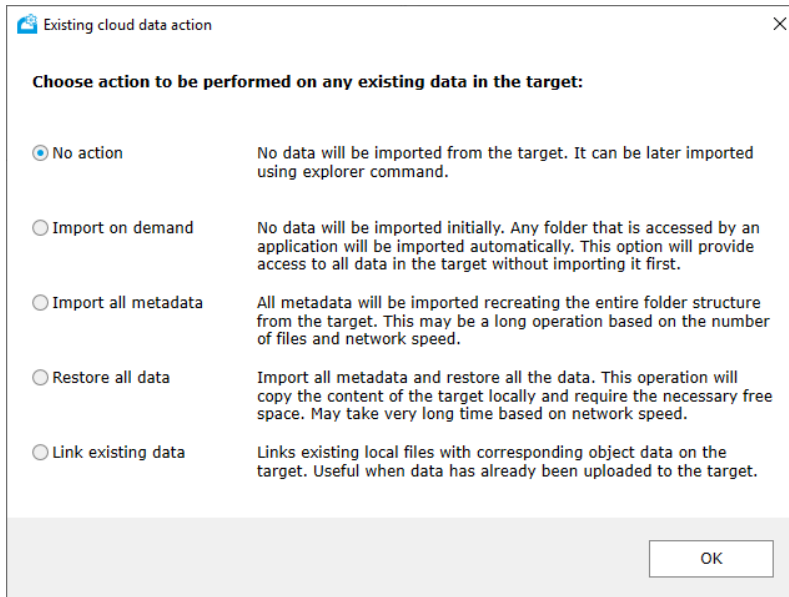
- Enter the server URL, access and secret keys of the RSTOR Space target.
- Choose whether to access the target using secure transfer (SSL/TLS) by selecting or clearing the check box.
- Click List buckets, to display the list of buckets available for the account you have specified and then select the bucket, which to pair with the source.

Note: If the user whose credentials you have provided, does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not use the same bucket for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, only when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active Sync” on page 95). Do not change the name of the bucket on the RSTOR Space target as this may prevent Tiger Bridge replication from operating.

Get Started with Tiger Bridge Using the Configuration

4. In the Existing cloud data action dialog, select what to do with data already existing in the bucket and then click OK.



5. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

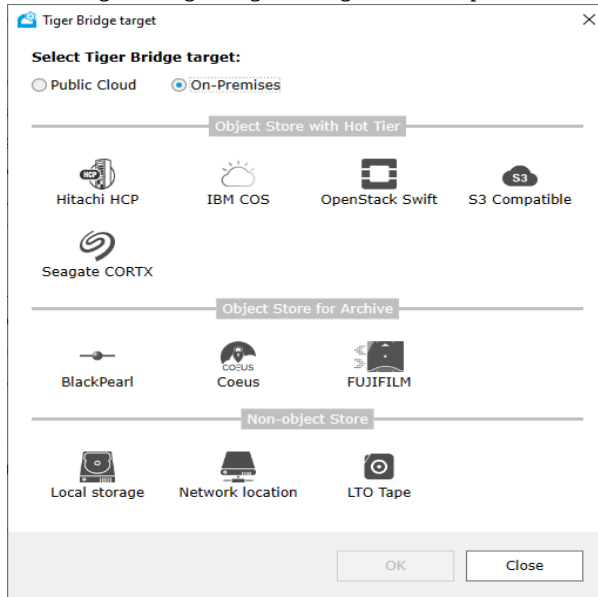
Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Pair a Source with Seagate CORTX Target

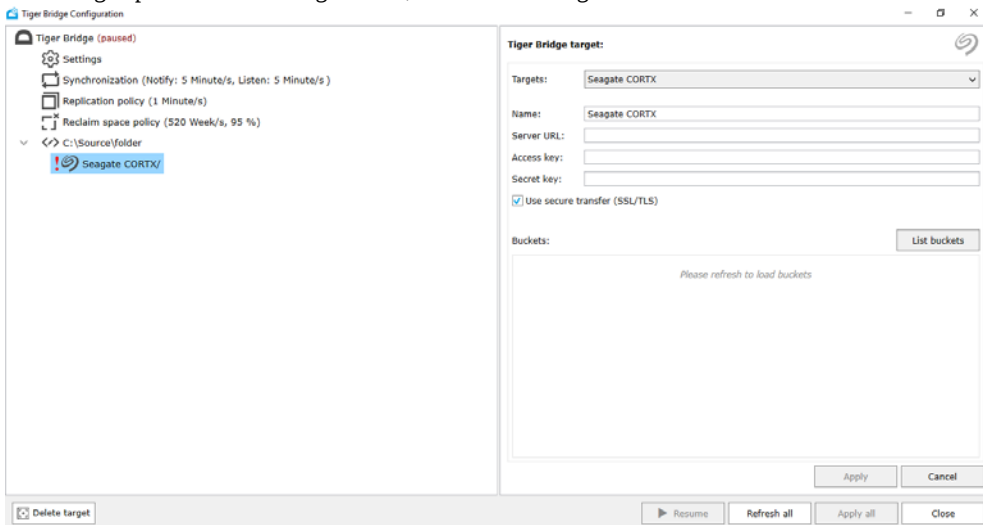
Note: Currently, you can pair a source with an Seagate CORTX target only in the Tiger Bridge Configuration.

To pair a source volume with Seagate CORTX target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select On-premises, then select Seagate CORTX and click OK.



3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

Get Started with Tiger Bridge Using the Configuration

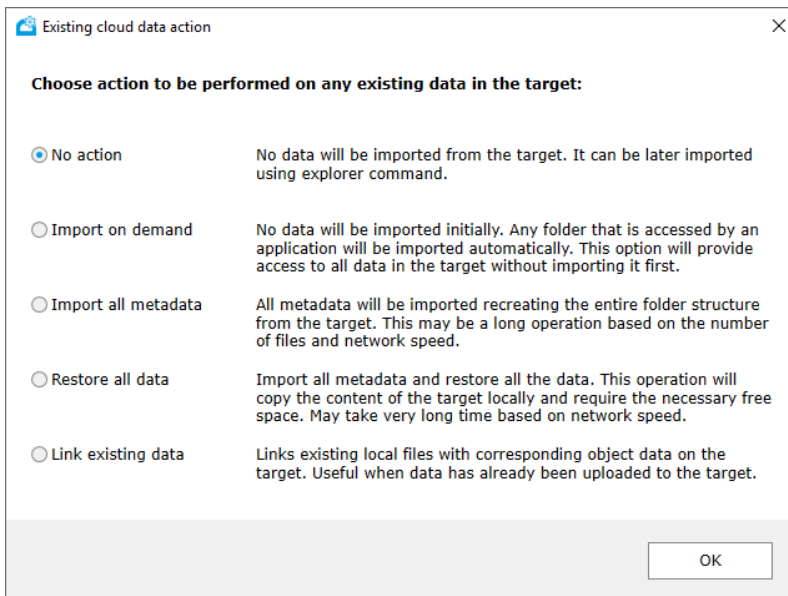
Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

- Enter the server URL, access and secret keys of the Seagate CORTX target.
- Choose whether to access the target using secure transfer (SSL/TLS) by selecting or clearing the check box.
- Click List buckets, to display the list of buckets available for the account you have specified and then select the bucket, which to pair with the source.

Note: If the user whose credentials you have provided, does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not use the same bucket for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, only when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active Sync” on page 95). Do not change the name of the bucket on the Seagate CORTX target as this may prevent Tiger Bridge replication from operating.

4. In the Existing cloud data action dialog, select what to do with data already existing in the bucket and then click OK.



The dialog box is titled "Existing cloud data action" and contains a close button (X) in the top right corner. Below the title bar, the text "Choose action to be performed on any existing data in the target:" is displayed. There are five radio button options, each with a description:

Action	Description
☒ No action	No data will be imported from the target. It can be later imported using explorer command.
☐ Import on demand	No data will be imported initially. Any folder that is accessed by an application will be imported automatically. This option will provide access to all data in the target without importing it first.
☐ Import all metadata	All metadata will be imported recreating the entire folder structure from the target. This may be a long operation based on the number of files and network speed.
☐ Restore all data	Import all metadata and restore all the data. This operation will copy the content of the target locally and require the necessary free space. May take very long time based on network speed.
☐ Link existing data	Links existing local files with corresponding object data on the target. Useful when data has already been uploaded to the target.

An "OK" button is located at the bottom right of the dialog box.

5. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global

data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

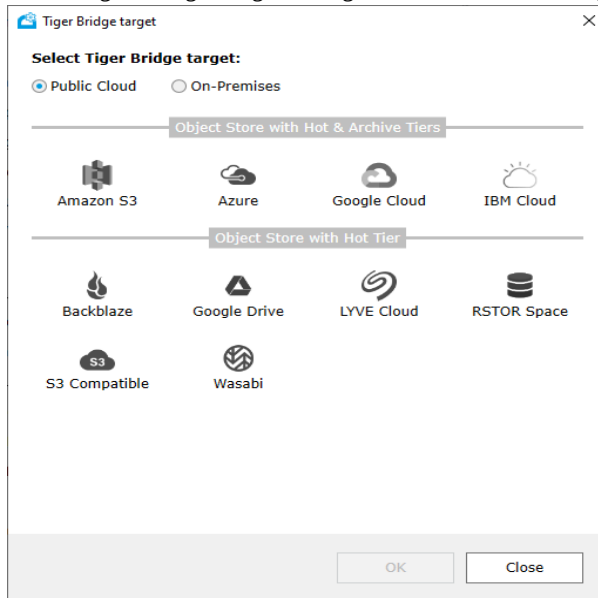
Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Pair a Source with S3-compatible Object Storage Target

Note: To see how to pair a source with S3-compatible target using the command-line interface of Tiger Bridge, refer to “Pair a Source with S3-compatible Object Storage Target” on page 114.

To pair a source volume with S3-compatible object storage target:

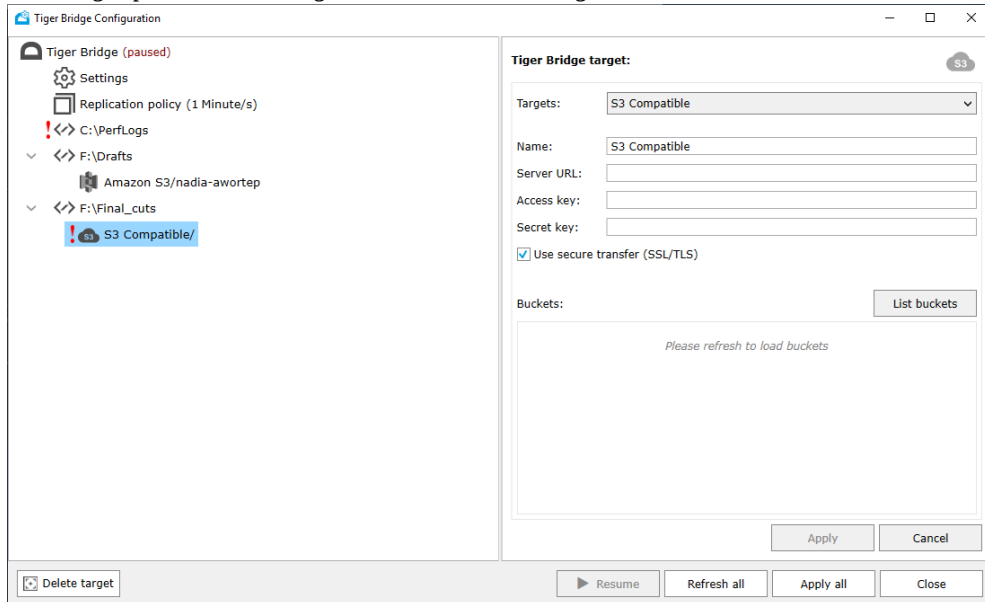
1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, do one of the following:



- if you are configuring a public S3-compatible object storage as a target, select Public Cloud, then select S3 Compatible and click OK.
- if you are configuring an on-premises S3-compatible object storage as a target, select On-premises, then select S3 Compatible and click OK.

Get Started with Tiger Bridge Using the Configuration

3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

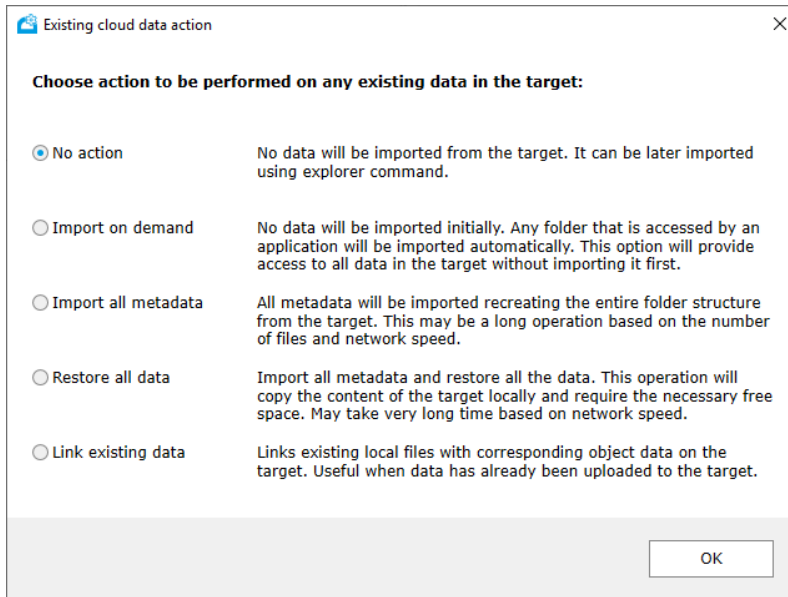
Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

- Enter the server URL, access and secret keys of the S3-compatible object storage target.
- Choose whether to access the target using secure transfer (SSL/TLS) by selecting or clearing the check box.
- Click List buckets, to display the list of buckets available for the account you have specified and then select the bucket, which to pair with the source.

Note: If the user whose credentials you have provided, does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not use the same bucket for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active Sync” on page 95). Do not change the name of the bucket on the S3-compatible object storage as this may prevent Tiger Bridge replication from operating.

4. In the Existing cloud data action dialog, select what to do with data already existing in the bucket and then click OK.



5. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

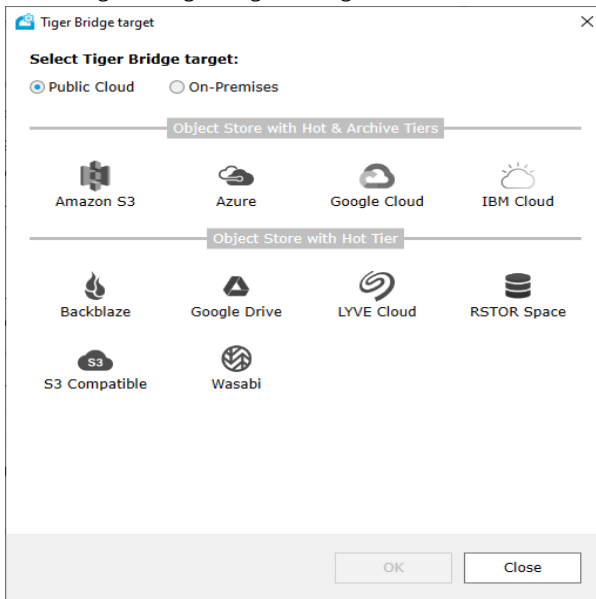
Pair a Source with Google Cloud Target

Note: Currently you can pair a source with a Google Cloud storage target only in the Tiger Bridge Configuration.

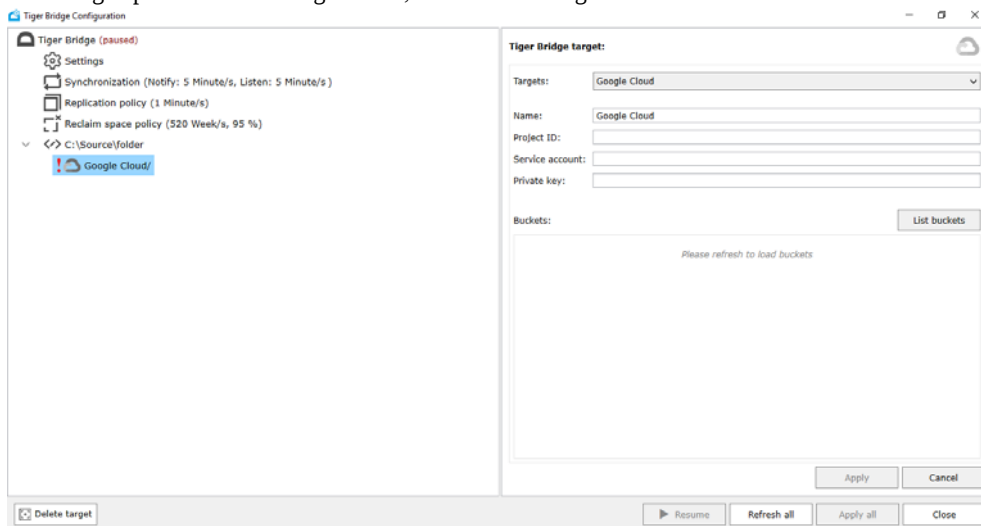
Get Started with Tiger Bridge Using the Configuration

To pair a source with Google cloud storage target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select Public Cloud, then select Google Cloud and click OK.



3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

- Enter the Project ID, service account email and private JSON key for access to the bucket(s) on the target.

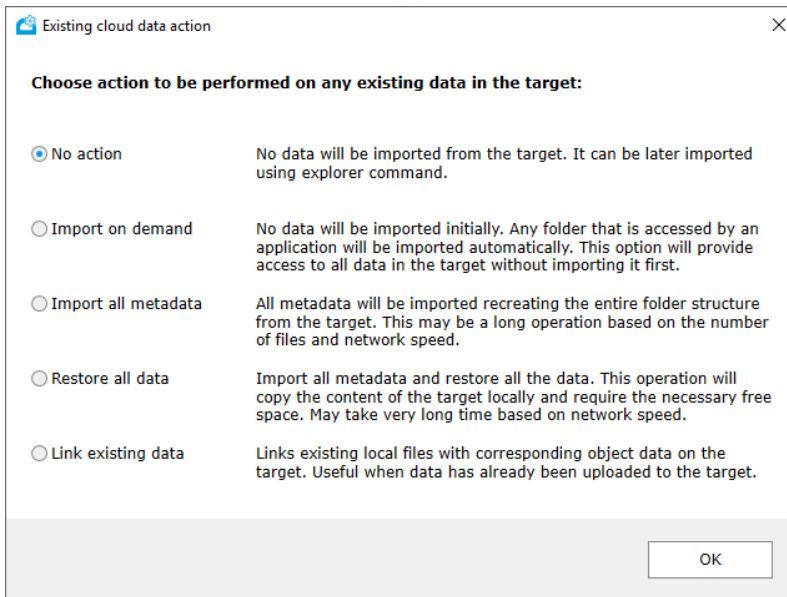
Note: For more information about creating a service account and retrieving its credentials, refer to the Google Cloud Console documentation.

- Click List buckets, to display the list of buckets available for the account you have specified and then select the bucket, which to pair with the source.

Note: If the user whose credentials you have provided, does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not use the same bucket for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active Sync” on page 95). Do not change the name of the bucket on the Google Cloud storage as this may prevent Tiger Bridge replication from operating.

4. In the Existing cloud data action dialog, select what to do with data already existing in the bucket and then click OK.



The dialog box titled "Existing cloud data action" contains a close button (X) in the top right corner. Below the title bar, the text "Choose action to be performed on any existing data in the target:" is displayed. There are five radio button options, each with a description:

- ☒ **No action**: No data will be imported from the target. It can be later imported using explorer command.
- ☐ **Import on demand**: No data will be imported initially. Any folder that is accessed by an application will be imported automatically. This option will provide access to all data in the target without importing it first.
- ☐ **Import all metadata**: All metadata will be imported recreating the entire folder structure from the target. This may be a long operation based on the number of files and network speed.
- ☐ **Restore all data**: Import all metadata and restore all the data. This operation will copy the content of the target locally and require the necessary free space. May take very long time based on network speed.
- ☐ **Link existing data**: Links existing local files with corresponding object data on the target. Useful when data has already been uploaded to the target.

An "OK" button is located at the bottom right of the dialog box.

5. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global

Get Started with Tiger Bridge Using the Configuration

data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

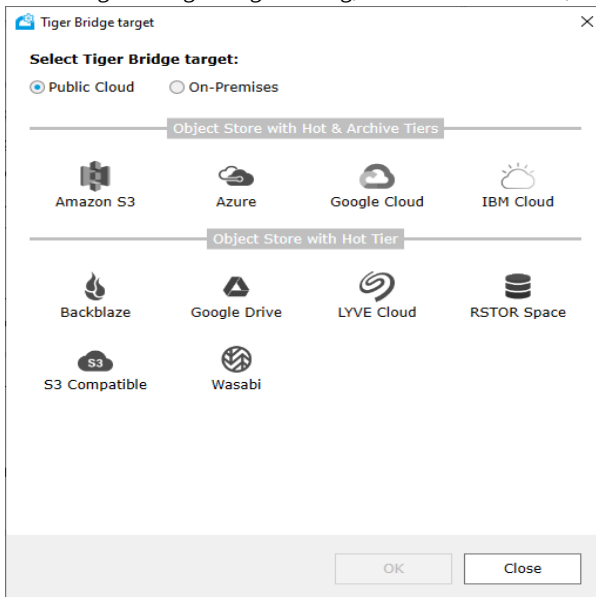
Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Pair a Source with Google Drive Target

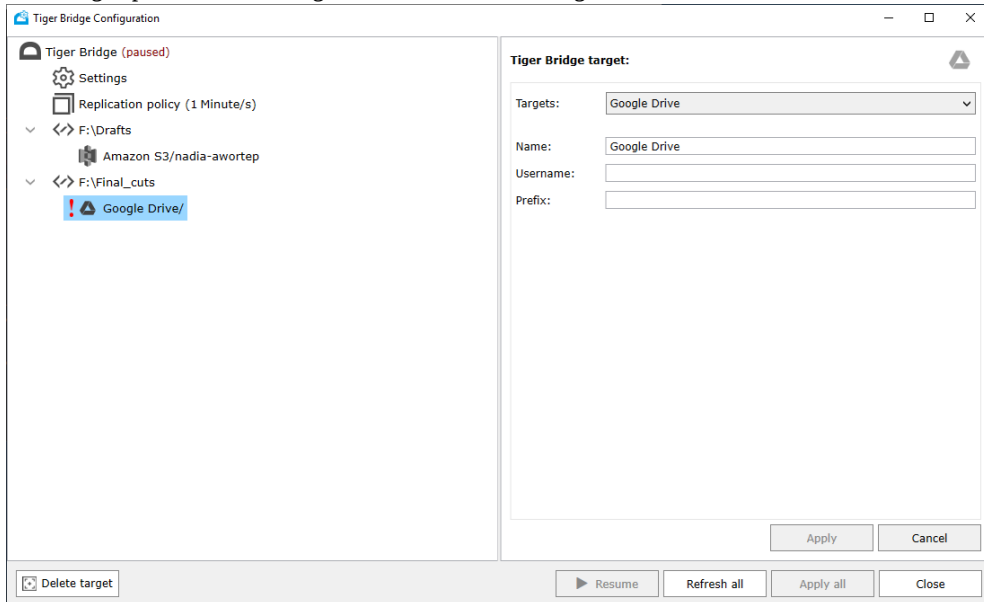
Note: Currently you can pair a source with a Google Drive target only in the Tiger Bridge Configuration.

To pair a source with Google Drive target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select Public Cloud, then select Google Drive and click OK.



3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

- Enter the username of the Google Drive account and the name of the folder to be used for Tiger Bridge-managed data and then click Apply.

Note: If the folder name you have specified does not exist, Tiger Bridge automatically creates it in your Google Drive.

Important: Do not use the same folder for two or more sources on the same computer. You must use the same folder for multiple sources each on a different computer, only when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active Sync” on page 95). Do not change the name of the folder on your Google Drive as this may prevent Tiger Bridge replication from operating.

- In the web browser that opens, log in to your Google Drive account and authorize Tiger Bridge to preview, edit, create and delete files in your Google Drive.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

Get Started with Tiger Bridge Using the Configuration

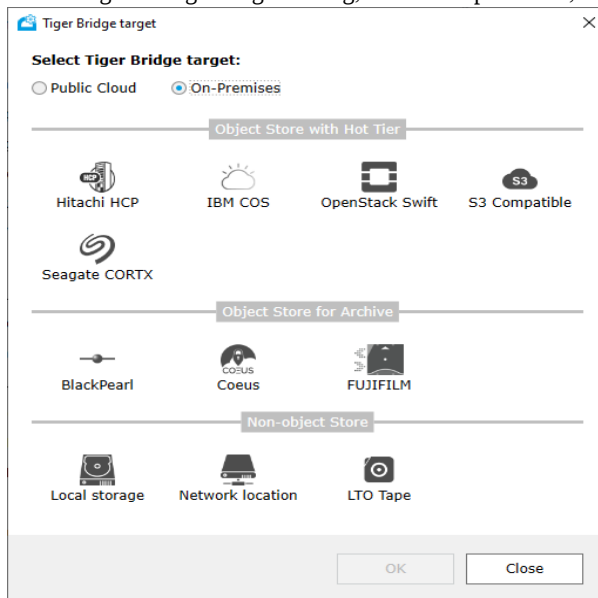
Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Pair a Source with BlackPearl Object Storage Target

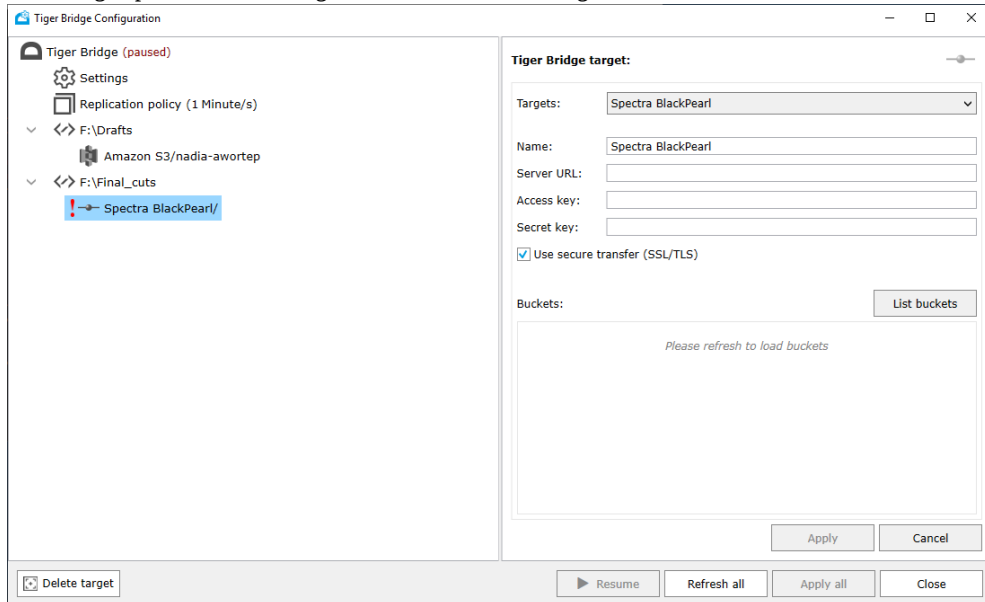
Note: To see how to pair a source with BlackPearl target using the command-line interface of Tiger Bridge, refer to “Pair a Source with BlackPearl Object Storage Target” on page 115.

