Tiger
Technology

Tiger Bridge Administration Guide

Version: 5.1

Revision: 11 October 2024

TIGER BRIDGE IS A BRAND OF TIGER TECHNOLOGY. 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

Title	Tiger Bridge Administration Guide
Software version:	5.1
Date:	11 October 2024

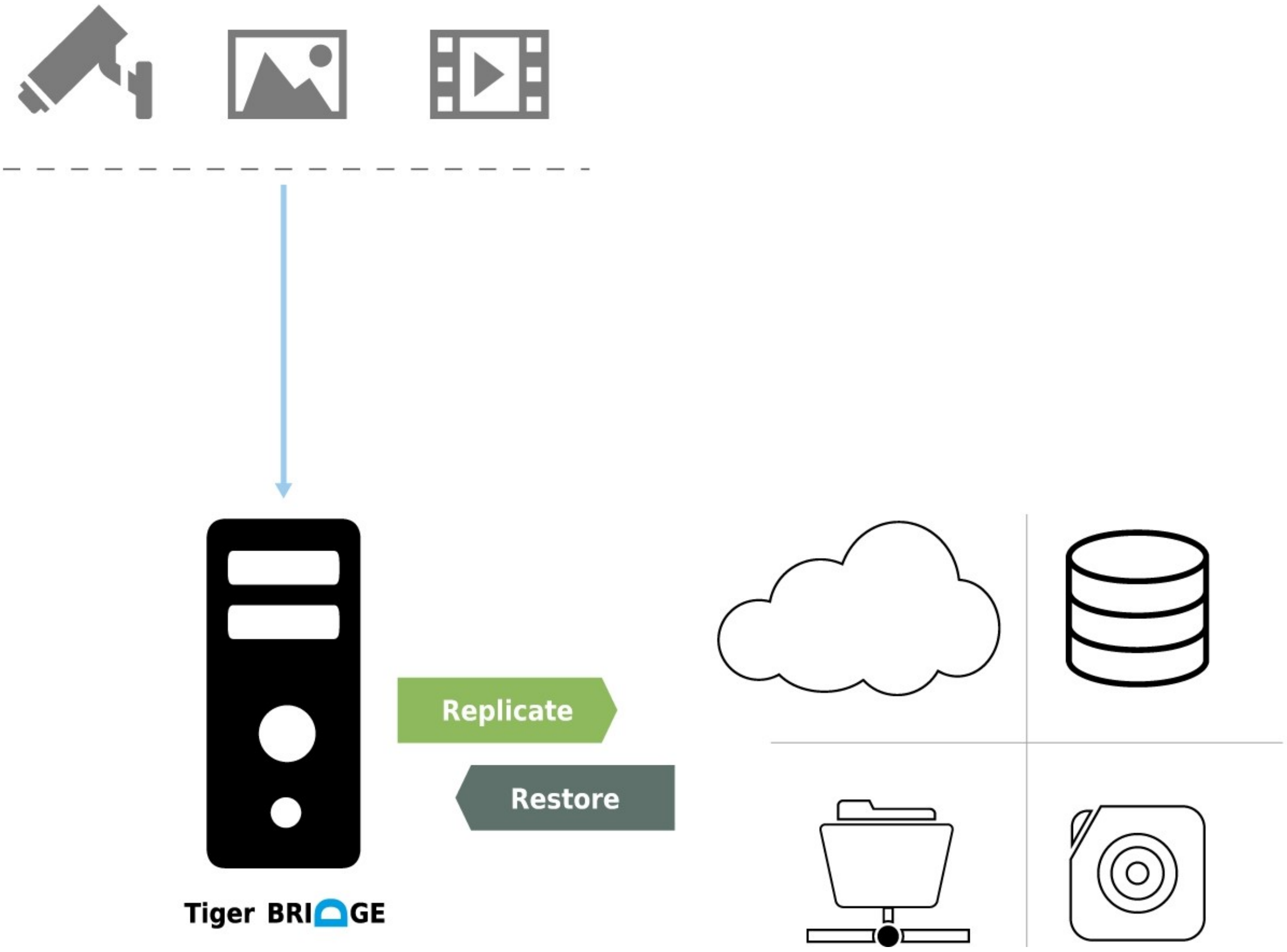
Table of Contents

Introduction to Tiger Bridge

Congratulations on your purchase of Tiger Bridge, Tiger Technology's data manager across heterogeneous storage tiers. It lets you pair a source (locally mounted NTFS/ReFS volume or an SMB/NFS network share) with a target of your choice (cloud 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 data backup and disaster recovery, 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. You can configure a policy, which instructs which files need to be copied to the target automatically and transparently, without obstructing your workflow. You can also manually replicate a file or a whole folder 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 73.

Space reclaiming - Tiger Bridge frees space on the source by replacing an already replicated file with a stub file - a file, which looks exactly like the actual file it replaces but does not contain any data. A stub file points to the actual file on the target, which allows its retrieval back to the source. In Tiger Bridge, there are two types of stub files depending on the tier of the target where the actual file is stored – a nearline file points to the actual file on the hot/cool tier of the target, and an offline file points to the actual file on the archival tier of the target. Attempting to open a nearline file on the source triggers its automatic retrieval from the target. On the other hand, by default, offline files can be retrieved only manually, through Tiger Bridge. You can configure a policy, which instructs Tiger Bridge which files need to be replaced by stubs on the source. You can also manually reclaim space through the Tiger Bridge shell extension or command-line interface. The most common scenario with space reclaiming is implementing hierarchical storage and alignment of data with storage costs. To learn more, refer to Configure Automatic Space Reclaiming on page 76.

Data archiving - Tiger Bridge moves an already replicated file from the hot/cool tier of the target to the archival tier. If space reclaiming is enabled and the archived file needs to be replaced by a stub to free space on the source, it is replaced by an offline file, which by default you can manage only manually – by rehydrating it to the hot/cool tier or by retrieving it on the source. You can configure an archiving policy, which instructs Tiger Bridge which files need to be archived. You can also manually archive files or whole folders using the Tiger Bridge shell extension or command-line interface. The most common scenario with data archiving is aligning data with storage costs and moving unused data to an archive. To learn more, refer to Automatic Archiving on page 79.

Sync — Tiger Bridge automatically synchronizes the contents of multiple sources, each on a different computer running Tiger Bridge, through a common target. The mechanism is designed to facilitate geo-replication scenarios. To learn more, refer to Configure Multi-Site Sync on page 84.

Data synchronization - manually or automatically synchronize the contents of a target with the source it is paired with. In case Tiger Bridge detects that a file on the target is not available on the source, the synchronization mechanism can recreate it, letting you choose from multiple options depending on the desired result. Data synchronization facilitates scenarios involving data migration from one source to another and disaster recovery of data. For more information, refer to Recover Data from The Target on page 131.

Data versioning – Tiger Bridge automatically creates versions of source files when replicating them on the target instead of overwriting them. You can configure a policy, which instructs Tiger Bridge how many versions of a file to keep on the target. You can also manually manage versions and switch between the version of a file or a folder that is available on the source as well as undelete a file from the source. For more information, refer to Configure Versioning on page 86.

Note: To benefit from data versioning your target must support keeping file versions.

By combining the above data management mechanisms with remote shell extension access, ransomware protection, progressive retrieval of data from the target, and all necessary tools to control and monitor every process, Tiger Bridge can be deployed for any of the following purposes:

- data backup and disaster recovery
- data archiving

- 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

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 below.
- The Tiger Bridge workflow supports applying any Windows techniques for controlling access to and protecting data at rest at the 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.
- 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 by relying on the target provider's own mechanism for protecting data in transit, like AWS libraries, for example.

Tiger Technology encourages you to use any applicable best practices for data protection specified by Microsoft Windows and by your target provider. To ensure the integrity of data at rest at the target, you enable and configure the Tiger Bridge checksum verification. For more information, refer to ???

Tiger Bridge Interfaces

Tiger Bridge Configuration

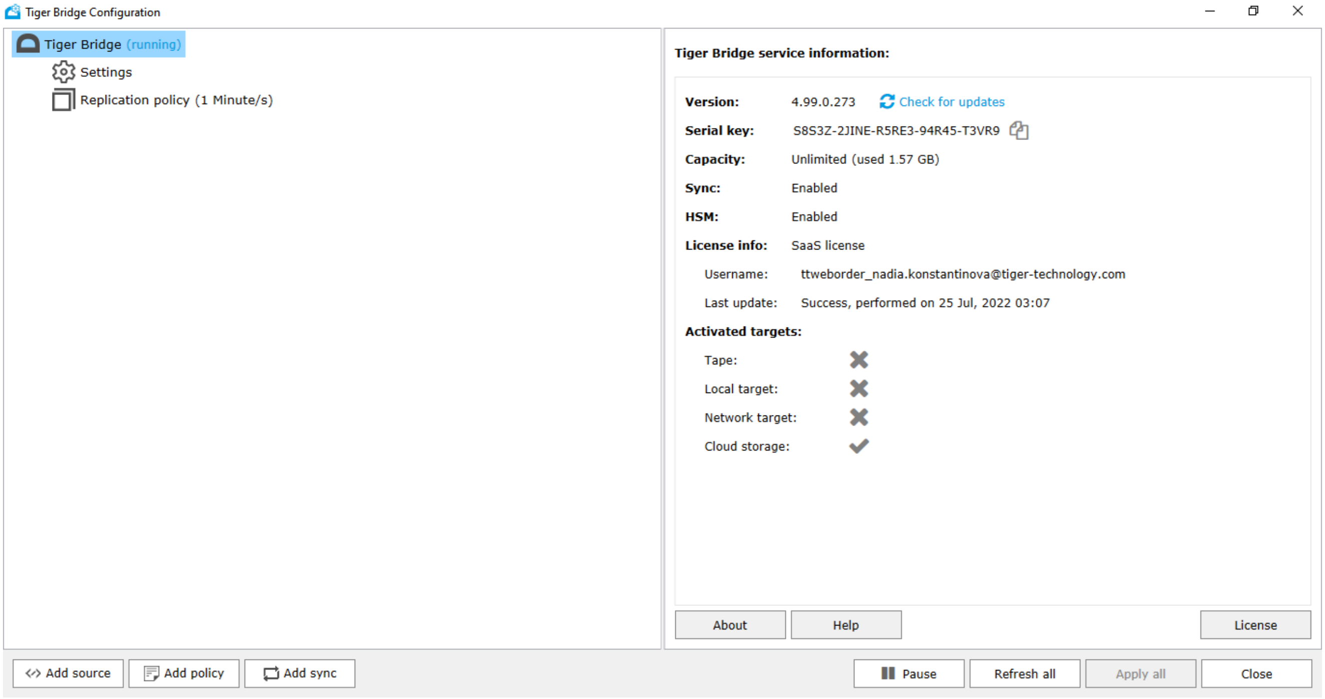
Use the graphic user interface of the product, the Tiger Bridge Configuration to create pairs of source and target and configure the automatic data management mechanisms.

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:

- Click the Tiger Bridge tray icon.
- Double-click the Tiger Bridge Configuration shortcut on the desktop.
- Navigate to the installation folder of the Tiger Bridge Configuration and double-click Tiger-BridgeConfiguration.exe.



Tiger Bridge service information:

Version: 4.99.0.273

Serial key: S8S3Z-2JINE-R5RE3-94R45-T3VR9

Capacity: Unlimited (used 1.57 GB)

Sync: Enabled

HSM: Enabled

License info: SaaS license

Username: ttweborder_nadia.konstantinova@tiger-technology.com

Last update: Success, performed on 25 Jul, 2022 03:07

Activated targets:

Tape: ✗

Local target: ✗

Network target: ✗

Cloud storage: ✓

Tiger Bridge Explorer

A graphic interface browser that allows you to explore the contents of your sources filtering the displayed results by source, data status, and target tier. You can also use the Tiger Bridge Explorer to perform manual operations, including bulk operations on multiple files with the same status.

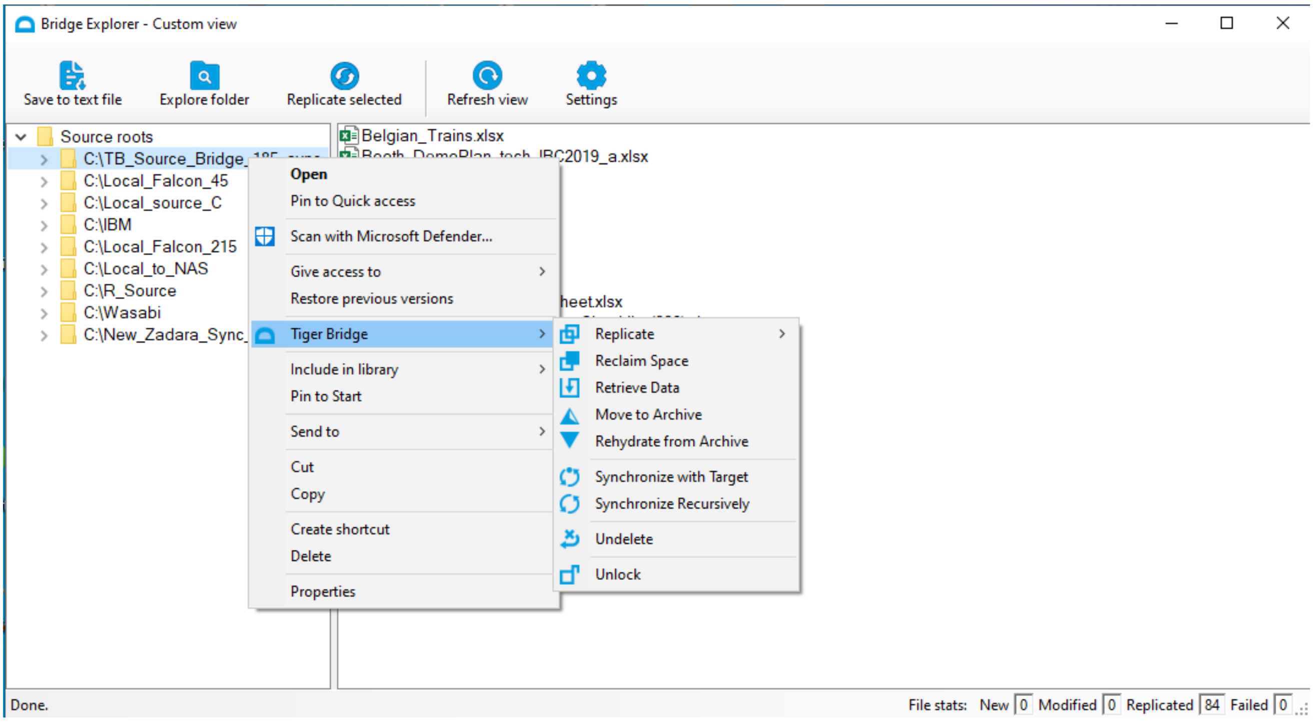
For more information about monitoring data in the Tiger Bridge Explorer, refer to Monitor Data in Tiger Bridge Explorer on page 144.

For more information about manually managing data in the Tiger Bridge Explorer, refer to Perform Manual Data Lifecycle Operations on page 129.

To access the Tiger Bridge Explorer:

Do one of the following:

- Double-click the Tiger Bridge tray icon to open the Tiger Bridge Explorer with a predefined filter showing you all files with pending replication.
- Right-click the Tiger Bridge tray icon and then click “Show failed files” to open the Tiger Bridge Explorer with a predefined filter showing you all files that have failed to replicate.



File stats: New 0 Modified 0 Replicated 84 Failed 0

Command-line Interface

The command-line interface of Tiger Bridge lets you activate and configure the product and perform manual operations on data. The main advantage of using the command-line interface is that you can automate specific tasks by including the commands in a script. For a full list of all available commands, refer to "Appendix 1: Tiger Bridge Command-line Interface" on page 154.

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 using icon overlays. 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 Perform Manual Data Lifecycle Operations on page 129.

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 a local storage source exported as an SMB share. `For this purpose, a Tiger Bridge administrator must allow remote shell extension access to the sources. For more information, refer to Enable Remote Shell Extension Access on page 98.

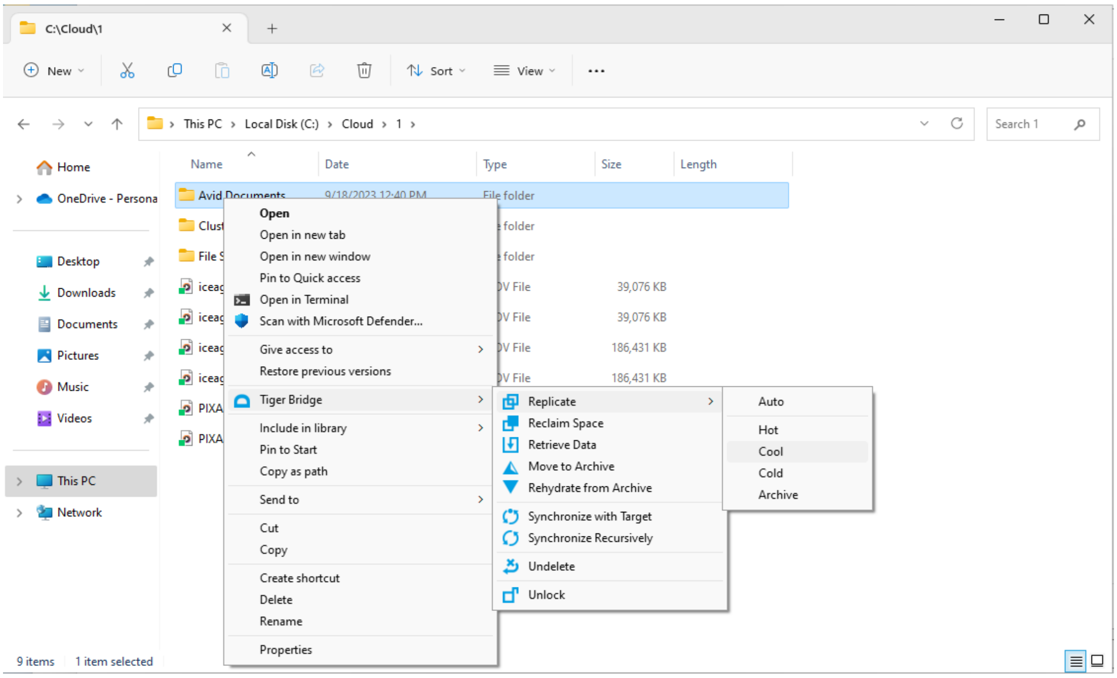
Only a user with administrative privileges on the remote computer can run the shell extension. Additionally, the user needs to provide the IP address of the Tiger Bridge computer and the full local path to the local storage source or the local control folder of a NAS source on the Tiger Bridge computer.

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

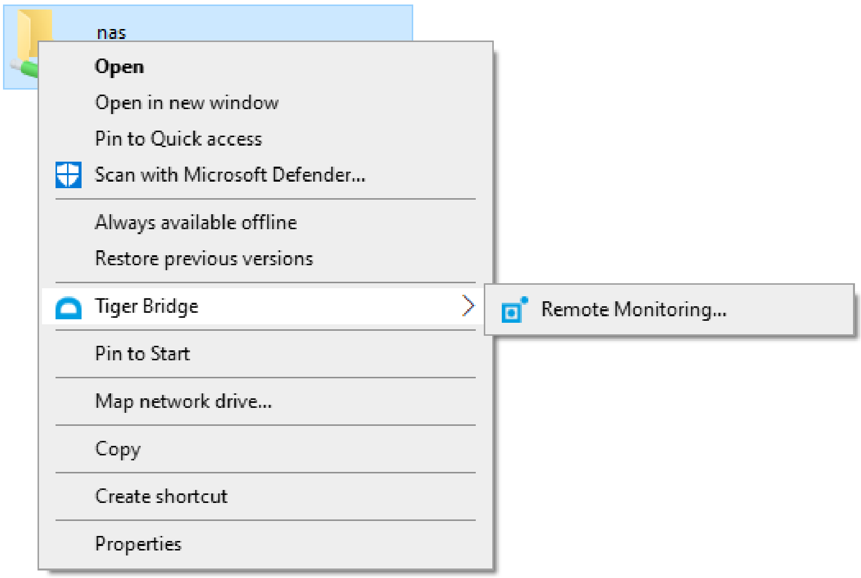
The shell extension can be installed together with Tiger Bridge or as a separate component on a remote computer. For more information, refer to Install Tiger Bridge on page 55.

To access the Tiger Bridge shell extension context menu:

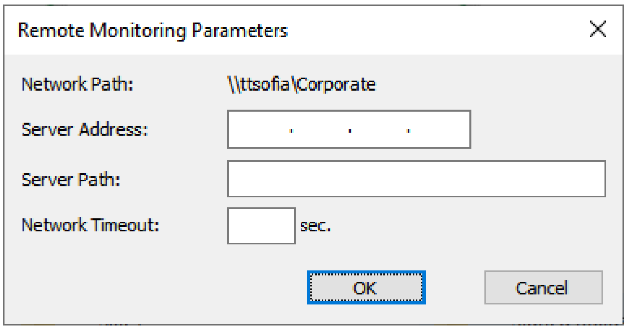
1. In Windows Explorer or the Tiger Bridge Explorer, navigate to a source paired with a target.
2. Right-click the file/folder you want to manage and in the context menu, select the respective command under Tiger Bridge.



3. On remote computers, before gaining access to the Tiger Bridge shell extension commands, you need to click Remote Monitoring under Tiger Bridge:



4. In Remote Monitoring Parameters, enter the following details to authorize your access to the source:


Remote Monitoring Parameters

Network Path: \\ttsofia\Corporate

Server Address: . . .

Server Path:

Network Timeout: sec.

- Server address - the IP address of the computer running Tiger Bridge.
- Server path (local storage source exported as an SMB share) - the full local path to the source on the computer running Tiger Bridge. For example, if you are accessing a local storage source folder “Source”, which is a sub-folder of the folder “Documents” in the root of drive D on the Tiger Bridge computer, enter the following in Server Path:
  D:\Documents\Source
- Server path (NAS source accessible as an SMB share) - the full local path to the control folder on the computer running Tiger Bridge. For example, if the control folder of the NAS share is named “Control” and is a sub-folder of the folder “Documents” in the root of drive D on the Tiger Bridge computer, enter the following in Server Path:
  D:\Documents\Control

Note: Currently, you cannot gain remote shell extension access to an NFS share source.

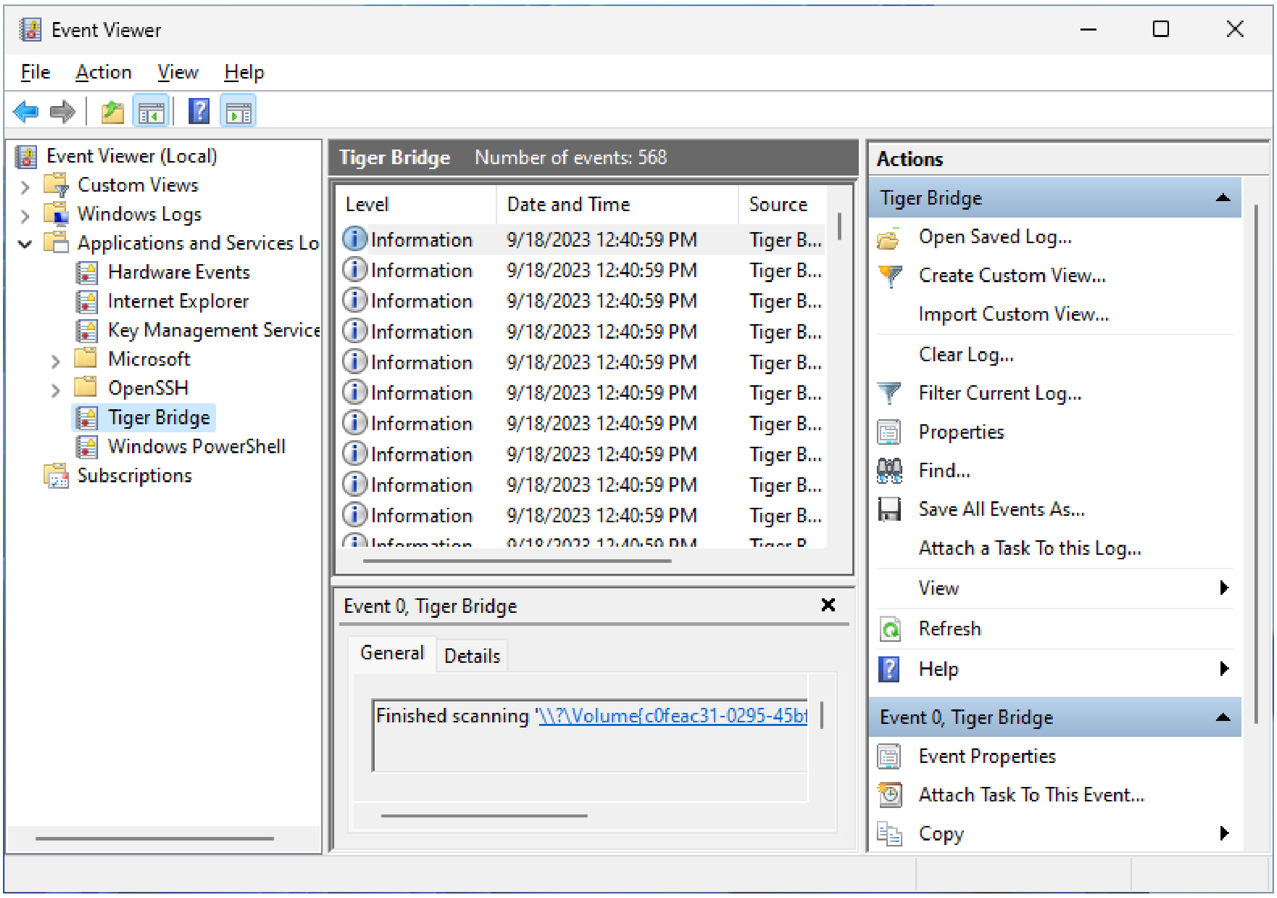
- Specify the timeout after which attempting to perform a shell extension operation should be considered failed, but not delayed. A few seconds are considered normal timeout for receiving a response to complete an operation.

Windows Event Viewer

To let you monitor its activity, Tiger Bridge logs all target/source connectivity events in the Windows Event Viewer. You can also configure Tiger Bridge to log an event each time a file is replicated or replaced with a nearline/offline file, a nearline file is retrieved from the target, or when the status of a directory on the source is changed. For more information, refer to Monitor Tiger Bridge in the Event Viewer on page 152.

To access the Tiger Bridge logs in the Event Viewer:

Right-click the Tiger Bridge tray icon and click “Open Event Viewer”.



Level	Date and Time	Source
Information	9/18/2023 12:40:59 PM	Tiger B...
Information	9/18/2023 12:40:59 PM	Tiger B...
Information	9/18/2023 12:40:59 PM	Tiger B...
Information	9/18/2023 12:40:59 PM	Tiger B...
Information	9/18/2023 12:40:59 PM	Tiger B...
Information	9/18/2023 12:40:59 PM	Tiger B...
Information	9/18/2023 12:40:59 PM	Tiger B...
Information	9/18/2023 12:40:59 PM	Tiger B...
Information	9/18/2023 12:40:59 PM	Tiger B...
Information	9/18/2023 12:40:59 PM	Tiger B...

Finished scanning '\\?\Volume{c0feac31-0295-45bt

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 59.

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 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, except for excluded locations (subfolders of your source, which you have specified that Tiger Bridge should not manage automatically). Thus, if you add a source containing 2 TB of data, even if only 1 TB of its files are currently replicated or replaced by stub files, the overall capacity of this source will be calculated as 2 TB. You can monitor your usage and billing history in your account on the Tiger Technology licensing server.

You can keep track of your current capacity usage, by following the steps in Monitor Tiger Bridge in the Configuration on page 143.

Tiger Bridge System Requirements

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

- PC with a 64-bit (x64) processor.

Note: Tiger Bridge actively uses the APIs provided by the target provider. These APIs may take a significant amount of CPU depending on the 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, Windows® 11/Server 2022.

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 would be approximately 100 MB. 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 – remote shell extension access

  ✓ 8537 - inbound and outbound rules

- The GlobalSign certification authority's currently used root certificate must be installed on the computer and its "Code Signing" purpose must not be disabled. For more information, refer to Digital Certificate Requirements below.
- Microsoft .NET Framework 4.8

Note: As long as your computer is connected to the Internet, the Tiger Bridge installation automatically installs Microsoft .NET Framework 4.8 if it is not already installed.

Digital Certificate Requirements

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

- R3 GlobalSign Root Certificate from GlobalSign
- R6 GlobalSign Root Certificate from GlobalSign
- DigiCert Assured ID Root CA from DigiCert

On computers operating in less restrictive environments, this is done automatically during the installation of Tiger Bridge. If the computer on which you want to install Tiger Bridge or any of its components operates in a more restrictive domain environment or is not connected to the Internet, you must manually download the above certificates from GlobalSign and install them yourself, before installing Tiger Bridge. In addition, you must ensure that the "Code Signing" purpose of the root certificate is enabled.

High Availability Requirements

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 and both 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.

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

Note: 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. For more details, refer to Disable NFS Locking on the Tiger Bridge Computer on page 106.

Important: 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 in case you enable space reclaiming and/or data archiving. For details about configuring a NAS source, refer to NAS Source Prerequisites and Setup on page 65.

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.

Supported Target Storage

Note: Refer to Target Storage Prerequisites on page 20 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

  ✓ Huawei Cloud

  ✓ Backblaze B2 Cloud Storage

  ✓ Google Drive storage

  ✓ LYVE Cloud

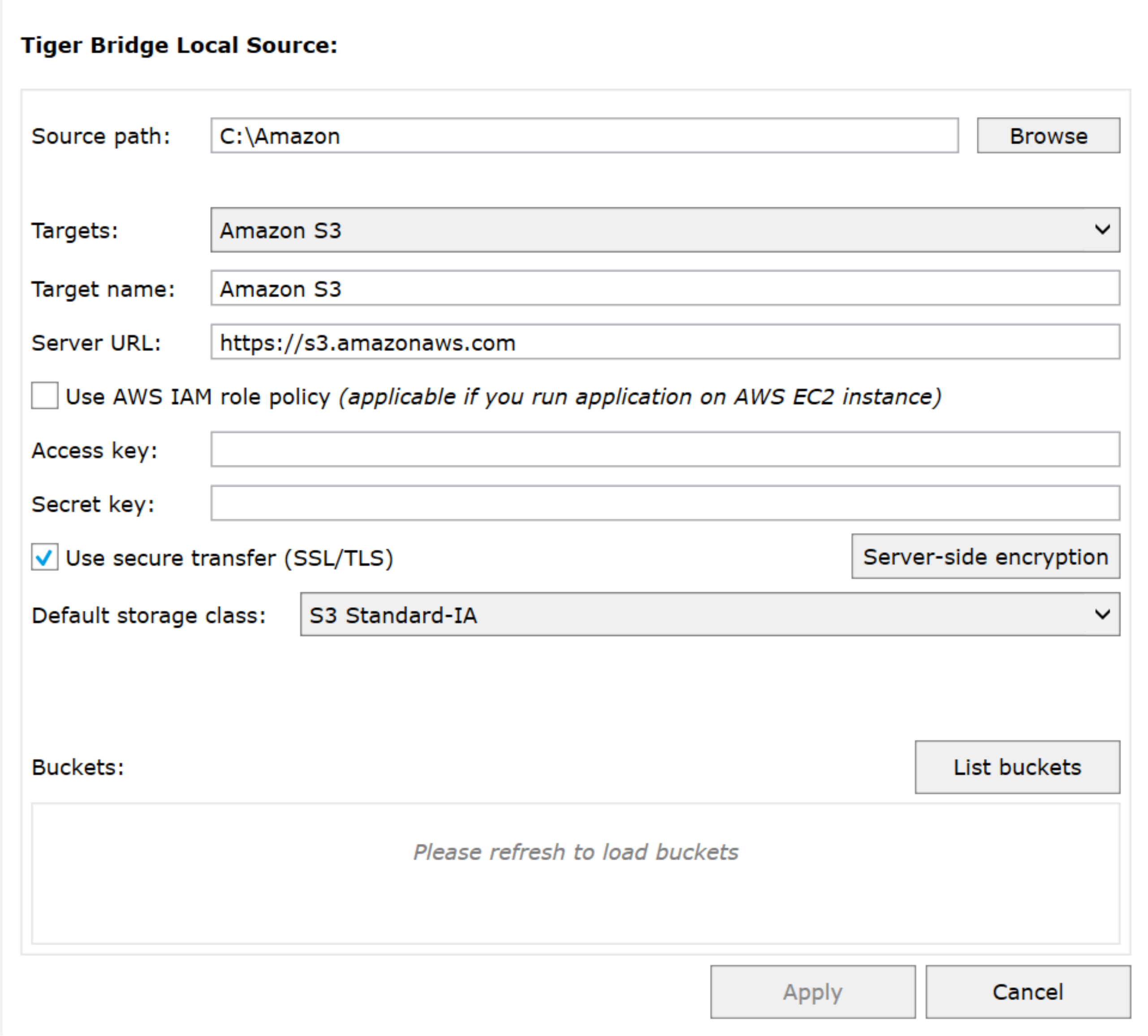
  ✓ ORockCloud

  - ✓ RSTOR Space
  - ✓ Symply NEBULA
  - ✓ Wasabi Hot Cloud Storage
  - ✓ S3-compatible object storage (using protocol signature version 2 or 4)
- On-premises object store with hot tier:
  - ✓ Cloudian object storage
  - ✓ Hitachi Content Platform (HCP)
  - ✓ IBM COS
  - ✓ OpenStack Swift
  - ✓ S3-compatible object storage (using protocol signature version 2)
  - ✓ Seagate CORTX
  - ✓ Zadara
- On-premises object store for archive:
  - ✓ Spectra BlackPearl Deep Storage Gateway
  - ✓ Coeus managed digital content library
  - ✓ FujiFilm Object Archive
- On-premises non-object store:
  - ✓ NTFS or ReFS volume mounted on the Tiger Bridge computer with Read & Write permissions
  - ✓ SMB or NFS network share

Target Storage Prerequisites

Amazon S3 Object Storage

To pair a source with an Amazon S3 object storage target, you must provide the following information:



Tiger Bridge Local Source:

Source path: C:\Amazon

Targets: Amazon S3

Target name: Amazon S3

Server URL: https://s3.amazonaws.com

□ Use AWS IAM role policy *(applicable if you run application on AWS EC2 instance)*

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Default storage class: S3 Standard-IA

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- URL of the Amazon S3 server

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

- IAM user credentials to be used by Tiger Bridge for access to the bucket designated for the respective source

Note: If Tiger Bridge runs on an AWS EC2 instance, instead of providing credentials for access to the respective bucket, you can specify that it should use the role attached to the EC2 policy as long as it provides the minimum required access rights to the bucket.

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.htm

Tip: 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 the normal work of Tiger Bridge 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",
"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

- If server-side encryption is enabled on the respective bucket, when configuring the target specify the option used - Amazon S3 key, AWS Key Management Service key, or a customer-provided encryption key and if required by the respective method provide the encryption key.
- Select whether to access the target using secure transfer (SSL/TLS)
- Select the Default storage class, to which Tiger Bridge should replicate data directly, omitting any intermediate tiers.

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

- To benefit from Tiger Bridge versioning, you must enable versioning on the target, by 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, by following the steps in Replicate File's Metadata to a Different Bucket/Container on page 114.

  ✓ if you use Governance mode, the account Tiger Bridge uses for access to the bucket(s) must not be an account, which has special permissions to alter the retention settings or delete the objects.
- Select a separate bucket for each source configured on the same computer

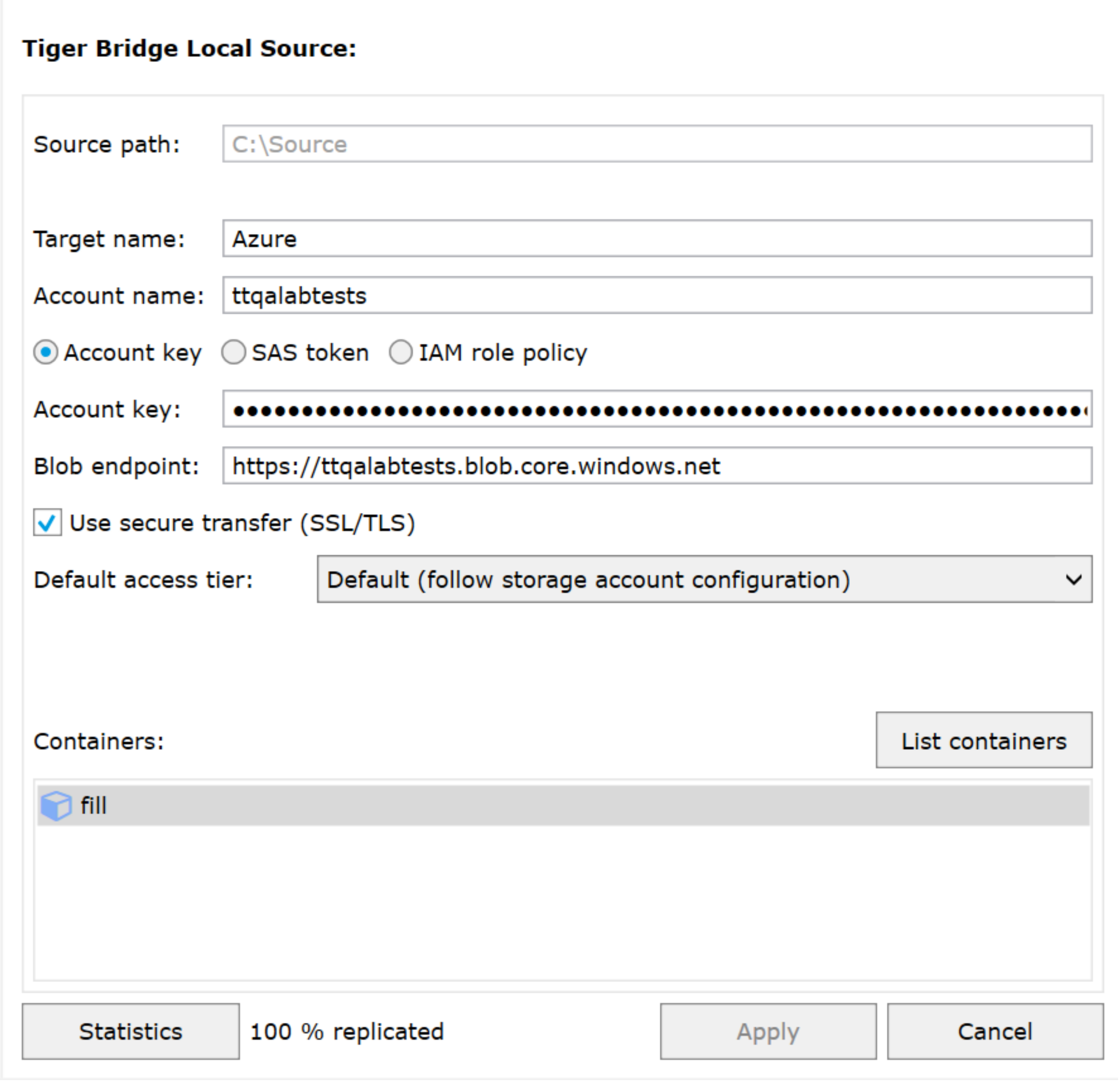
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the specific source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

Important: Access key rotation is not supported and must be disabled.

Microsoft Azure Blob Storage

To pair a source with an Azure Blob Storage target, you must provide the following information:



Tiger Bridge Local Source:

Source path: C:\Source

Target name: Azure

Account name: ttqalabtests

● Account key ○ SAS token ○ IAM role policy

Account key: ●●

Blob endpoint: https://ttqalabtests.blob.core.windows.net

☑ Use secure transfer (SSL/TLS)

Default access tier: Default (follow storage account configuration)

Containers:

fill

100 % replicated

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another container on the same target. The target name and its parameters will appear in the Targets drop-down box.

- The name of the account used for authenticating Tiger Bridge's access to the designated Azure Blob endpoint as well as the method for authenticating the access:

  ✓ account key

  ✓ SAS token with all permissions enabled. Additionally, you must manually enter the name of the container designated for the selected source.

  ✓ Azure IAM role policy

  ✓ SAS connection string

Note: Currently, you can pair a source with an Azure target using an SAS connection string only through the command-line interface of Tiger Bridge, by following the steps in Pair Source with a Microsoft Azure Target on page 156.

- Select whether to access the target using secure transfer (SSL/TLS).
- Select the Azure tier to be used for direct Tiger Bridge replication or select to use the default access tier set up at Azure for the storage account.
- Select a separate container for each source you pair with the same target, to which the account you have provided has at least write access

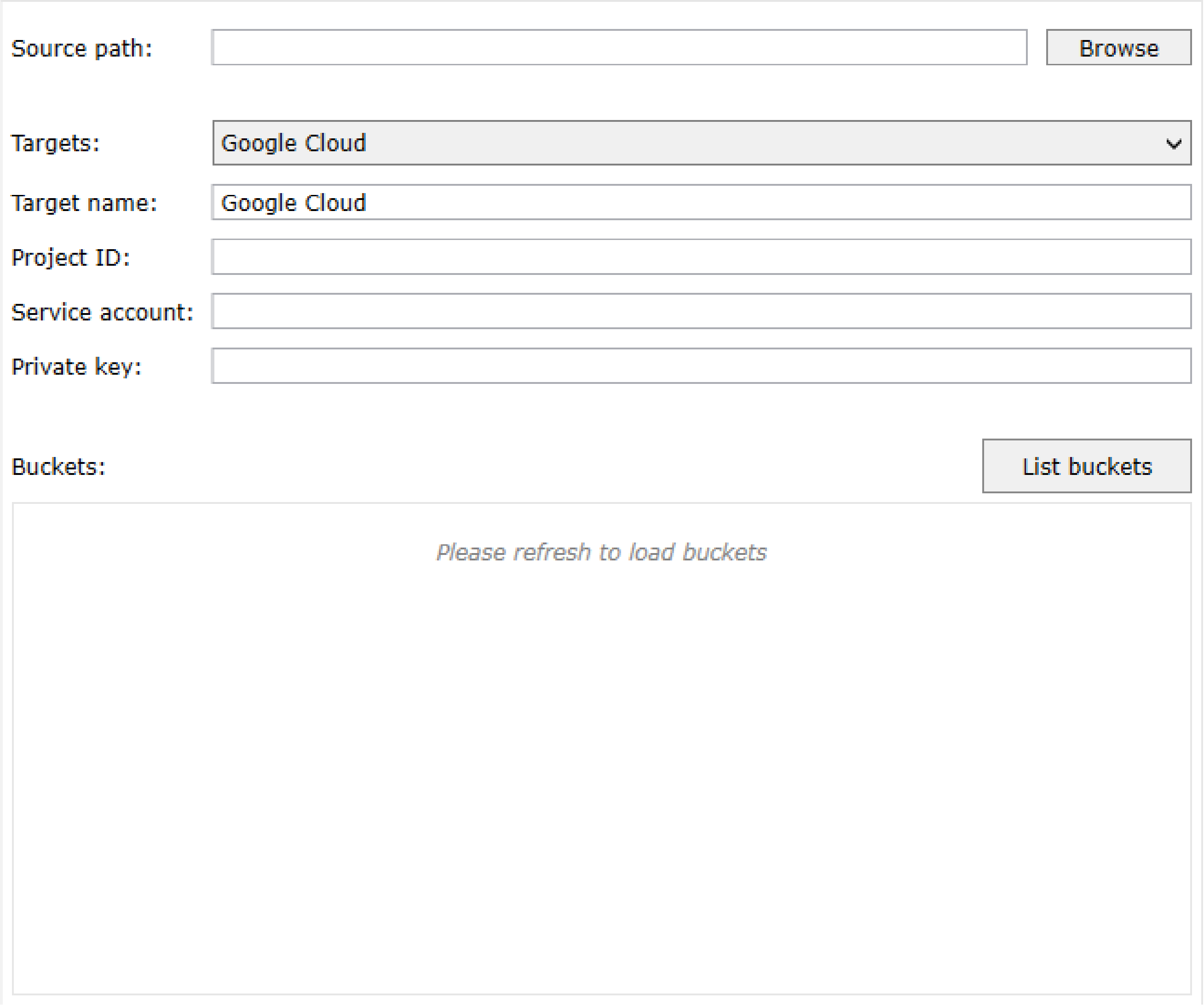
Note: If the user whose credentials you have provided does not have sufficient permissions to list all containers, Tiger Bridge displays a text box for you to manually enter the name of the container, which will be paired with the source.