To pair a source with BlackPearl object storage target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select On-premises, then select BlackPearl and click OK.



3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

- Enter the server URL, access and secret keys of the BlackPearl target.
- Choose whether to access the target using secure transfer (SSL/TLS) by selecting or clearing the check box.
- Click List buckets, to display the list of buckets available for the account you have specified and then select the bucket, which to pair with the source.

Note: If the user whose credentials you have provided, does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not use the same bucket for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, when you intend to deploy Tiger Bridge for geo replication (for more information, see "Configure Active Sync" on page 95). Do not change the name of the bucket on the BlackPearl object storage as this may prevent Tiger Bridge replication from operating.

4. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global

Get Started with Tiger Bridge Using the Configuration

data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

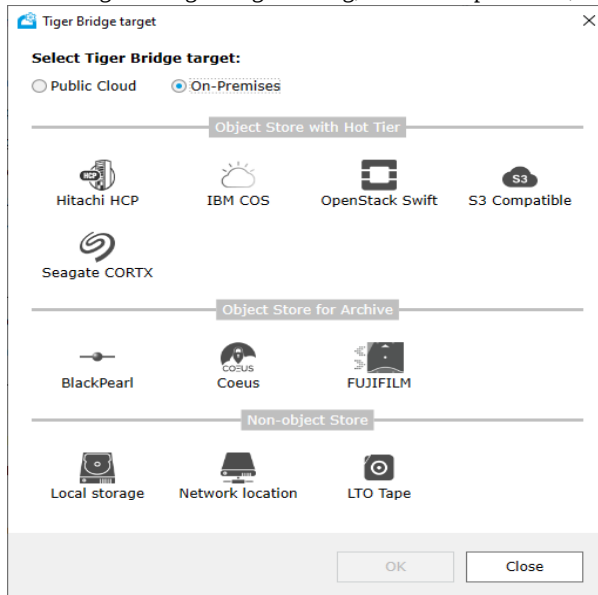
Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Pair a Source with Coeus Target

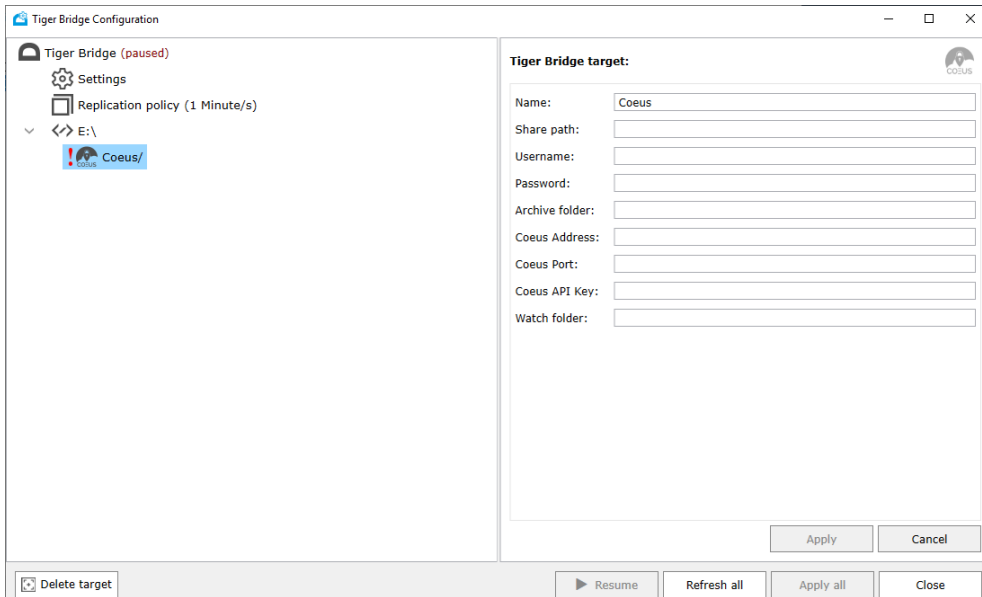
Note: To see how to pair a source with Coeus target using the command-line interface of Tiger Bridge, refer to “Pair a Source with Coeus Target” on page 116.

To pair a source with Coeus target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select On-premises, then select Coeus and click OK.



3. In the right pane of the Configuration, enter the details required for access to the Coeus target and click Apply:



Note: If the Coeus account details you have specified are already used for another source, you cannot pair the current source with it.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

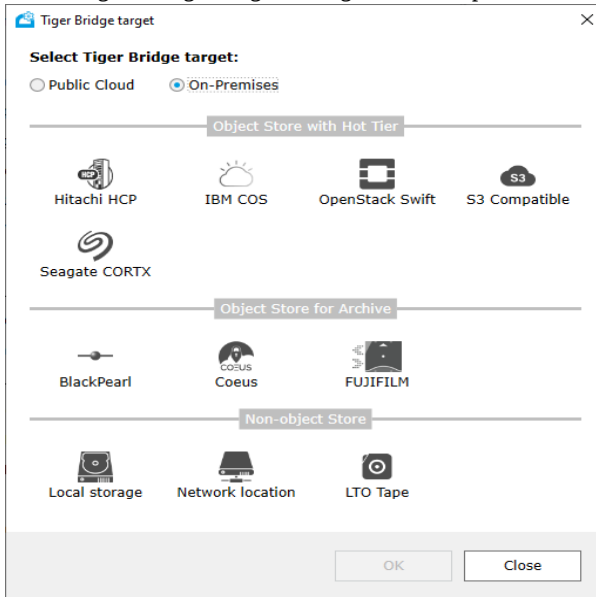
Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Get Started with Tiger Bridge Using the Configuration

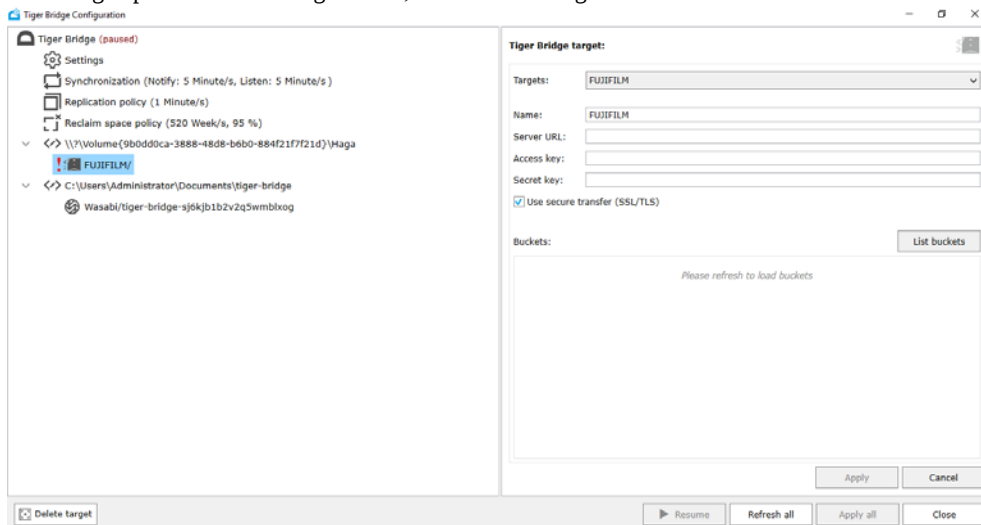
Pair a Source with a FujiFilm Object Archive Target

To pair a source volume with FujiFilm object archive target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select On-premises, then select FUJIFILM and click OK.



3. In the right pane of the Configuration, do the following:



- Enter a name for the target.

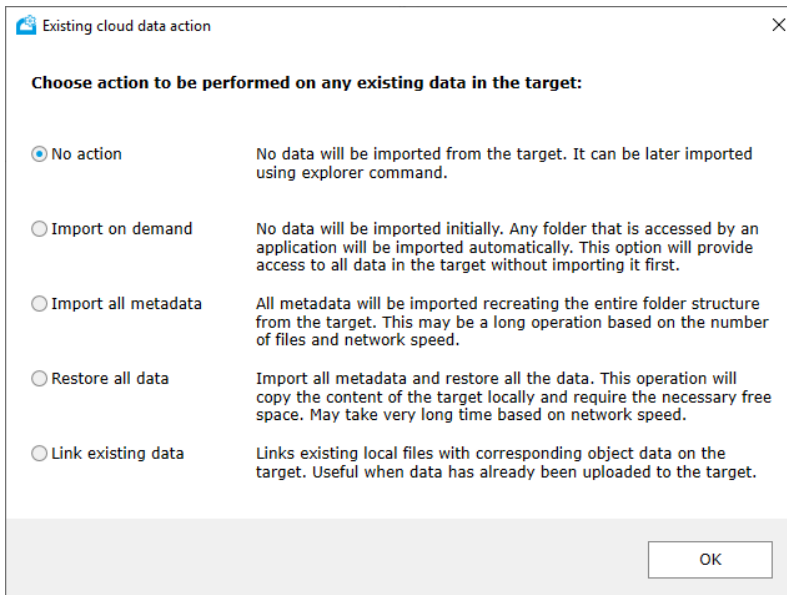
Tip: Specifying a unique name of the target lets you re-use its parameters, when you pair another source with the same target. The target and its parameters will appear in the Targets drop-down box.

- Enter the server URL, access and secret keys of the FujiFilm object archive storage target.
- Choose whether to access the target using secure transfer (SSL/TLS) by selecting or clearing the check box.
- Click List buckets, to display the list of buckets available for the account you have specified and then select the bucket, which to pair with the source.

Note: If the user whose credentials you have provided, does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not use the same bucket for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, when you intend to deploy Tiger Bridge for geo replication (for more information, see “Configure Active Sync” on page 95). Do not change the name of the bucket on the FujiFilm object storage as this may prevent Tiger Bridge replication from operating.

4. In the Existing cloud data action dialog, select what to do with data already existing in the bucket and then click OK.



The dialog box titled "Existing cloud data action" contains a close button (X) in the top right corner. Below the title bar, the text "Choose action to be performed on any existing data in the target:" is displayed. There are five radio button options, each with a corresponding description:

- ☒ **No action**: No data will be imported from the target. It can be later imported using explorer command.
- ☐ **Import on demand**: No data will be imported initially. Any folder that is accessed by an application will be imported automatically. This option will provide access to all data in the target without importing it first.
- ☐ **Import all metadata**: All metadata will be imported recreating the entire folder structure from the target. This may be a long operation based on the number of files and network speed.
- ☐ **Restore all data**: Import all metadata and restore all the data. This operation will copy the content of the target locally and require the necessary free space. May take very long time based on network speed.
- ☐ **Link existing data**: Links existing local files with corresponding object data on the target. Useful when data has already been uploaded to the target.

An "OK" button is located at the bottom right of the dialog box.

Get Started with Tiger Bridge Using the Configuration

5. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

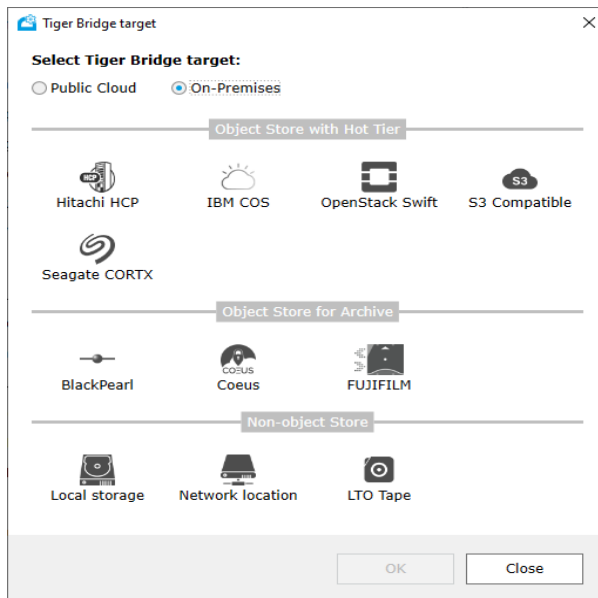
Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Pair a Source with a Network Share Target

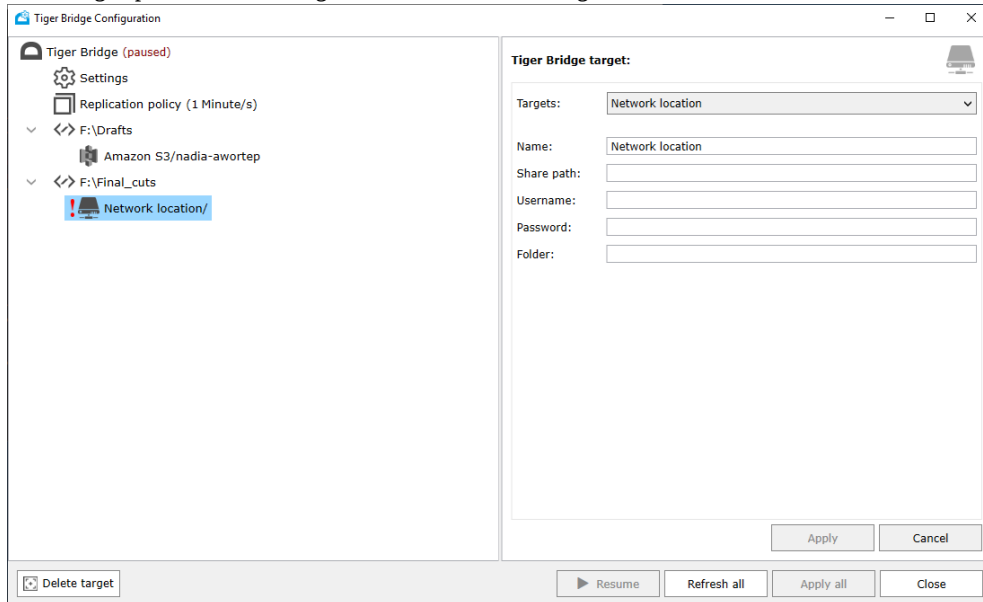
Note: To see how to pair a source with network share target using the command-line interface of Tiger Bridge, refer to “Pair a Source with a Network Share Target” on page 118.

To pair a source with a network share target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select On-premises, then select Network location and click OK.



3. In the right pane of the Configuration, do the following:



- Enter a name of the target.
- Enter the path to the network share.
- (SMB share only) Enter credentials for access to the share.

Important: You must enter the username in the following format [NAS server domain name or IP address]\[username]. For example, if the IP address of your NAS server is 10.200.0.65 and the name of the user, whose credentials you are providing is “test”, enter the following in the Username field:

10.200.0.65\test

Note: If you are configuring an NFS share target, leave the username and password fields empty.

- Enter the name of an existing folder on the share designated for container of the selected source.

Note: If you want to use the root of the network share as a container for the source, specify the path to the share without the root folder and then enter the name of the root as folder to be used. For example, if you want to use as a target network share with name “Projects” exported by the server server.com, enter as Share path: \\server.com and as folder to be used as container: Projects.

4. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global

Get Started with Tiger Bridge Using the Configuration

data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

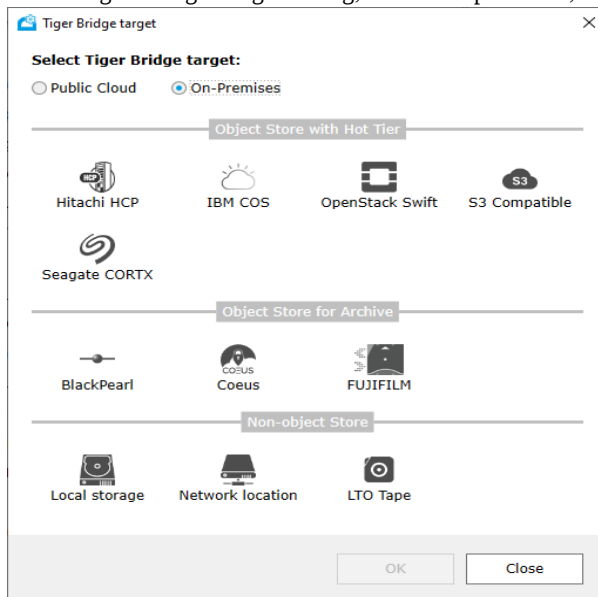
Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Pair a Source with a Local Volume Target

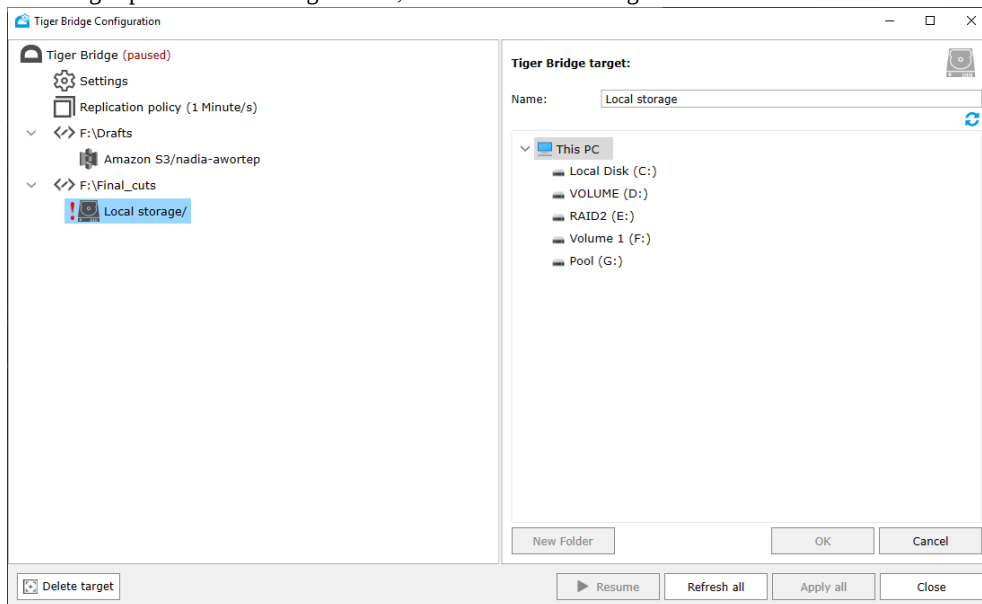
Note: To see how to pair a source with local volume as a target using the command-line interface of Tiger Bridge, refer to “Pair a Source with a Local Volume Target” on page 119.

To pair a source with a local volume target:

1. In the left pane select the source and click Add Target.
2. In the Tiger Bridge Target dialog, select On-premises, then select Local storage and click OK.



3. In the right pane of the Configuration, enter name of the target and then do one of the following:



- To add an existing folder as a target, browse to and select the folder or the root of the volume and click OK.
- To create a new folder as a target, browse to the location where you want to create it, click New Folder, specify the name of the new folder and then click OK.

4. Click Apply.

Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. You can change the settings of the global data replication policy or configure a policy valid for just a specific pair of source and target, following the steps in “Configure Automatic Data Replication” on page 83.

Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Configure Automatic Data Replication

Note: To see how to configure automatic data replication using the command-line interface of Tiger Bridge, refer to “Automatic Data Replication” on page 121.

To allow Tiger Bridge to automatically replicate files from the source to the target, you should simply specify for how long a file should not have been modified in order Tiger Bridge to queue it for replication. You can configure the global data replication policy, which is valid for all pairs of

Get Started with Tiger Bridge Using the Configuration

source and target. By default, the global replication policy is set to queue for replication data not modified within the last 1 minute. You can also overwrite the global data replication policy by specifying different parameters for a given pair of source and target.

You can disable automatic data replication both globally or just for a specific pair of source and target. For the purpose you need to configure either the global replication policy or the policy of a specific pair to replicate files, when they have not been modified for 0 minutes. In this case, you will be able to replicate files only manually.

When configuring the global data replication policy, you can also refine the list of automatically managed locations on all sources. For more information, refer to “Refine the List of Automatically Managed Locations” on page 84.

You can also fine-tune your data replication workflow by configuring several advanced settings. For more information, refer to “Advanced Data Replication Settings” on page 137.

Refine the List of Automatically Managed Locations

Depending on the interface you have used to pair a source with a target, Tiger Bridge assumes that:

- (Tiger Bridge Configuration) it should automatically manage all data on the source.
- (command-line interface) it should not automatically manage any data on the source.

You can refine the list of locations on your sources, in which data should be automatically managed, by specifying a list of included and excluded locations, thus instructing Tiger Bridge to automatically manage (replicate, reclaim space, archive):

- all data on a source, when the root of the source is added as an included location;
- all data on a source, except data in subfolders added as excluded locations, when the root of the source is added as an included location;
- no data on the source except data in subfolders added as included locations, when the root of the volume is not added as an included location;

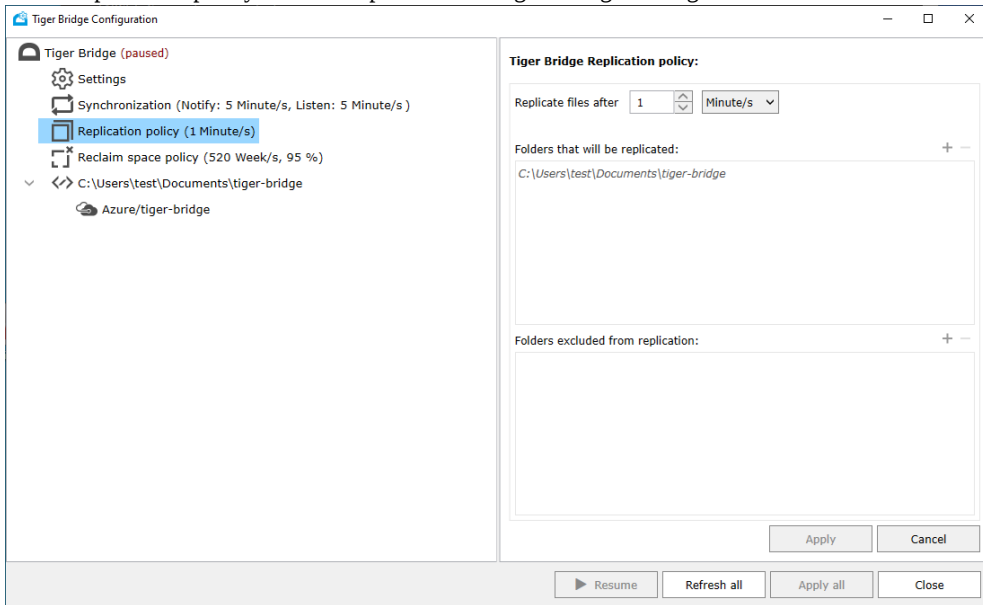
Note: *Although data in the excluded locations is not subject to Tiger Bridge’s automatic data lifecycle management, you can manually perform such operations on files/folders in an excluded location. For more information, see “Manually Manage Data” on page 153.*

You can edit the list of included and excluded locations at any time as part of the global data replication policy configuration, following the steps below.

Note: *To see how to refine the list of automatically managed locations, using the command-line interface of Tiger Bridge, refer to “Refine the List of Automatically Managed Locations” on page 120.*

To configure global data replication policy:

1. Click Replication policy in the left pane of the Tiger Bridge Configuration.



2. In the right pane, specify for how long a file should not have been modified for Tiger Bridge to replicate it, by entering the desired number and selecting the unit of measure in the drop-down box beside it.

Note: To disable automatic data replication and allow only manual replication of files, specify that files should not have been modified for 0 minutes.

3. (optional) Refine the list of automatically managed locations on all sources, by doing one of the following:

- To add a folder to the list of included or excluded locations, click the + next to the respective list and browse to and select the respective folder, then click OK.

Note: You can also create a new folder in an existing source to add it as an included or excluded location.

- To remove a folder from the list of included or excluded locations, select the folder in the respective list and click the - button.

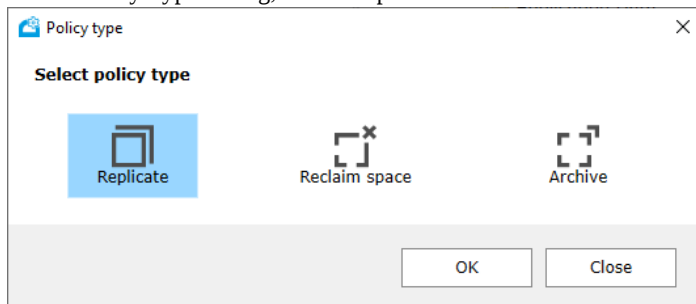
4. Click Apply.

Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in "Pause/Resume Automatic Tiger Bridge Operations" on page 102.

Get Started with Tiger Bridge Using the Configuration

To overwrite the global replication policy for a specific pair:

1. In the Tiger Bridge Configuration, select the source in the left pane and click Add policy.
2. In the Policy Type dialog, select Replicate and click OK.



Important: If the selected source already has its own replication policy assigned, you cannot add a new replication policy, but can edit the existing policy, following the steps below.

Note: To make the source use the global replication policy set for all pairs, simply delete its own policy by selecting it and clicking Delete policy.

3. In the right pane, specify for how long a file should not have been modified for Tiger Bridge to replicate it, by entering the desired number and selecting the unit of measure in the drop-down box beside it.

Note: To disable automatic data replication and allow only manual replication of files, specify that files should not have been modified for 0 minutes.

4. Click Apply.

Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in "Pause/Resume Automatic Tiger Bridge Operations" on page 102.

Configure Space Reclaiming

Note: To see how to configure automatic space reclaiming using the command-line interface of Tiger Bridge, refer to "Space Reclaiming" on page 122.

Aside from turning space reclaiming on, to instruct Tiger Bridge under what conditions it should replace replicated files on the source(s) with nearline files, you must configure the following parameters:

space reclaiming policy — Tiger Bridge decides which replicated files to replace with nearline files on the source volume based on 2 parameters - minimal file size and time interval for which the file has not been accessed. For example, if you set the file size threshold to 10MB and the time interval to 2 weeks, Tiger Bridge will replace with nearline files all replicated files with size 10MB or above that have not been accessed for at least 2 weeks, leaving on the source volume

replicated files whose size is smaller than 10MB and also replicated files with bigger size that have been accessed by a client computer in less than 2 weeks. By default, Tiger Bridge is set to replace any file, which has not been accessed for more than 4 weeks, regardless of its size.

used space thresholds for space reclaiming — the default used space threshold is 0% and space reclaiming is triggered as soon as any file meets the criteria for replacement with a nearline file. You can increase the used space threshold and let Tiger Bridge reclaim space only when a given amount of your source is full. You can also specify maximum used space threshold on your source - it specifies when all files subject to replication are queued for replacement with nearline files regardless of their size and last access time. By default, maximum used space value is set to 90% for all source volumes.

Note: *Tiger Bridge processes the queue of files scheduled for replacement with nearline files starting from the ones, which are least recently accessed.*

processes triggering file retrieval — By default, each process, attempting to open a nearline file on the source volume, triggers its retrieval from the target. To prevent useless retrieval of nearline files by your antivirus software, for example, you can specify which processes exactly can trigger the file retrieval operation. You can do this by creating either a list of processes allowed to trigger retrieval or by creating a list of processes, which cannot trigger retrieval of nearline files. There is no need to create both lists. In case you create a list of processes allowed to trigger nearline file retrieval from the target, any process not included in the list will not trigger the operation, when this process attempts to open the file. In case you decide to specify the processes, which are not allowed to trigger file retrieval from the target, any process not mentioned in the list will trigger the nearline file retrieval, when this process attempts to open that file.

Important: *With a NAS source, nearline files are located in the control folder and not on the network share. Still, when retrieving them, actual data is retrieved directly on the NAS source. To learn more about space reclaiming on NAS sources, refer to “NAS Source Prerequisites and Setup” on page 36.*

You can configure a global space reclaiming policy, valid for each pair of source and target, which does not have its own space reclaiming policy assigned. You can overwrite the global space reclaiming policy for a given pair of source and target or disable space reclaiming for that pair only.

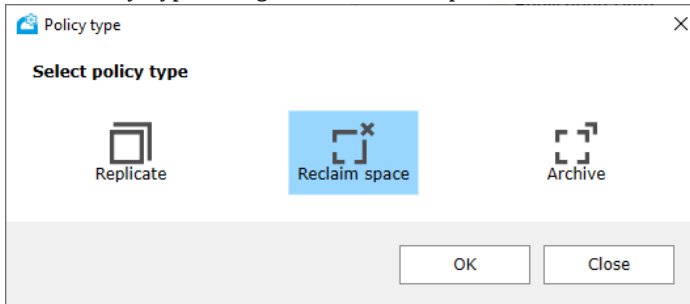
Important: *If the storage class of your cloud storage target is an archival tier (Amazon S3 Glacier/S3 Glacier Deep Archive or Azure Archive), when Tiger Bridge reclaims space on your source, files are not replaced by nearline stubs, but by offline files, which can be retrieved back on the source only manually through the Tiger Bridge shell extension or the command-line interface.*

You can also fine-tune your space reclaiming workflow by configuring several advanced settings. For more information, refer to “Advanced Space Reclaiming and Data Archiving Settings” on page 141.

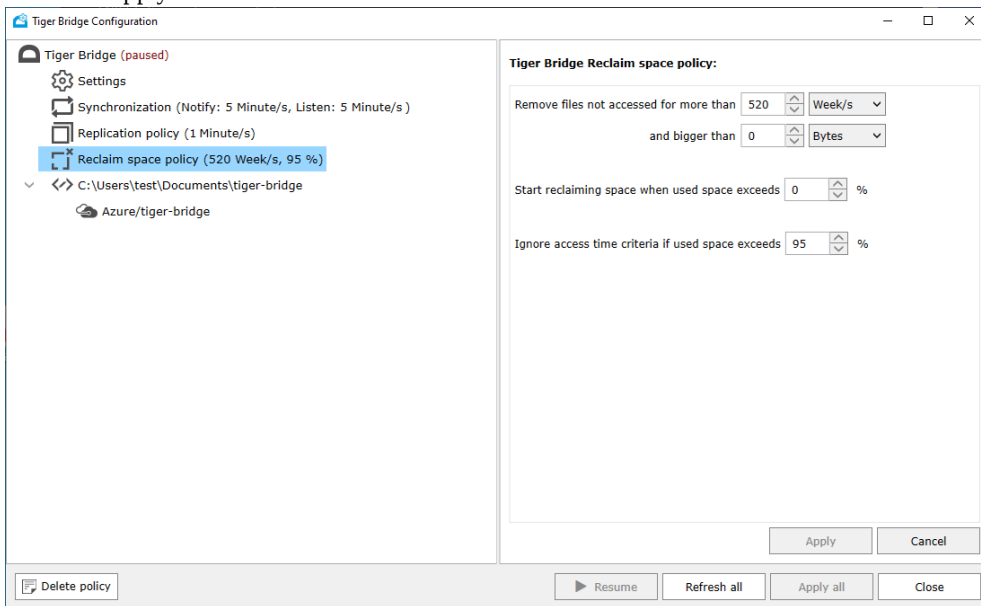
Get Started with Tiger Bridge Using the Configuration

To configure global space reclaiming policy:

1. Select Tiger Bridge in the left pane and then click Add policy.
2. In the Policy Type dialog, select Reclaim space and click OK.



3. In the right pane, specify the parameters for file access time and size, for used space thresholds and click Apply.

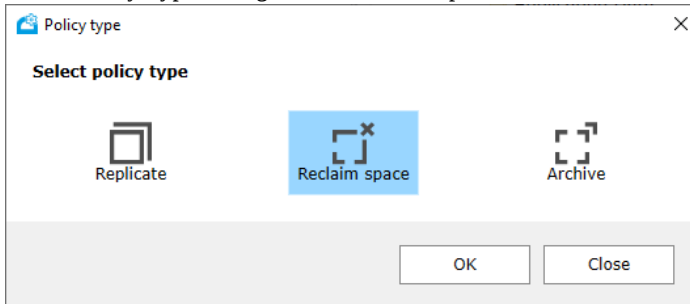


The global space reclaiming policy is valid for all sources that do not have their own policy assigned. To edit the global policy, simply select it in the left pane, edit the desired parameter and click Apply. To delete the global policy, select it in the left pane and click Delete policy.

Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

To overwrite the global space reclaiming policy for a specific source:

1. In the Tiger Bridge Configuration, select the source in the left pane and then click Add policy.
2. In the Policy Type dialog, select Reclaim space and click OK.



Important: If the selected source already has its own space reclaiming policy assigned, you cannot add a new space reclaiming policy, but can edit the existing policy, following the steps below.

3. In the right pane, make sure the Enabled check box is selected and specify the parameters for file access time and size, for used space thresholds, then click Apply.

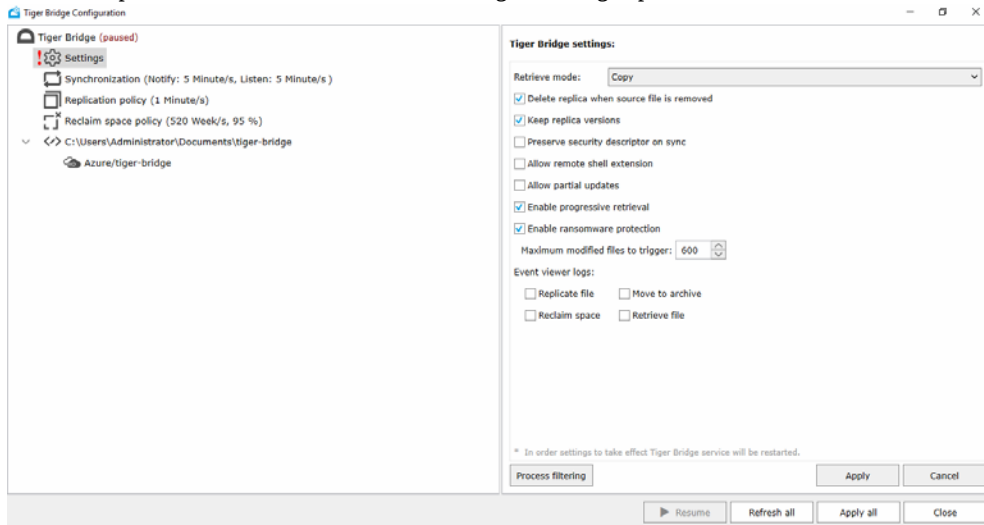
Tip: To make the source use the global space reclaiming policy set for all sources, either disable the space reclaiming policy specified just for it by clearing the Enabled check box in the right pane, or delete the policy by selecting it in the left pane and clicking Delete policy.

Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

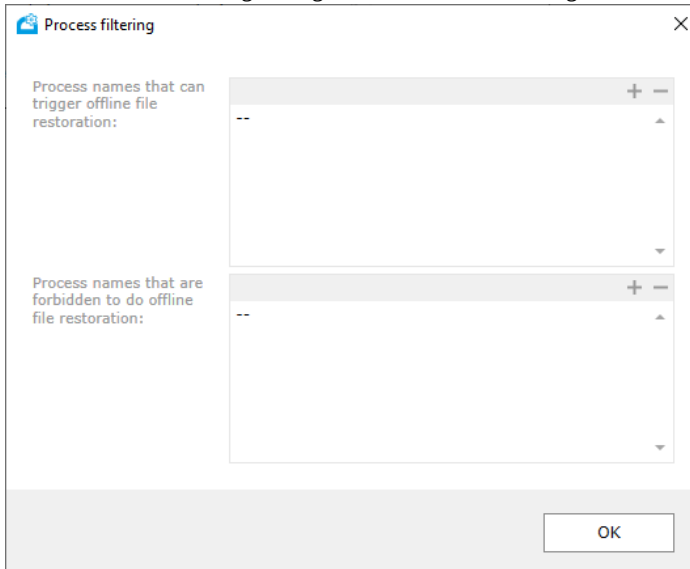
Get Started with Tiger Bridge Using the Configuration

To configure the processes, which can or cannot trigger retrieval of files from the target:

1. in the left pane and then click Process Filtering in the right pane.



2. In the Process Filtering dialog, do one of the following:



- Enter the name of a process in either the list of processes allowed to trigger the retrieving of nearline files or in the list of processes forbidden to trigger the retrieving of nearline files and click OK.

Tip: Click the + button on top of each list to place the cursor at the end of each respective list.

- Delete a process from either list and then click OK.

Tip: Click the - button on top of each list to remove the last process of the respective list.

3. In the Tiger Bridge Configuration, click Apply.

Configure Data Archiving

Note: Currently, Tiger Bridge supports data archiving only on cloud storage targets with the exception of Backblaze B2 cloud storage, Wasabi cloud storage and S3-compatible targets, which do not provide data archiving.

To enable automatic data archiving, you should configure a data archiving policy for a specific pair of source and target. On targets, which allow third-party policies to manage the moving of data from their hot/cool tier to the archival tier, you can use Tiger Bridge's archive policy. Currently, the following targets allow using Tiger Bridge's own archiving policy:

- Microsoft Azure
- Amazon S3
- Google Cloud

Important: If you have configured Tiger Bridge to use as a target the archival tier (Amazon S3 Glacier/Glacier Deep Archive or Azure Archive) or the storage class of the Google Cloud bucket paired with the source is Archive, there is no need to configure archiving policy as files from the source will be replicated directly on the archival tier. Additionally, if you want to reclaim space on your source by replacing a replicated file with a stub, you must configure space reclaiming policy instead. Thus, when Tiger Bridge reclaims space on your source it will replace replicated files with offline files instead of nearline files.

On targets, which do not support third-party policies for moving of data from their hot/cool tier to the archival tier, you can synchronize Tiger Bridge with the target's own archiving policy and thus let it verify when a file is moved to the archival tier and update the status of such files on the source to offline. Currently, you can synchronize Tiger Bridge with the target's own archiving policy on IBM Cloud Object Storage Archive and S3-compatible object storage, which supports data archiving.

Configure Tiger Bridge Archiving Policy

Note: To see how to configure the Tiger Bridge archiving policy using the command-line interface of Tiger Bridge, refer to "Automatic Data Archiving" on page 124.

Tiger Bridge's archiving policy allows you to specify which files on your source must be moved to the archival tier of the target and replaced by offline counterpart on the source. The policy uses two parameters - minimal file size and time interval for which the file has not been accessed on the source. For example, if you set the file size threshold to 10MB and the time interval to 2 weeks,

Get Started with Tiger Bridge Using the Configuration

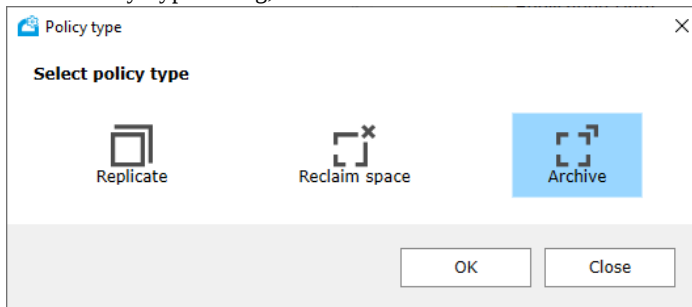
Tiger Bridge will move to the archival tier all replicated files with size 10MB or above that have not been accessed for at least 2 weeks and will replace them on the source with offline files, thus designating that they can be retrieved only manually. By default, Tiger Bridge replaces files with offline files only if they are bigger than 10MB and if they have not been accessed for more than 50 weeks. Tiger Bridge processes the queue of replicated files scheduled for archiving starting from the ones, which are least recently accessed.

Note: *You cannot specify a global archiving policy, valid for all targets. You can configure an archiving policy only for a specific pair of source and target.*

Important: *With a NAS source, offline files are located in the control folder and not on the network share itself. To rehydrate an offline file, you need to perform the operation on the stub file in control folder. To learn more about data archiving on NAS sources, refer to “NAS Source Prerequisites and Setup” on page 36.*

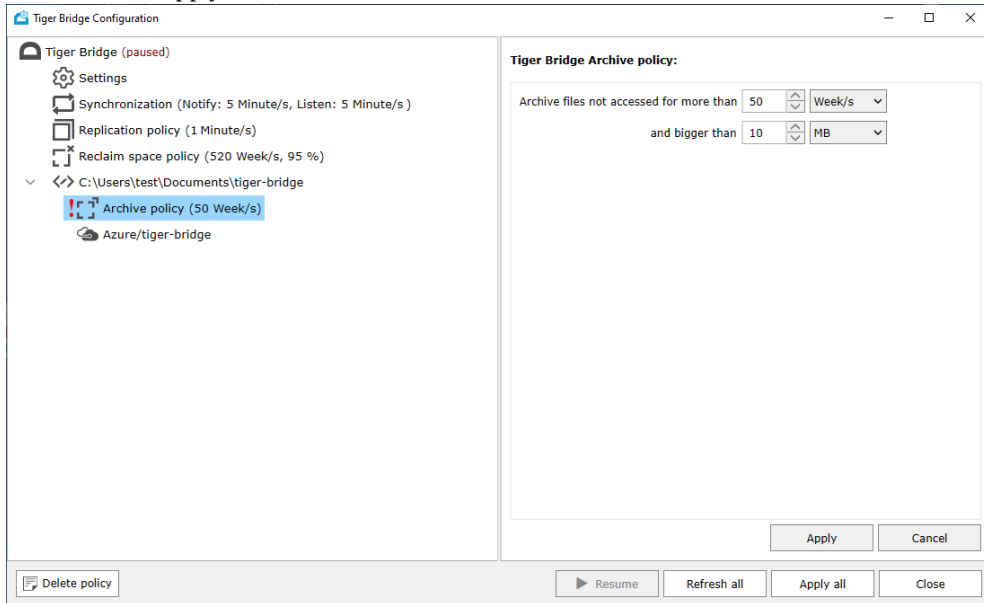
To configure Tiger Bridge archiving policy:

1. In the Tiger Bridge Configuration, select the source in the left pane and then click Add policy.
2. In the Policy Type dialog, select Archive and click OK.



Note: *Archive policy is greyed out, when the target does not provide archival tier.*

3. In the right pane, specify the minimum file size and for how long a file should not have been accessed on the source in order to be moved to the archival tier and replaced with an offline file and then click **Apply**.



Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Synchronize Tiger Bridge with the Target’s Own Archiving Policy

Note: Currently, you can synchronize Tiger Bridge with the target’s own archiving policy only on IBM Cloud Object Storage Archive and S3-compatible object storage, which supports data archiving.

On targets, which do not allow third-party policies to move data between the hot/cool tier and the archival tier, you can synchronize Tiger Bridge with the target’s own policy by specifying at what interval Tiger Bridge should check for files moved to the archival tier in order to update their status on the source to offline.

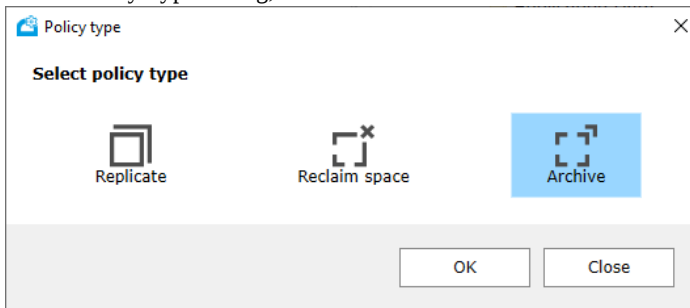
You can also overwrite the target’s own archiving policy by synchronizing it with the time interval at which Tiger Bridge checks for files moved to the archival tier. Thus, each time the target’s policy checks for files meeting the criteria for archiving and moves them to archival tier, Tiger Bridge checks which files have been moved and immediately changes their status to offline on your source. For example, if you set Tiger Bridge to check for archived files every 30 days, the target’s policy will move to the archival tier only replicated files which have not been modified on the hot/cool tier within 30 days.

Get Started with Tiger Bridge Using the Configuration

Note: Currently, you can synchronize Tiger Bridge with the target's own archiving policy in the Configuration only.

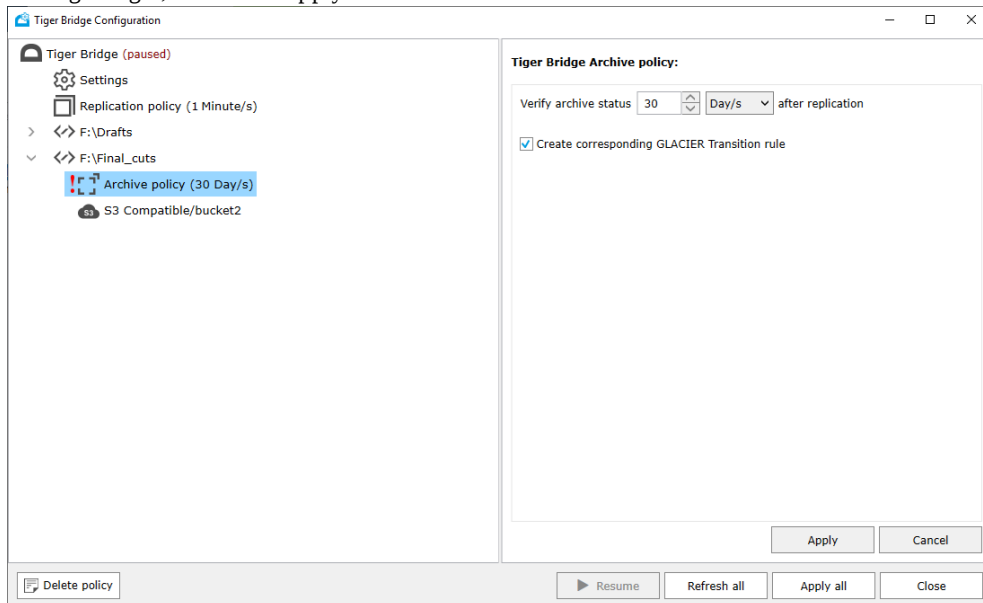
To synchronize Tiger Bridge with the target's own archiving policy:

1. In the Tiger Bridge Configuration, select the source in the left pane and then click Add policy.
2. In the Policy Type dialog, select Archive and click OK.



Note: Archive policy is greyed out, when the target does not provide archival tier.

3. In the right pane, specify the time interval at which Tiger Bridge should check for files moved to the archival tier and optionally, select the “Create corresponding Glacier Transition rule” check box to synchronize the archiving policy of Tiger Bridge with that of the S3-compatible object storage target, then click Apply.



Important: By selecting the check box you overwrite the target rule for moving files to the archival tier, if there is such a rule already configured. If the check box is cleared, you need to configure a transition rule in the interface of the target.

Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Additional Archiving Options

With targets, which allow third-party policies for moving files from the hot/cool tier to the archival tier, you can manually replace replicated files with offline ones on your source volume and thus free space on it. You can also manually rehydrate files (move them from the archive to the hot/cool tier) and allow Tiger Bridge to retrieve them from the target on demand, when a user or application attempts to access them on the source.

On targets, which do not allow third-party policies to move files between the hot/cool tier and the archival tier, you can manually check if the status of a replicated file on your source needs to be changed to offline.

For more details, see “Manually Manage Data” on page 153.

You can also fine-tune your data archiving workflow by configuring several advanced settings. For more information, refer to “Advanced Space Reclaiming and Data Archiving Settings” on page 141.

Configure Active Sync

Note: To see how to configure active sync using the command-line interface of Tiger Bridge, refer to “Active Sync” on page 125.

Tiger Bridge's active sync allows you to synchronize the contents of two or more sources, each on a separate computer, through a common target. For the purpose you must pair all sources with the same target and configure the active sync policy. The active sync mechanism operates using two parameters - the time interval at which a source sends notifications to other sources about changes to its content on the target, and the time interval at which a source checks for notifications from other sources about modified content (new replicated data available, deleted content, etc.) on the target. After a source receives a notification for updated contents from other sources, Tiger Bridge automatically creates a nearline file for each new file replicated from other sources. Nearline files are created on the source on demand, only upon receiving a request (by a user or application) for access to the directory, which should contain them and each nearline file can then be retrieved manually or automatically, should a user or application attempt to open it. You can also set Tiger Bridge to begin retrieving new nearline files immediately after it finishes the synchronization. This can be useful when you are synchronizing the contents of a NAS source, as data from other sources will otherwise appear as nearline files in the NAS source's control folder.

Get Started with Tiger Bridge Using the Configuration

Note: *If you have configured Tiger Bridge to use as a target an archival tier (Amazon S3 Glacier/ S3 Glacier Deep Archive or Azure Archive), the contents of the synchronized sources is updated with offline files instead of nearline.*

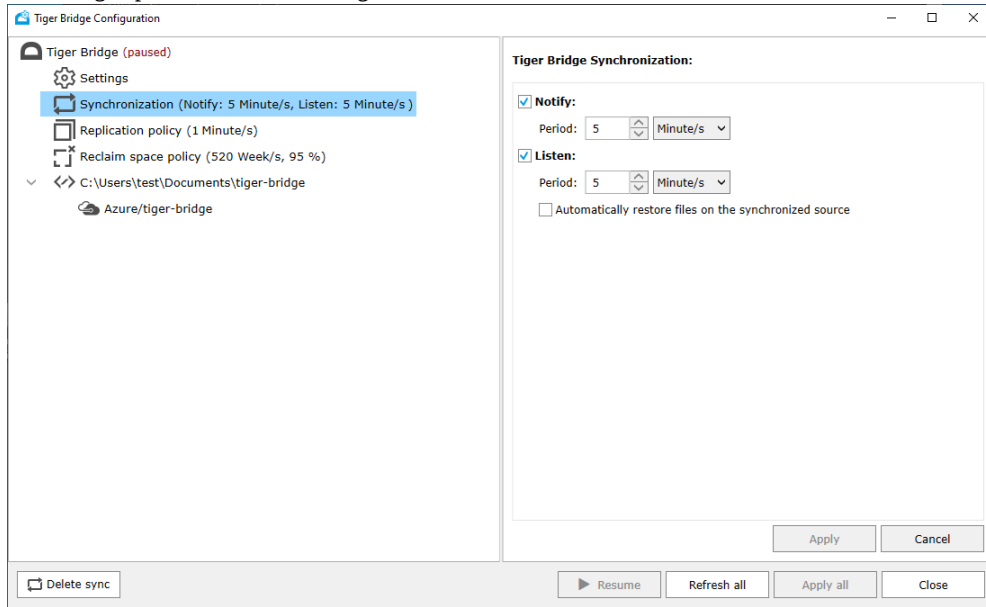
You can use a global active sync policy, valid for all sources paired with the same target or you can create a separate policy, valid only for the source it is assigned to. You can choose to enable just one of the parameters on specific computers - thus one computer can be set to just send notifications about changes introduced on its source, letting sources on other computers synchronize their contents with these changes, but disable notifications from other sources paired with the same target, thus not synchronizing its own content with the changes introduced on other sources.

Additionally, you set Tiger Bridge to keep a file's security descriptor when it is being retrieved on other sources. It is advisable to enable this option only if all sources are in the same Active Directory domain.

To allow for the proper contents synchronization, it is advisable on all sources to set up Tiger Bridge operation mode parameters in such a way that a file on the target is not deleted when it is retrieved on one of the sources and also not to delete the file from the target, if it is deleted on any of the sources. Otherwise, other sources may fail to retrieve the respective file, even though the retrieve mode and delete mode on them are set to keep the replica. For more information, refer to "Configure Operation Mode" on page 100.

To configure global active sync policy:

1. In the Tiger Bridge Configuration, select Tiger Bridge in the left pane and then click Add sync.
2. In the right pane, do the following:



- Below Notify, enter the time interval at which the computer should send notifications to other computers about changes to its source contents and select the unit of measure in the drop-down box beside the Period box.

- Below Listen, enter the time interval at which the computer should check for notifications from other computers about changes in the contents of their sources and select the unit of measure in the drop-down box beside the Period box.

Note: It is advisable to leave both the Notify and the Listen check boxes selected, when specifying the global active sync policy.

- Select the “Automatically restore files on the synchronized source” check box, to let Tiger Bridge begin retrieving the files immediately after contents is synchronized.

3. Click Apply.

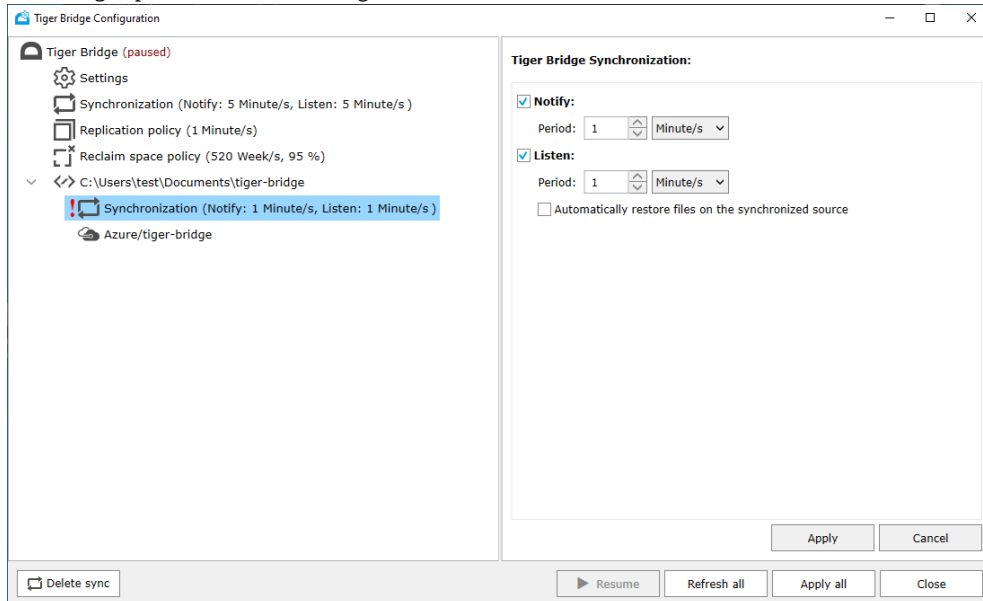
The global active sync policy is valid for all sources, which do not have their own policy assigned. To edit the global policy, simply select it in the left pane, edit the desired parameter and click Apply.

Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

Get Started with Tiger Bridge Using the Configuration

To overwrite the global active sync policy for a specific source:

1. In the Tiger Bridge Configuration, select the source in the left pane and click Add sync.
2. In the right pane, do the following:



- Below Notify, enter the time interval at which the computer should send notifications to other computers about changes to its source contents and select the unit of measure in the drop-down box beside the Period box.

- Below Listen, enter the time interval at which the computer should check for notifications from other computers about changes in the contents of their sources and select the unit of measure in the drop-down box beside the Period box.