Important: Do not change the name of the container as this may prevent Tiger Bridge replication from operating.

- To benefit from Tiger Bridge versioning, you must enable versioning (Blob snapshots or Blob versioning) and Soft delete on the target.

Google Cloud Storage

To pair a source with a Google cloud storage target, you must provide the following information:



Source path:

Targets: Google Cloud

Target name: Google Cloud

Project ID:

Service account:

Private key:

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The Project ID, service account email, and private JSON key for access to the bucket designated for the respective source.

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

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.

- To benefit from the Tiger Bridge versioning, you must enable object versioning on the respective bucket(s).

Note: You can enable object versioning using the Google Cloud SDK. For more information, see: https://cloud.google.com/storage/docs/using-object-versioning

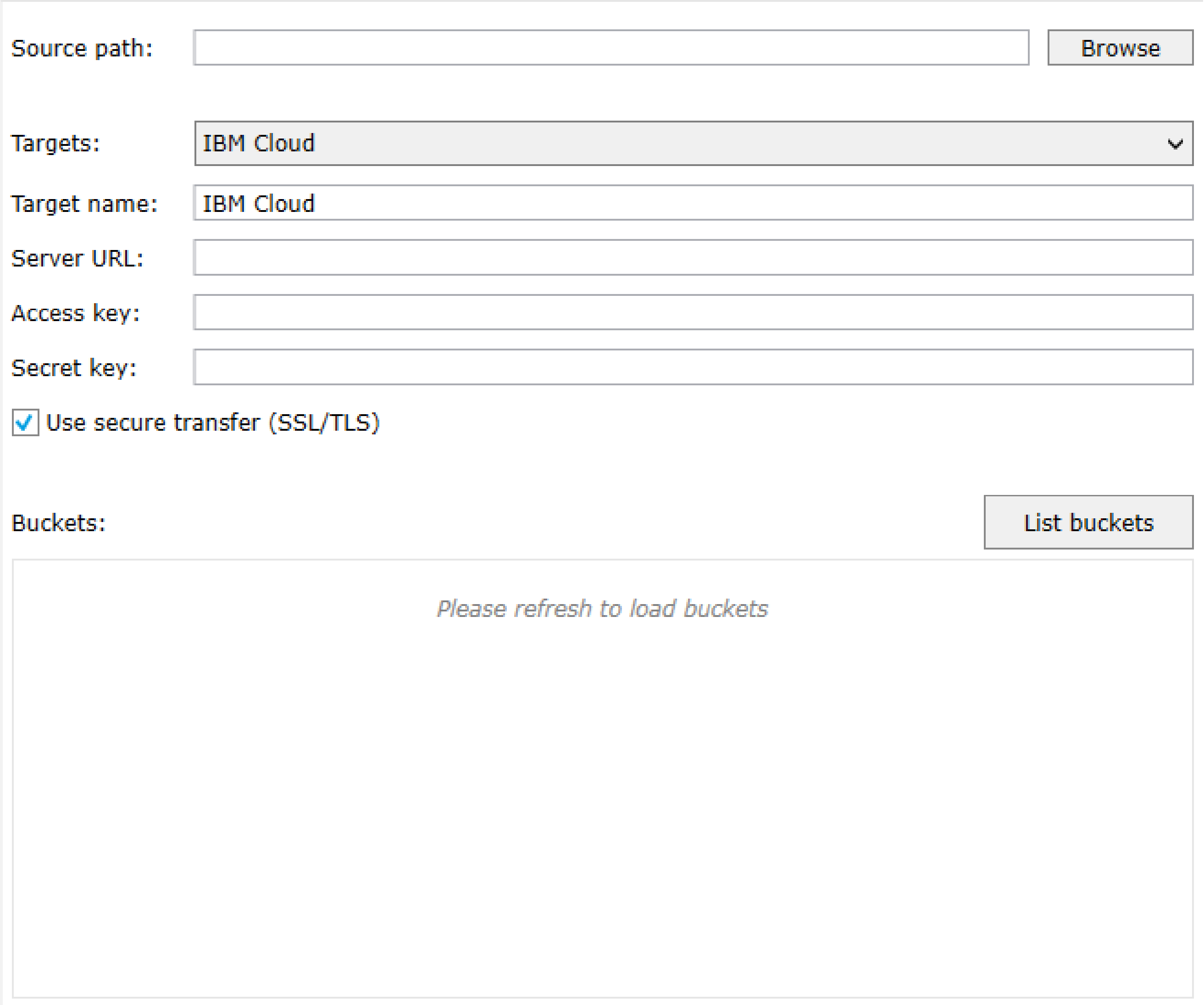
Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- Select a separate bucket for each source you want to pair with the Google Cloud target. The service account must have an IAM role, which has at least Storage Admin permissions for the bucket.

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

IBM Cloud Object Storage Prerequisites

To pair a source with an IBM Cloud Object Storage target, you must provide the following information:



Source path:

Targets: IBM Cloud

Target name: IBM Cloud

Server URL:

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets:

Please refresh to load buckets

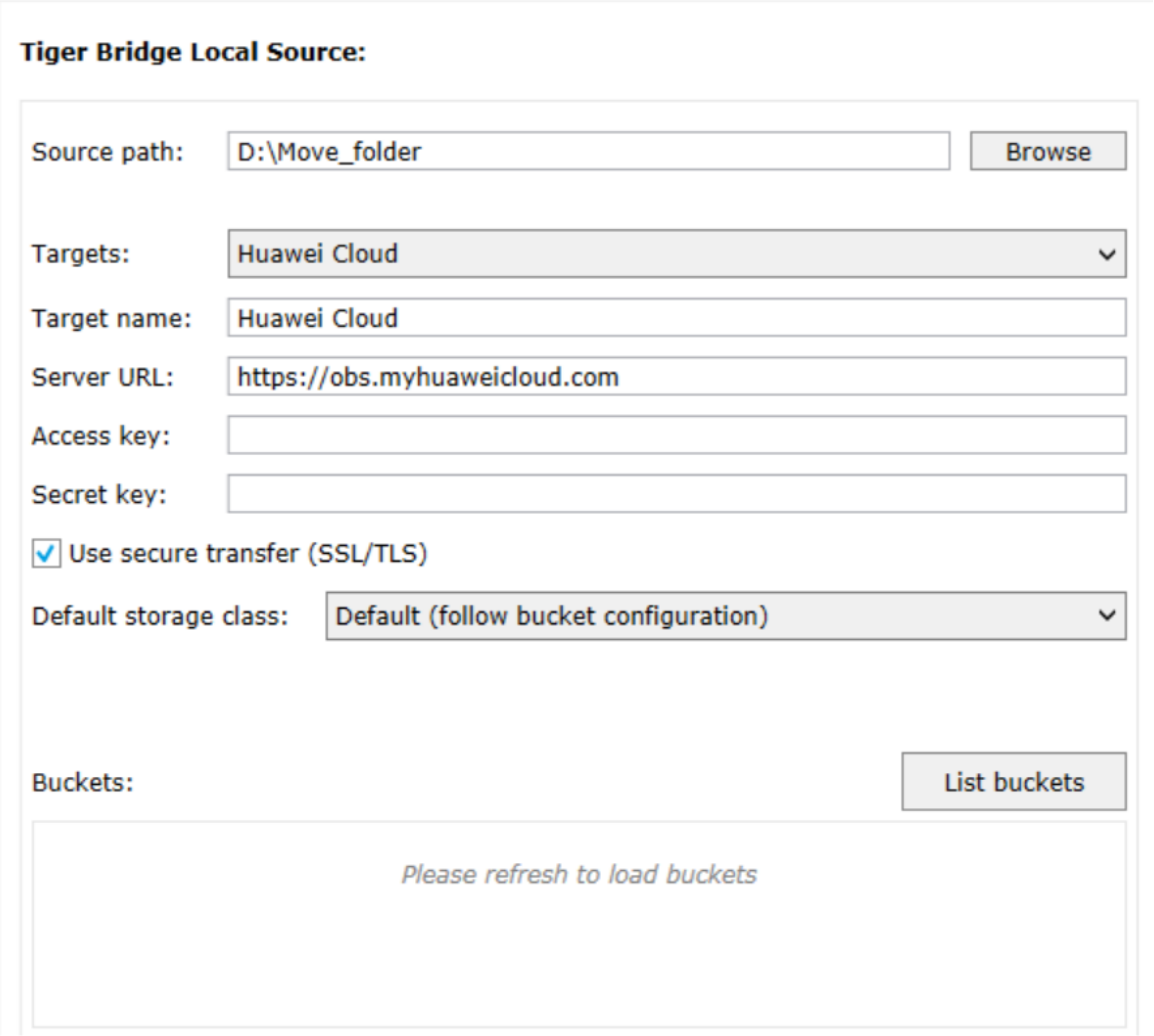
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from Tiger Bridge versioning, you must enable object versioning on the respective bucket (s).
- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The IP address of the IBM COS server.
- The access key ID and secret access key, which provide at least write access to the respective bucket.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

Huawei Cloud Storage

To pair a source with a Huawei Cloud storage target, you must provide the following information:



Tiger Bridge Local Source:

Source path: D:\Move_folder

Targets: Huawei Cloud

Target name: Huawei Cloud

Server URL: https://obs.myhuaweicloud.com

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Default storage class: Default (follow bucket configuration)

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The URL of the Huawei Cloud server.
- The access key ID and secret access key of the account, which will be used by Tiger Bridge for access to the Huawei Cloud storage.
- Select whether to access the target using secure transfer (SSL/TLS) or not.
- Select the Default storage class, to which Tiger Bridge to replicate data directly, omitting any intermediate tiers.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

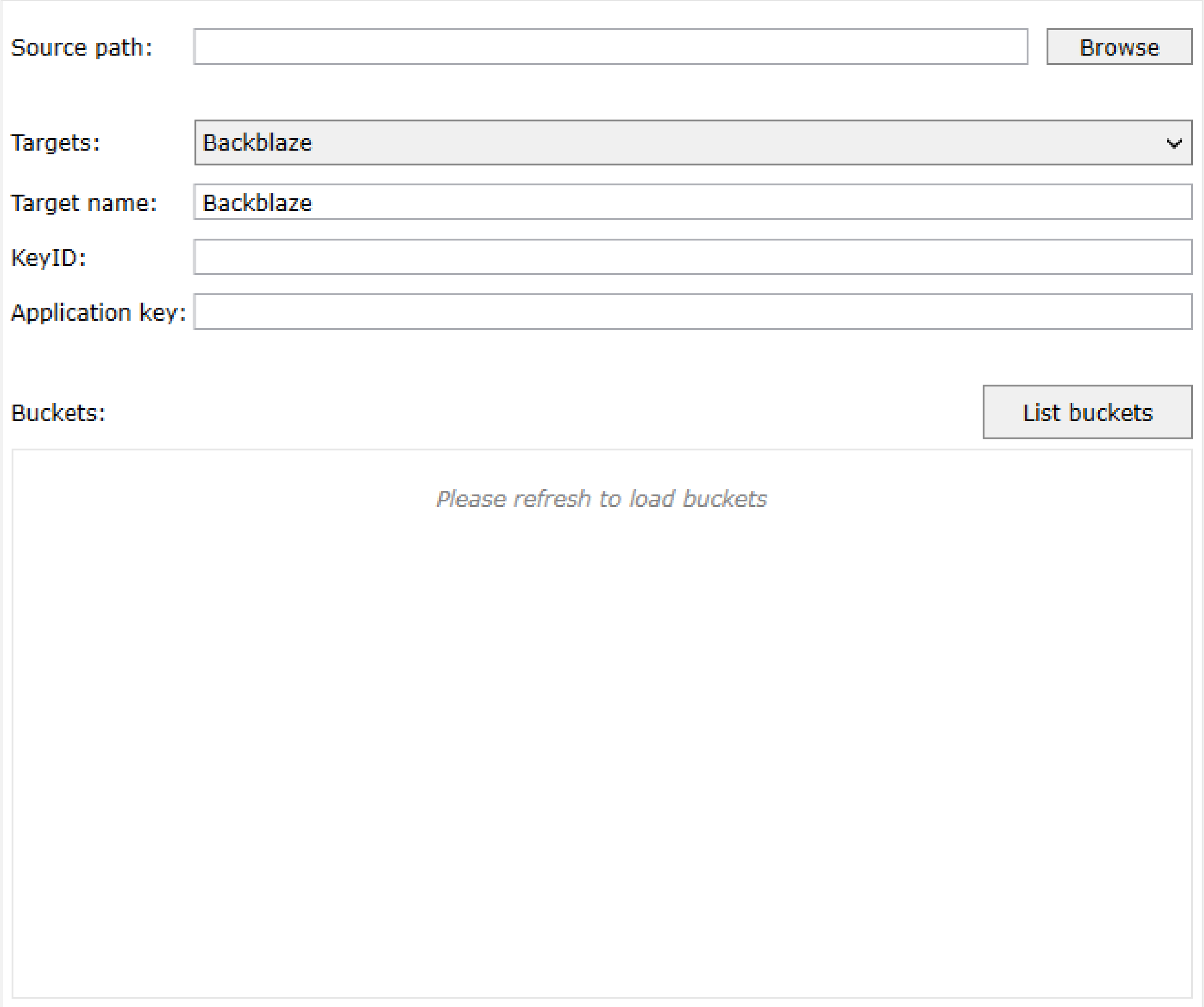
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from the Tiger Bridge versioning, you must enable object versioning on the respective bucket(s).

Backblaze B2 Cloud Storage Prerequisites

To pair a source with a Backblaze B2 cloud storage target, you must provide the following information:



Source path:

Targets: Backblaze

Target name: Backblaze

KeyID:

Application key:

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.

- A Backblaze application key and keyID for access to the Backblaze B2 cloud storage.

- Select a separate bucket for each source you want to pair with the target, to which the account whose credentials you have provided has access.

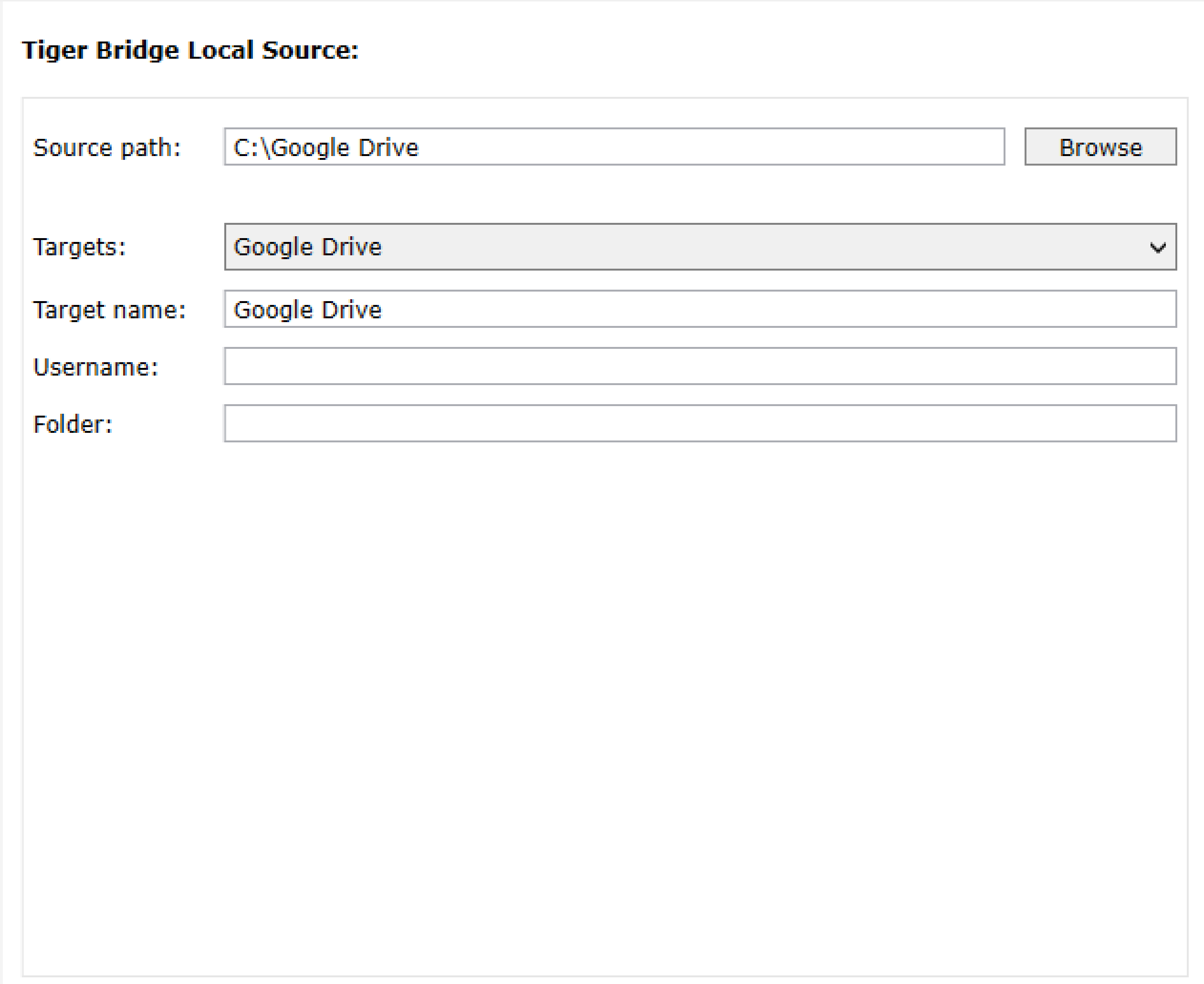
Note: If the user whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from the Tiger Bridge versioning, you must enable object versioning on the respective bucket(s).

Google Drive

To pair a source with Google Drive storage, you must provide the following information:



Tiger Bridge Local Source:

Source path: C:\Google Drive

Targets: Google Drive

Target name: Google Drive

Username:

Folder:

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another folder in your Google Drive.

- Provide the credentials for access to your Google Drive account.

Note: You will be asked to provide the credentials of your Google Drive account when Tiger Bridge attempts to pair the source and target.

- Provide the name of a folder (prefix) on your Google Drive, which is to be used for storing data from the source.