Note: You can disable either the Notify check box or the Listen check box for a selected source, thus configuring this computer to only send notifications about changes to the contents at its source side, but not letting it synchronize its source contents with changes from other sources and vice versa. To disable active sync for this pair of source and target, disable both the Notify and Listen check boxes.

- Select the “Automatically restore files on the synchronized source” check box, to let Tiger Bridge begin retrieving the files immediately after contents is synchronized.

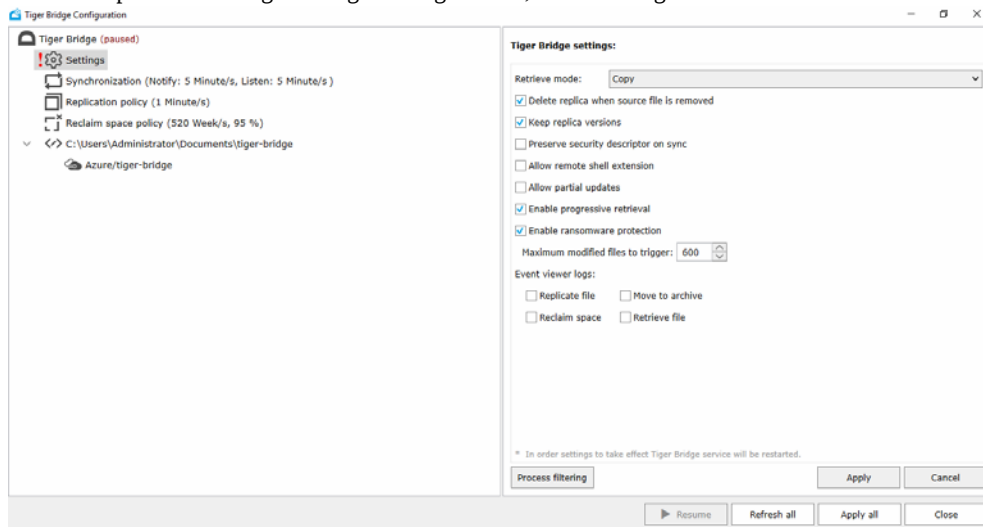
3. Click Apply.

To edit the active sync policy for this source, simply select it in the left pane, edit the desired parameter and click Apply. To delete the policy and let the source use the global active sync policy, select it in the left pane and then click Delete sync.

Note: By default, all automatic Tiger Bridge operations are initially paused. To resume them, follow the steps in “Pause/Resume Automatic Tiger Bridge Operations” on page 102.

To set Tiger Bridge to preserve the files security descriptor on all sources:

1. In the left pane of the Tiger Bridge Configuration, click Settings.



2. Do one of the following:
 - Select the “Preserve security descriptor on sync” check box, to keep the security of all files on each source after contents synchronization.
 - Clear the “Preserve security descriptor on sync” check box, to retrieve all files without security on each source after contents synchronization.
3. Click Apply.

Configure Versioning

By default, if a replicated file is modified on the source and is queued for replication again, the new copy on the target overwrites the previous one. As long as your target supports versioning, you can set Tiger Bridge to not overwrite the replica on the target and allow the versioning software to keep each copy as a separate version.

Important: Before enabling versioning in Tiger Bridge, make sure you have enabled versioning on your target, following the instructions of your cloud object storage provider.

When versioning is enabled, using Tiger Bridge you can retrieve from the target a specific version of a replicated file or restore the contents of a whole folder to the latest submitted version of all files

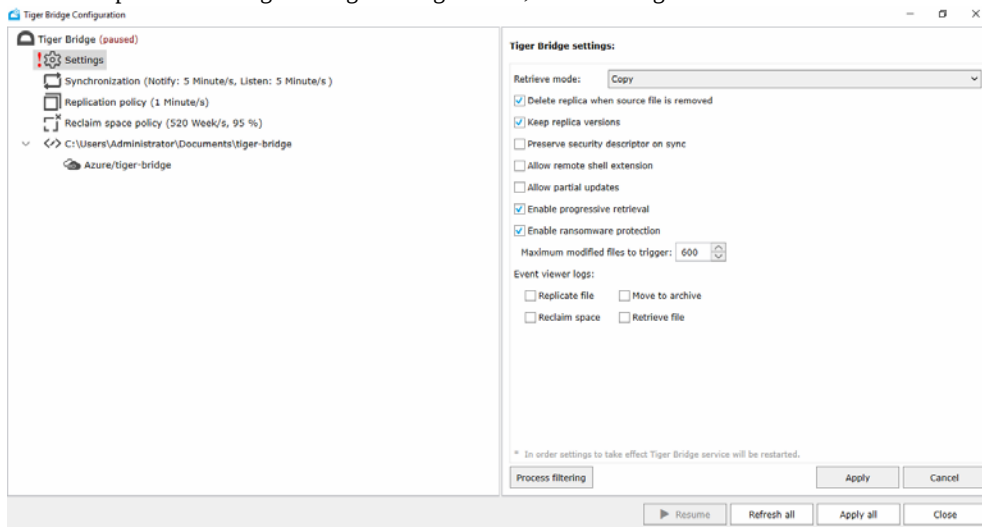
Get Started with Tiger Bridge Using the Configuration

in it by specific time. For more information refer to “Manage Files and Folders Versions” on page 162.

Should you decide to disable versioning after it had been enabled, all versions of a specific replicated file will be kept on the target, but you will be able to retrieve them using the target provider’s own method. Additionally, any modifications of a file on the source will overwrite only the latest version of the file on the target and you will be able to retrieve only this version using Tiger Bridge.

To enable/disable versioning during replication:

1. In the left pane of the Tiger Bridge Configuration, click Settings.



2. Do one of the following:
 - Select the “Keep replica versions” check box, to enable versioning.
 - Clear the “Keep replica versions” check box, to disable versioning.
3. Click Apply.

Configure Operation Mode

Note: To see how to configure Tiger Bridge operation mode parameters using the command-line interface, refer to “Operation Mode Parameters” on page 127.

There are two operation mode parameters that you can specify:

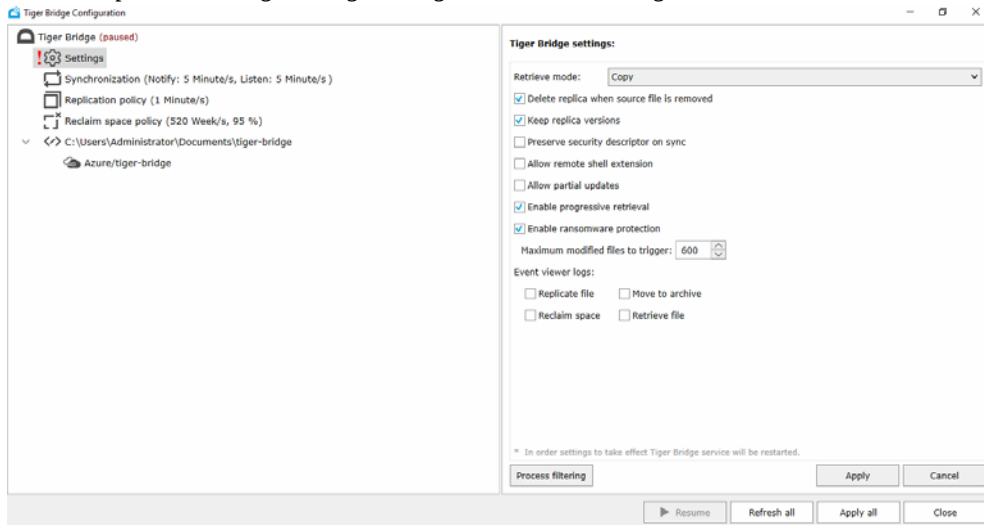
retrieve mode — By default, Tiger Bridge is set up to keep the replica on the target when you retrieve it on the source. You can set Tiger Bridge to remove file replica from target when it is successfully retrieved on the source, which is useful when you want to configure the target as an extension to your source.

delete mode — By default, when a file is deleted from the source, Tiger Bridge automatically deletes its replica from the target as well. As long as soft delete is supported and enabled on your target, you can restore a deleted file, following the steps in “Undelete Data on the Source” on page 160. In case your target provider does not support soft deletion of data, to ensure against accidental deletion of valuable data, you can set Tiger Bridge to delete just the instance of the file on the source, but keep the copy on the target. In this case, to retrieve a file deleted only from the source, you have to manually synchronize the contents of the source and the target (see “Synchronize Data on the Source and the Target” on page 111).

Note: When you set Tiger Bridge to delete just the instance of the file on the source, to delete it from the target as well you should access the target and manually delete the file.

To configure retrieve mode:

1. In the left pane of the Tiger Bridge Configuration, click Settings.



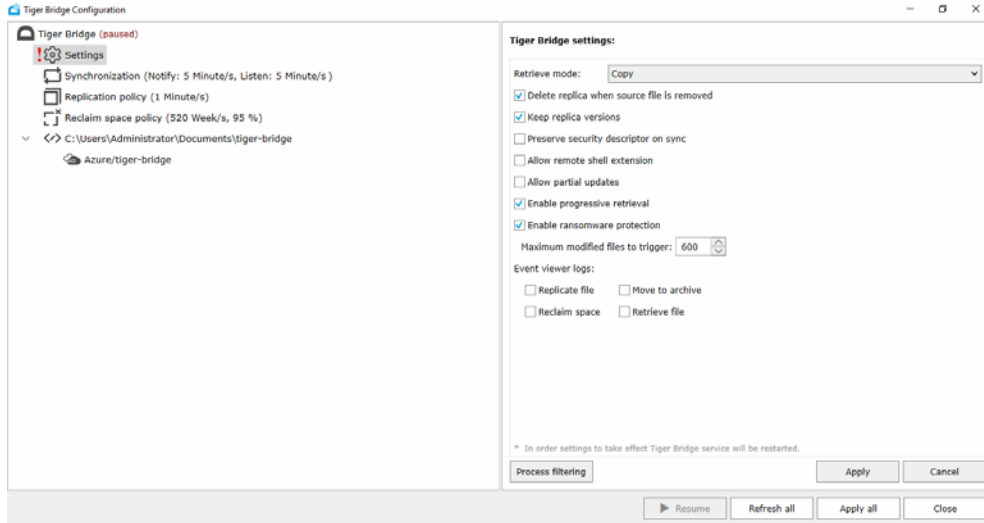
2. In the Retrieve mode drop-down box, do one of the following:
 - To let Tiger Bridge keep the replica on the target, when the file is successfully retrieved on the source volume, select Copy.
 - To let Tiger Bridge remove the replica from the target, when the file is successfully retrieved on the source volume, select Move.

Get Started with Tiger Bridge Using the Configuration

3. Click Apply.

To configure delete mode setting:

1. In the left pane of the Tiger Bridge Configuration, click Settings.



2. Do one of the following:

- Select the “Delete replica when source file is removed” check box, to let Tiger Bridge remove the replica from the target, upon deleting the file from the source volume.
- Clear the “Delete replica when source file is removed” check box, to let Tiger Bridge keep the replica on the target, upon deleting the file from the source volume.

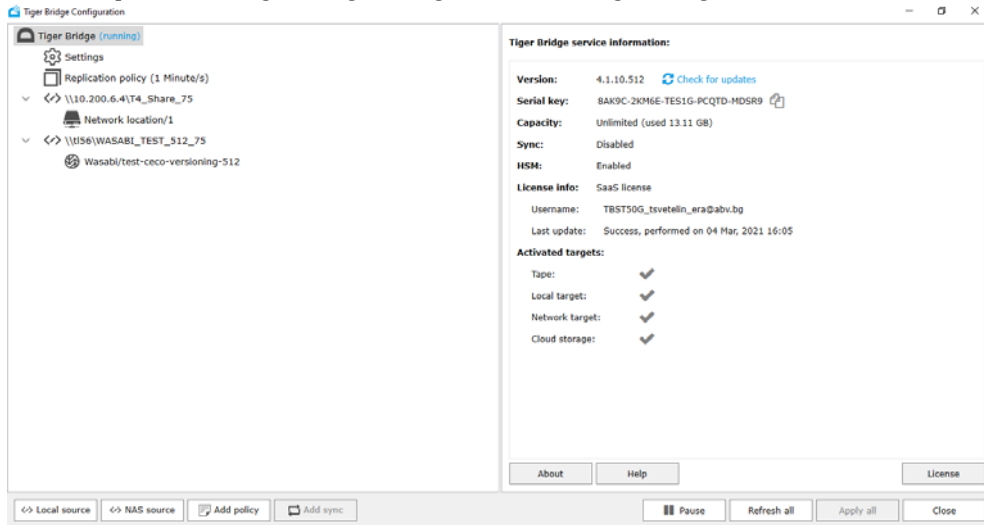
3. Click Apply.

Pause / Resume Automatic Tiger Bridge Operations

By default, all automatic data lifecycle operations are initially paused and even though you may have configured the policies for data replication, space reclaiming and archiving, Tiger Bridge does not manage any data until you resume the operations. You can pause and resume all automatic Tiger Bridge operations at any time, following the steps below.

To pause/resume automatic Tiger Bridge operations:

1. In the left pane of the Tiger Bridge Configuration, click Tiger Bridge.



2. Do one of the following:

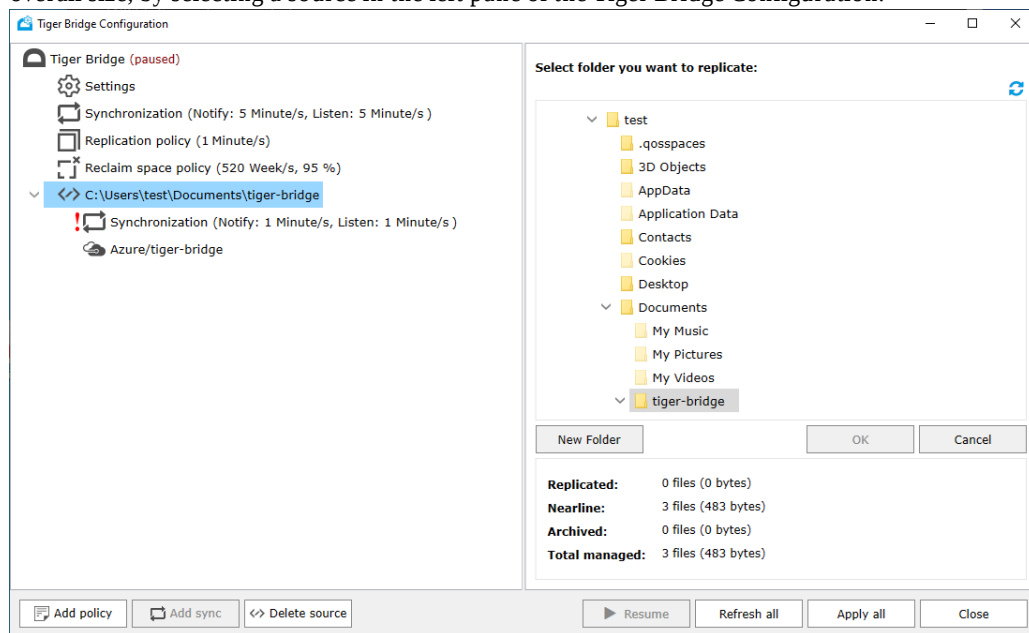
- To resume all automatic Tiger Bridge operations, click Resume in the taskbar.
- To pause all automatic Tiger Bridge operations, click Pause in the taskbar.

Monitor Data Management Statistics

Note: To see how to monitor data management statistics, using the command-line interface, refer to “Monitor Data Management Statistics” on page 128.

Get Started with Tiger Bridge Using the Configuration

You can view per-source statistics about the number of files managed by Tiger Bridge and their overall size, by selecting a source in the left pane of the Tiger Bridge Configuration.



The statistics field gives you the following information about data on the selected source:

Replicated — the number and overall size of files, which have copies both on the source and the target.

Nearline — the number and overall size of files, which have copies only on the nearline tier of the target i.e. nearline stub files.

Archived — the number and overall size of files, which have copies on the archival tier of the target i.e. replicated files, which have copies on both the source and the archival tier as well as offline stub files.

Total managed — the number and overall size of files Tiger Bridge has already managed as well as of files potentially manageable by Tiger Bridge, with the exception of files in excluded locations. You can use information in this field to calculate what part of the total storage capacity associated with your Tiger Bridge license is used on the selected source.

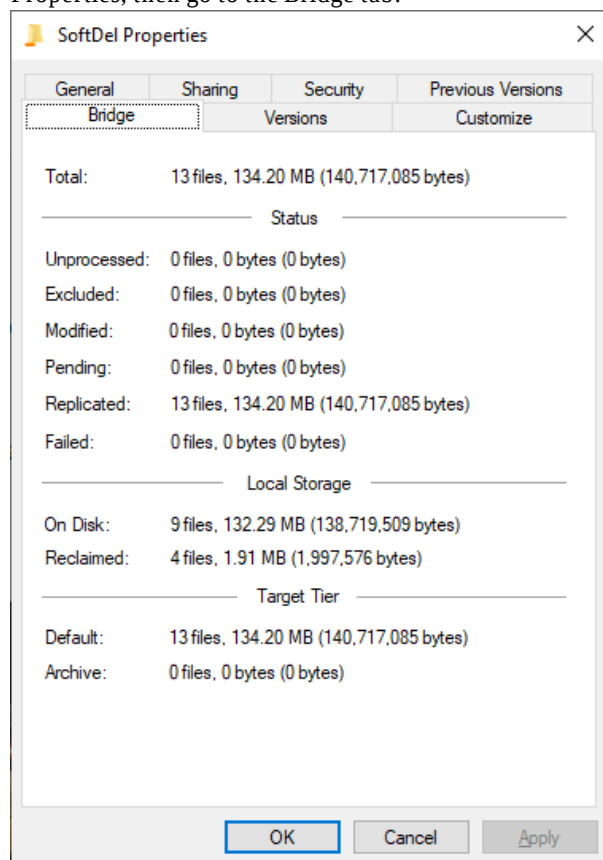
Note: As long as the Tiger Bridge shell extension is installed, you can keep track of individual files' and folders' status in Windows Explorer. For more information, see "Manually Manage Data" on page 153.

The Tiger Bridge shell extension also gives you statistic about the number of files and their size on a source or just a folder on it:

- total number of files and their size
- size and number of unprocessed, excluded, modified, pending, replicated and failed files
- number of files and their size on the disk of the source
- number of files and their size, which have been reclaimed on the source
- number of files and their size, which are on the nearline tier of the target
- number of files and their size, which are on the archival tier of the target

Note: *You cannot view per-source statistics if the root of a volume is added as a source.*

To view the Tiger Bridge shell extension statistics, right-click the source or a folder on it and select Properties, then go to the Bridge tab:



Get Started with Tiger Bridge Using the Configuration

Note: *Statistics in the Source Properties dialog are updated dynamically, allowing you to keep track of data retrieval from the target, for example.*

4

Get Started with Tiger Bridge Using the Command-line Interface

<i>Activate Tiger Bridge</i>	<i>108</i>
<i>Pair Source with a Target</i>	<i>109</i>
<i>Refine the List of Automatically Managed Locations</i>	<i>120</i>
<i>Automatic Data Replication</i>	<i>121</i>
<i>Space Reclaiming</i>	<i>122</i>
<i>Automatic Data Archiving</i>	<i>124</i>
<i>Active Sync</i>	<i>125</i>
<i>Operation Mode Parameters</i>	<i>127</i>
<i>Monitor Data Management Statistics</i>	<i>128</i>
<i>Disable Tiger Bridge</i>	<i>129</i>

Activate Tiger Bridge

You can activate Tiger Bridge using one of the following options:

- software activation key;
- software protection dongle, if such is detected;
- Software as a service (SaaS) license;

To view the activation status of Tiger Bridge on your computer:

In command prompt, execute the following:

```
tiercli license info
```

Tiger Bridge displays the activation status of the product and the targets allowed for your license.

To activate Tiger Bridge with a software activation key:

1. To display the Tiger Bridge serial key, execute the following:

```
tiercli license info
```
2. Copy the serial number and in a web browser go to
<https://license.tiger-technology.com>.
3. In the home page of the licensing server, enter your order name and password in the corresponding fields, and click Log in.

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

4. In the Licensing Server menu, click Activate License.
5. Paste the serial number and click Generate Activation Key.
6. Copy the activation key generated for your license.
7. In command prompt, execute the following:

```
tiercli license soft <activation key>
```

where <activation key> is the key generated for your serial number on the Tiger Technology licensing server.

To activate a Tiger Bridge SaaS license in command-line:

In command prompt, execute the following:

```
tiercli license saas <username> <password>
```

where <username> and <password> are the username and password for your software subscription.

To activate Tiger Bridge using a software protection dongle in command-line:

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.
Important: *The order name and the password are case sensitive.*
3. Next to the dongle name in the list, click “Download lic file”.
Note: *The dongle name is its number, printed on the dongle itself.*
4. In command prompt, execute the following:
`tiercli license hasp <lic_file_path>`
where <lic_file_path> is the full path to the downloaded license file on your computer.

Pair Source with a Target

In the command-line interface you can set a global target, valid for all sources and overwrite the global setting by assigning a different target for a specific source.

Pair a Source with Microsoft Azure Blob Storage Target

For more details about the parameters you need to provide when pairing a source with Microsoft Azure Blob storage, refer to “Pair a Source with Microsoft Azure Blob Storage Target” on page 109.

To pair a source with Microsoft Azure:

1. In command prompt, set Microsoft Azure as target, by executing the following:
`tiercli config <path to source> target azure <account_name>
<account_key> <blob_endpoint>`
where:
 - <path to source> is the full path to the source;
 - <account_name> is the name of your account for the Azure service;
 - <account_key> is the key for your account for the Azure service;
 - <blob_endpoint> is the URL or IP address of Azure Blob storage provider including the protocol type you will use for access to it (http or https);

For example, to pair volume mounted as drive letter F:\ with Microsoft Azure Blob storage accessible with storage account `rwaccount` and account key:
`OPEkmf7v9ZHZPvNy2HWoxhDZu6QSFw011Cxam+1toPegcAyw9YoJu8suuA/
QvDPQ4WdbekaTuoDn0wmDwoZ6pg==`, and the Azure Blob storage provider is accessible as

Get Started with Tiger Bridge Using the Command-line Interface

test.blob.core.windows.net through https protocol, execute the following:
tiercli config F: target azure rwaccount
OPEkmf7v9ZHZPvNy2HWoxhDZu6QSFw01lCxam+1toPegcAyw9YoJu8suuA/
QvDPQ4WdbekaTuoDn0wmDwoZ6pg== https://test.blob.core.windows.net/

Note: To set Microsoft Azure as global target, valid for all sources, which are not paired with a specific target, simply execute the above command without specifying a source:

```
tiercli config target azure <account_name> <account_key>  
<blob_endpoint>
```

2. Pair the source with its container on the target, by executing the following:

```
tiercli config <path to source> container <container name>
```

For example, to pair volume “Projects” mounted as drive letter F: to a container “container1” on the Azure object storage, execute the following:

```
tiercli config F: container container1
```

Note: If you want to pair other source volumes with the same target, repeat the step above for each new source volume, changing the name of the container on the Azure object storage.

3. Check if all settings are correctly configured, by executing the following:

```
tiercli config show
```

4. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:

```
tiercli config reload
```

Important: Until you specify the list of included/excluded locations on the source, Tiger Bridge doesn't automatically manage any data on the source. For information refer to “Refine the List of Automatically Managed Locations” on page 120.

Note: Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. For more information, see “Configure Automatic Data Replication” on page 83.

Pair a Source with Amazon S3 Target

For more details about the parameters you need to provide when pairing a source with Amazon S3 object storage, refer to “Pair a Source with Amazon S3 Target” on page 110.

To pair a source with Amazon S3 object storage in the command-line interface:

1. In command prompt, execute the following:

```
tiercli config <path to source> target s3 <access_id> <secret_key>  
<server>
```

where:

- <path to source> is the full path to the source;
- <access_id> is the IAM user access key ID used for access to this server;

- `<secret_key>` is the IAM user secret access key for access to this server;
- `<host name>` is the URL or IP address of the S3 object storage server;

Note: To use Tiger Bridge with an acceleration-enabled buckets, include “accelerate” in the server URL as described in the Amazon documentation.

For example, to pair volume mounted as drive letter F:\ with Amazon’s web storage service (s3.amazonaws.com), accessible with access key ID: AKIAI633LOZJPNTZUIBA and secret access key: Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4Lff, execute the following:

```
tiercli config F: target s3 AKIAI633LOZJPNTZUIBA
Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4Lff s3.amazonaws.com
```

Note: To set Amazon S3 object storage as global target, valid for all sources, which are not paired with a specific target, simply execute the above command without specifying a source:

```
tiercli config target s3 <access_id> <secret_key> <server>
```

2. Pair the source with its designated bucket on the target, by executing the following:
- ```
tiercli config <path to source> container <name of the bucket on the S3 object storage>
```

For example, to pair the local volume “Projects” mounted as drive letter F:\ with S3 object storage and replicate data in the bucket named “replicas”, execute the following:

```
tiercli config F: container replicas
```

**Note:** If you want to pair other source volumes with the same target, repeat the step above for each new source volume, changing the name of the bucket on the S3 object storage.

3. Check if all settings are correctly configured, by executing the following:
- ```
tiercli config show
```
4. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:
- ```
tiercli config reload
```

**Important:** Until you specify the list of included/excluded locations on the source, Tiger Bridge doesn’t automatically manage any data on the source. For information refer to “Refine the List of Automatically Managed Locations” on page 120.

**Note:** Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. For more information, see “Configure Automatic Data Replication” on page 83.

## Pair a Source with IBM Cloud Object Storage Target

For more details about the parameters you need to provide when pairing a source with IBM cloud object storage, refer to “Pair a Source with IBM Cloud Object Storage Target” on page 111.

### To pair a source with IBM cloud object storage:

1. In command prompt, set IBM cloud object storage as target, by executing the following:  
`tiercli config <path to source> target icos <access_id> <secret_key>  
<accesser IP> [alternative accesser IP] [alternative accesser IP] ...`

where:

- <path to source> is the full path to the source;
- <access\_id> is the Access Key ID used for access to this server;
- <secret\_key> is the Secret Access Key for access to this server;
- <accesser IP> is the URL or IP address of the main IBM cloud object storage server;
- [alternative accesser IP] is any alternative IP address through which you can access the server providing access to your account for the IBM cloud object storage;

**Note:** You can add as many alternative IP addresses for access to the IBM cloud object storage server, keeping in mind that the main IP address for access to it must be specified first in the command.

For example, to pair volume mounted as drive letter F:\ with an IBM cloud object storage server accessible through main IP address 10.200.4.10 and additional IP address 10.200.4.12, accessible with Access Key ID: AKIAI633LOZJPNTZUIBA and Secret Access Key ID:

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, execute the following:

```
tiercli config F: target icos AKIAI633LOZJPNTZUIBA
```

```
Y2n1rXwda3T9yB7DEE7hRfTC6sMP83jeecwd4LfF 10.200.4.10 10.200.4.12
```

**Note:** To set IBM cloud object storage as global target, valid for all sources, which are not paired with a specific target, simply execute the above command without specifying a source:

```
tiercli config target icos <access_id> <secret_key> <accesser IP>
[alternative accesser IP] [alternative accesser IP] ...
```

2. Pair the source with its container on the target, by executing the following:  
`tiercli config <path to source> container <name of the bucket on the  
IBM cloud object storage server>`

For example, to pair volume “Projects” mounted as drive letter F:\ with an IBM cloud object storage server and replicate data in the bucket named “replicas“, execute the following:

```
tiercli config F: container replicas
```

**Note:** If you want to pair other source volumes with the same target, repeat the step above for each new source volume, changing the name of the bucket on the IBM cloud object storage.