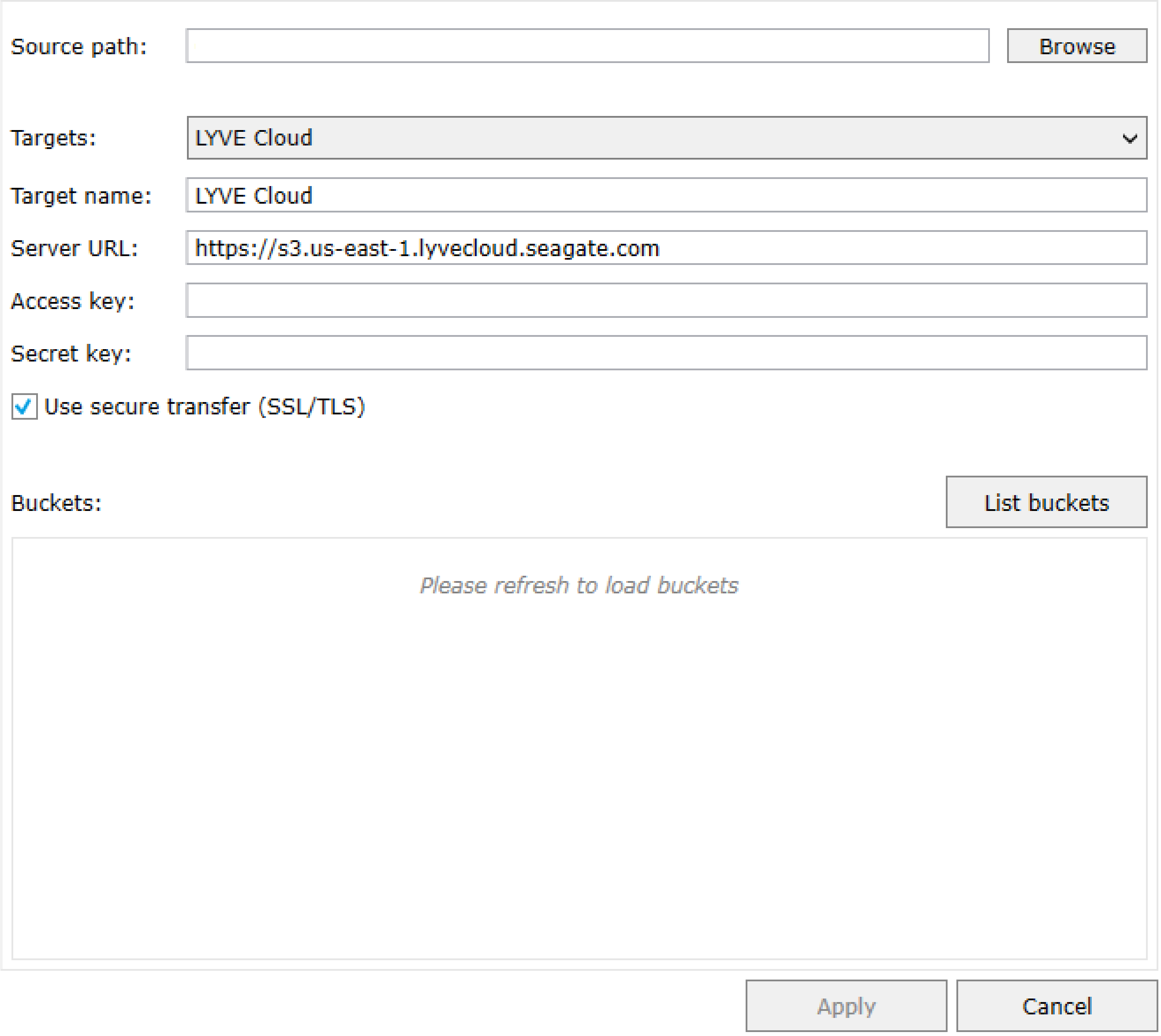
Note: If the folder name you have specified does not exist, Tiger Bridge automatically creates it in your Google Drive.

- If prompted, ensure Tiger Bridge is authorized to preview, edit, create, and delete files in your Google Drive.

Important: Do not change the name of the folder as this may prevent Tiger Bridge replication from operating.

LYVE Cloud Prerequisites

To pair a source with a LYVE Cloud target, you must provide the following information:



Source path:

Targets: LYVE Cloud

Target name: LYVE Cloud

Server URL: https://s3.us-east-1.lyvecloud.seagate.com

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The URL of the LYVE Cloud server.

Note: If the account 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.

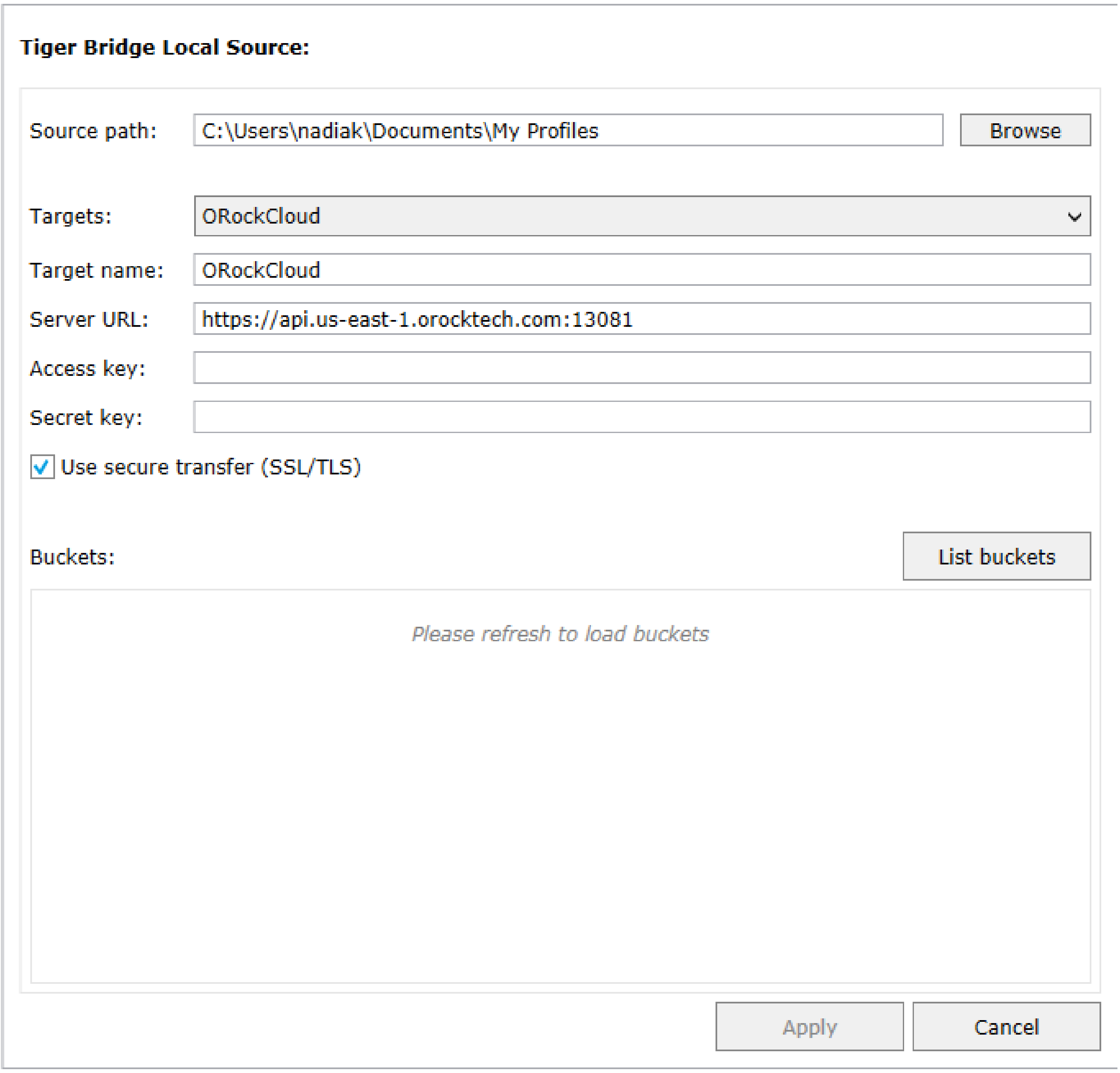
Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from the Tiger Bridge versioning, you must enable object versioning on the respective bucket(s).

- The access key ID and secret access key of the account, which will be used by Tiger Bridge for access to the LYVE Cloud storage.
- Select whether to access the target using secure transfer (SSL/TLS) or not.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

ORockCloud Prerequisites

To pair a source with a LYVE Cloud target, you must provide the following information:



Tiger Bridge Local Source:

Source path: C:\Users\nadiak\Documents\My Profiles

Targets: ORockCloud

Target name: ORockCloud

Server URL: https://api.us-east-1.orocktech.com:13081

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets:

Please refresh to load buckets

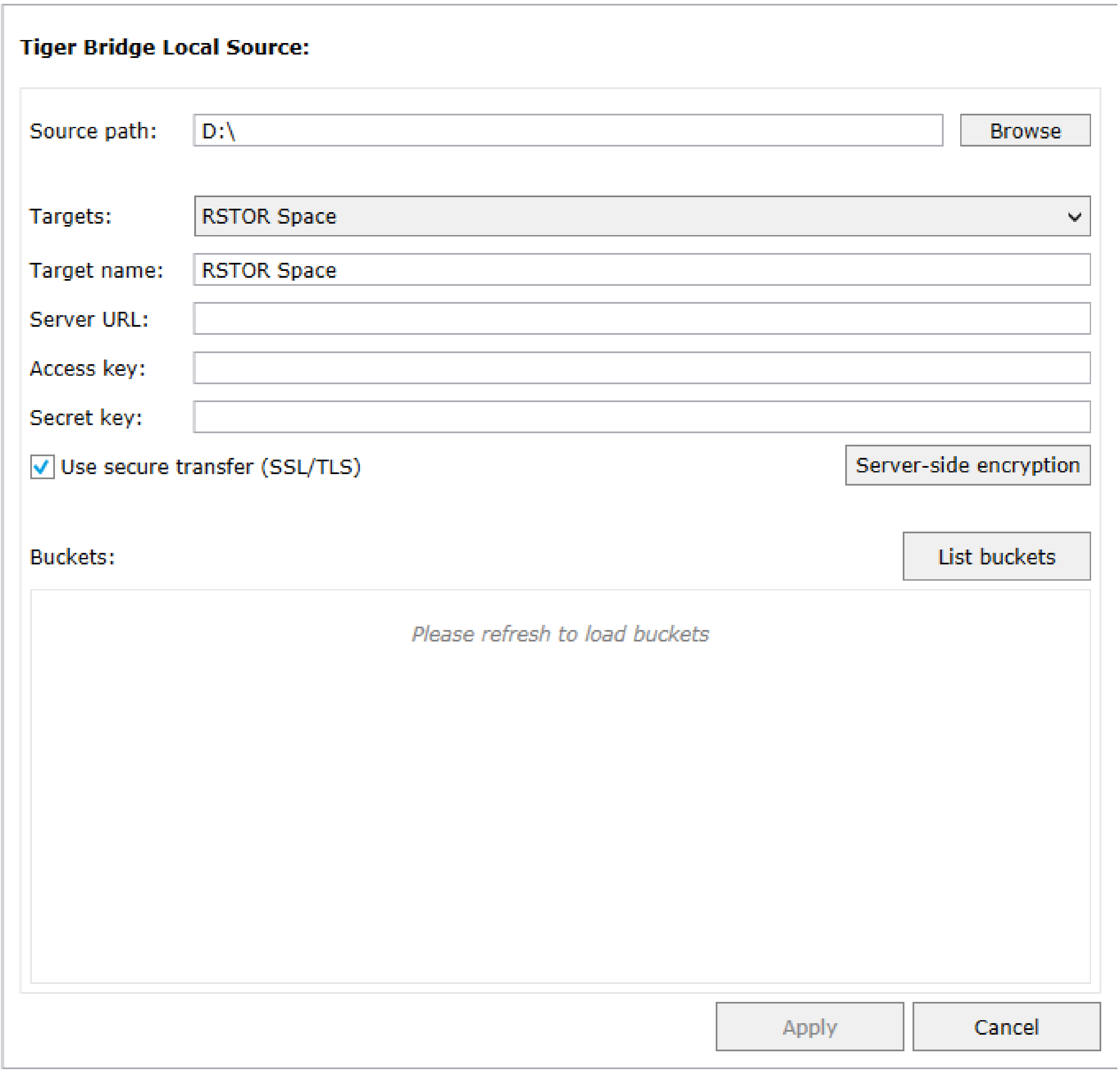
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from the Tiger Bridge versioning, you must enable object versioning on the respective bucket(s).
- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The URL of the ORockCloud server.
- The access key ID and secret access key of the account, which will be used by Tiger Bridge for access to the ORockCloud storage.
- Select whether to access the target using secure transfer (SSL/TLS) or not.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

RSTOR Space Prerequisites

To pair a source with a RSTOR Space storage target, you must provide the following information:



Tiger Bridge Local Source:

Source path: D:\

Targets: RSTOR Space

Target name: RSTOR Space

Server URL:

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.

- The URL of the RSTOR Space server.

- The access key ID and secret access key of the account, which will be used by Tiger Bridge for access to the RSTOR Space storage.

- Select whether to access the target using secure transfer (SSL/TLS) or not.

- If server-side encryption using a customer-provided encryption key is enabled on the respective bucket, when configuring the target select the respective option and provide the encryption key.

- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

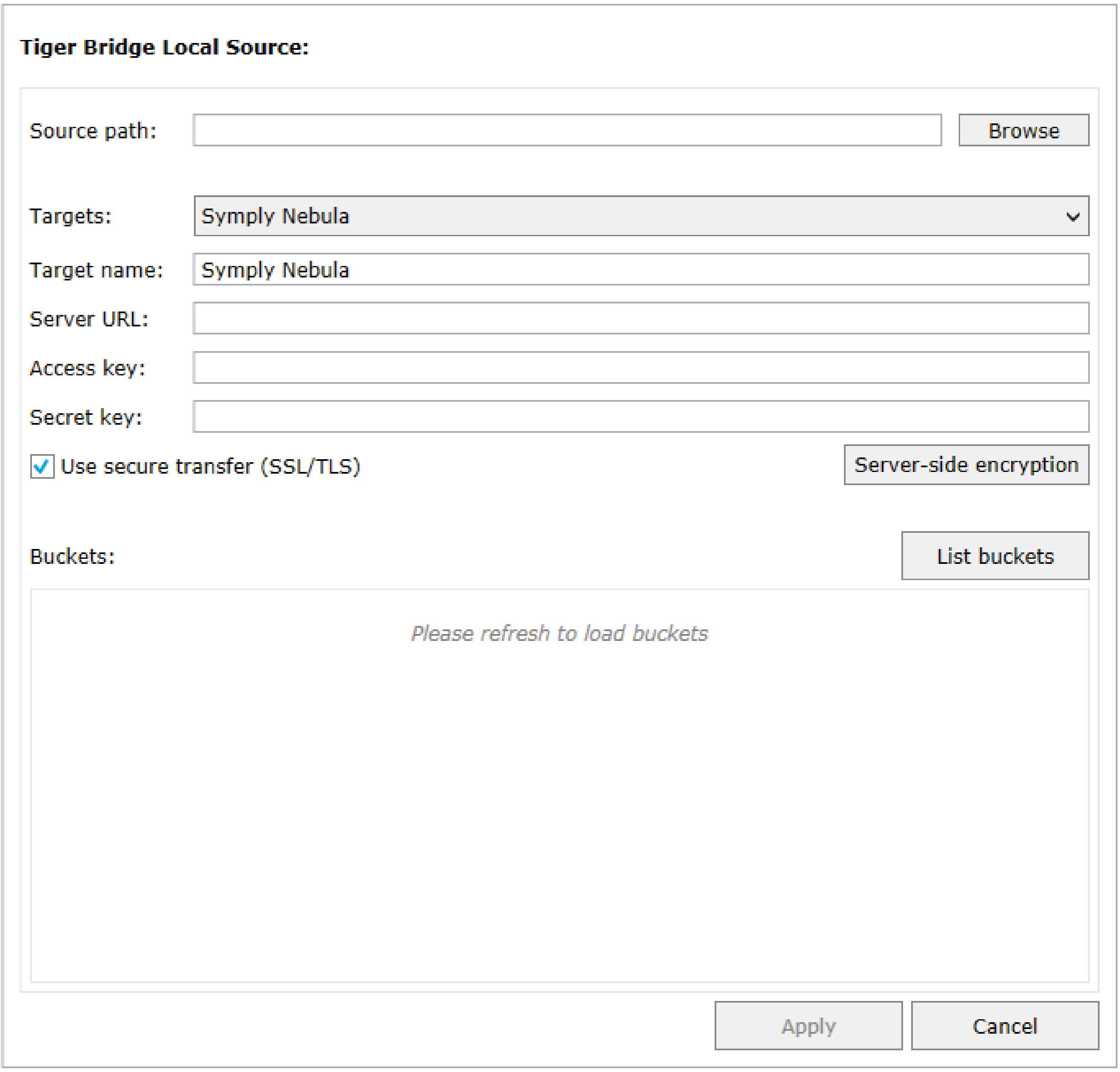
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from the Tiger Bridge versioning, you must enable object versioning on the respective bucket(s).

Symply NEBULA Prerequisites

To pair a source with a Symply NEBULA storage target, you must provide the following information:



Tiger Bridge Local Source:

Source path:

Targets: Symply Nebula

Target name: Symply Nebula

Server URL:

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The URL of the Symply NEBULA server.
- The access key ID and secret access key of the account, which will be used by Tiger Bridge for access to the Symply NEBULA storage.
- Select whether to access the target using secure transfer (SSL/TLS) or not.
- If server-side encryption using a customer-provided encryption key is enabled on the respective bucket, when configuring the target select the respective option and provide the encryption key.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

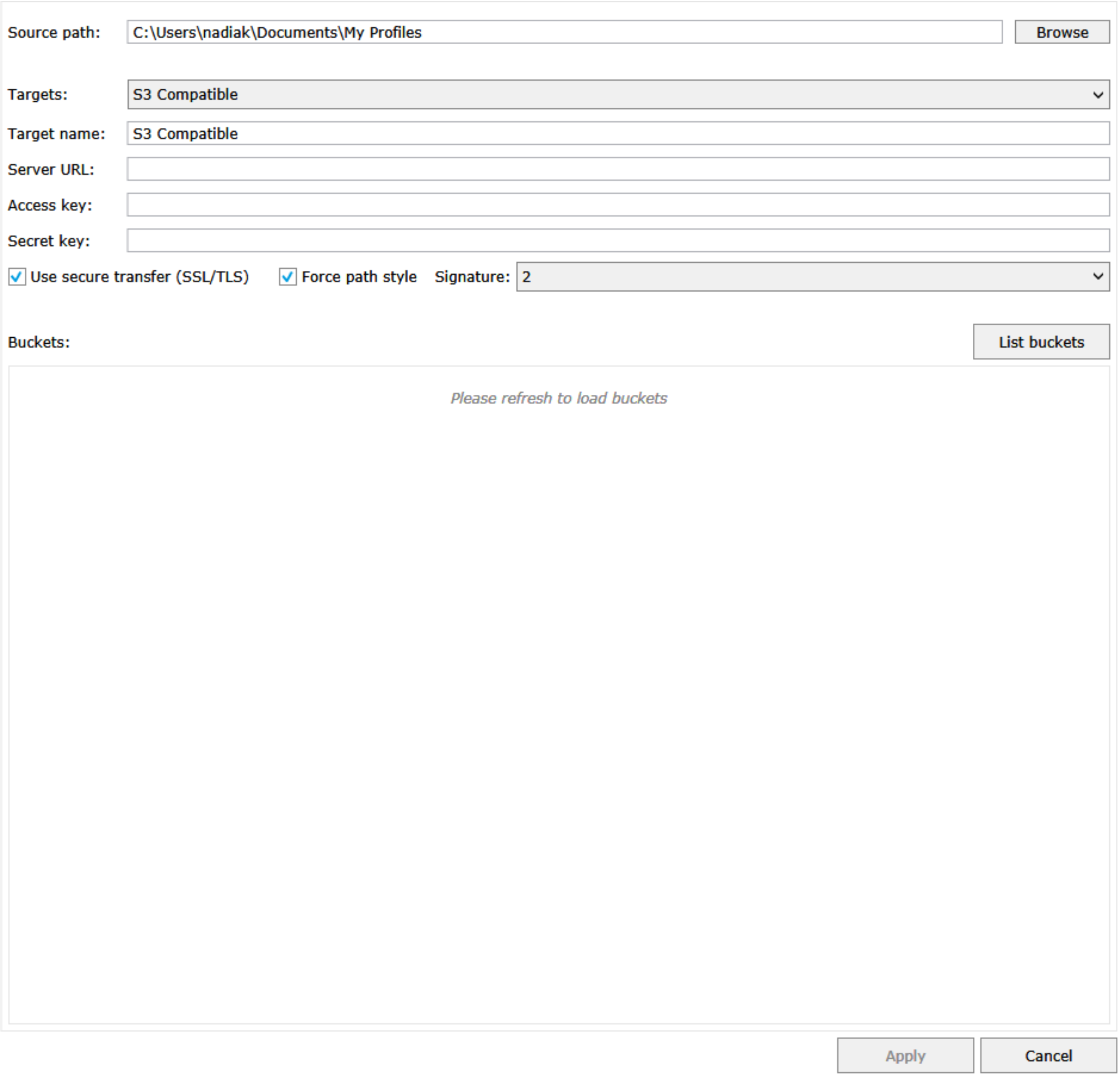
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from Tiger Bridge versioning, you must enable object versioning on the respective bucket (s)

S3-Compatible Object Storage Prerequisites

To pair a source with a public cloud or on-premises S3-compatible object storage target, you must provide the following information:



Source path: C:\Users\nadiak\Documents\My Profiles

Targets: S3 Compatible

Target name: S3 Compatible

Server URL:

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS) ☑ Force path style Signature: 2

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The URL or IP address of the S3-compatible object storage server.
- The access key ID and secret access key of the account, which will be used by Tiger Bridge for access to the S3-compatible object storage.
- Select whether to access the target using secure transfer (SSL/TLS) or not.
- Select whether to use virtual-hosted-style or path-style URLs to access the designated bucket.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