3. Check if all settings are correctly configured, by executing the following:  
`tiercli config show`
4. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:  
`tiercli config reload`

**Important:** *Until you specify the list of included/excluded locations on the source, Tiger Bridge doesn't automatically manage any data on the source. For information refer to "Refine the List of Automatically Managed Locations" on page 120.*

**Note:** *Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. For more information, see "Configure Automatic Data Replication" on page 83.*

## Pair a Source with Backblaze Target

For more details about the parameters you need to provide when pairing a source with Backblaze B2 cloud storage, refer to "Pair a Source with Backblaze Target" on page 113.

### To pair a source with Backblaze B2 cloud storage:

1. In command prompt, execute the following:

```
tiercli config <path to source> target b2 <account_id>
<application_key>
```

where:

- <path to source> is the full path to the source;
- <account\_id> is the Backblaze keyID, used for access to the object storage;
- <application\_key> is the Backblaze application key, used for access to the object storage;

For example, to pair volume mounted as drive letter F:\ with Backblaze B2 cloud storage, accessible with key ID: 63cd7057483d and application key:

000d6f3065670683d6250863c0746278cbbad71771, execute the following:

```
tiercli config F: target b2 63cd7057483d
000d6f3065670683d6250863c0746278cbbad71771
```

**Note:** *To set Backblaze B2 cloud storage as global target, valid for all sources, which are not paired with a specific target, simply execute the above command without specifying a source:*  
 tiercli config target b2 <account\_id> <application\_key>

2. Pair the source with its designated bucket on the target, by executing the following:  
 tiercli config <path to source> container <name of the bucket on the Backblaze cloud>

For example, to pair the local volume "Projects" mounted as drive letter F:\ with Backblaze B2 cloud storage and replicate data in the bucket named "replicas", execute the following:

```
tiercli config F: container replicas
```

**Note:** *If you want to pair other source volumes with the same target, repeat the step above for each new source volume, changing the name of the bucket on the Backblaze storage.*

3. Check if all settings are correctly configured, by executing the following:  
 tiercli config show

Get Started with Tiger Bridge Using the Command-line Interface

4. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:  
`tiercli config reload`

**Important:** *Until you specify the list of included/excluded locations on the source, Tiger Bridge doesn't automatically manage any data on the source. For information refer to "Refine the List of Automatically Managed Locations" on page 120.*

**Note:** *Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. For more information, see "Configure Automatic Data Replication" on page 83.*

## Pair a Source with S3-compatible Object Storage Target

For more details about the parameters you need to provide when pairing a source with S3-compatible object storage, refer to "Pair a Source with S3-compatible Object Storage Target" on page 114.

### To pair a source volume with S3-compatible object storage target:

1. In command prompt, set S3-compatible object storage as target, by executing the following:  
`tiercli config <path to source> target s3compat <access_id>  
<secret_key> <server>`

where:

- <path to source> is the full path to the source;
- <access\_id> is the user access key ID used for access to this server;
- <secret\_key> is the user secret access key for access to this server;
- <server> is the URL or IP address of the S3-compatible object storage server;

For example, to pair volume mounted as drive letter F:\ with a provider of S3-compatible object storage accessible through IP address 10.200.6.30, access key ID: AKIAI633LOZJPNTZUIBA and secret access key ID: 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, execute the following:

```
tiercli config F: target s3compat AKIAI633LOZJPNTZUIBA
Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4LfF 10.200.6.30
```

**Note:** *To set S3-compatible object storage as global target, valid for all sources, which are not paired with a specific target, simply execute the above command without specifying a source:  
`tiercli config target s3compat <access_id> <secret_key> <server>`*

2. Pair the source with its container on the target, by executing the following:  
`tiercli config <path to the source> container <name of the bucket on the S3-compatible object storage>`

For example, to pair a volume “Projects” mounted as drive letter F:\ to an S3-compatible object storage and replicate data in the bucket named “replicas”, execute the following:

```
tiercli config F: container replicas
```

**Note:** *If you want to pair other source volumes with the same target, repeat the step above for each new source volume, changing the name of the bucket on the S3-compatible object storage.*

3. Check if all settings are correctly configured, by executing the following:  
`tiercli config show`
4. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:  
`tiercli config reload`

**Important:** *Until you specify the list of included/excluded locations on the source, Tiger Bridge doesn't automatically manage any data on the source. For information refer to “Refine the List of Automatically Managed Locations” on page 120.*

**Note:** *Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. For more information, see “Configure Automatic Data Replication” on page 83.*

## Pair a Source with BlackPearl Object Storage Target

For more details about the parameters you need to provide when pairing a source with Spectra BlackPearl Deep Storage Gateway, refer to “Pair a Source with BlackPearl Object Storage Target” on page 115.

### To pair a source with BlackPearl object storage:

1. In command prompt, set BlackPearl object storage as target, by executing the following:  
`tiercli config <path to source> target blackpearl <access_id>  
<secret_key> <endpoint>`

where:

- <path to source> is the full path to the source;
- <access\_id> is the Access Key ID used for access to the BlackPearl server;
- <secret\_key> is the Secret Access Key for access to the BlackPearl server;
- <endpoint> is the URL or IP address of the BlackPearl server;

For example, to pair volume mounted as drive letter F:\ with a BlackPearl object storage server accessible through IP address 10.200.6.30, Access Key ID: AKIAI633LOZJPNTZUIBA and

## Get Started with Tiger Bridge Using the Command-line Interface

Secret Access Key ID: Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4LFF, execute the following:

```
tiercli config F: target blackpearl AKIAI633LOZJPNTZUIBA
Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4LFF 10.200.6.30
```

**Note:** To set BlackPearl object storage as global target, valid for all sources, which are not paired with a specific target, simply execute the above command without specifying a source:  
`tiercli config target blackpearl <access_id> <secret_key> <endpoint>`

2. Pair the source with its container on the target, by executing the following:  
`tiercli config <path to source> container <name of the bucket on the BlackPearl object storage>`

For example, to pair a volume “Projects” mounted as drive letter F:\ to a BlackPearl object storage and replicate data in a bucket named “replicas”, execute the following:

```
tiercli config F: container replicas
```

**Note:** If you want to pair other source volumes with the same target, repeat the step above for each new source volume, changing the name of the bucket on the BlackPearl object storage.

3. Check if all settings are correctly configured, by executing the following:  
`tiercli config show`
4. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:  
`tiercli config reload`

**Important:** Until you specify the list of included/excluded locations on the source, Tiger Bridge doesn't automatically manage any data on the source. For information refer to “Refine the List of Automatically Managed Locations” on page 120.

**Note:** Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. For more information, see “Configure Automatic Data Replication” on page 83.

## Pair a Source with Coeus Target

For more details about the parameters you need to provide when pairing a source with Coeus managed digital content library, refer to “Pair a Source with Coeus Target” on page 76.

### To pair a source with Coeus target:

1. In command prompt, set Coeus as target of a particular source, by executing the following:  
`tiercli config <path to source> target era <username> <password>  
“<share path>;<archive folder>;<address>;<port>;<API Key>”`

where:

- <path to source> is the full path to the source;
- <username> is user name with which you can access the Coeus share on the network;

- <password> is the password with which you can access the Coeus share on the network;
- <share path> is the path to the Coeus share on your network;
- <archive folder> is the name of the archive folder of the specified Coeus account;
- <address> is the Coeus address;
- <port> is the port through which the Coeus library is accessible;
- <API Key> is the API key with which the Coeus library is accessible

For example, to pair volume mounted as drive letter F:\ with a Coeus target accessible as share \\server\coeus1 with user name “test”, password “coeuspassword123”, the archive folder name is “wip”, the Coeus library address is “10.24.17.141”, the port through which it is accessible is 99 and the API key for access to it is “96dae217960124398ck676e2c6543140”, execute the following:

```
tiercli config F: target era test coeuspassword123 \\server\coeus1
"wip;10.24.17.141;99;96dae218960144398cb676e2c6543140"
```

2. To pair the source with the watch folder on the Coeus library, execute the following:

```
tiercli config <source path> container "<watch folder>"
```

where:

- <path to source> is the full path to the source;
- <watch folder> is the name of the watch folder associated with your Coeus account;

For example, to pair volume mounted as drive letter F:\ with a Coeus watch folder “incoming”, execute the following:

```
tiercli config F: container "incoming"
```

3. Check if all settings are correctly configured, by executing the following:  
tiercli config show
4. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:  
tiercli config reload

**Important:** Until you specify the list of included/excluded locations on the source, Tiger Bridge does not automatically manage any data on the source. For information refer to “Refine the List of Automatically Managed Locations” on page 120.

**Note:** Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. For more information, see “Configure Automatic Data Replication” on page 83.

## Pair a Source with a Network Share Target

For more details about the parameters you need to provide when pairing a source with SMB/CIFS, refer to “Pair a Source with a Network Share Target” on page 118.

### To pair a source with a network share:

1. In command prompt, set a network share as target, by executing the following:

```
tiercli config <path to source> target network <sharepath> <username>
<password>
```

where:

- <path to source> is the full path to the source;
- <sharepath> is the full path to the SMB/CIFS network share;
- <username> is the name of the account that has Read & Write permissions to the network share;
- <password> is the password of the account that has Read & Write permissions to the network share;

**Note:** As no credentials for access are required for NFS shares, execute the command without specifying username and password, like this:

```
tiercli config <path to source> target network <sharepath> "" ""
```

For example, to pair volume mounted as drive letter F:\ with a SMB/CIFS network share accessible as \\server\share using the following credentials for access to the share - account name: rwaccount and account password: rwaccountpassword, execute the following:

```
tiercli config F: target network \\server\share rwaccount
rwaccountpassword
```

**Important:** The path to the share must be provided without a final backslash.

**Important:** If the account for access to the SMB share is an Active Directory domain account, you must specify it with its full domain name. For example, user@domain.com.

**Note:** To set the network share as global target, valid for all sources, which are not paired with a specific target, simply execute the above command without specifying a source:

```
tiercli config target network <sharepath> <username> <password>
```

2. Pair the source with its designated container on the network share, by executing the following:  
tiercli config <path to source> container <name of the folder on the network share>

For example, to pair volume “Projects” mounted as drive letter F: to a network share and replicate data in the folder “backup” on the network share, execute the following:  
tiercli config F: container backup

**Note:** If you want to pair other source volumes with the same target, repeat the step above for each new source, changing the name of the folder on the network share.

3. Check if all settings are correctly configured, by executing the following:  
`tiercli config show`
4. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:  
`tiercli config reload`

**Important:** *Until you specify the list of included/excluded locations on the source, Tiger Bridge doesn't automatically manage any data on the source. For information refer to "Refine the List of Automatically Managed Locations" on page 120.*

**Note:** *Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. For more information, see "Configure Automatic Data Replication" on page 83.*

## Pair a Source with a Local Volume Target

For more details about the parameters you need to provide when pairing a source with a local volume target, refer to "Pair a Source with a Local Volume Target" on page 119.

### To pair a source with a local volume target:

1. In command prompt, set a local volume as target, by executing the following:  
`tiercli config <path to source> target local set`  
 For example, to pair volume "Projects" mounted as drive letter F: with a local volume target, execute the following:  
`tiercli config F: target local set`  

**Note:** *To set a local volume as a global target, valid for all sources, which are not paired with a specific target, simply execute the above command without specifying a source:*  
`tiercli config target local set`
2. Pair the source with its designated container on the target volume, by executing the following:  
`tiercli config <path to source> container <full path to the folder on the target>`  
 For example, to pair volume "Projects" mounted as drive letter F: with the folder "Projects" in the root of the NTFS volume mounted as drive letter G:, execute the following:  
`tiercli config F: container G:\Projects`  

**Note:** *If you want to pair other source volumes with the same target, repeat the step above for each new source volume, changing the name of the folder on the target volume.*
3. Check if all settings are correctly configured, by executing the following:  
`tiercli config show`
4. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:  
`tiercli config reload`

**Important:** *Until you specify the list of included/excluded locations on the source, Tiger Bridge doesn't automatically manage any data on the source. For information refer to "Refine the List of Automatically Managed Locations" on page 120.*

**Note:** *Until you specify data lifecycle management parameters, Tiger Bridge uses the default global data replication policy for all pairs of source and target. For more information, see "Configure Automatic Data Replication" on page 83.*

## Refine the List of Automatically Managed Locations

**Note:** *For more information about specifying included and excluded locations on your source(s), refer to "Refine the List of Automatically Managed Locations" on page 84.*

When refining the list of automatically managed locations through the command-line interface, you should keep in mind that the list is valid for all sources and as long as at least one included/excluded location is already specified, all other locations not included in the list are not automatically managed, except if they are locations on sources paired with a target through the Tiger Bridge Configuration.

**Important:** *Each time you want to update the list of included/excluded locations, you should specify the full list anew.*

### To specify a list of included and excluded locations:

1. To configure the list of included locations on all sources, from which data should be automatically managed, execute the following:  
`tiercli config include <path to source><path to a subfolder on the source> ...`

**Important:** *You must add all included locations using one command. For the purpose separate each added location with a space. Issuing the command anew will overwrite the previous setting.*

For example, to add to the list of included locations the root of source volume F: and the folder "Data" in the root of source volume G:, execute the following:

```
tiercli config include F: G:\Data
```

**Tip:** *To clear the included locations list and start configuring it anew, execute the following:*  
`tiercli config include ""`

2. To configure the list of excluded locations on all sources, from which data should not be automatically managed, execute the following:  
`tiercli config exclude <path to source><path to a subfolder on the source> ...`

**Important:** You must add all excluded locations using one command. For the purpose separate each added location with a space. Issuing the command anew will overwrite the previous setting.

For example, to add as excluded locations the root of source volume H: and the folder “Drafts”, which is subfolder of the folder “Data” in the root of source volume G:, execute the following:

```
tiercli config exclude H: G:\Data\Drafts
```

**Tip:** To clear the excluded locations list and start configuring it anew, execute the following:

```
tiercli config exclude ""
```

3. Check if all settings are correctly configured, by executing the following:  

```
tiercli config show
```
4. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:  

```
tiercli config reload
```

## Automatic Data Replication

To learn more about Tiger Bridge’s automatic data replication mechanism, refer to “Configure Automatic Data Replication” on page 83.

### To configure automatic data replication:

1. To configure global replication policy, execute the following:  

```
tiercli config policy replicate <period>
```

Where <period> can be the desired period in seconds (s), minutes (m), hours (h), days (d), weeks (w).

For example, to specify that Tiger Bridge should replicate data only after it has not been modified for 36 hours, execute the following:  

```
tiercli config policy replicate 36h
```
2. (optional) To overwrite the global replication policy for a specific source, execute the following:  

```
tiercli config <path to source> policy replicate <period>
```

For example, to specify that data from source volume mounted as drive letter E: should be replicated only after it has not been modified for one day, execute the following:  

```
tiercli config E policy replicate 1d
```
3. Check if all settings are correctly configured, by executing the following:  

```
tiercli config show
```
4. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:  

```
tiercli config reload
```

## Space Reclaiming

To learn more about Tiger Bridge's automatic space reclaiming mechanism, refer to "Configure Space Reclaiming" on page 86.

### To configure automatic space reclaiming:

1. To enable space reclaiming, execute the following:

```
tiercli config policy reclaimspace turn on
```

**Note:** To disable space reclaiming for all source volumes, execute the following:

```
tiercli config policy reclaimspace turn off
```

2. To configure for how long a replicated should not have been accessed in order to be replaced by a nearline file, execute the following:

```
tiercli config policy reclaimspace age <period>
```

Where <period> can be the desired period in seconds (s), minutes (m), hours (h), days (d), weeks (w).

For example, to specify that Tiger Bridge should replace files with nearline files only after they have not been accessed for 36 hours, execute the following:

```
tiercli config policy reclaimspace age 36h
```

3. To configure what is the minimal size of a file for it to be replaced by a nearline file, execute the following:

```
tiercli config policy reclaimspace size <size>
```

Where <size> is the size in bytes (b), KB (k), MB (m), GB (g), TB (t).

For example, to specify that Tiger Bridge should replace files with nearline files only if they are bigger than 1GB, execute the following:

```
tiercli config policy reclaimspace size 1g
```

4. To configure what used space on the source volumes should be reached for Tiger Bridge to trigger space reclaiming, execute the following:

```
tiercli config policy reclaimspace minused <percent>
```

Where <percent> is just the percent value without the % sign.

For example, to specify that Tiger Bridge should begin replacing files with nearline counterparts once used space on the source volumes reaches 65%, execute the following:

```
tiercli config policy reclaimspace minused 65
```

5. To configure what used space on the source volumes should be reached for Tiger Bridge to trigger space reclaiming of all replicated files regardless of their size and last access time,

execute the following:

```
tiercli config policy reclaimspace maxused <percent>
```

Where <percent> is just the percent value without the % sign.

For example, to specify that Tiger Bridge should begin replacing all files with nearline counterparts once used space on the source volumes reaches 85%, execute the following:

```
tiercli config policy reclaimspace maxused 85
```

6. To limit the processes, which trigger the retrieval of a nearline file from the target, execute one of the following:

- to specify the processes allowed to trigger the retrieving of nearline files, execute the following:  
tiercli config global whiteproc <process> ... <process>

Where <process> is the full name of the process with its extension.

**Note:** To specify more than one process, list all processes separating them with a space.

For example, to specify that only Microsoft Paint and AutoCAD can trigger the retrieving of a nearline file that they are attempting to open/read, execute this:

```
tiercli config global whiteproc mspaint.exe acad.exe
```

- to specify the processes, which cannot trigger the retrieving of nearline files, execute the following:

```
tiercli config global blackproc <process> ... <process>
```

Where <process> is the full name of the process with its extension.

**Note:** To specify more than one process, list all processes separating them with a space.

For example, to specify that only Windows Explorer and Eset NOD32 antivirus cannot trigger the retrieving of a nearline file that they are attempting to open/read, execute this:

```
tiercli config global blackproc explorer.exe nod32.exe
```

7. Check if all settings are correctly configured, by executing the following:  
tiercli config show
8. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:  
tiercli config reload

### **To overwrite the space reclaiming policy for a specific source:**

Simply execute the command for a given parameter, including the drive letter of the source, for which you want to overwrite it.

For example, to specify that files on source volume mounted as drive letter E: must be replaced by nearline files when their size is equal to or bigger than 350MB, execute the following:

```
tiercli config E policy reclaimspace size 350m
```

**Note:** You cannot overwrite the parameter specifying which processes can trigger the retrieving of a nearline file from the target for a specific volume.

## Automatic Data Archiving

**Note:** Currently, Tiger Bridge lets you configure data archiving in the command-line interface only on Microsoft Azure and Amazon S3 Glacier targets.

To learn more about Tiger Bridge's automatic data archiving mechanism, refer to “Configure Data Archiving” on page 91.

### To configure Tiger Bridge archiving policy in the command-line interface:

1. To enable archiving of data on the source, execute the following:  
`tiercli config <path to source> policy archive turn on`  
**Note:** To disable archiving for the source, execute the following:  
`tiercli config <path to source> policy archive turn off`
2. To configure for how long a replicated file should not have been accessed in order to be replaced by an offline file, execute the following:  
`tiercli config <path to source> policy archive age <period>`  
Where <period> can be the desired period in seconds (s), minutes (m), hours (h), days (d), weeks (w).

For example, to specify that on source volume mounted as drive letter D Tiger Bridge should replace replicated files with offline counterparts only after they have not been accessed for 36 hours, execute the following:

```
tiercli config D policy archive age 36h
```

3. To configure what is the minimal size of a file for it to be replaced by an offline file, execute the following:  
`tiercli config <path to source> policy archive size <size>`  
Where <size> is the size in bytes (b), KB (k), MB (m), GB (g), TB (t).

For example, to specify that on source volume mounted as drive letter D Tiger Bridge should replace replicated files with offline counterparts only if they are bigger than 1GB, execute the following:

```
tiercli config D policy archive size 1g
```

4. Check if all settings are correctly configured, by executing the following:  
`tiercli config show`
5. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:  
`tiercli config reload`

# Active Sync

To learn more about Tiger Bridge's active sync mechanism, refer to "Configure Active Sync" on page 95.

## To configure global active sync policy:

1. To configure whether the policy will use just the notify parameter, just the listen parameter or both, execute the following:

```
tiercli config sync mode <parameter>
```

where <parameter> can be one of the following:

- **listen** - the computer will just receive notifications about updated contents from other computers.
- **notify** - the computer will only notify other computers about updates, but will not update its source with changes from them.
- **both** - the computer will synchronize the contents with changes from other computers and will send notifications about changes made by itself.

For example, to specify that the global replication policy on the computer will operate using both the notify and listen parameters, execute the following:

```
tiercli config sync mode both
```

2. To configure at what interval sources should send notifications about changes to their contents, execute the following:

```
tiercli config sync notify <period>
```

Where <period> can be the desired period in seconds (s), minutes (m), hours (h), days (d), weeks (w).

For example, to specify that each source should send out notification to other sources every hour, execute the following:

```
tiercli config sync notify 1h
```

3. To configure at what interval sources should receive notifications from other sources about changes in their contents, execute the following:

```
tiercli config sync listen <period>
```

Where <period> can be the desired period in seconds (s), minutes (m), hours (h), days (d), weeks (w).

For example, to specify that each source should check for notifications from other sources every 50 minutes, execute the following:

```
tiercli config sync listen 50m
```

4. To configure whether Tiger Bridge should begin retrieving new nearline files immediately after it finishes the synchronization, do one of the following:

## Get Started with Tiger Bridge Using the Command-line Interface

- To set Tiger Bridge to automatically retrieve a newly created nearline file on the source, execute the following:

```
tiercli config sync autorestore on
```

- To disable automatic retrieval of newly created nearline files once sources' contents are synchronized, execute the following:

```
tiercli config sync autorestore off
```

5. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:

```
tiercli config reload
```

**Note:** *To disable the global active sync policy, execute the following and reload the configuration:*

### To overwrite the global active sync policy for a source:

1. To configure whether the policy will use just the notify parameter, just the listen parameter or both, execute the following:

```
tiercli config <path to source> sync mode <parameter>
```

where <parameter> can be one of the following:

- **listen** - the computer will just receive notifications about updated contents from other computers.
- **notify** - the computer will only notify other computers about updates, but will not update its source with changes from them.
- **both** - the computer will synchronize the contents with changes from other computers and will send notifications about changes made by itself.

For example, to specify that the active sync policy for source D:\source will operate using just the notify parameter, execute the following:

```
tiercli config d:\source sync mode notify
```

2. To configure at what interval the source should send notifications about changes to its contents, execute the following:

```
tiercli config <path to source> sync notify <period>
```

Where <period> is the desired period in seconds (s), minutes (m), hours (h), days (d), weeks (w).

For example, to specify that source volume mounted as drive letter E: should send out notification to other sources every hour, execute the following:

```
tiercli config E: sync notify 1h
```

3. To configure at what interval the source should receive notifications from other sources about changes to their contents, execute the following:

```
tiercli config <path to source> sync listen <period>
```

Where <period> can be the desired period in seconds (s), minutes (m), hours (h), days (d), weeks (w).

For example, to specify that source volume mounted as drive letter E: should check for notifications from other sources every 50 minutes, execute the following:

```
tiercli config E: sync listen 50m
```

4. To configure whether Tiger Bridge should begin retrieving new nearline files immediately after it finishes the synchronization, do one of the following:

- To set Tiger Bridge to automatically retrieve a newly created nearline file on the source, execute the following:

```
tiercli config <path to source> sync autorestore on
```

- To disable automatic retrieval of newly created nearline files once sources' contents are synchronized, execute the following:

```
tiercli config <path to source> sync autorestore off
```

5. To reload the updated configuration and allow Tiger Bridge to use it without a restart, execute the following:

```
tiercli config reload
```

**Note:** To disable the active sync policy for this source and use the global policy instead, execute the following:

```
tiercli config <path to source> sync mode off
```

## Operation Mode Parameters

To learn more about the operation mode in which Tiger Bridge can operate, refer to “Configure Operation Mode” on page 100.

### To specify the retrieve mode settings:

Do one of the following:

- To let Tiger Bridge keep the replica on the target, when the file is successfully retrieved on the source volume, execute the following:

```
tiercli config global resmode copy
```

- To let Tiger Bridge remove the replica from the target, when the file is successfully retrieved on the source volume, execute the following:

```
tiercli config global resmode move
```

### To specify the delete mode settings:

Do one of the following:

- To let Tiger Bridge remove the replica from the target, upon deleting the file from the source, execute the following:  
`tiercli config global delmode on`
- To let Tiger Bridge keep the replica on the target, upon deleting the file from the source , execute the following:  
`tiercli config global delmode off`

## Monitor Data Management Statistics

**Note:** To see how to monitor data management statistics, using the Tiger Bridge Configuration, refer to “Monitor Data Management Statistics” on page 103.

Using the command-line interface of Tiger Bridge you can view the following statistics about the number and overall size of files Tiger Bridge manages:

**Not processed** — data with unknown status at the moment of the statistics report.

**Excluded** — the number and overall size of files, which are omitted by automatic Tiger Bridge operations.

**Failed** — the number and overall size of files, which Tiger Bridge has failed to automatically manage.

**Pending** — the number and overall size of files, queued for automatic Tiger Bridge management.

**Replicated** — the number and overall size of files, which have copies both on the source and the target.

**Nearline** — the number and overall size of files, which have copies only on the nearline tier of the target i.e. nearline stub files.

**Archived** — the number and overall size of files, which have copies on the archival tier of the target i.e. replicated files, which have copies on both the source and the archival tier as well as offline stub files.

**Total managed** — the number and overall size of files Tiger Bridge has already managed as well as of files potentially manageable by Tiger Bridge, with the exception of files in excluded locations. You can use information in this field to calculate what part of the total storage capacity associated with your Tiger Bridge license is used on the selected source.

**To view data management statistics per source:**

In command prompt, execute the following:

```
tiercli op info <full path to source>
```

**Note:** *To view data management statistics about a specific file or folder, execute the command providing the full path to that file/folder. For example, to view data management statistics about folder "Projects" on volume F, added as a source location, execute the following:*

```
tiercli op info f:\projects
```

## Disable Tiger Bridge

You can disable Tiger Bridge at any time without uninstalling it. Keep in mind that once you disable Tiger Bridge, you will not be able to retrieve any nearline or offline files from the target either on demand or manually. To enable Tiger Bridge again, you will have to configure all parameters anew.