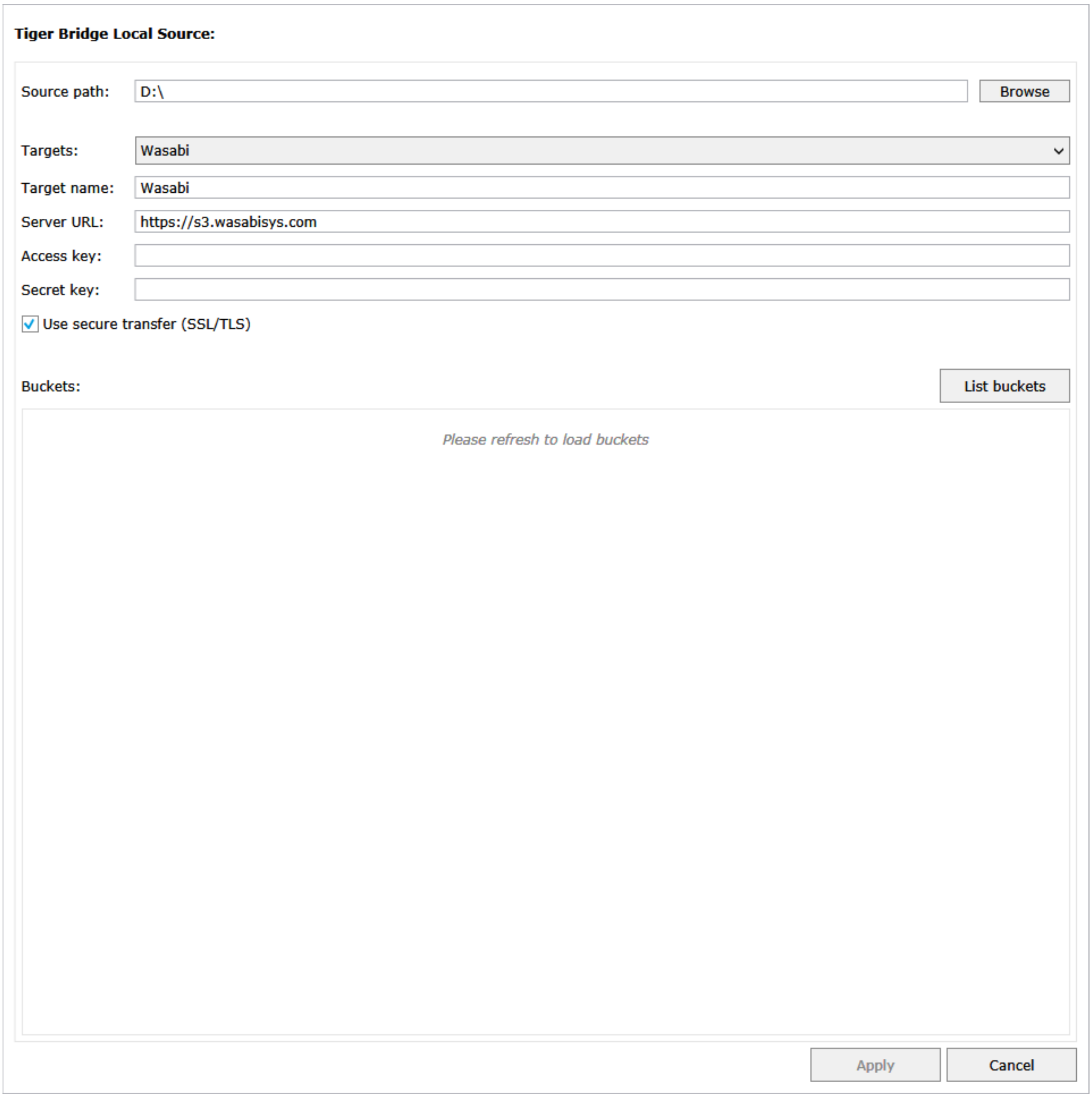
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from the Tiger Bridge versioning, you must enable object versioning on the respective bucket(s)

Wasabi Cloud Object Storage Prerequisites

To pair a source with a Wasabi cloud object storage target, you must provide the following information:



Tiger Bridge Local Source:

Source path: D:\

Targets: Wasabi

Target name: Wasabi

Server URL: https://s3.wasabisys.com

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The URL of the Wasabi cloud object storage server.

Note: Region-specific target URL may be required.

- The access key ID and secret access key of the account, which will be used by Tiger Bridge for access to the Wasabi cloud object storage.
- Select whether to access the target using secure transfer (SSL/TLS) or not.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

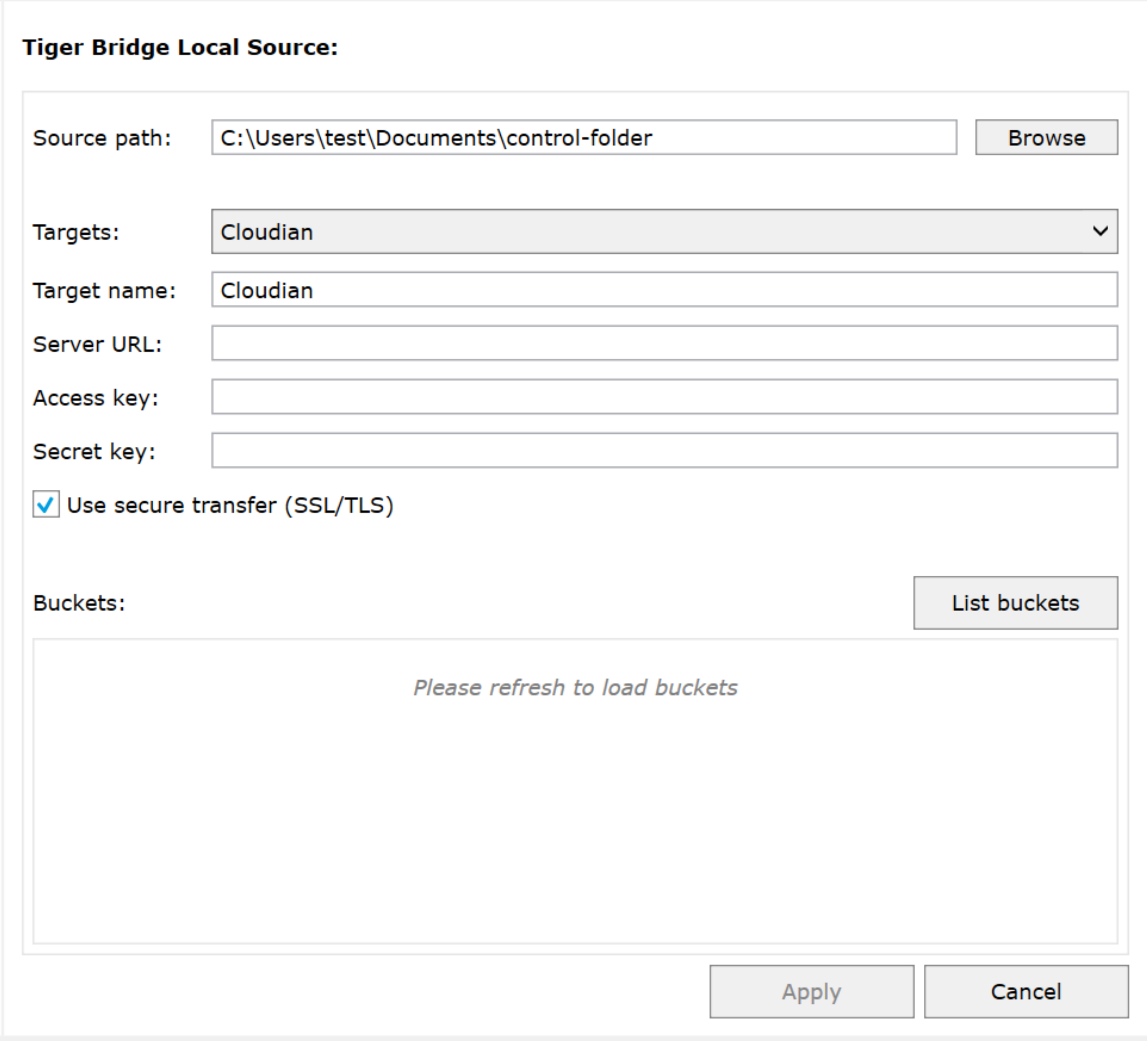
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from the Tiger Bridge versioning, you must enable object versioning on the respective bucket(s).

Cloudian Object Storage Prerequisites

To pair a source with a Cloudian object storage target, you must provide the following information:



Tiger Bridge Local Source:

Source path: C:\Users\test\Documents\control-folder

Targets: Cloudian

Target name: Cloudian

Server URL:

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The URL of the Cloudian server.
- The access key ID and secret access key of the account, which will be used by Tiger Bridge for access to the Cloudian object storage.
- Select whether to access the target using secure transfer (SSL/TLS) or not.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

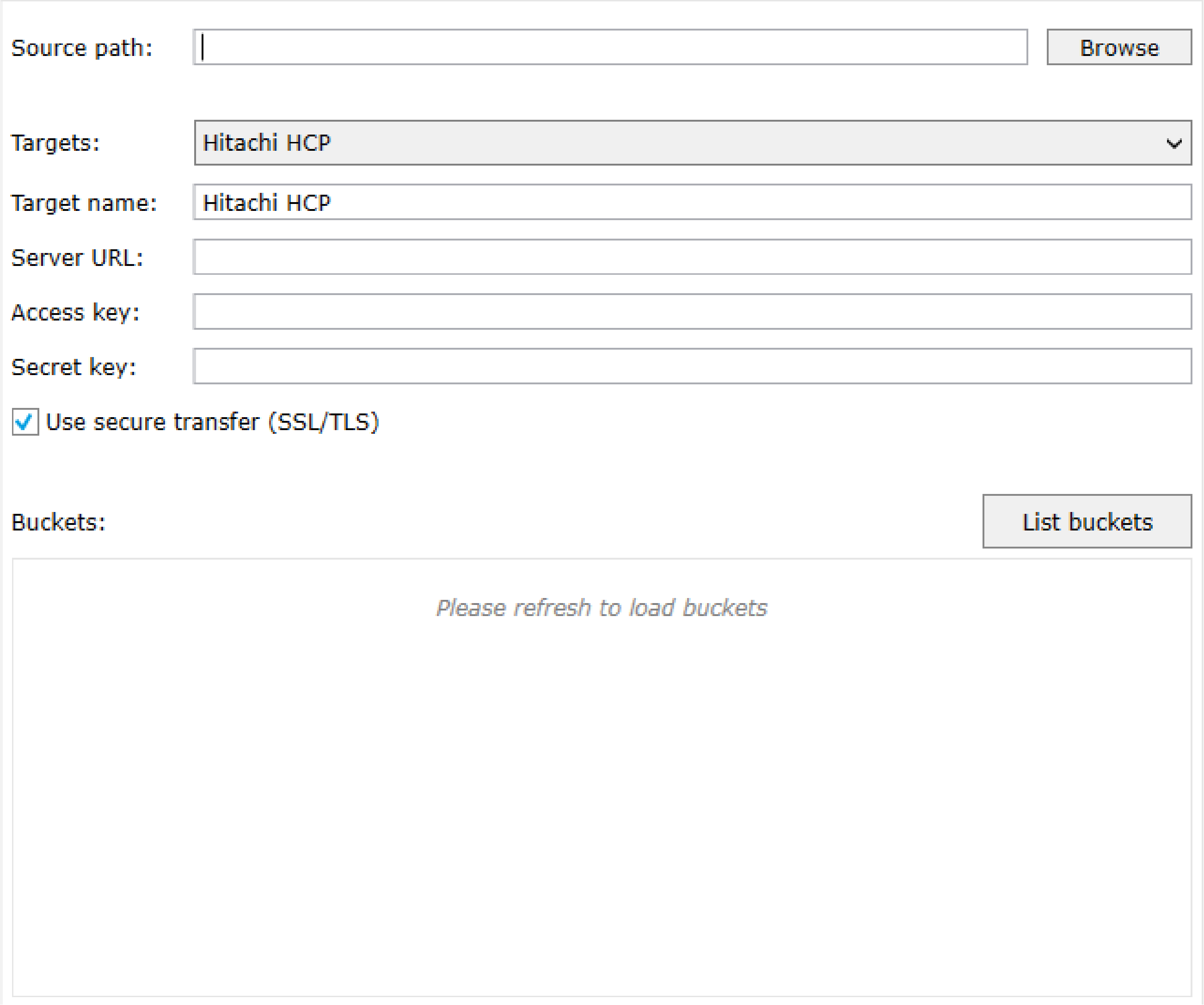
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from the Tiger Bridge versioning, you must enable object versioning on the respective bucket(s).

Hitachi Content Platform (HCP) Prerequisites

To pair a source with a Hitachi HCP target, you must provide the following information:



Source path: | Browse

Targets: Hitachi HCP

Target name: Hitachi HCP

Server URL:

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets: List buckets

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The URL of the Hitachi HCP server.
- The access key ID and secret access key of the account, which will be used by Tiger Bridge for access to the Hitachi HCP storage.
- Select whether to access the target using secure transfer (SSL/TLS) or not.

- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

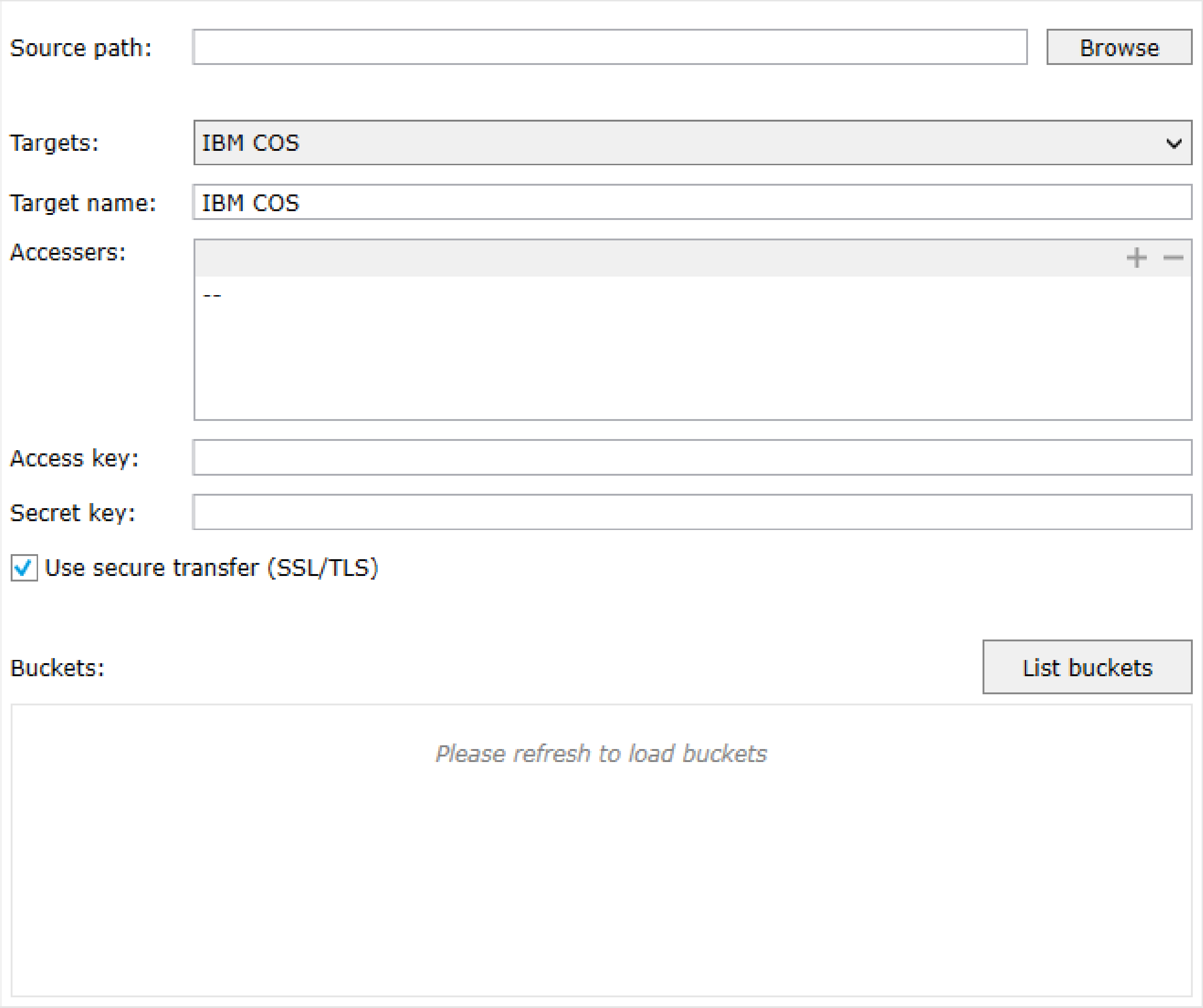
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from the Tiger Bridge versioning, you must enable object versioning on the respective bucket(s).

IBM COS Prerequisites

To pair a source with an on-premises IBM COS storage target, you must provide the following information:



Source path:

Browse

Targets: IBM COS

Target name: IBM COS

Accessers: --

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets:

List buckets

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The IP address of the IBM COS server.
- The access key ID and secret access key, which provide at least write access to the respective bucket.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

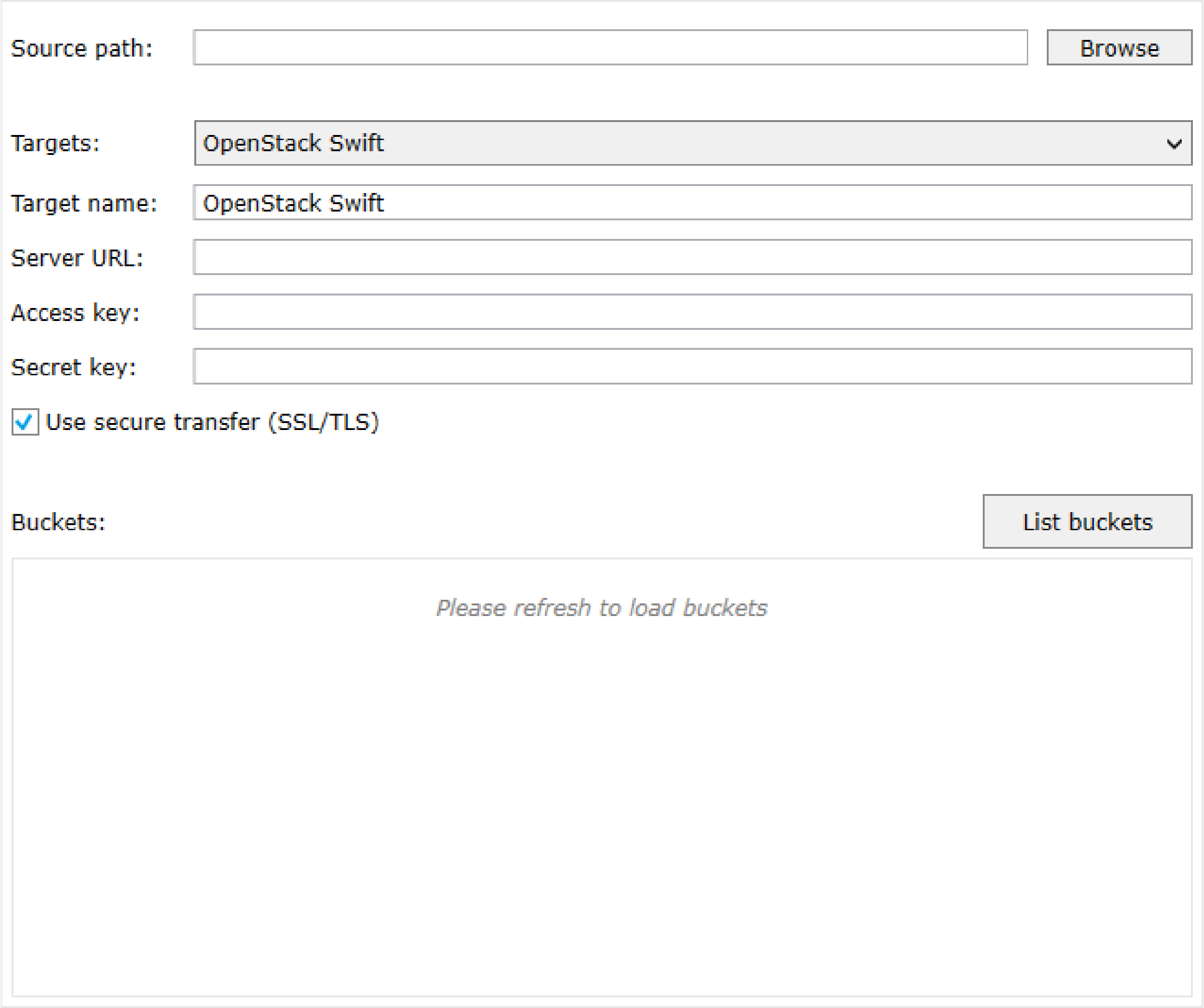
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from Tiger Bridge versioning, you must enable object versioning on the respective bucket (s).