**To disable Tiger Bridge:**

In command prompt, execute the following:

```
tiercli config disable
```



# 5

## **Manage Advanced Settings**

|                                                                  |            |
|------------------------------------------------------------------|------------|
| <i>General Advanced Settings . . . . .</i>                       | <i>132</i> |
| <i>Advanced Data Replication Settings . . . . .</i>              | <i>137</i> |
| <i>Advanced Space Reclaiming and Data Archiving Settings . .</i> | <i>141</i> |
| <i>Manage Tiger Bridge Logs . . . . .</i>                        | <i>148</i> |

## Manage Advanced Settings

To let you fine-tune your workflow with Tiger Bridge, you can manage the following advanced settings:

- general advanced settings:
  - enable and configure ransomware protection (see “Enable and Configure Ransomware Protection” on page 132).
  - enable or disable remote usage of the Tiger Bridge shell extension (see “Enable/Disable Remote Shell Extension Access” on page 134).
  - specify proxy server to be used by Tiger Bridge for access to Amazon S3 and Microsoft Azure targets (see “Specify Proxy Server Settings” on page 135).
  - specify for how long Tiger Bridge should wait on startup for the file system scan before beginning to perform data lifecycle management operations (see steps on page 136)
  - disable NFS locking on the Tiger Bridge computer to allow using NFS shares as target (see steps on page 137)
- settings that optimize data replication (see “Advanced Data Replication Settings” on page 137)
- settings that optimize space reclaiming and/or data archiving (see “Advanced Space Reclaiming and Data Archiving Settings” on page 141)
- manage Tiger Bridge logs (see steps on page 148)

## General Advanced Settings

### Enable and Configure Ransomware Protection

To prevent replication of files, which have been encrypted on your source due to ransomware attack, Tiger Bridge provides you with a fail-safe setting, which automatically pauses replication, once specific conditions are present. As ransomware attacks usually result in encryption of as many files as possible, Tiger Bridge lets you specify the maximum number of already replicated files, queued for replication, because they have been modified on the source. When the number of modified files queued for re-replication reaches the threshold you have specified, Tiger Bridge automatically pauses all its operations and logs this in the Windows Event Viewer. You can then delete the encrypted files (if there are any), retrieve from the target their unencrypted copies, and then resume normal operations.

You should keep in mind that this setting protects only already replicated data and prevents Tiger Bridge from overwriting a healthy copy on the target with an encrypted version. Tiger Bridge cannot prevent a ransomware attack on your source.

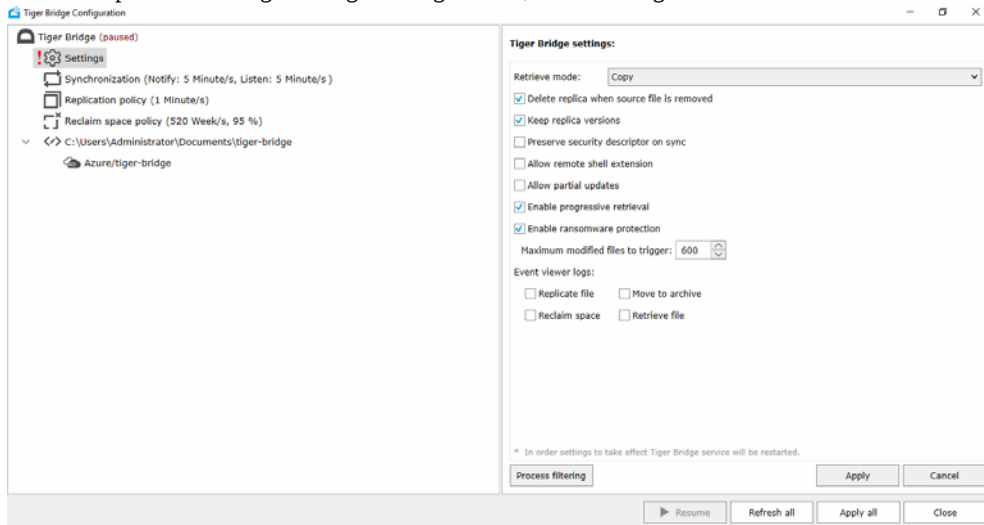
By default, when you enable Tiger Bridge's ransomware protection, the maximum number of files triggering the protection mechanism is 600. You can change this number depending on your specific workload calculations. You can use the statistics about modified files per source provided by the Tiger Bridge shell extension as a starting point (see “Monitor Data Management Statistics” on page 103). You should also keep in mind that:

- the maximum number of files, which triggers the protection mechanism, is valid for each configured source i.e. the workload on one source may differ from that on another.
- a replicated file, which has been modified on the source is replicated again once it meets the replication policy criteria, but is added to the Tiger Bridge queue immediately after it has been modified on the source i.e. the longer the time interval in the replication policy, the bigger the chance that healthy files stay in the queue, waiting to be replicated anew.

You can disable Tiger Bridge's ransomware protection mechanism at any time, thus guaranteeing that no matter how many replicated files are queued to be re-replicated, automatic Tiger Bridge operations are never paused.

### To enable and configure the ransomware protection mechanism:

1. In the left pane of the Tiger Bridge Configuration, click Settings.

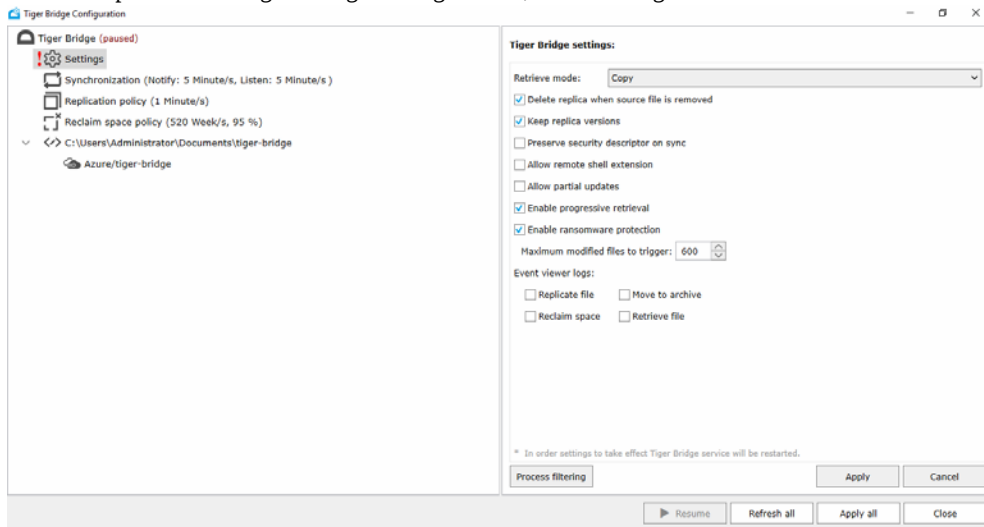


2. In the right pane, select the “Enable ransomware protection” check box and in “Maximum modified files to trigger” enter the desired number.
3. Click Apply.

## Manage Advanced Settings

### To disable Tiger Bridge's ransomware protection mechanism:

1. In the left pane of the Tiger Bridge Configuration, click Settings.



2. In the right pane, clear the “Enable ransomware protection” check box and then click Apply.

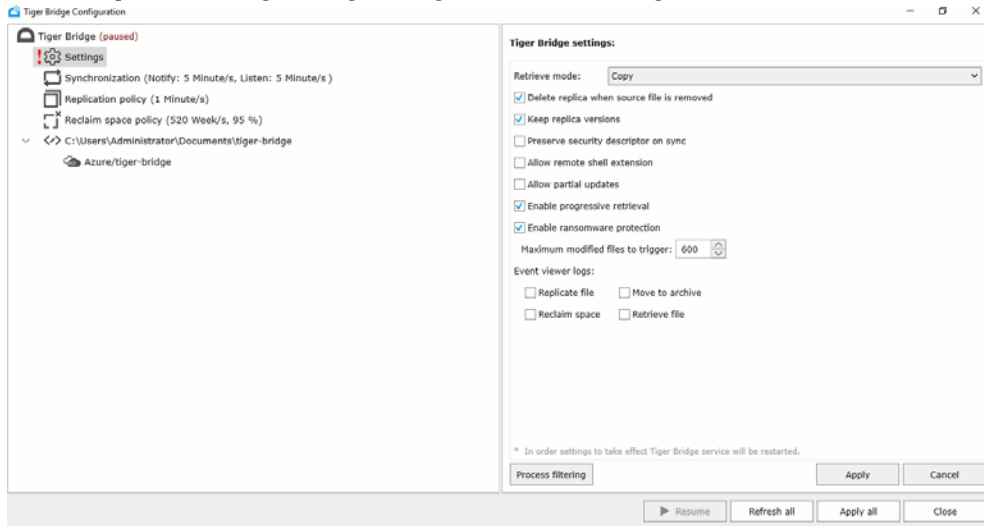
## Enable / Disable Remote Shell Extension Access

You can install the Tiger Bridge shell extension as a standalone component on a remote computer and thus allow users to perform manual Tiger Bridge operations on a NAS source or on a local source exported as a network share. To be able to use the shell extension from a remote computer, a Tiger Bridge administrator must enable remote shell extension access. You can enable and disable the remote shell extension access run-time. Should you disable it while a user is accessing the source, the shell extension commands will become unavailable immediately until you enable the access again.

**Important:** *Disabling the remote shell extension access only prevents users from executing the commands in the Tiger Bridge context menu in Windows Explorer, but does not restrict their access to data on your source.*

## To enable/disable remote shell extension access:

1. In the left pane of the Tiger Bridge Configuration, click Settings.



2. In the right pane, do one of the following:
  - select the “Allow remote shell extension” check box to enable the execution of shell extension commands from remote computers.
  - clear the “Allow remote shell extension” check box to prevent users on remote computers from executing Tiger Bridge shell extension commands on files on your source.
3. Click Apply.

## Specify Proxy Server Settings

You can let Tiger Bridge access Amazon S3 and Microsoft Azure targets using a proxy server, already set up on your network.

### To specify proxy server settings:

1. In command prompt, execute the following:

```
tiercli config global proxy <server:port> <username> <password>
```

where:

<server:port> is the proxy server IP address and the port through which it will access the targets;

<username> is the user name with which for authentication on the proxy server;

<password> is the password used for authentication on the proxy server;

## Manage Advanced Settings

**Note:** If your proxy server does not require authentication, enter empty values in quotation marks for the user name and password. For example, if your proxy server has IP address 10.200.9.16 and communication with the targets will go through port 3128, execute the following:

```
tiercli config global proxy 10.200.9.16:3128 "" ""
```

- Restart the Tiger Bridge service, by executing the following in command-prompt:

- net stop tiersvc
- net start tiersvc

## Set Startup Scan Wait Time

On startup Tiger Bridge scans the file systems of the source volumes it manages to determine what data on them needs to be processed. By default, Tiger Bridge is set to wait until this scan finishes, before beginning with data lifecycle management operations, thus ensuring maximum precision of the scheduled file operations. On source volumes with much data this scan may take significant time and you can set up Tiger Bridge to reduce this wait time before the scan finishes.

### To set Tiger Bridge startup scan wait time:

- Start the Registry Editor.

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

- Navigate to:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Tiger Technology\tiger-bridge\tiersvc\settings

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

- Rename the new REG\_SZ value to:  
step\_ready\_wait\_time

- Right-click the step\_ready\_wait\_time value and select Modify.

- Do one of the following:

- to set Tiger Bridge to wait until the startup scan finishes completely, change the value to 0 and click OK.
- enter the time in seconds, for which Tiger Bridge should wait before beginning to process data and click OK.

- Restart the Tiger Bridge service, by executing the following in command-prompt:

- net stop tiersvc
- net start tiersvc

## Disable NFS Locking on the Tiger Bridge Computer

For Tiger Bridge to use an NFS share as a target, NFS locking must be disabled. The steps below demonstrate how to disable it on the Tiger Bridge computer as long as it runs services for NFS. For steps on disabling NFS locking using a third-party solution, refer to their documentation.

**Important:** *If you have added a network share source, be it an SMB or an NFS share, Tiger Bridge automatically disables NFS locking on the computer and the change takes effect once the computer is restarted. In this case there is no need to disable NFS locking following the steps below.*

### To disable NFS locking on the Tiger Bridge computer:

1. 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\Microsoft\ClientForNFS\CurrentVersion\Users\Default\Mount
3. Right-click in the right pane and select New | DWORD Value.
4. Rename the new DWORD value to:  
Locking
5. Right-click the Locking value and select Modify.
6. Do the following:
  - In Value data, enter 0.
  - In Base, select Hexadecimal.
  - Click OK.
7. Restart the Tiger Bridge computer.

## Advanced Data Replication Settings

The advanced data replication settings, which you can manage, include:

- specify the minimum size of a file for it to be replicated (see steps on page 138)
- allow only the modified parts of a file to be re-replicated instead of replicating the whole file again (see steps on page 138)
- change the number of parallel threads run by Tiger Bridge when replicating files to the target (see steps on page 139)
- replicate file's data and metadata to different containers/buckets (see steps on page 140)

## Minimum File Size for Replication

By default, the only criteria for queuing a file for replication is for how long this file have not been modified. You can also set Tiger Bridge to queue for replication only files whose size is above a given threshold, thus ignoring small files like log files, for example.

**Note:** *The minimum file size for replication setting is valid only for files scheduled for automatic replication. Should you manually replicate a file with size below this minimum, this file will be replicated.*

### To specify minimum file size for it to be replicated:

1. 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\tiger-bridge\tiersvc\settings
3. Right-click the replication\_min\_filesize value and select Modify.
4. Do one of the following:
  - to set Tiger Bridge to replicate any file regardless of its size, change the value to 0 and click OK.
  - to set Tiger Bridge to schedule for automatic replication only files with size above the one you specify, enter the minimum file size in bytes and click OK.

For example, to set Tiger Bridge to replicate only files whose size is above 100MB, enter 104857600 and click OK.

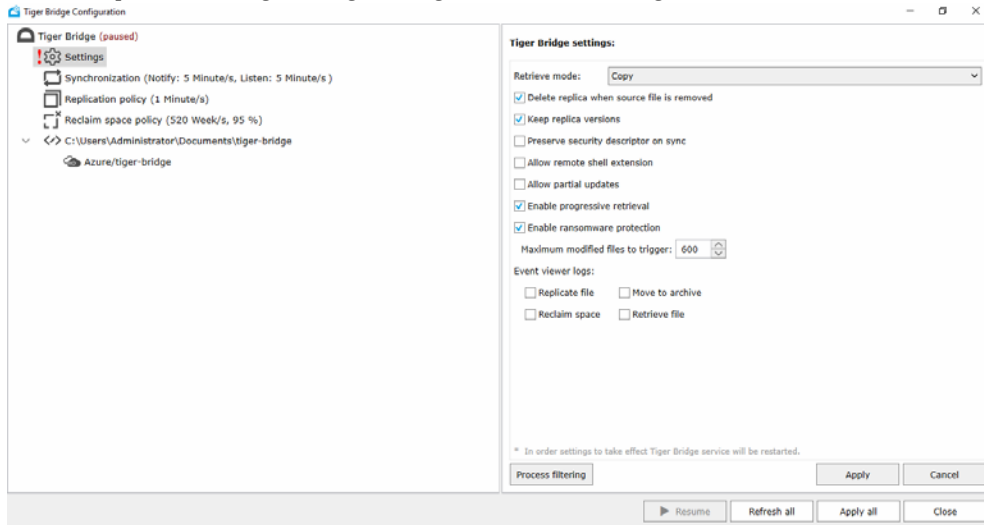
5. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - net stop tiersvc
  - net start tiersvc

## Enable Partial File Updates

By default, when an already replicated file is modified on the source and needs to be replicated again, Tiger Bridge replicates the whole file on the target. By enabling partial file updates, you let Tiger Bridge overwrite on the target just the parts of the file, which have been modified. Keep in mind that currently, partial file updates are supported only on Microsoft Azure, Backblaze B2 cloud storage, Amazon S3 object storage, Wasabi and IBM COS targets and on local volume source. Even if you enable it on other targets or on a NAS source, Tiger Bridge replaces the whole file and not just the modified parts of it.

**To enable/disable partial file updates:**

1. In the left pane of the Tiger Bridge Configuration, click Settings.



2. In the right pane, do one of the following:
  - Select the “Allow partial updates” check box, to let Tiger Bridge upload on the target only the modified parts of an already replicated file.
  - Clear the “Allow partial updates” check box, to replicate anew the whole file each time it is modified on the source.
3. Click Apply.

**Set Number of Parallel Threads during Data Replication**

By default, Tiger Bridge replicates files using four threads. You can increase or decrease the number of parallel threads in order to increase the replication speed, keeping in mind that using too many threads may hamper the performance of the Tiger Bridge computer.

**To set the number of parallel threads during data replication:**

1. 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\tiger-bridge\tiersvc\settings
3. Right-click the work\_threads\_count value and select Modify.

#### Manage Advanced Settings

4. Enter the number of threads that Tiger Bridge should use when replicating data to the target and click OK.
5. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - `net stop tiersvc`
  - `net start tiersvc`

## Replicate File's Data and Metadata to Different Containers

With both Amazon S3 and Microsoft Azure targets you can configure Tiger Bridge to replicate files' data and metadata to different buckets/containers.

This can be instrumental when you want to use Amazon S3 immutable storage. By configuring Tiger Bridge to replicate only files' data to the bucket configured with Amazon S3 Object Lock, you will ensure that each modification of the file on the source is uploaded as a new version and that no user can delete it, by deleting the copy on the source, as the metadata is stored in another bucket. For the purpose, you must designate another container for storing just replicated files' metadata and ensure that it is accessible with the same credentials as the ones used for access to the container storing replicated files' data.

### To separate the replication of files' data and metadata to different buckets:

1. 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\tiger-bridge\tiersvc\settings\sources

3. Expand the node of a source, whose data and metadata you want to be replicated to different containers and then select the sub-node named "1".

**Tip:** As source nodes are presented in the registry with a unique ID, to identify the node of the source you want to configure, look up the `source_vol_guid` string value for identification of the volume serial number (executing `vol [drive letter]:` in command prompt returns the serial number) and the `source_vol_path` string value for identification of the exact path on the volume added as a source (`source_vol_path` is empty if the root of the volume has been added as a source).

4. Right-click the `s3_meta_bucket` (Amazon S3) or the `azure_meta_container` (Microsoft Azure) value and select Modify.

**Note:** If the value does not exist, create it yourself - right-click in the right pane and select New | String Value, then rename the new REG\_SZ value to `s3_meta_bucket` (on Amazon S3) or to `azure_meta_container` (on Microsoft Azure).

5. In the Value data field, paste the name of the container on your Azure target, designated for storing replicated files' metadata and then click OK.
6. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - `net stop tiersvc`
  - `net start tiersvc`

## Advanced Space Reclaiming and Data Archiving Settings

The advanced space reclaiming and data archiving settings, which you can manage, include:

- specify whether a file should be retrieved from the target each time a user or application attempts to open it (default behaviour) or only when you manually retrieve it through Tiger Bridge (see steps on page 141)
- specify whether an offline file can be rehydrated only manually (default behaviour) or can be automatically triggered by attempting to open it on the source, in which case it will be automatically rehydrated and then retrieved. Also specify the processes, which can trigger automatic rehydration and retrieval of offline files. See steps on page 142.
- specify whether an application can begin reading a file before it has been fully retrieved from the target (see steps on page 144)
- specify whether Tiger Bridge should retrieve the whole file, when a user or application attempts to access it or just the portion of the file, which is being currently read (see steps on page 145)
- specify the timeout after which a file retrieve operation should be considered unsuccessful (see steps on page 146)
- change the space reclaiming policy parameter from file access time to file modification time (see steps on page 146)
- specify whether Tiger Bridge should show the actual size of a nearline/offline file or the size of the replicated file it replaces (see steps on page 147)
- specify nearline/offline file head and tail size (see steps on page 147)

### Retrieve Nearline Files Behaviour

By default, Tiger Bridge is set up to automatically retrieve a nearline file from the target each time a user or application accesses it. You can change this default behaviour and specify that nearline files should be retrieved from the target only when a manual retrieve operation is executed through the command-line interface or the shell extension of Tiger Bridge.

### To specify file retrieve behaviour:

1. 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\tiger-bridge\tiersvc\settings
3. Right-click the `active_restore` string value and select Modify.
4. Do one of the following:
  - to set Tiger Bridge to automatically retrieve a nearline file, when a user or application accesses it, change the value to 1 and click OK.
  - to set Tiger Bridge to retrieve a nearline file, only if manual retrieve operation is executed from the command-line interface or the shell extension, change the value to 0 and click OK.
5. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - `net stop tiersvc`
  - `net start tiersvc`

## Configure Offline Files Rehydration Behaviour

By default, when you want to retrieve an offline file, you must first manually rehydrate it to the hot/cool tier of the target and only after that retrieve it on the source either manually or automatically. You can change this behaviour and allow the automatic rehydration and consequent retrieval of the file, when a user or application attempts to open the offline file on the source. For the purpose you must configure the following string values in the Tiger Bridge registry:

- `active_restore_rehydrate_always_update_tier` - specifies whether Tiger Bridge should check the tier of the target, on which a file is located. By default, this setting is disabled. Enabling it is indispensable, when you want to enable automatic rehydration on targets, like FujiFilm object archive, which do not notify Tiger Bridge when they move a file to their archive.
- `active_restore_rehydrate` - specifies whether Tiger Bridge should automatically rehydrate and then retrieve an offline file on the source.

Additionally, you can configure the processes, which can trigger the process of automatic rehydration of offline files as long as it is enabled. By default, all processes are allowed to rehydrate a file from the archive. You can disable automatic rehydration by specifying that no process can trigger it. You can also specify which processes are allowed to trigger automatic rehydration or which ones cannot trigger it.

**To enable/disable automatic rehydration of offline files:**

1. 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\tiger-bridge\tiersvc\settings
3. Right-click the active\_restore\_rehydrate\_always\_update\_tier string value and select Modify.
4. Do one of the following:
  - to set Tiger Bridge to check the actual tier of the target a file is located on, change the value to 1 and click OK.
  - to prevent Tiger Bridge from checking the actual tier of the target a file is located on, change the value to 0 and click OK.
5. Right-click the active\_restore\_rehydrate string value and select Modify.
6. Do one of the following:
  - to set Tiger Bridge to automatically rehydrate and then retrieve a file from the archival tier of the target when a user or an application attempts to open an offline file on the source, change the value to 1 and click OK.
  - to prevent Tiger Bridge from automatically rehydrating and retrieving offline files, when a user or an application attempts to open them on the source, change the value to 0 and click OK.
7. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - net stop tiersvc
  - net start tiersvc

**To specify the processes allowed to trigger automatic rehydration of offline files:**

1. 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\tiger-bridge\tiersvc\settings
3. Right-click the active\_restore\_rehydrate\_process\_filter string value and select Modify.
4. Do one of the following:
  - to allow any process to trigger the automatic rehydration of files, change the value to ! and click OK.

## Manage Advanced Settings

- to prevent any process from triggering the automatic rehydration of files, leave the value empty and click OK.
- to specify which processes can trigger the automatic rehydration of files, enter their names, starting and ending the list with a colon and separating each name with a colon, then click OK.

**Tip:** For example, to specify that only Microsoft Paint and AutoCAD can trigger the automatic rehydration of files, enter the following:

`:mspaint.exe:acad.exe:`

- to specify the processes which cannot trigger automatic rehydration of files, enter their names, starting the list with an exclamation mark followed by a colon, separating each process name with a colon and ending the list with a colon, then click OK.

**Tip:** For example, to specify that any process except Microsoft Paint and AutoCAD can trigger the automatic rehydration of files, enter the following:

`!:mspaint.exe:acad.exe:`

5. Restart the Tiger Bridge service, by executing the following in command-prompt:

- `net stop tiersvc`
- `net start tiersvc`

## Partial File Retrieve Behaviour

By default, when retrieving a file from the target, you can begin reading it before it is fully retrieved. Tiger Bridge allows you to change this behavior and let an application begin reading a file only after it has been fully retrieved on the source.

### To specify partial file retrieve behaviour:

1. 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\tiger-bridge\tiersvc\settings`

3. Right-click the `active_restore_partial` string value and select Modify.

4. Do one of the following:

- to set Tiger Bridge to allow reading a nearline file, only when it has been fully retrieved, change the value to 0 and click OK.
- to set Tiger Bridge to allow reading a nearline file, when just a part of it has been retrieved only, change the value to 1 and click OK.

5. Restart the Tiger Bridge service, by executing the following in command-prompt:

- `net stop tiersvc`

```
• net start tiersvc
```

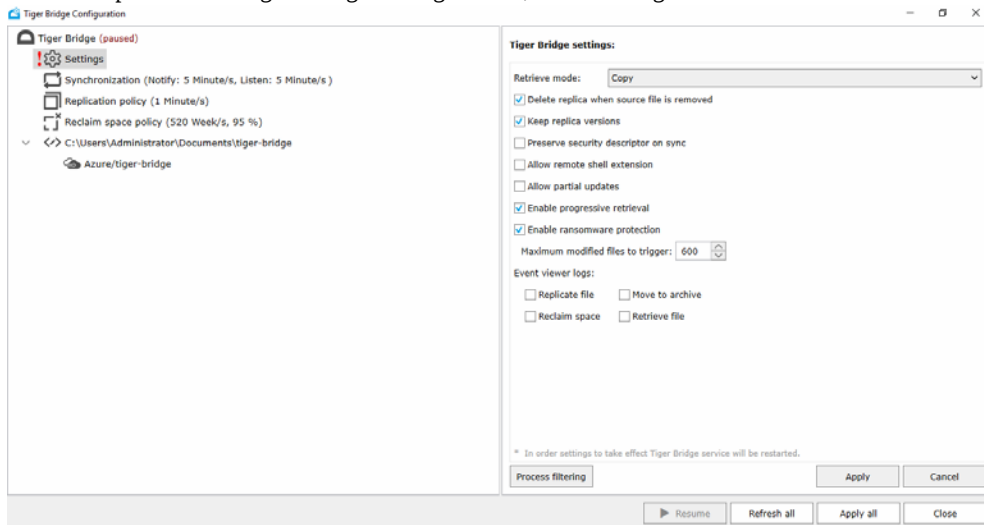
## Enable Progressive File Retrieval

By default, when retrieving a file from the target on demand i.e. when an application attempts to open its stub counterpart on the source, Tiger Bridge starts retrieving data from the offset requested by the application (with most application this is the beginning of the file) and consecutively retrieves the rest, unless you close the file before reading it to its end. You can disable the progressive retrieval of data and configure Tiger Bridge to retrieve only the portion of the file, which is currently being read by the application as long as the respective application supports reading only portions of a file.

**Important:** For progressive file retrieval to work, partial file retrieval must not be disabled. For more information, see “Partial File Retrieve Behaviour” on page 144.

### To enable/disable progressive file retrieval:

1. In the left pane of the Tiger Bridge Configuration, click Settings.



2. In the right pane, do one of the following:
  - Select the “Enable progressive retrieval” check box, to let Tiger Bridge retrieve the whole file.
  - Clear the “Enable progressive retrieval” check box, to let Tiger Bridge retrieve just the portion of the file, which is currently being read.
3. Click Apply.

## Set File Retrieve Timeout

When a user or application opens a nearline file on the source, Tiger Bridge attempts to retrieve it from the target before a specified timeout elapses. If no data begins retrieving before the timeout elapses, Tiger Bridge displays an error. If data begins retrieving, the timeout is reset, until data retrieval is halted or the file is fully retrieved on the source. By default, the timeout is set to 60 seconds. You can change the value of the timeout, thus adjusting it to the response time of your target and the connection to it.