OpenStack Swift Object Storage Prerequisites

To pair a source with a Swift object storage target, you must provide the following information:


Source path:

Targets: OpenStack Swift

Target name: OpenStack Swift

Server URL:

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The access key ID and secret access key of an OpenStack Swift object storage account, which has at least Write access to the respective bucket.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

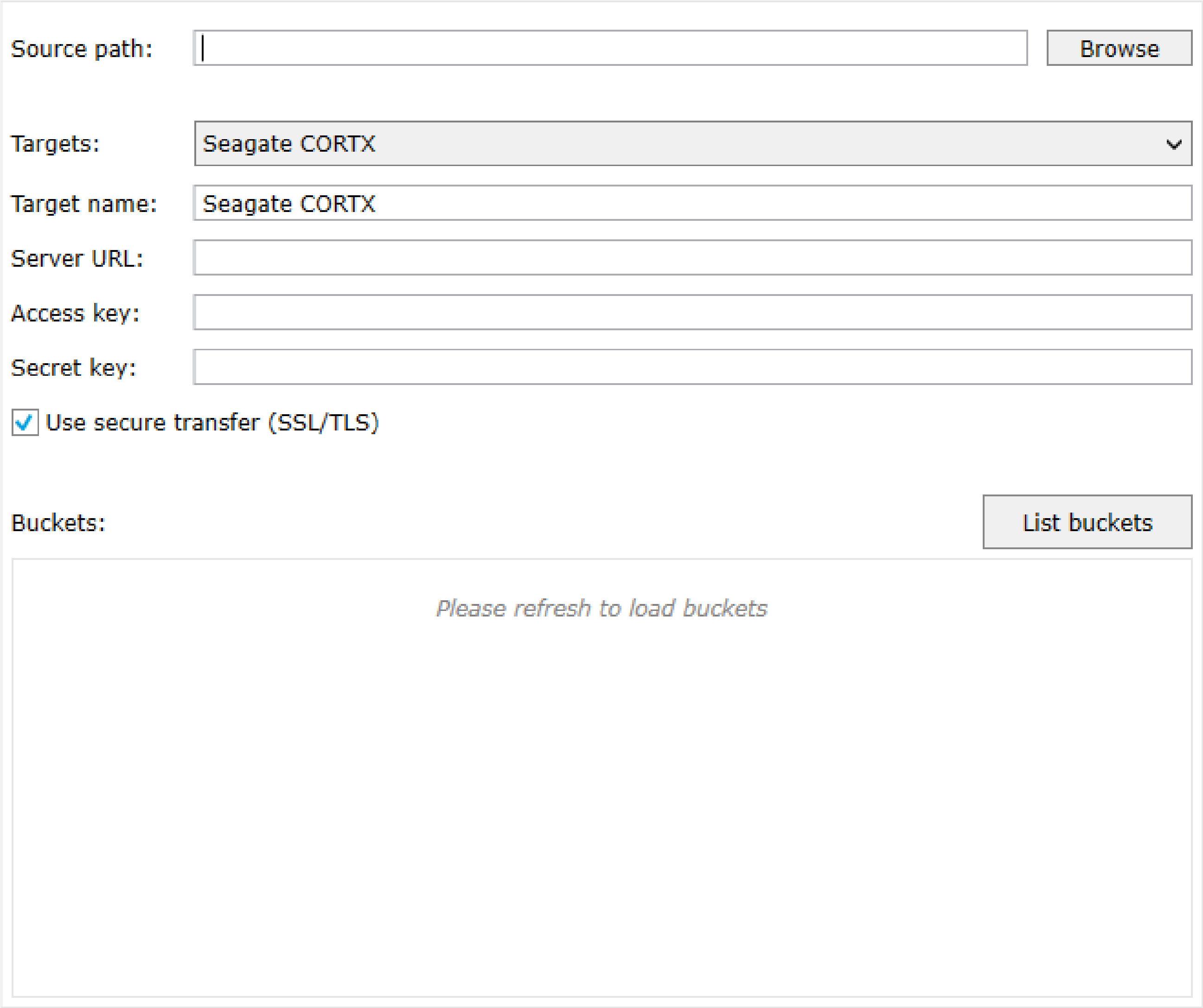
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from Tiger Bridge versioning, you must enable object versioning on the respective bucket (s).

Seagate CORTX Prerequisites

To pair a source with a Seagate CORTX target, you must provide the following information:



Source path:

Targets: Seagate CORTX

Target name: Seagate CORTX

Server URL:

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The CORTX server URL.
- The access key ID and secret access key of a CORTX object storage account, which has at least Write access to the respective bucket.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

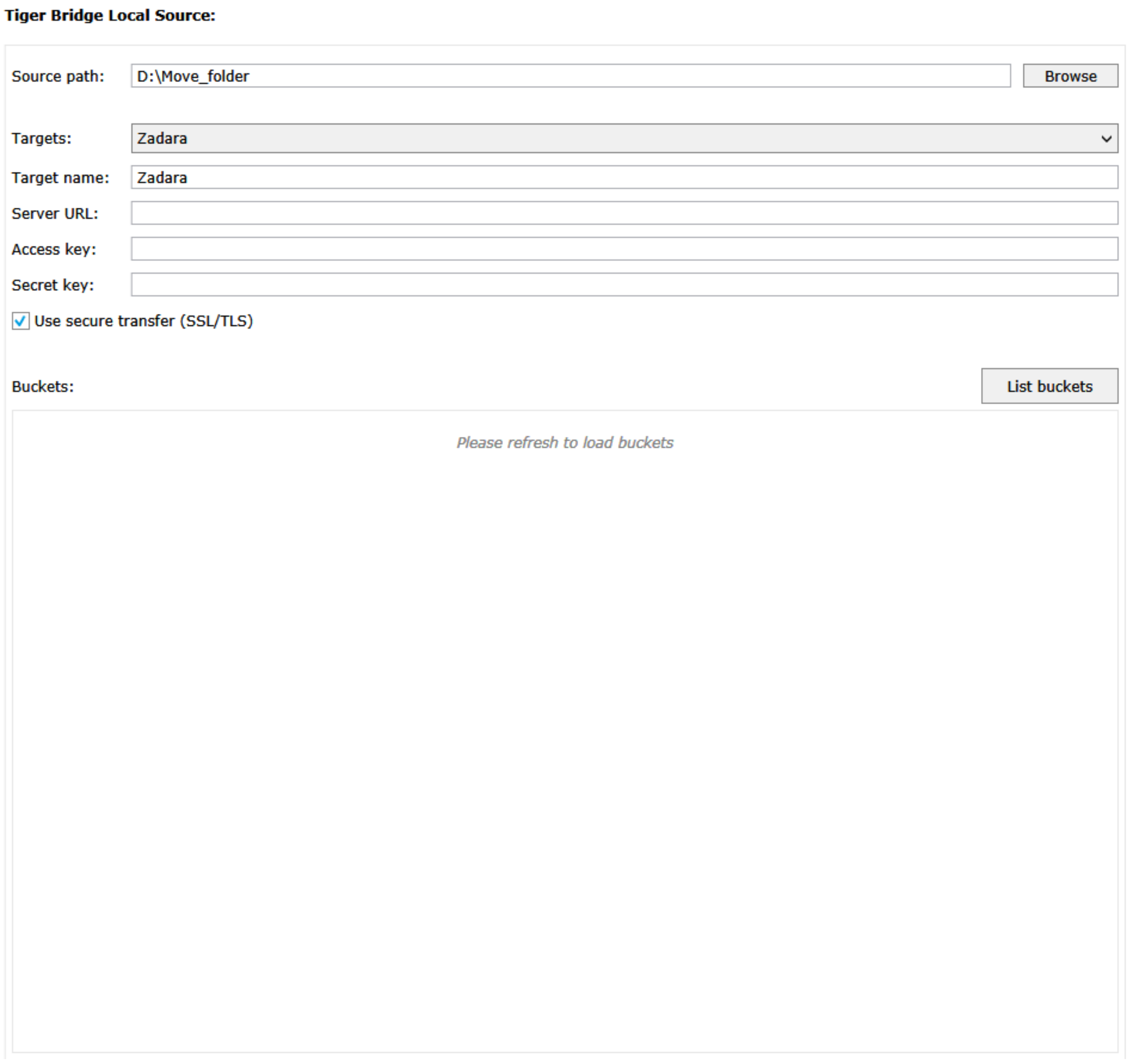
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from Tiger Bridge versioning, you must enable object versioning on the respective bucket (s).

Zadara Object Storage

To pair a source with a Zadara object storage target, you must provide the following information:



Tiger Bridge Local Source:

Source path: D:\Move_folder

Targets: Zadara

Target name: Zadara

Server URL:

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.

- The URL of the Zadara storage server.

- The access key ID and secret access key of the account, which will be used by Tiger Bridge for access to the Zadara storage.

- Select whether to access the target using secure transfer (SSL/TLS) or not.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

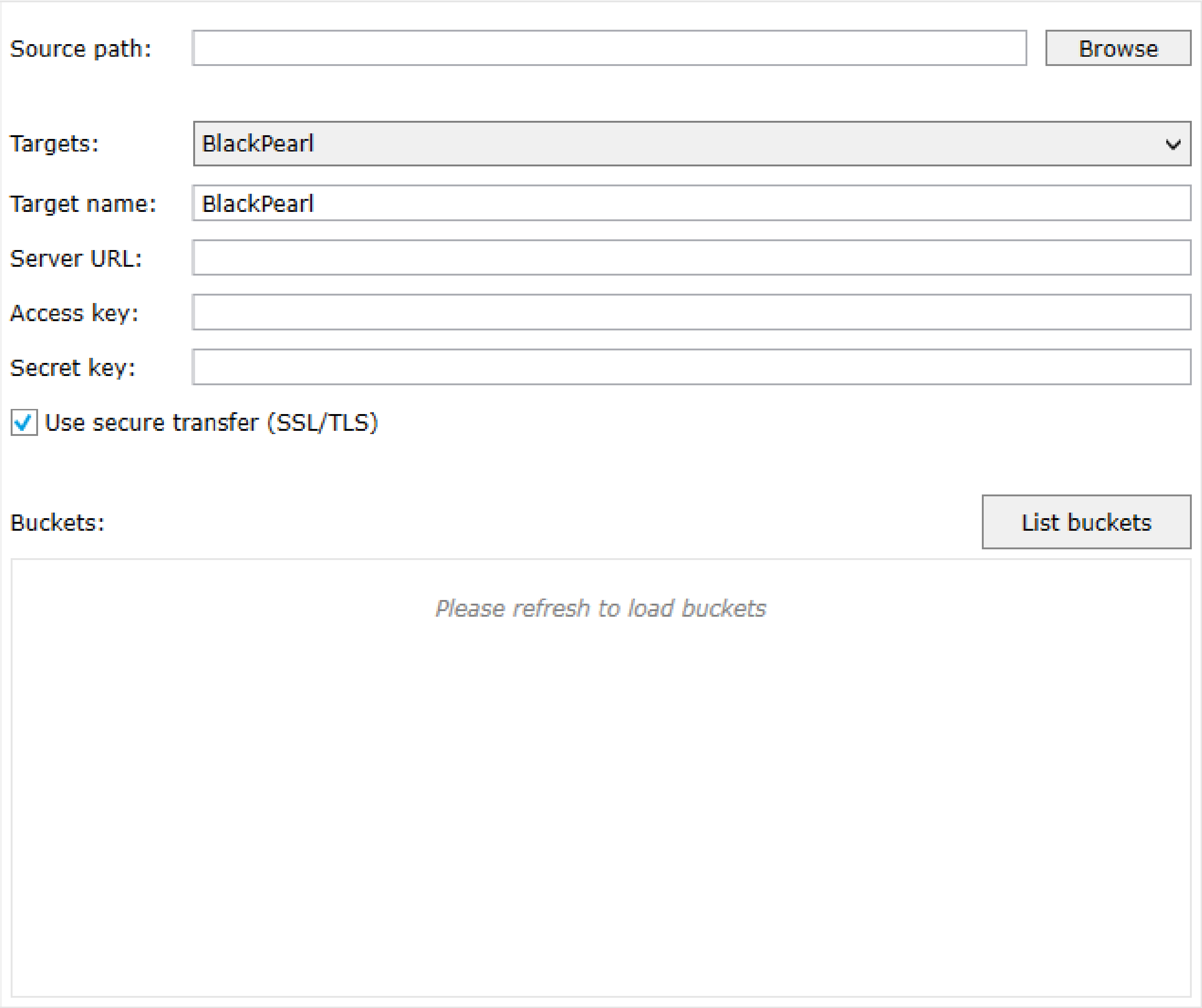
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from the Tiger Bridge versioning, you must enable object versioning on the respective bucket(s)

BlackPearl Object Storage Prerequisites

To pair a source with a BlackPearl object storage target, you must provide the following information:



Source path:

Targets: BlackPearl

Target name: BlackPearl

Server URL:

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with the same target. The target name and its parameters will appear in the Targets drop-down box.
- The IP address of the BlackPearl object storage server.
- The access key ID and secret access key of the account, which will be used by Tiger Bridge for access to the BlackPearl object storage.
- Choose whether to access the target using secure transfer (SSL/TLS) or not.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

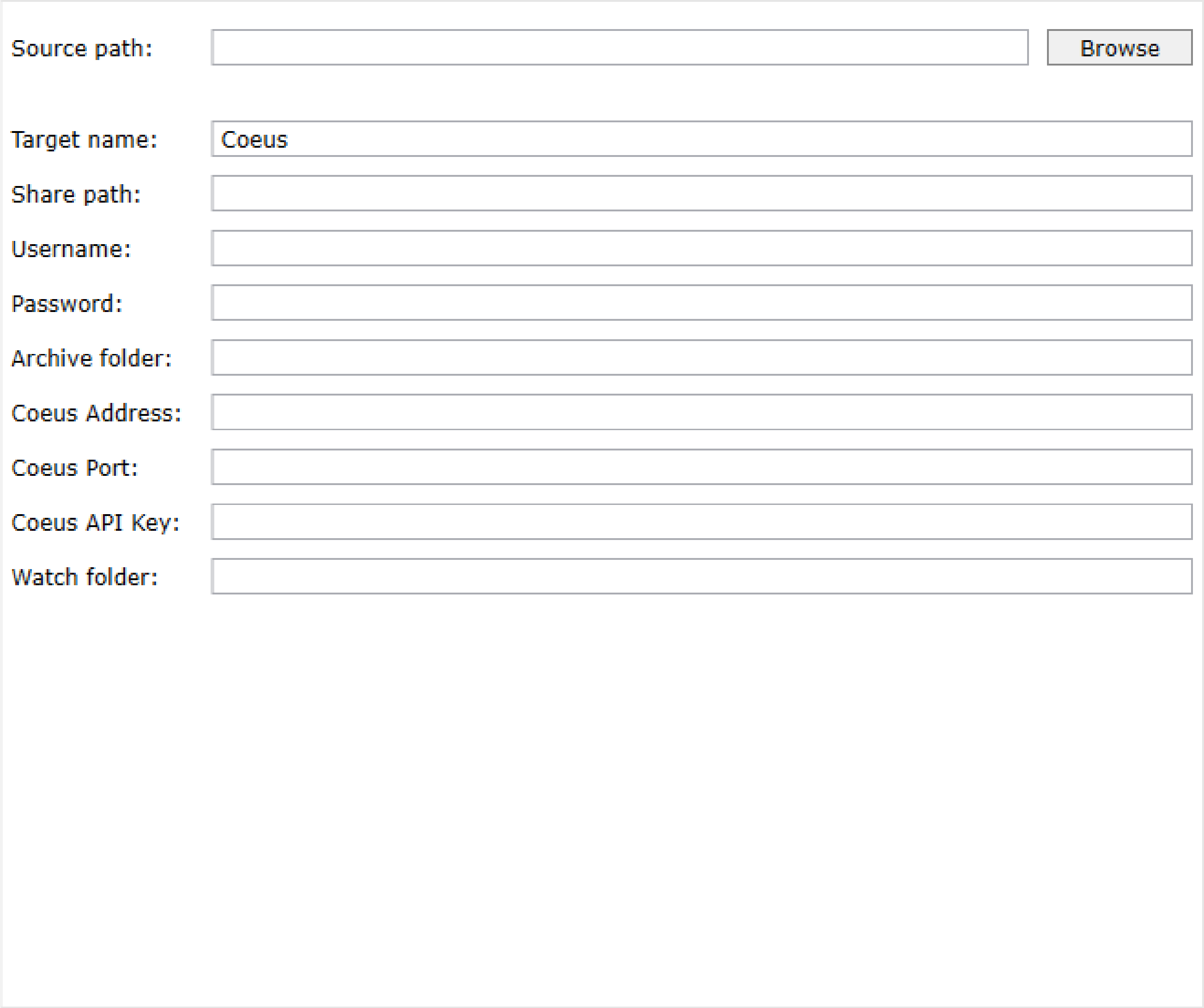
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from Tiger Bridge versioning, you must enable object versioning on the respective bucket (s).

Coeus Managed Digital Content Library Prerequisites

To pair a source with a Coeus managed digital content library target, you must provide the following information:



Source path:

Target name: Coeus

Share path:

Username:

Password:

Archive folder:

Coeus Address:

Coeus Port:

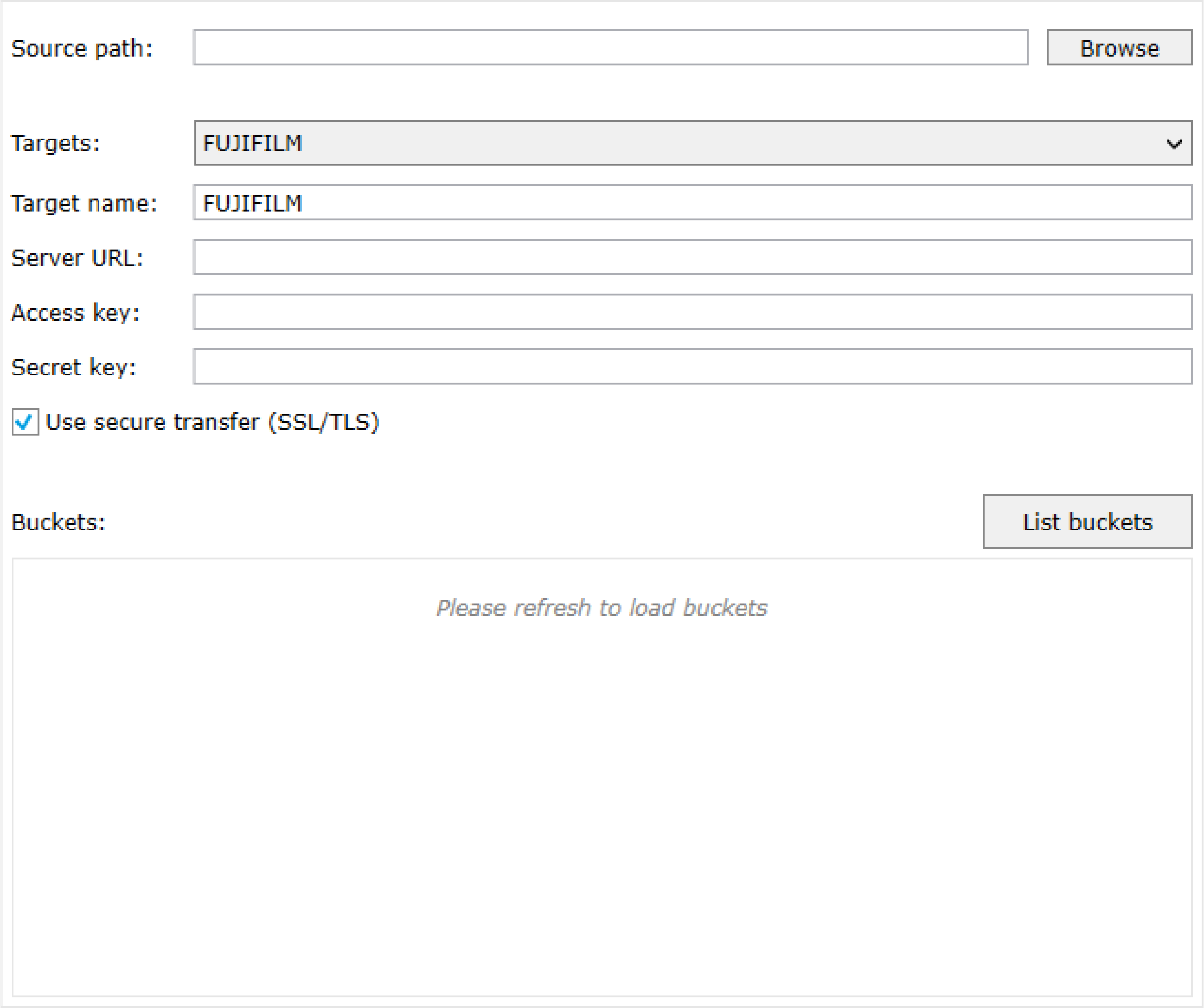
Coeus API Key:

Watch folder:

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with the same target. The target name and its parameters will appear in the Targets drop-down box.
- Create a separate Coeus account for each source paired with the Coeus managed digital content library.
- The path to the Coeus account's share on your network.
- The user name and password for access to the Coeus share path.
- The names of the Watch and Archive folders associated with the Coeus account.
- Provide the Coeus address and port through which it is accessible from the computer running Tiger Bridge and API key.

FujiFilm Object Archive Prerequisites

To pair a source with a FujiFilm Object Archive target, you must provide the following information:



Source path:

Targets: FUJIFILM

Target name: FUJIFILM

Server URL:

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

Buckets:

Please refresh to load buckets

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another bucket on the same target. The target name and its parameters will appear in the Targets drop-down box.
- The URL of the FujiFilm object archive server.
- The access key ID and secret access key of the account, which will be used by Tiger Bridge for access to the FujiFilm object archive.
- Choose whether to access the target using secure transfer (SSL/TLS) or not.
- Select a separate bucket for each source you want to pair with the target, to which the account has at least write access.