**Note:** *When the target cannot be reached or there is another problem, the timeout is not taken into consideration and Tiger Bridge displays an error.*

### To set the fixed timeout value for successfully retrieving a file:

1. 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\tiger-bridge\tiersvc\settings
3. Right-click the active\_restore\_timeout value and select Modify.
4. Enter the fixed timeout value in seconds and click OK.  
For example, to set the fixed timeout value to 2 minutes, enter 120 and click OK.
5. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - net stop tiersvc
  - net start tiersvc

## Set Reclaim Space Criteria Parameter

By default, one of the parameters for replacing a replicated file with a stub file in order to reclaim space is for how long this file has not been accessed. To let you fine tune your workflow, Tiger Bridge allows you to change this parameter of the space reclaiming policy to the time interval for which a file has not been modified on the source.

**Important:** *If you set Tiger Bridge to use the file modification time as space reclaiming policy criteria, in both the Tiger Bridge Configuration and the command-line interface use the file last access time to specify the value.*

### To change the space reclaiming policy file timestamp parameter:

1. 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\tiger-bridge\tiersvc\settings

3. Right-click the `reclaim_space_time_type` value and select Modify.
4. Do one of the following:
  - to use the file access time as parameter, change the value to 0 and click OK.
  - to use the file modification time as parameter, change the value to 1 and click OK.
5. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - `net stop tiersvc`
  - `net start tiersvc`

## Set Stub File Allocation Size Display Option

By default, when you request to view the actual size of a nearline or an offline file on the source volume, Tiger Bridge displays the actual size of the original file it has replaced. You can set Tiger Bridge to display the actual size of the nearline/offline file instead, keeping in mind that using this option may disturb the workflow of some applications.

### To set stub file allocation size display option:

1. 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\tiger-bridge\tiersvc\settings`
3. Right-click the `stub_show_actual_size` value and select Modify.
4. Do one of the following:
  - to set Tiger Bridge to display the allocation size of the original file instead of the actual size of the stub file, change the value to 0 and click OK.
  - to set Tiger Bridge to display the actual size of the stub file, change the value to 1 and click OK.
5. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - `net stop tiersvc`
  - `net start tiersvc`

## Set Nearline File Head and Tail Sizes

By default, nearline files keep none of the original file's data or metadata and take no space on the source volume. Because of this, it is possible a nearline file to be retrieved from the target simply because Windows Explorer, for example, attempts to read the supplemental data placed in the header of the nearline file (with some file types this information may also be stored in the end of a file). To prevent needless retrieving of nearline files, you can set Tiger Bridge to keep the beginning

### Manage Advanced Settings

and/or the end of nearline files, specifying the size of respectively the head and the tail of the file. Thus, if the specified size is enough to hold the information from the header of a file, upon requesting to read it, Windows Explorer will not trigger the retrieving the original file from the target. With most file types a head/tail size of 64KB would be sufficient to include the information from the file header. Keep in mind that by specifying head and/or tail size, you automatically increase the size of each nearline file on your source volume with the sum of the head/tail sizes.

#### To set nearline file head size:

1. 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\tiger-bridge\tiersvc\settings
3. Right-click the `stub_sparse_head_size` value and select Modify.
4. Enter the file head size in KB and click OK.
5. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - `net stop tiersvc`
  - `net start tiersvc`

#### To set nearline file tail size:

1. 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\tiger-bridge\tiersvc\settings
3. Right-click the `stub_sparse_tail_size` value and select Modify.
4. Enter the file tail size in KB and click OK.
5. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - `net stop tiersvc`
  - `net start tiersvc`

## Manage Tiger Bridge Logs

Tiger Bridge can log most events related to its operations, using a standard Windows output console like DebugView, for example. You can set Tiger Bridge to output its logs as files in the Windows Event Viewer. You can find a detailed description of the logs generated by Tiger Bridge in “Appendix: Tiger Bridge Logs” on page 173.

**Important:** *It is advisable to keep track of the amount of log files generated by Tiger Bridge, in order to avoid running out of disk space.*

Tiger Bridge logs all target/source connectivity events, additionally you can set it to create logs for the following events:

- a file is replicated
- a file is replaced with a nearline/offline file
- a nearline file is retrieved from the target
- the status of a directory is changed (replicated, nearline, offline)

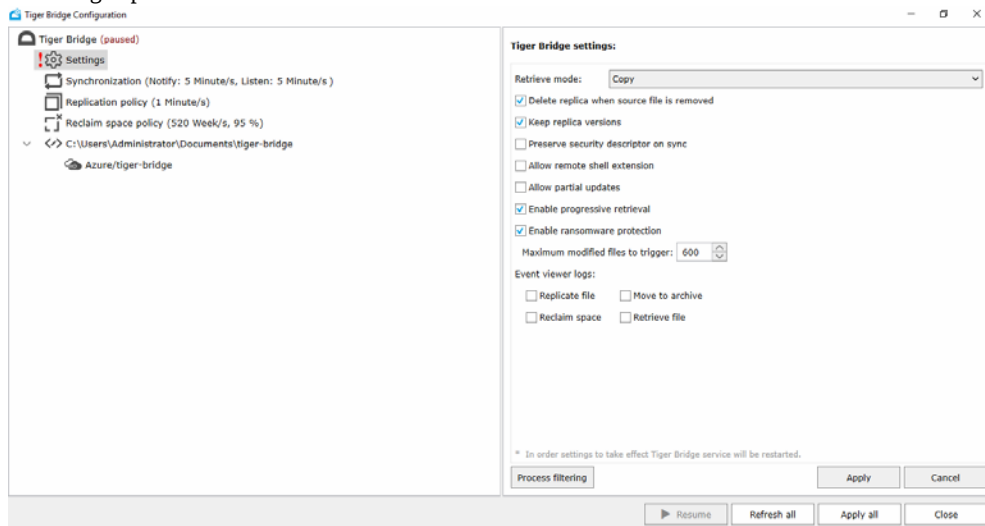
## Manage Tiger Bridge Logs in the Configuration

The Tiger Bridge Configuration lets you specify which of the following events should be output as logs in Windows Event Viewer:

- a file is replicated
- a file is replaced with a nearline/offline file
- a nearline file is retrieved from the target

### To configure Tiger Bridge logs in the Configuration:

1. In the left pane of the Tiger Bridge Configuration, click Settings and then do one of the following in the right pane:



- Select the check box of an operation, to let Tiger Bridge output logs for it in Windows Event Viewer.

### Manage Advanced Settings

- Clear the check box of an operation, to prevent Tiger Bridge from outputting logs for it in Windows Event Viewer.

2. Click Apply.

## Manage Tiger Bridge Logs in the Registry

### To enable/disable Tiger Bridge logging on each file replicate operation:

1. 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\tiger-bridge\tiersvc\settings`
3. Right-click the `log_replicate` value and select Modify.
4. Do one of the following:
  - To enable Tiger Bridge logging, change the value to 1 and click OK.
  - To disable Tiger Bridge logging, change the value to 0 and click OK.
5. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - `net stop tiersvc`
  - `net start tiersvc`

### To enable/disable Tiger Bridge logging on replace with a nearline/offline file operation:

1. Start the Registry Editor.

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

2. Right-click the `log_reclaim_space` value and select Modify.
3. Do one of the following:
  - To enable Tiger Bridge logging, change the value to 1 and click OK.
  - To disable Tiger Bridge logging, change the value to 0 and click OK.
4. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - `net stop tiersvc`
  - `net start tiersvc`

**To enable/disable Tiger Bridge logging on file retrieve operation:**

1. Start the Registry Editor.

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

2. Right-click the `log_restore` value and select Modify.
3. Do one of the following:
  - To enable Tiger Bridge logging, change the value to 1 and click OK.
  - To disable Tiger Bridge logging, change the value to 0 and click OK.
4. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - `net stop tiersvc`
  - `net start tiersvc`

**To enable/disable Tiger Bridge logging on directory status change:**

1. Start the Registry Editor.

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

2. Right-click the `log_dir_status` value and select Modify.
3. Do one of the following:
  - To enable Tiger Bridge logging, change the value to 1 and click OK.
  - To disable Tiger Bridge logging, change the value to 0 and click OK.
4. Restart the Tiger Bridge service, by executing the following in command-prompt:
  - `net stop tiersvc`
  - `net start tiersvc`





# Manually Manage Data

- Perform Manual Tiger Bridge Operations . . . . . 154*
- Synchronize Data on the Source and the Target . . . . . 159*
- Undelete Data on the Source . . . . . 160*
- Manage Files and Folders Versions . . . . . 162*

## Manually Manage Data

Using the shell extension or the command-line interface of Tiger Bridge you can manually manage data in the following ways:

- perform data lifecycle management operations on separate files or whole folders. For more information, see “Perform Manual Tiger Bridge Operations” on page 154.
- synchronize the contents of a source or just a folder on it with the contents of the target. For more information, see “Synchronize Data on the Source and the Target” on page 159.
- undelete deleted files on the source. For more information, see “Undelete Data on the Source” on page 160.
- restore a selected version of a replicated file on the source or restore the contents of a whole folder to the last committed version of all files in it by a selected point in time. For more information, see “Manage Files and Folders Versions” on page 162.

## Perform Manual Tiger Bridge Operations

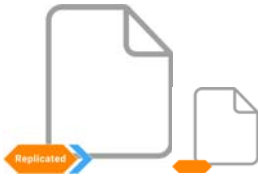
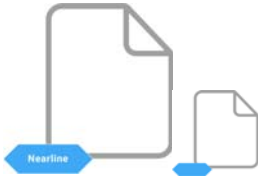
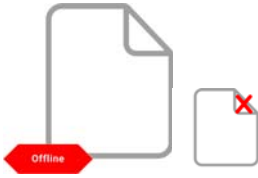
Initiating a Tiger Bridge operation manually always takes precedence over the automatically scheduled tasks. That means that if you choose to manually replicate files through the shell extension or the command-line interface, for example, the execution of the operation will begin immediately and will pause the automatic replication queue that is being processed at the moment.

**Important:** *With a NAS source, stub files are located in the control folder and not on the network share itself. To perform a manual operation on a stub file (retrieve a nearline file or rehydrate an offline file), you need to perform it on the stub file in control folder. To learn more, refer to “NAS Source Prerequisites and Setup” on page 36.*

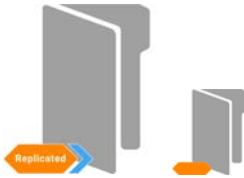
## Manage Data Through the Shell Extension

Tiger Bridge is integrated with Windows Explorer and displays files and folders subject to replication, space reclaiming and/or archiving with separate icons.

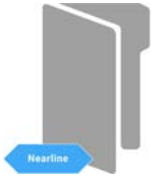
**File icons:**

| Large icon                                                                         | Small icon | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   |            | This is a replicated file, which has a copy on both the source volume and the target.                                                                                                                                                                                                                                                                                                                                                                                                                               |
|   |            | This is a nearline file, pointing to the actual file, which exists only on the target. A nearline file can be automatically retrieved whenever a user or application attempts to open it on the source.                                                                                                                                                                                                                                                                                                             |
|   |            | This is an offline file, pointing to the actual file, which exists only on the archival tier of the target. An offline file can be retrieved only manually, through Tiger Bridge. When you retrieve an offline file, it is first rehydrated to an intermediate tier of the target and only after that is retrieved on the source. Optionally, you can choose to rehydrate an offline file i.e. make it nearline, which allows its automatic retrieval when a user or application attempts to open it on the source. |
|  |            | Tiger Bridge is currently performing a data lifecycle management operation on the file. Wait until the operation finishes for the file icon to change.                                                                                                                                                                                                                                                                                                                                                              |

**Folder icons:**

| Large icon                                                                          | Small icon | Description                                                                                                                 |
|-------------------------------------------------------------------------------------|------------|-----------------------------------------------------------------------------------------------------------------------------|
|  |            | All files in the folder are replicated. Some of the replicated files may be replaced with nearline or offline counterparts. |

## Manually Manage Data

| Large icon                                                                         | Small icon                                                                         | Description                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   |   | The folder contains only nearline files.<br><b>Note:</b> When the retrieve mode of Tiger Bridge is set to move (see “Configure Operation Mode” on page 100), this folder icon designates that the folder contains at least one nearline file. |
|   |   | The folder contains at least one offline file.                                                                                                                                                                                                |
|   |   | Tiger Bridge is currently performing data lifecycle management operations on data in the folder. Wait until the operation finishes for the folder icon to change.                                                                             |
|  |  | Tiger Bridge is currently scanning the contents of the folder and is unable to display its status.                                                                                                                                            |

### To perform data lifecycle management operations through the Tiger Bridge shell extension:

**Note:** The respective commands are available only to files/folders to which they apply i.e. you cannot issue the “Reclaim space” command for a nearline file, for example.

1. In Windows Explorer, right-click the file/folder you want to manage.
2. (for access from remote computer) In the context menu, under Tiger Bridge click Remote Monitoring and enter the IP address of the Tiger Bridge computer and the local path of the source you are accessing. For more information, refer to “Tiger Bridge Shell Extension” on page 10.
3. In the context menu, do one of the following:
  - Select “Tiger Bridge | Replicate” to replicate the selected file or all files in the selected folder on the target.

- Select “Tiger Bridge | Reclaim space” to replace the selected replicated file or all replicated files in the selected folder with nearline file(s), pointing to the actual replicas on the target.
- Select “Tiger Bridge | Move to archive” to move the selected replicated file or all replicated files in the selected folder from the hot/cool tier to the archival tier on the target and on the source replace with offline file(s), pointing to the actual replicas on the target.

**Note:** *On targets, which do not support third-party policies for moving files between the hot/cool and the archival tiers, this command only performs a check for files moved to the archival tier and if such files are found, updates their status to “offline” on the source.*

- Select “Tiger Bridge | Rehydrate from archive” to change the status of an offline file to nearline i.e. to move a file from the archival tier of the target to the hot/cool tier.

**Note:** *This command is not available on targets, which do not support third-party policies for moving files between the hot/cool and the archival tiers.*

- Select “Tiger Bridge | Retrieve data” to retrieve from the target the selected nearline/offline file or all nearline/offline files in the selected folder.

**Note:** *Before retrieving an offline file on the source, the file is first rehydrated on an intermediate tier of the target. Retrieving a file from the target is possible only if there's enough free space on the volume.*

## Manage Data Through the Command-line Interface

You can perform the following manual data lifecycle management operations through the Tiger Bridge command-line interface:

| action:                                                                                                                                                             | command:                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show file/folder lifecycle status                                                                                                                                   | tiercli op info <path to file/folder on source volume>                                                                                                                                                                                                                     |
| replicate a file/folder to the target                                                                                                                               | tiercli op replicate <path to file/folder on source volume>                                                                                                                                                                                                                |
| replace a replicated file with a nearline file. When you perform this command for a whole folder, all files in it are replicated and replaced by nearline files.    | tiercli op offline <path to file/folder on source volume>                                                                                                                                                                                                                  |
| retrieve a nearline/offline file from the target. When you perform this command for a whole folder, all nearline/offline files in it are retrieved from the target. | tiercli op restore <path to file/folder on source volume><br><br><b>Note:</b> To preserve the last access time of the retrieved file(s), execute the command adding -p before the path to the file/folder:<br>tiercli op restore -p <path to file/folder on source volume> |
| delete a file or folder from the source volume.                                                                                                                     | tiercli op delete <path to file/folder on source volume>                                                                                                                                                                                                                   |
| rehydrate an offline file, changing its status to nearline.                                                                                                         | tiercli op move_hot <path to file/folder on source volume>                                                                                                                                                                                                                 |
| move a nearline or offline file from the hot or archival tier of the target to the cool tier (Azure Cool, Amazon Standard-IA, Google Cloud Nearline, for example).  | tiercli op move_cool <path to file/folder on source volume>                                                                                                                                                                                                                |
| replace a replicated file on the source volume with an offline file.                                                                                                | tiercli op move_archive <path to file/folder on source volume>                                                                                                                                                                                                             |
| display the status of the currently performed data lifecycle operation                                                                                              | tiercli op status <path to file/folder on source volume>                                                                                                                                                                                                                   |
| abort the currently performed data lifecycle operation                                                                                                              | tiercli op abort <path to file/folder on source volume>                                                                                                                                                                                                                    |
| display a list of all queued data lifecycle operations.                                                                                                             | tiercli op list <path to file/folder on source volume>                                                                                                                                                                                                                     |
| check if the replica of a nearline/offline file is available on the target.                                                                                         | tiercli op avail <path to file/folder on source volume>                                                                                                                                                                                                                    |
| show the content of a selected replicated folder on the target                                                                                                      | tiercli op target_enum <path to folder on source volume>                                                                                                                                                                                                                   |
| pause a manually initiated data lifecycle operation                                                                                                                 | tiercli op pause <path to file/folder on source volume>                                                                                                                                                                                                                    |

To execute any of the above operations you should specify the full path to the file/folder on the source volume. For example, to manually replicate file “Schedule” in the folder “Schedules” on

source volume F, execute the following:

```
tiercli op replicate F:\Schedules\Schedule
```

## Synchronize Data on the Source and the Target

As means of disaster recovery, Tiger Bridge offers you the possibility to synchronize the contents of the source with the target. Thus, in case a replicated file has no nearline or offline counterpart on the source volume, Tiger Bridge automatically creates it as a stub file after synchronizing the contents with the target.

**Note:** *If versioning is enabled and there is more than one version of a file on the target, Tiger Bridge restores the version, which has been last used on the source i.e. this may not be the latest version of the file.*

You can choose to synchronize the contents of the current directory on the source only or to execute the command recursively, also synchronizing all data in all subfolders.

**Important:** *With a NAS source, you need to synchronize the contents of the control folder and the target. The missing files appear as nearline or offline files in the control folder and a placeholder file with .reclaimed extension is created in the source. To retrieve the file on the NAS source, you need to perform the respective operation on the nearline/offline file in the control folder.*

### To synchronize source and target contents through the shell extension:

1. In Windows Explorer, right-click the folder, whose contents you want to synchronize with the target.
2. In the context menu, do one of the following:
  - To synchronize just the contents of the folder with the target, select “Tiger Bridge | Synchronize with Target”.
  - To synchronize the contents recursively i.e. the contents of the selected folder and the contents of all its subfolders, select “Tiger Bridge | Synchronize Recursively”.

### To synchronize source and target contents through the command-line interface:

1. In command prompt, do one of the following:
  - To synchronize just the contents of a folder on a source with the target, execute the following:  

```
tiercli op sync <path to folder on the source>
```

For example, to synchronize the content of the folder “Projects” in the root of the source volume mounted as drive letter F:, execute the following:

```
tiercli op sync F:\Projects
```

### Manually Manage Data

- To synchronize the contents recursively - the specified folder on a source and all its subfolders, execute the following:

```
tiercli op sync -r <path to folder on the source>
```

For example, to synchronize the content of the folder “Projects” in the root of the source volume mounted as drive letter F: and all data in its subfolders, execute the following:

```
tiercli op sync -r F:\Projects
```

2. To check the progress of the synchronization operation, execute the following:

```
tiercli op status
```

## Undelete Data on the Source

**Note:** *Currently, undeleting files is supported only on cloud storage targets except on Google Cloud. To benefit from the undelete feature, versioning (Amazon S3 and S3-compatible targets) or soft-delete (Azure target) must be enabled.*

Tiger Bridge provides you with two methods for recovering accidentally deleted data from your source. If you have configured Tiger Bridge's delete mode to keep the file replica on the target, even if it is deleted on the source, you can easily recover the deleted file by synchronizing the contents of its parent folder with the contents on the target (for more information, refer to “Synchronize Data on the Source and the Target” on page 159).

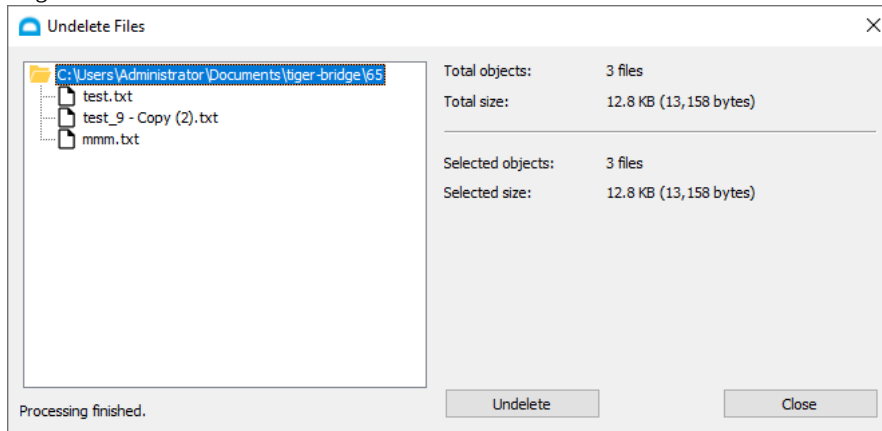
In case Tiger Bridge's delete mode is configured to delete the file replica from the target as soon as it is deleted from the source, your only means to recover an accidentally deleted file is to undelete it, following the steps below. Once you undelete a file, it appears on your source as a nearline or offline file, which you can then retrieve manually, through Tiger Bridge or on demand, by attempting to open it.

**Important:** *To undelete a file from a NAS source, you need to perform the operation in its control folder.*

**To undelete data on the source through the shell extension:**

1. In Windows Explorer, right-click the folder, containing the file you want to undelete.
2. In the context menu, select “Tiger Bridge | Undelete”.

The Undelete Files dialog lists all files deleted from the selected folder and having copies on the target.



3. Browse to and select a file in the list, then click Undelete.

**Note:** To undelete all files in a folder or a sub-folder, select it in the left pane and click Undelete.

The undeleted files appear on your source as nearline or offline files, which you can retrieve manually or on demand.

**Important:** Undeleted files from a NAS source appear as nearline or offline files in the control folder and a placeholder file with `.reclaimed` extension is created in the source. To retrieve the file on the NAS source, you need to perform the respective operation on the nearline/offline file in the control folder.

**To undelete data on the source through the command-line interface:**

In command prompt, execute the following:

```
tiercli op sync -u <dir_path>
```

Where `<dir_path>` is the full path to the directory on the source, whose deleted files you want to undelete. For example, to undelete all deleted files from the directory “Projects”, which is in the root of volume mounted with drive letter F and added as a source, execute the following:

```
tiercli op sync -u F:\Projects
```

Tiger Bridge undeletes all deleted files in the selected folder as long as they have a copy on the target. The undeleted files appear on your source as nearline or offline files, which you can retrieve manually or on demand.

**Important:** *Undeleted files from a NAS source appear as nearline or offline files in the control folder and a placeholder file with .reclaimed extension is created in the source. To retrieve the file on the NAS source, you need to perform the respective operation on the nearline/offline file in the control folder.*

## Manage Files and Folders Versions

As long as versioning is enabled on your cloud storage target and also in Tiger Bridge, following the steps in “Configure Versioning” on page 99, you can restore on your source any specific version of a replicated file as well as delete a specific version from the target. When providing you with the list of available versions for a file to select from, Tiger Bridge gives you information about the size of each version, the modification time and the specific tier on target the respective version is stored on:



the version of the file is stored on the tier for frequently accessed data (Azure Hot, Amazon S3 Standard, etc.)



the version of the file is stored on the tier for infrequently accessed data (Azure Cool, Amazon S3 Standard -IA, etc.)



the version of the file is stored on the archival tier of the target (Azure Archive, Amazon S3 Glacier, etc.)

To help you manage versions more efficiently, Tiger Bridge allows you to analyze the contents of a whole folder on your source using a selected point in time as a starting point. The analysis gives you information not only about the total number of files with versions in the folder and the overall size of all versions on the target, but also about the number and size of versions replicated before the selected date and time, and the number and size of file versions, replicated on the target after the selected date and time. With this information in mind, Tiger Bridge then allows you to:

- Delete any selected or all older versions of a file from the target, discarding them as obsolete and thus freeing space on the target. In case the deleted version of a file is the one to which the file on the source is actually linked (i.e. the one that would normally be retrieved, if you attempt to open it), Tiger Bridge automatically links the file to the newest version on the target.
- Delete any selected or all newer versions of a file from the target, discarding them as obsolete and thus freeing space on the target. Newer versions of a file can be considered obsolete, if, for example, they are encrypted versions, replicated on the target after your source has suffered a ransomware attack. In case the deleted version of a file is the one to which the file on the source is actually linked (i.e. the one that would normally be retrieved if you attempt to open it), Tiger Bridge automatically links the file to the last version on the target, which has been submitted before the selected date and time. In case the deleted version of the file is the only version of the file, it is deleted from both the source and the target, but you can undelete it from the source, as long as a copy is still available in a snapshot on the target.

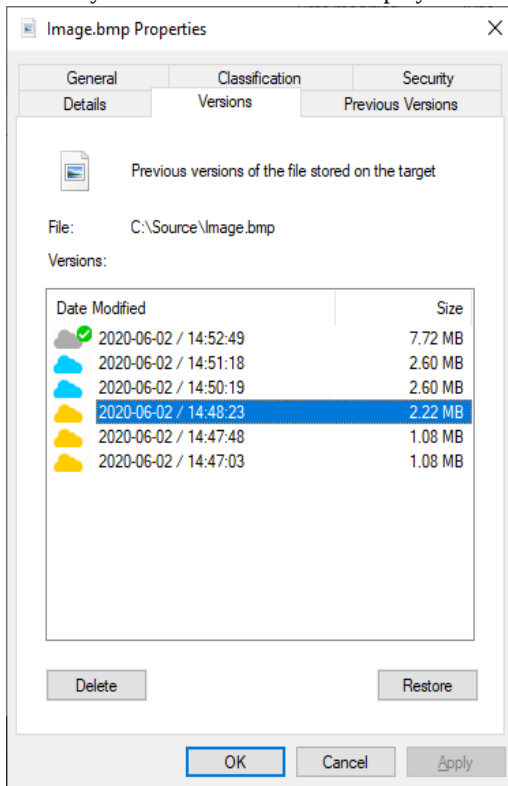
- Restore the version of one or all files in the folder to the last submitted version before the selected date and time. When performing this operation you also can select to automatically retrieve on the source each restored version and also to add the restored version as the newest copy on the target.

**Important:** You can manage the versions of files/folders on a NAS source in its control folder. The restored version of a file is automatically retrieved on the NAS source.

### To restore a specific version of a file:

1. In Windows Explorer, right-click the file and select Properties.
2. In the Properties dialog, select the Versions tab.

Tiger Bridge lists all available versions of the file in descending order, starting with the newest one. The icon of each version designates the tier on the target it is stored on and the version currently stored on the source is displayed with a check mark.



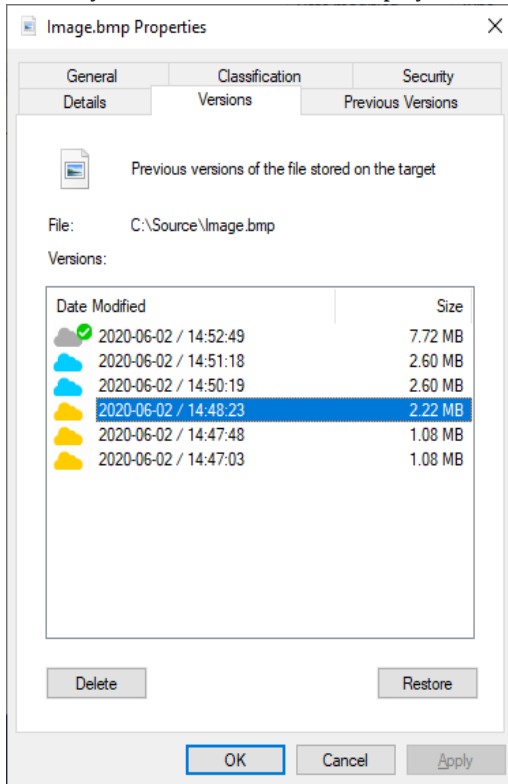
3. Select a file version in the list and click Restore.