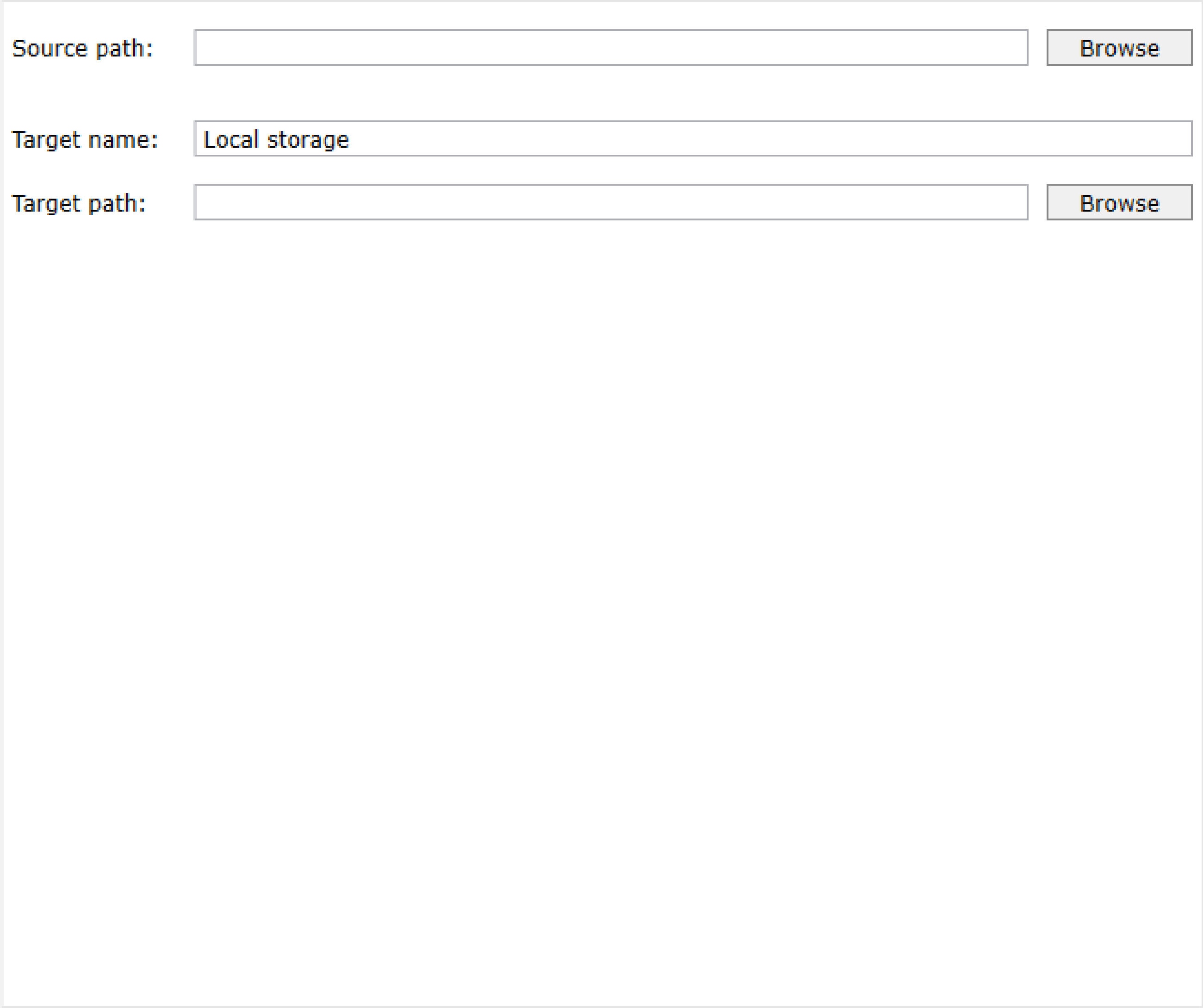
Note: If the account whose credentials you have provided does not have sufficient permissions to list all buckets, Tiger Bridge displays a text box for you to manually enter the name of the bucket, which will be paired with the source.

Important: Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

- To benefit from Tiger Bridge versioning, you must enable object versioning on the respective bucket (s).

Local Storage Target Prerequisites

To pair a source with a local NTFS/ReFS volume target, you must provide the following information:



Source path:

Target name: Local storage

Target path:

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with another sub-folder on the same volume. The target name and its parameters will appear in the Targets drop-down box.

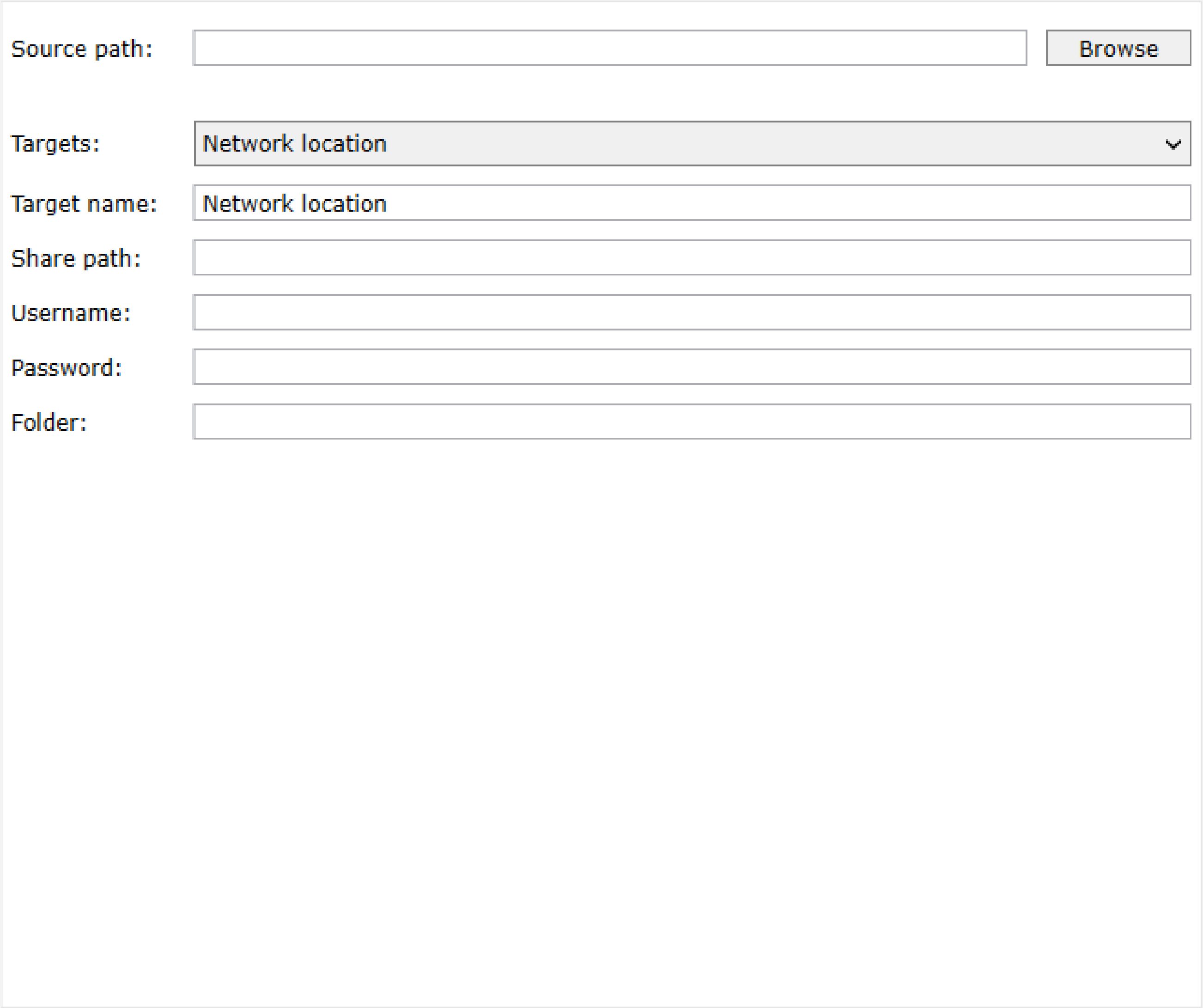
- Browse to and select a unique path on the locally mounted volume (the root of the volume or a subfolder) for each source, you want to pair with the target.

Important: Do not change the name of the folder as this may prevent Tiger Bridge replication from operating.

Note: If the selected path and its subfolders contain data prior to pairing it with the source, all files will be recreated on the source in the form of nearline files.

Network Share Target Prerequisites

To pair a source with a network share target, you must provide the following information:



Source path:	
Targets:	Network location
Target name:	Network location
Share path:	
Username:	
Password:	
Folder:	

- Name of the target - specifying a unique name allows you to reuse the target parameters when you pair another source with the same target. The target name and its parameters will appear in the Targets drop-down box.
- Provide the path to the share.
- Provide the name of a separate folder on the network share for each source you want to pair with the network share.

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 a folder to be used. For example, if you want to use as a target a network share with the name “Projects” exported by the server server.com, enter as Share path: \\server.com and as a folder to be used as container: Projects.

Important: If the folder contains data prior to pairing it with the source, all files will be recreated on the source in the form of nearline files.

- (SMB share only) provide a dedicated account (Active Directory domain or a 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.

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.

- (NFS share) allow the computer running Tiger Bridge to access the NFS share and disable NFS locking on it. You can find sample steps in Disable NFS Locking on the Tiger Bridge Computer on page 106.

Tiger Bridge Installation

Install Tiger Bridge

During the installation of Tiger Bridge, 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 through icon overlays, and to manually manage data through the Windows Explorer context menu.

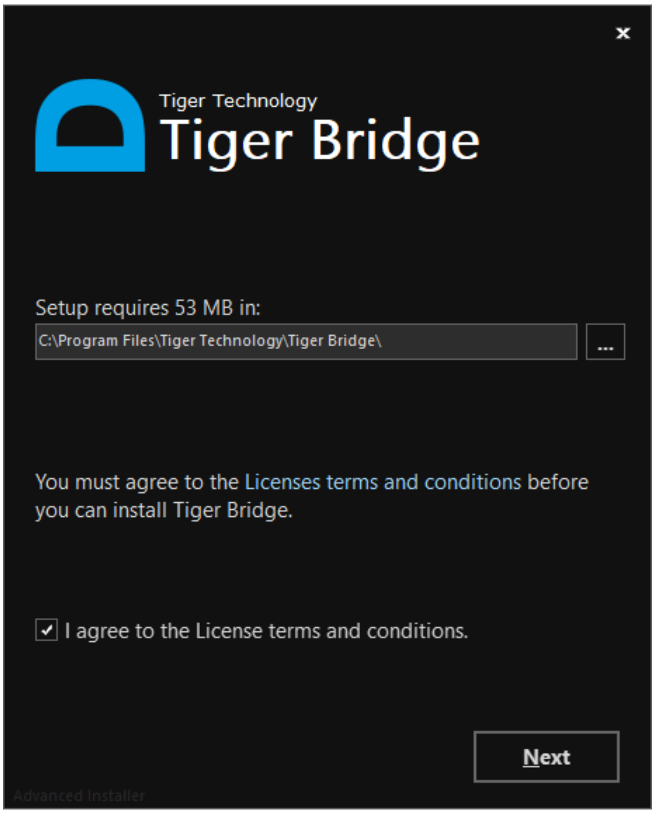
Note: Note: To use the Tiger Bridge shell extension from a remote computer, you must install it as a standalone component, using its own installation file.

To install Tiger Bridge and additional components:

1. Double-click the Tiger Bridge installation file.

Note: If the setup wizard detects that the prerequisites needed to run Tiger Bridge are not installed on the computer, click Next to install them. If the computer is not connected to the Internet, download the necessary prerequisites on another computer and then install them on the current one before proceeding with the installation.

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



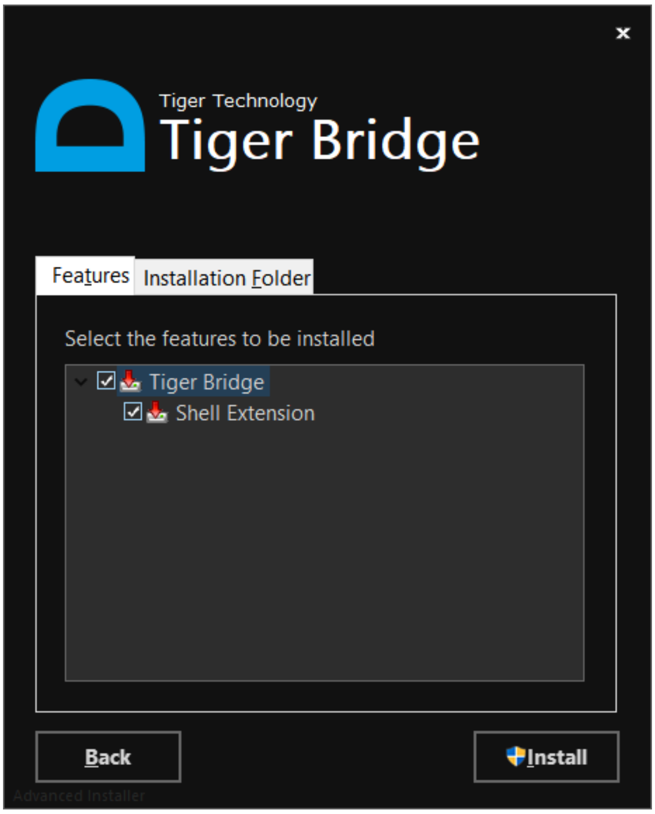
Setup requires 53 MB in:

C:\Program Files\Tiger Technology\Tiger Bridge\

You must agree to the Licenses terms and conditions before you can install Tiger Bridge.

☑ I agree to the License terms and conditions.

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



Tiger Technology

Tiger Bridge

Select the features to be installed

☑ Tiger Bridge

☑ Shell Extension

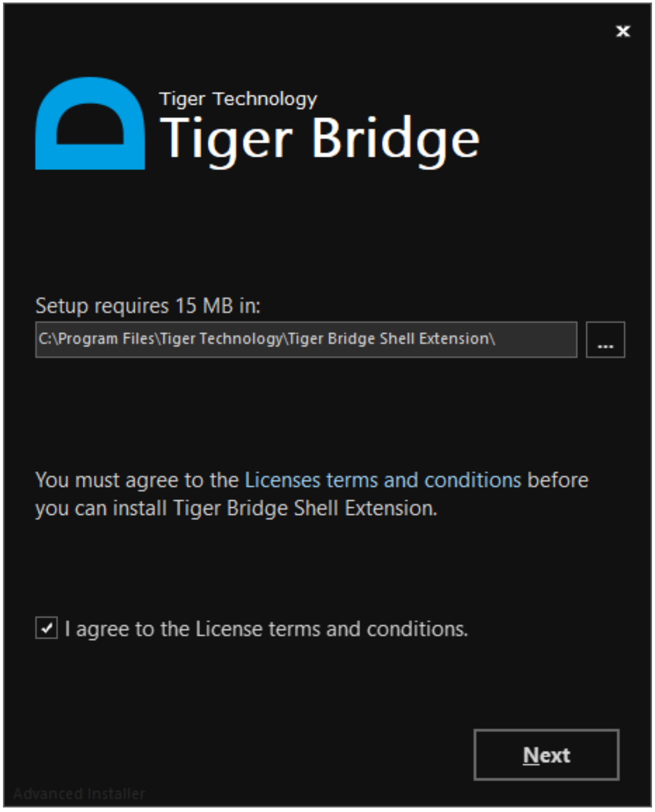
Note: If you clear the check box of a component, you can install it later, by following the same installation steps.

4. When the installation is complete, click Finish.

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.



Setup requires 15 MB in:

C:\Program Files\Tiger Technology\Tiger Bridge Shell Extension\

You must agree to the Licenses terms and conditions before you can install Tiger Bridge Shell Extension.

☑ I agree to the License terms and conditions.

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 on how to use the shell extension from a remote computer, refer to Tiger Bridge Shell Extension on page 12.

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.

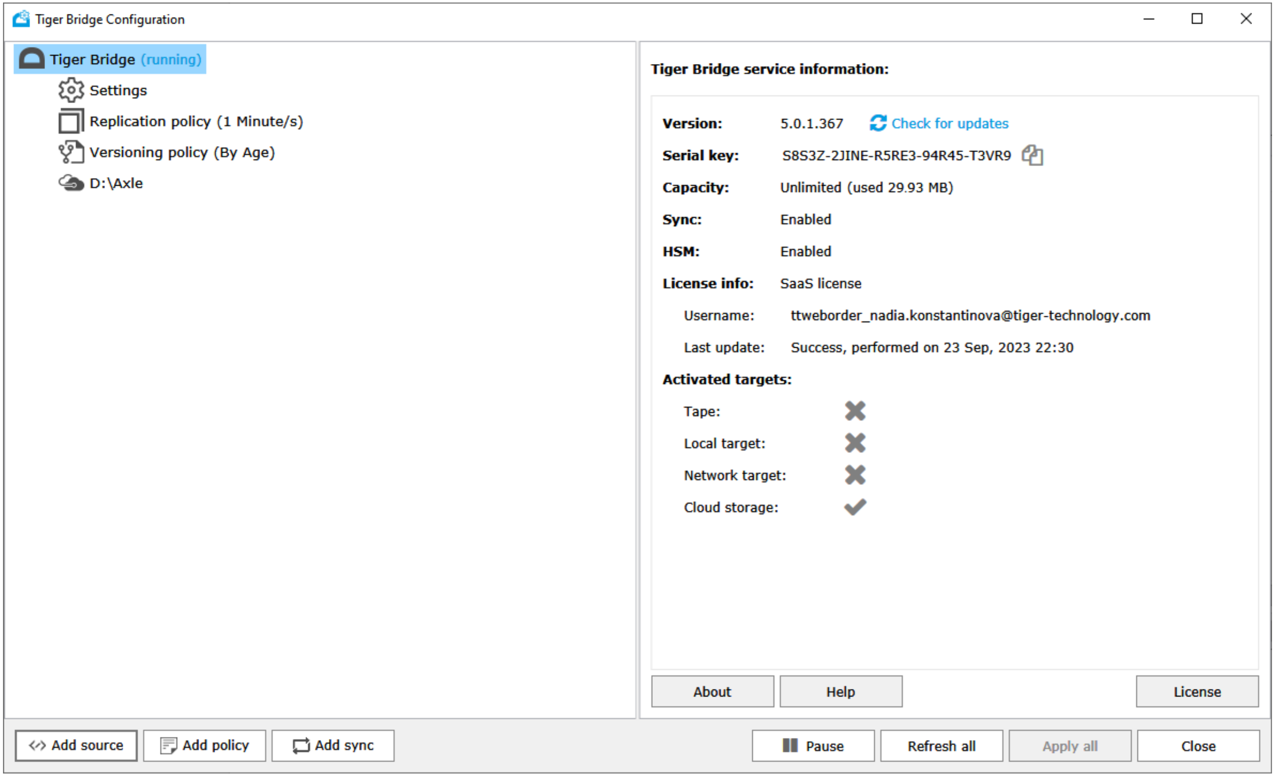
Update Tiger Bridge

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, by following the steps in Install Tiger Bridge on page 55. 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 Configuration

Tiger Bridge (running)
- Settings
- Replication policy (1 Minute/s)
- Versioning policy (By Age)
- D:\Axle

Tiger Bridge service information:

Version:	5.0.1.367 Check for updates
Serial key:	S8S3Z-2JINE-R5RE3-94R45-T3VR9
Capacity:	Unlimited (used 29.93 MB)
Sync:	Enabled
HSM:	Enabled
License info:	SaaS license
Username:	ttweborder_nadia.konstantinova@tiger-technology.com
Last update:	Success, performed on 23 Sep, 2023 22:30

Activated targets:

Tape:	✗
Local target:	✗
Network target:	✗
Cloud storage:	✓

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.

Get Started with Tiger Bridge

To get started with Tiger Bridge you need to activate it and configure at least one pair of source and target, and finally resume automatic Tiger Bridge operations that are paused each time you change something in its configuration.

Once you do that, even if you do not configure any other parameters and Tiger Bridge is not paused, it will operate using the following default settings:

Data replication – Tiger Bridge automatically replicates all data in all configured sources using the default parameters of the global data replication policy. You can edit this global policy's settings or configure a separate replication policy for a specific pair of source and target, by following the steps in Configure Automatic Data Replication on page 73. You can also manually replicate data to the target, by following the steps in Perform Manual Data Lifecycle Operations on page 129.

Space reclaiming – until you configure a global Reclaim Space policy or one that is valid just for a specific pair of a source and a target, Tiger Bridge does not automatically reclaim space. Still, you can manually reclaim space, by following the steps in Perform Manual Data Lifecycle Operations on page 129. For more information about configuring a Reclaim Space policy, refer to Configure Automatic Space Reclaiming on page 76.

Data archiving – unless you have configured Tiger Bridge to replicate directly to the archival tier of the target, no data is automatically archived. To let Tiger Bridge automatically move an already replicated file from the hot/cool tier of the target to the archival tier, you must configure a data archiving policy for each pair of source and target, by following the steps in Automatic Archiving on page 79. Even without a configured policy, you can manually archive data, by following the steps in Perform Manual Data Lifecycle Operations on page 129.

Sync - even if you have paired two or more sources, each on a different Tiger Bridge computer, with the same bucket/container, until you configure a Sync policy, no data on the source(s) is automatically synchronized and you can only synchronize it manually, by following the steps in Manually Synchronize Sources Through a Common Target on page 131. For information about configuring a global Sync policy or one valid for just a specific pair of a source and a target, refer to Configure Multi-Site Sync on page 84.