## Manually Manage Data

### To delete a specific version of a file:

1. In Windows Explorer, right-click the file and select Properties.
2. In the Properties dialog, select the Versions tab.

Tiger Bridge lists all available versions of the file in descending order, starting with the newest one. The icon of each version designates the tier on the target it is stored on and the version currently stored on the source is displayed with a check mark.



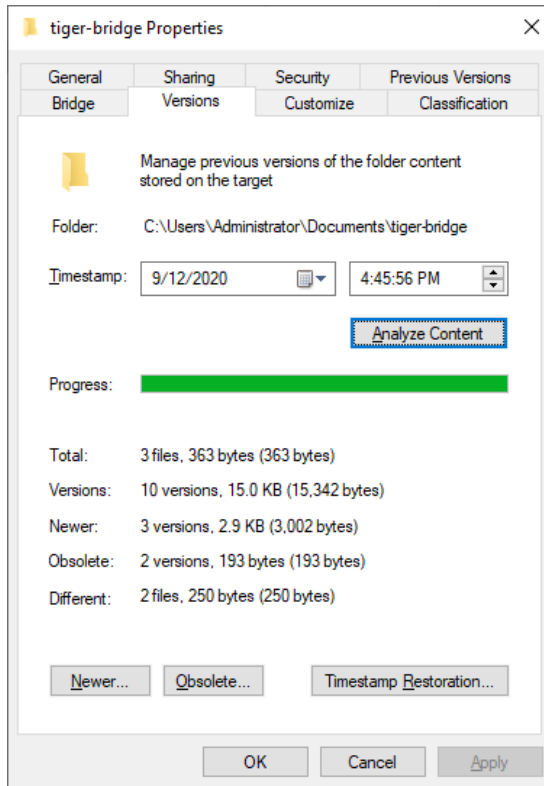
3. Select a file version in the list and click Delete to delete it from the target.

**Note:** If you delete the version, which is currently stored on your source i.e. the one with a check mark in its icon, the file on the source is automatically linked to the newest version of the file on the target. You cannot delete a version of a file, if it is the only version on the target.

### To analyze the contents of a folder:

1. In Windows Explorer, right-click the folder and select Properties.
2. In the Properties dialog, select the Versions tab.
3. Select the desired date and time in the Timestamp boxes and then click Analyze Content.

**Note:** Depending on the number of files in the folder and their size the analysis may take time. Keep track of the progress bar below, to make sure Tiger Bridge has gathered complete information.



Tiger Bridge gives you the following information:

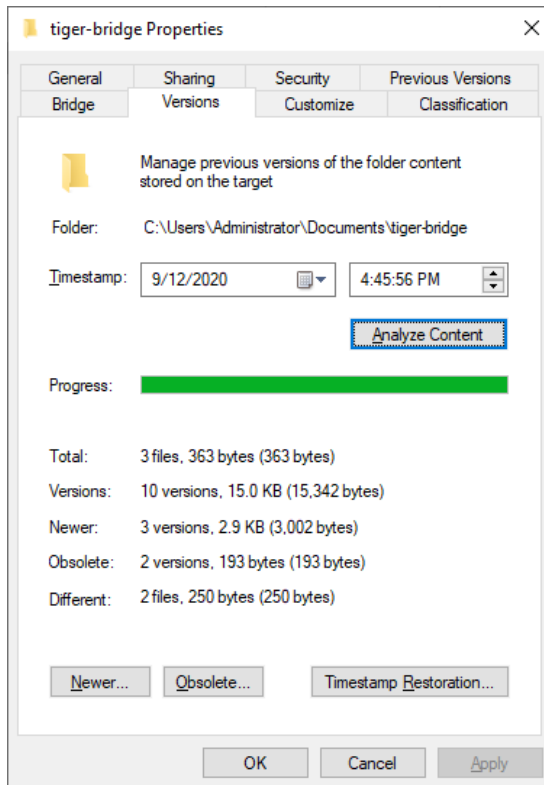
- Total - the total number of files on the source and their size
- Versions - the number of overall file versions and their size on the target.
- Newer - the number of file versions, which were replicated on the target after the selected date and time as well as their size on the target.
- Obsolete - the number of file versions, which were stored on the target before the selected date and time as well as their size on the target.
- Different - the number of files and their size, which will be changed on the source, if you decide to restore the state of the folder to the state it had on the selected date and time.

## Manually Manage Data

### To restore files in a folder to their state before selected date and time:

1. In Windows Explorer, right-click the folder and select Properties.
2. In the Properties dialog, select the Versions tab.
3. Select the desired date and time in the Timestamp boxes and then click Analyze Content.

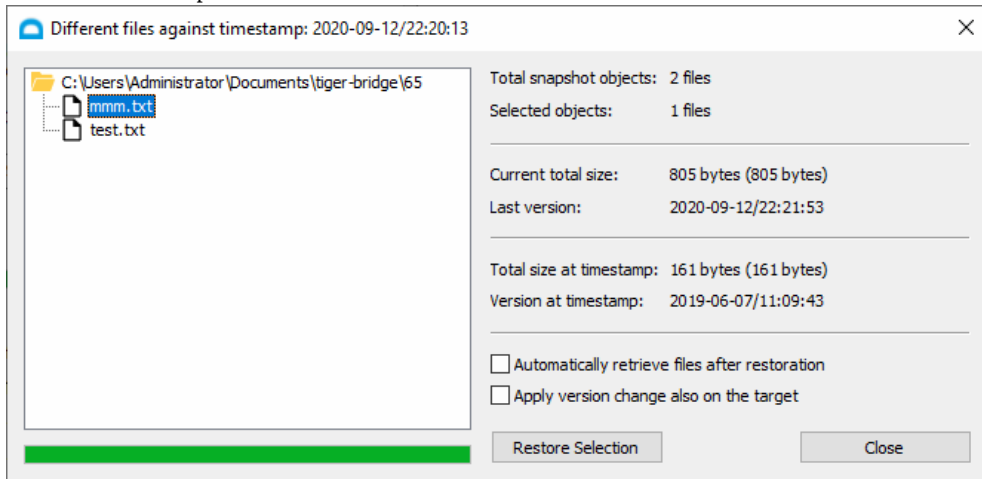
**Note:** Depending on the number of files in the folder and their size the analysis may take time. Keep track of the progress bar below, to make sure Tiger Bridge has gathered complete information.



4. Click Restore Timestamp.

Tiger Bridge displays a dialog, listing all files, whose current version on the source is different from the version, replicated before the selected date and time. It also gives you information about the size of the current version on the source and the date the last version has been

replicated as well as about the size and date of the version, which will be restored against the selected timestamp.



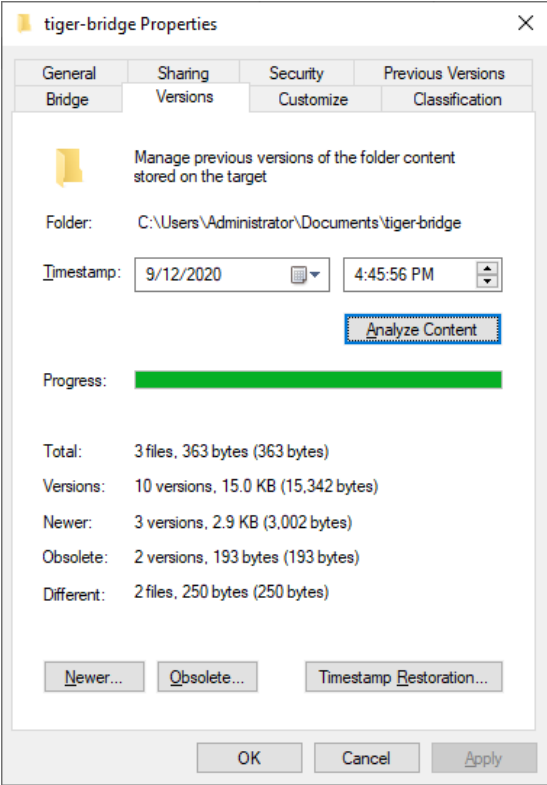
5. Do one of the following:
  - In the left pane of the dialog, select a folder, to restore all its files to their version, replicated before the selected timestamp.
  - Browse to and select a file, to restore its version to the one, replicated before the selected timestamp.
6. Select whether to automatically retrieve on the source each file, whose current version differs from the one, which will be restored.
7. Select whether the version, which will be restored on the source should be added as a newest version on the target.
8. Click Restore Selection.

#### **To delete obsolete versions of files in a folder:**

1. In Windows Explorer, right-click the folder and select Properties.
2. In the Properties dialog, select the Versions tab.
3. Select the desired date and time in the Timestamp boxes and then click Analyze Content.

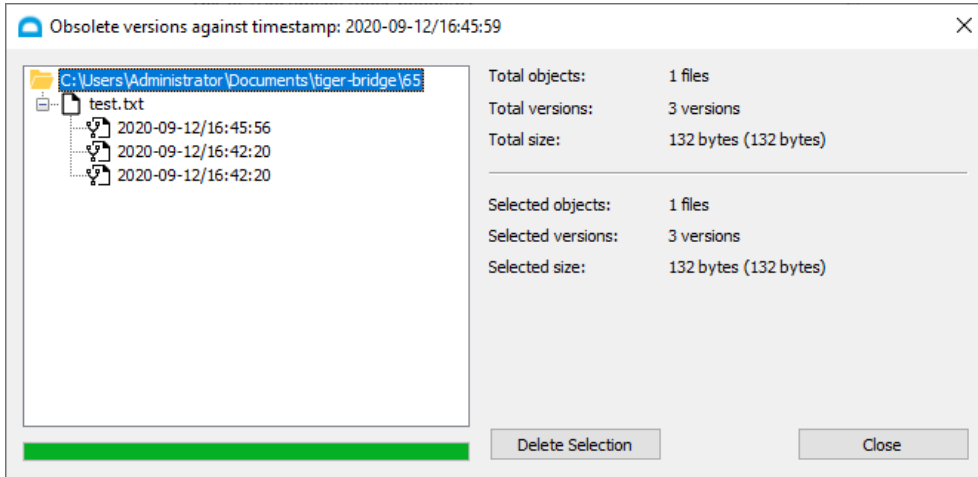
Manually Manage Data

**Note:** Depending on the number of files in the folder and their size the analysis may take time. Keep track of the progress bar below, to make sure Tiger Bridge has gathered complete information.



## 4. Click Obsolete.

Tiger Bridge displays a dialog, listing all versions of a file, which have been replicated before the selected time and date, giving you information about the size of each version as well as about the total size of all versions.



## 5. Do one of the following:

- Select a whole folder, to delete all versions of all its files, which have been replicated before the selected date and time.
- Select a file, to delete all its versions, which have been replicated before the selected date and time.
- Select a file version, to delete just this version of the file.

**Important:** *If you are deleting the version of a file, to which the current file on the source is pointing, the file will automatically be linked to the newest version on the source. If you are attempting*

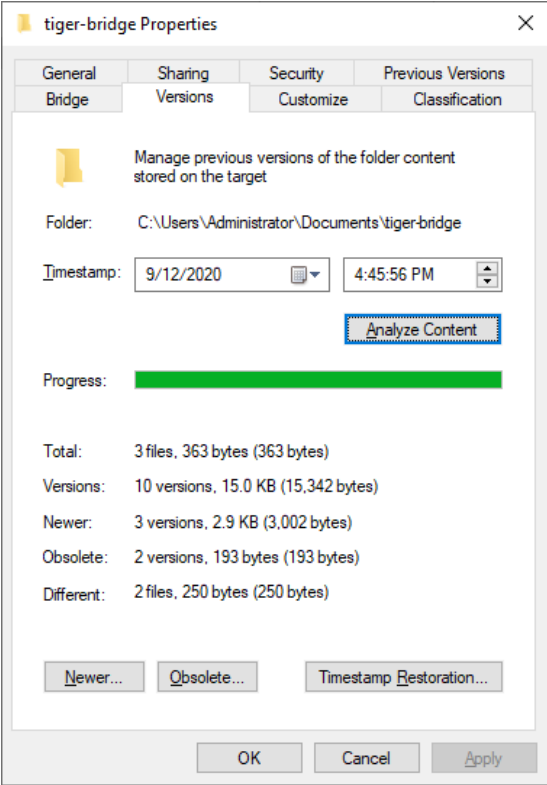
## 6. Click Delete Selection.

**To delete newer versions of files in a folder:**

1. In Windows Explorer, right-click the folder and select Properties.
2. In the Properties dialog, select the Versions tab.
3. Select the desired date and time in the Timestamp boxes and then click Analyze Content.

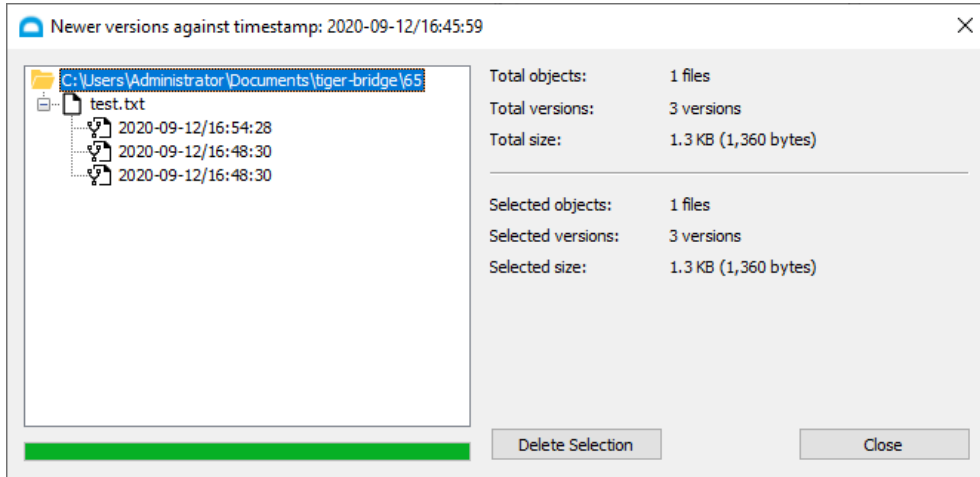
Manually Manage Data

**Note:** Depending on the number of files in the folder and their size the analysis may take time. Keep track of the progress bar below, to make sure Tiger Bridge has gathered complete information.



4. Click Newer.

Tiger Bridge displays a dialog, listing all versions of a file, which have been replicated before the selected time and date, giving you information about the size of each version as well as about the total size of all versions.



5. Do one of the following:

- Select a whole folder, to delete all versions of all its files, which have been replicated after the selected date and time.
- Select a file, to delete all its versions, which have been replicated after the selected date and time.
- Select a file version, to delete just this version of the file.

6. Click Delete Selection.



# Appendix: Tiger Bridge Logs

## Information Logs

| Log message                                                                                        | Description                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source <source path> connected to <target type> target.                                            | Tiger Bridge successfully connected the specified source to its target.                                                                                                                                                                                                                                                                                                    |
| Replication target for source <source path> is online now.                                         | Displayed after unsuccessful attempt(s) to connect the specified source to the target, once the target is accessible to Tiger Bridge and it can perform data lifecycle management operations on it.                                                                                                                                                                        |
| File <path to file on source> is successfully replicated on the target.                            | The specified file has been successfully replicated on the target by the automatic or manual data replication mechanism.                                                                                                                                                                                                                                                   |
| Replication of file <path to file on source> has been aborted due to requested write access to it. | The replication of the specified file has been aborted, because a user or application has opened it on the source. If the file has been scheduled for automatic data replication, once it is no longer in use, it will be queued for replication anew.                                                                                                                     |
| File <path to file on source> is replaced with a stub file on the source.                          | The specified replicated file has been successfully replaced by a nearline file on the source by the automatic or manual space reclaiming mechanism.                                                                                                                                                                                                                       |
| File <path to file on source> <process name> is successfully retrieved on the source.              | The specified nearline file on the source has been successfully retrieved from the target. If the nearline file has been retrieved manually through the shell extension or the command-line interface, the process name is “user operation”, if the nearline file has been retrieved by attempting to open it on the source, the message displays the name of the process. |
| File <path to file on source> is moved to <tier type> storage on the target.                       | A replicated file has successfully been moved from the hot/cool tier of the target to the archival tier, the automatic or manual data archiving mechanism. The stub file icon on the source changes from nearline to offline.                                                                                                                                              |
| License capacity exceeded.                                                                         | You have reached the capacity of your license and Tiger Bridge will not replicate any more data until you upgrade your license or delete data on your source.                                                                                                                                                                                                              |

## Warning Logs

| Log message                                                        | Description                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source <path to source> failed to connect to <target type> target. | The target of the specified source is currently inaccessible. The reason for the problem may be lost connection or changed credentials for access to the target. Tiger Bridge attempts to connect to the target and in case it fails to do so until a specified timeout expires, it displays an error message. |

## Appendix: Tiger Bridge Logs

| Log message                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Replication target for source <path to source> is not accessible.                 | The specified source has been disconnected from its target, because it is currently inaccessible. The reason for the problem may be lost connection or changed credentials for access to the target. Tiger Bridge attempts to re-connect to the target and in case it fails to do so until a specified timeout expires, it displays an error message.                                                                                                                                                         |
| Replication of file <path to file on source> failed.                              | Tiger Bridge's attempt to replicate the specified file to the target has failed. The reason for the failed operation may be temporary inaccessibility of the target, for example. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.                                                                                                                                                              |
| Replacing file <path to file on source> with a stub file on the source failed.    | Tiger Bridge's attempt to automatically reclaim space on the source by replacing the specified file with a nearline file has failed. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.                                                                                                                                                                                                           |
| Moving file <path to file on source> to <tier type> storage on the target failed. | Tiger Bridge's attempt to move the specified replicated/nearline file from the hot/cool tier of the target to the archival tier has failed. The reason for the failed operation may be temporary inaccessibility of the target, for example. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.                                                                                                   |
| Adding file <file name> failed.                                                   | Tiger Bridge's attempt to synchronize the contents of two sources through a common target by creating a nearline/offline file in the source of one computer upon receiving notification for replicated file from another computer has failed. The reason for the failed operation may be temporary inaccessibility of the target, for example. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message. |
| Removing file <file name> failed.                                                 | Tiger Bridge's attempt to synchronize the contents of two sources through a common target by removing a nearline/offline file in the source of one computer upon receiving notification for removed file from another computer has failed. The reason for the failed operation may be temporary inaccessibility of the target, for example. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.    |

| Log message                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Renaming file <current file name> to <updated file name> failed. | Tiger Bridge's attempt to synchronize the contents of two sources through a common target by renaming a nearline/offline file in the source of one computer upon receiving notification for file rename on another computer has failed. The reason for the failed operation may be temporary inaccessibility of the target, for example. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message. |
| Failed to parse sync notification <notification ID>.             | Tiger Bridge's attempt to parse a notification for updated contents on one computer when synchronizing it with the contents of another computer through a common target (active sync) has failed. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.                                                                                                                                        |
| Failed to process notification <notification ID>.                | Tiger Bridge's attempt to process a notification for updated contents on one computer when synchronizing it with the contents of another computer through a common target (active sync) has failed. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.                                                                                                                                      |

## Error Logs

| Log message                                                                | Description                                                                                                                                                    | Suggested action                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source location is missing. Volume with guid <volume GUID> is not mounted. | Tiger Bridge failed to load a source, because the GUID of the volume, on which it is stored, does not match the GUID of any volume accessible to Tiger Bridge. | <p>Check for the following:</p> <ul style="list-style-type: none"> <li>• Verify that the volume is mounted on the computer.</li> <li>• If the volume cannot be mounted (is corrupted, for example), to recover replicated data from it, configure a new source on a healthy volume, pair it with the same target and synchronize their contents.</li> </ul> |

# Appendix: Tiger Bridge Logs

| Log message                                                                     | Description                                                                                                                                                                                        | Suggested action                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source location <path to source> is missing.                                    | Tiger Bridge managed to load the volume on which the specified source is stored, but failed to load the source itself, because the path to it has changed.                                         | <p>Check for the following:</p> <ul style="list-style-type: none"> <li>• Verify that the path to the folder added as a source is not changed (a folder is renamed or deleted, for example).</li> <li>• If the folder added as a source is deleted, to recover replicated data from it, configure a new source on the same or another volume, pair it with the same target and synchronize their contents.</li> </ul> |
| Source <path to source> cannot be loaded.                                       | Tiger Bridge failed to load a source, because it does not match the source storage requirements any more.                                                                                          | <p>Check for the following:</p> <ul style="list-style-type: none"> <li>• Verify that the permissions for access to the source have not changed. Refer to “Source Storage Requirements” on page 15 for more information.</li> <li>• Verify that a source on a Tiger Store-managed is not now mounted as a Tiger Client on the Tiger Bridge computer.</li> </ul>                                                       |
| Replication of file <path to file on source> failed.                            | <p>All attempts to replicate the specified file on the target have failed.</p> <p><b>Note:</b> <i>To let Tiger Bridge attempt to replicate the file again, you must restart Tiger Bridge.</i></p>  | <p>Check for the following:</p> <ul style="list-style-type: none"> <li>• Make sure the file is not corrupted.</li> <li>• Make sure the target is still accessible and has not returned any errors.</li> </ul>                                                                                                                                                                                                        |
| Retrieving file <path to file on source> <process name> from the target failed. | <p>All attempts to retrieve the specified file from the target have failed.</p> <p><b>Note:</b> <i>To let Tiger Bridge attempt to replicate the file again, you must restart Tiger Bridge.</i></p> | <p>Check for the following:</p> <ul style="list-style-type: none"> <li>• Make sure the target is accessible.</li> <li>• If the target is accessible, make sure the replicated file is not deleted from the target.</li> <li>• If the file is deleted and your target has versioning turned on, attempt to undelete it on the target.</li> </ul>                                                                      |

| Log message                                                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                        | Suggested action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modified files count threshold has been reached. Replication has been paused for source <path to source>. | <p>The number of already replicated files queued for replication again because they have been modified has exceeded the number you have set as a ransomware protection threshold and Tiger Bridge paused all its automatic operations.</p> <p><b>Note:</b> <i>Once the problem is resolved, to resume automatic Tiger Bridge operations, follow the steps in "Pause/Resume Automatic Tiger Bridge Operations" on page 102.</i></p> | <p>Check for the following:</p> <ul style="list-style-type: none"> <li>• Make sure that none of the files on your source is encrypted as part of a ransomware attack.</li> <li>• If one or more files are encrypted, restore their unencrypted versions, following the steps in "Manage Files and Folders Versions" on page 162.</li> <li>• If none of the files is encrypted, change the ransomware protection threshold, following the guidelines provided in "Enable and Configure Ransomware Protection" on page 132.</li> </ul> |
| License capacity exceeded.                                                                                | <p>The amount of data, managed by Tiger Bridge has exceeded the capacity specified in your license and Tiger Bridge has stopped replicating any new data.</p>                                                                                                                                                                                                                                                                      | <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• Contact your Tiger Bridge reseller to exceed your license capacity.</li> <li>• Delete files on your source(s). For more information, refer to "Tiger Bridge Licensing" on page 13.</li> </ul>                                                                                                                                                                                                                                                               |

## Appendix: Tiger Bridge Logs

# index

## A

- access
  - command-line interface 10
  - shell extension 11
  - Tiger Bridge Configuration 9
- activate
  - Tiger Bridge 31
- active sync
  - configure 95, 125
- archived data
  - statistics 104, 128
- archiving
  - configure 91, 124
- Azure Blob storage
  - configure for work with Tiger Bridge 40

## B

- Backblaze storage
  - configure for work with Tiger Bridge 49, 113
- BlackPearl
  - configure for work with Tiger Bridge 74, 115

## C

- Coeus
  - configure for work with Tiger Bridge 76, 116
- command-line interface
  - access 10
  - manually manage data 157
- configure
  - active sync 95, 125
  - archiving 91, 124
  - data replication 83, 121
  - operation mode 100, 127
  - space reclaiming 86, 122

## D

- data
  - manage through command-line 157
  - manage through shell extension 156
  - statistics 104, 128
- data replication
  - configure 83, 121
- disable
  - remote shell extension access 135
  - Tiger Bridge 129

## E

- enable
  - ransomware protection 133
  - remote shell extension access 135

## F

- FujiFilm object archive storage
  - configure for work with Tiger Bridge 78

## G

- Google Cloud
  - configure for work with Tiger Bridge 70
- Google Drive
  - configure for work with Tiger Bridge 72

## H

- Hitachi HCP target
  - configure for work with Tiger Bridge 55

## I

- IBM cloud object storage
  - configure for work with Tiger Bridge 46, 111

install

Tiger Bridge 24

Tiger Bridge shell extension 26

L

local volume target

configure for work with Tiger Bridge 82, 119

locations

excluded 84, 120

included 84, 120

LYVE Cloud target

configure for work with Tiger Bridge 60, 62

M

manage

data through command-line 157

data through shell extension 156

Tiger Bridge logs 148

monitor

data statistics 104, 128

N

nearline data

statistics 104, 128

network share

configure for work with Tiger Bridge 80, 118

O

operation mode

configure 100, 127

P

proxy server

specify 135

R

ransomware protection

enable 133

replicated data

statistics 104, 128

requirements

source 15

target 16

S

S3 object storage

configure for work with Tiger Bridge 43, 110

S3-compatible object storage

configure for work with Tiger Bridge 67, 114

Seagate CORTX target

configure for work with Tiger Bridge 65

shell extension

access 11

disable remote access 135

enable remote access 135

manually manage data 156

source

requirements 15

synchronize with target 159

space reclaiming

configure 86, 122

specify

proxy server 135

statistics

monitor 104, 128

Swift target

configure for work with Tiger Bridge 57

synchronize

source and target content 159

T

target

requirements 16

synchronize with source 159

Tiger Bridge

activate 31

check for updates 27

configure with Azure Blob storage 40

configure with Backblaze B2 cloud storage 49,  
113

configure with BlackPearl 74, 115

configure with Coeus 76, 116

configure with FujiFilm object archive 78

configure with Google Cloud storage 70

configure with Google Drive 72

configure with Hitachi HCP target 55

configure with IBM cloud object storage 46,  
111

configure with local volume target 82, 119

configure with LYVE Cloud target 60, 62

configure with network share 80, 118

configure with S3 object storage 43, 110

configure with S3-compatible storage 67, 114

configure with Seagate CORTX target 65

- configure with Swift target 57
- configure with Wasabi cloud storage 52
- disable 129
- disable configuration 129
- how it works 6
- install 24
- license 31
- system requirements 14
- uninstall 27
- update 27
- view activation status 31, 108

Tiger Bridge Configuration

- access 9

Tiger Bridge logs

- manage 148

Tiger Bridge shell extension

- install on remote computer 26

## U

- uninstall
  - Tiger Bridge 27
- update
  - Tiger Bridge 27

## V

- view
  - activation status 31, 108

## W

Wasabi storage

- configure for work with Tiger Bridge 52