Data versioning – even if versioning is enabled on your target, but you have not enabled it in Tiger Bridge, each new copy of the same file, which is being replicated on the target, overwrites the previous one. To see how to enable data versioning and control the number of versions kept on the target, refer to Configure Versioning on page 86.

Delete mode – when you delete a file from the source, its replica on the target is automatically deleted as well. 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. For more information, refer to Configure File Operation Mode on page 91.

Retrieve mode – should you retrieve a stub file on the source from the target, the replica is not deleted. To reduce duplication of data and configure the target to act like an extension of the source, you can configure Tiger Bridge to delete the replica of a file from the target, once it is retrieved back on the source. For more information, refer to Configure File Operation Mode on page 91.

Soft delete policy – specify by how long after a file is deleted from the source it should also be deleted from the target in case Delete mode is configured to synchronize the deletion and use this time interval to undelete accidentally deleted files. For more information, refer to Configure Soft Delete Policy on page 93.

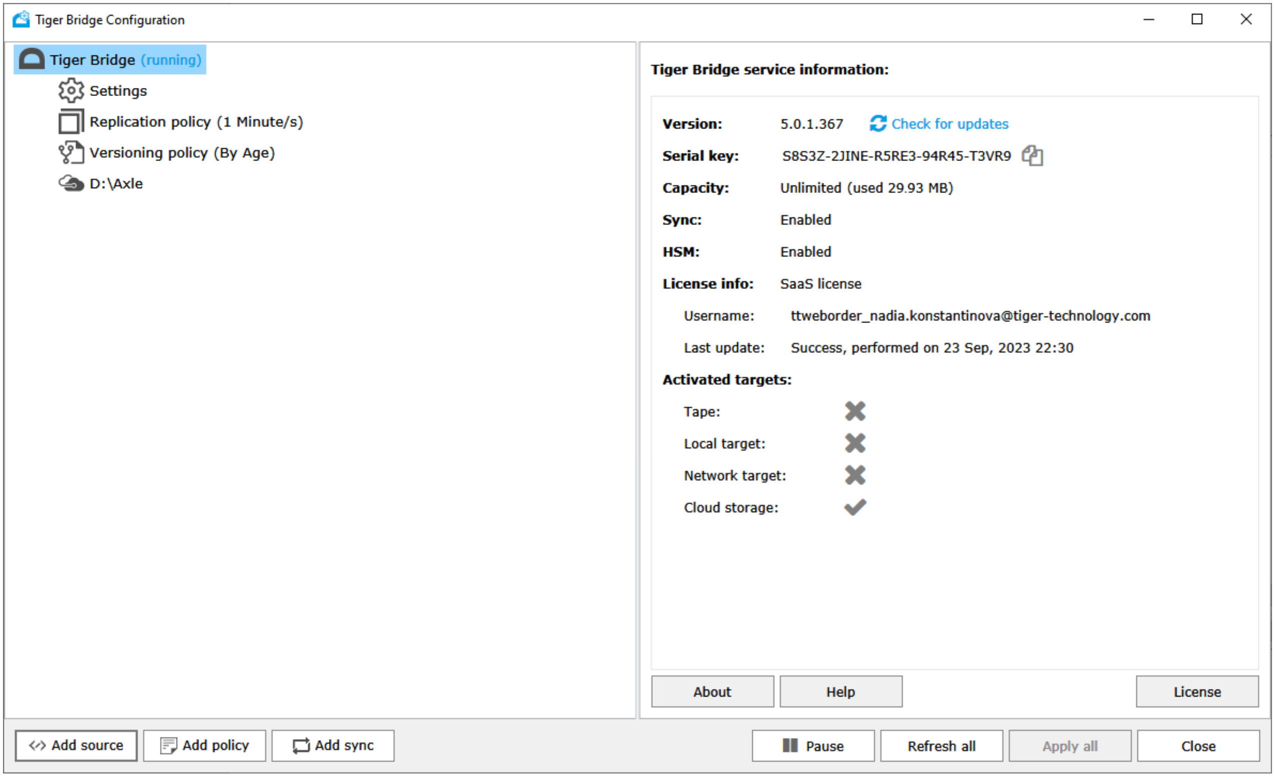
Activate Tiger Bridge

You can activate Tiger Bridge using one of the following:

- software as a service (SaaS) license
- software activation key
- software protection dongle

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.



Tiger Bridge service information:

Version: 5.0.1.367

Serial key: S8S3Z-2JINE-R5RE3-94R45-T3VR9

Capacity: Unlimited (used 29.93 MB)

Sync: Enabled

HSM: Enabled

License info: SaaS license

Username: ttweborder_nadia.konstantinova@tiger-technology.com

Last update: Success, performed on 23 Sep, 2023 22:30

Activated targets:

Tape: ✗

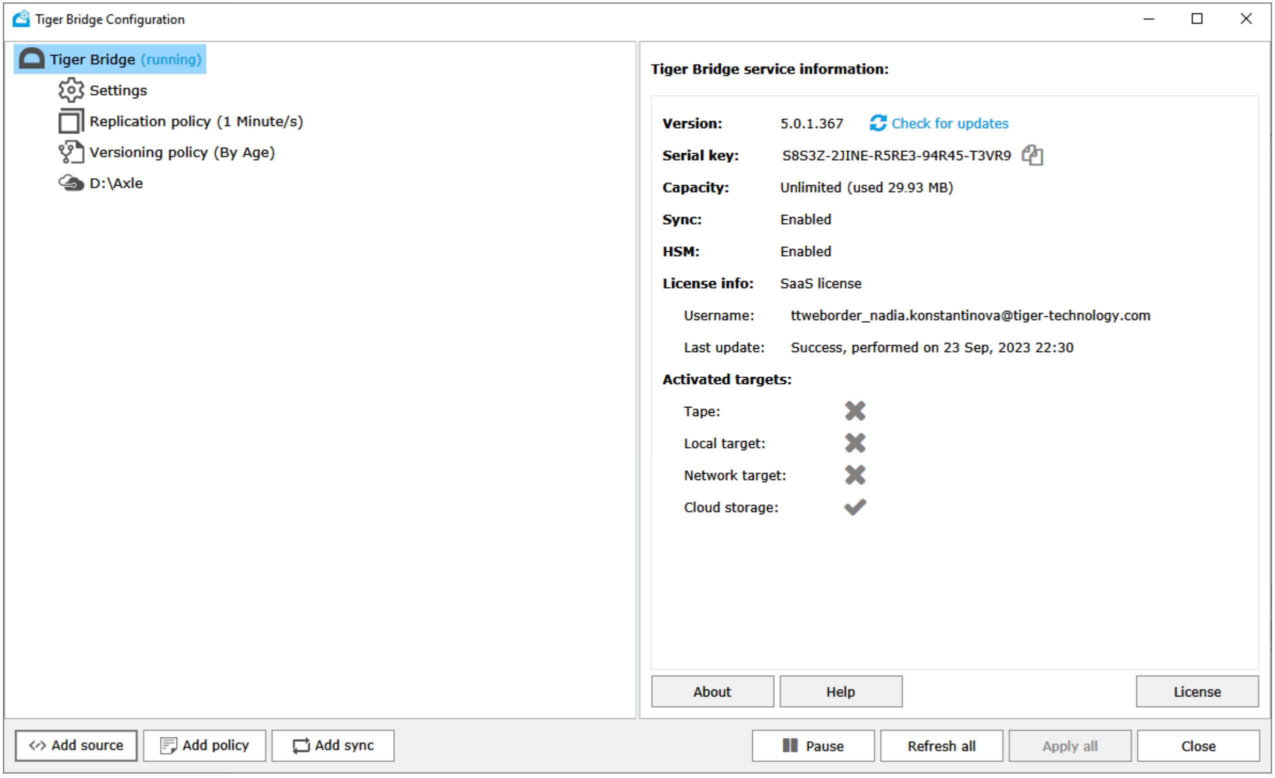
Local target: ✗

Network target: ✗

Cloud storage: ✓

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.



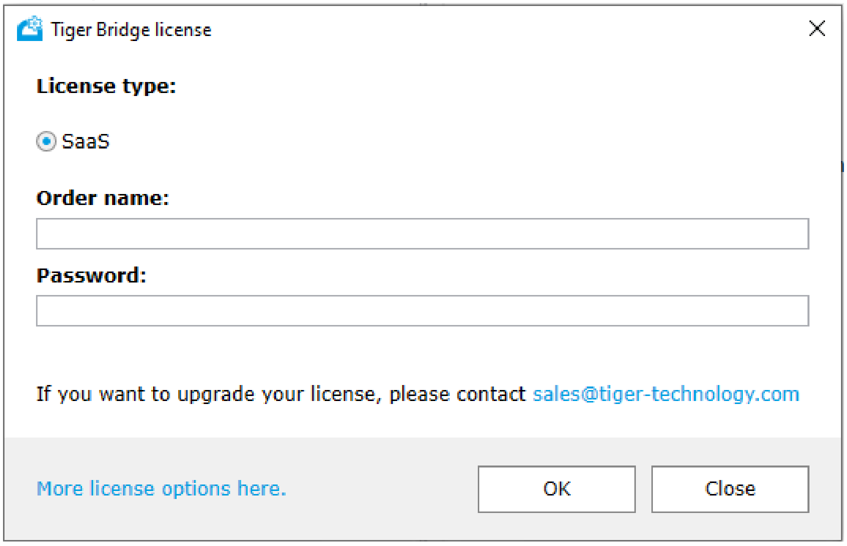
Tiger Bridge service information:

Version:	5.0.1.367 Check for updates
Serial key:	S8S3Z-2JINE-R5RE3-94R45-T3VR9
Capacity:	Unlimited (used 29.93 MB)
Sync:	Enabled
HSM:	Enabled
License info:	SaaS license
Username:	ttweborder_nadia.konstantinova@tiger-technology.com
Last update:	Success, performed on 23 Sep, 2023 22:30

Activated targets:

Tape:	✗
Local target:	✗
Network target:	✗
Cloud storage:	✓

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



License type:

● SaaS

Order name:

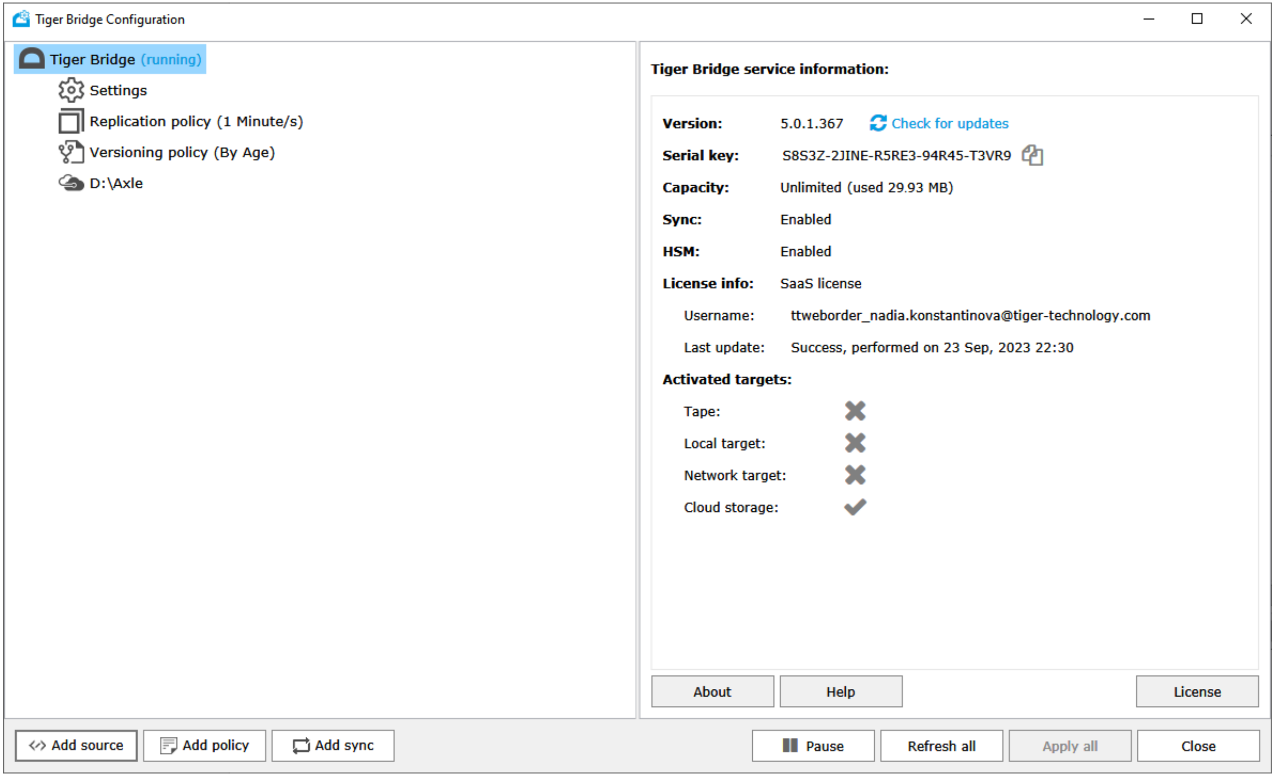
Password:

If you want to upgrade your license, please contact sales@tiger-technology.com

More license options here.

To activate Tiger Bridge with a software activation key:

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



Tiger Bridge Configuration

Tiger Bridge service information:

Version: 5.0.1.367 Check for updates

Serial key: S8S3Z-2JINE-R5RE3-94R45-T3VR9

Capacity: Unlimited (used 29.93 MB)

Sync: Enabled

HSM: Enabled

License info: SaaS license

Username: ttweborder_nadia.konstantinova@tiger-technology.com

Last update: Success, performed on 23 Sep, 2023 22:30

Activated targets:

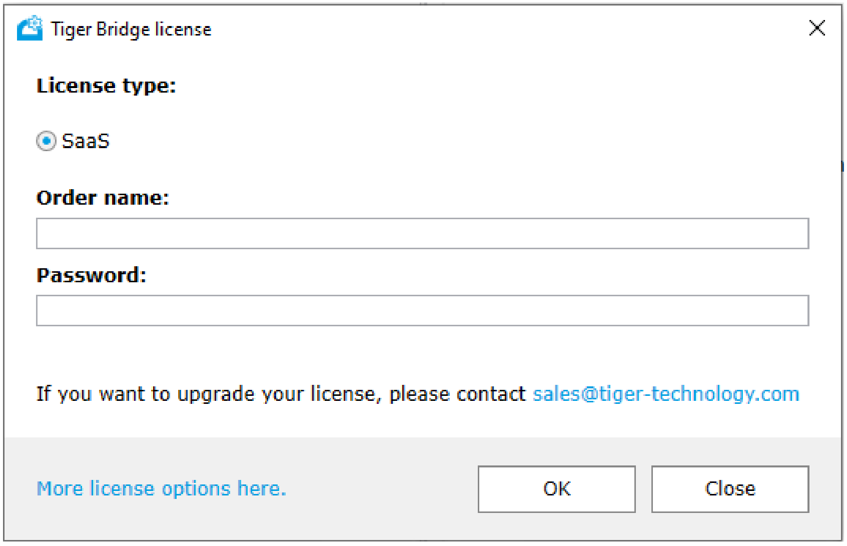
Tape: ✗

Local target: ✗

Network target: ✗

Cloud storage: ✓

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



Tiger Bridge license

License type:

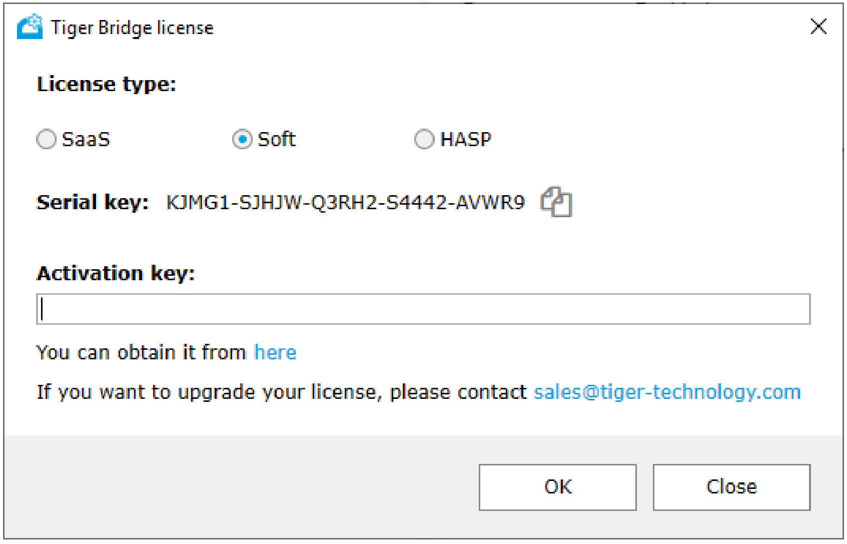
● SaaS

Order name:

Password:

If you want to upgrade your license, please contact sales@tiger-technology.com

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



License type:

○ SaaS ● Soft ○ HASP

Serial key: KJMG1-SJHJW-Q3RH2-S4442-AVWR9 ⧉

Activation key:

You can obtain it from here

If you want to upgrade your license, please contact sales@tiger-technology.com

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. On the home page of the licensing server, enter your username/email and password in the corresponding fields, and click Log in.

6. In the Licensing Server menu, click Home and then find your Tiger Bridge license order.

7. Click the order name and in the Licensing Server menu, click Activate License.

8. Paste the serial number and click Generate Activation Key.

9. Copy the activation key generated for your license.

10. 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

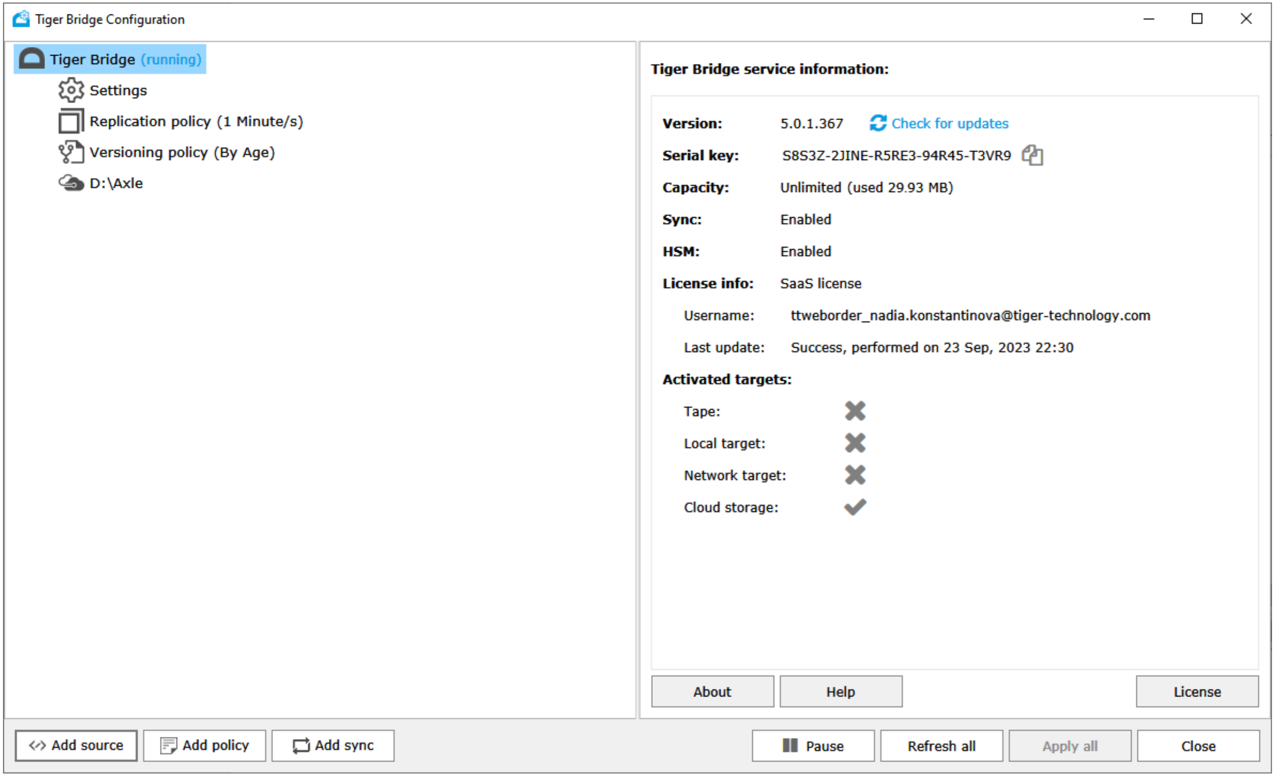
2. On the home page of the licensing server, enter your username/email and password in the corresponding fields, and click Log in.

3. In the Licensing Server menu, click Home and then find your Tiger Bridge license order.

4. Next to the dongle name in the list, click “Download lic file”.

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

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



Tiger Bridge service information:

Version: 5.0.1.367

Serial key: S8S3Z-2JINE-R5RE3-94R45-T3VR9

Capacity: Unlimited (used 29.93 MB)

Sync: Enabled

HSM: Enabled

License info: SaaS license

Username: ttweborder_nadia.konstantinova@tiger-technology.com

Last update: Success, performed on 23 Sep, 2023 22:30

Activated targets:

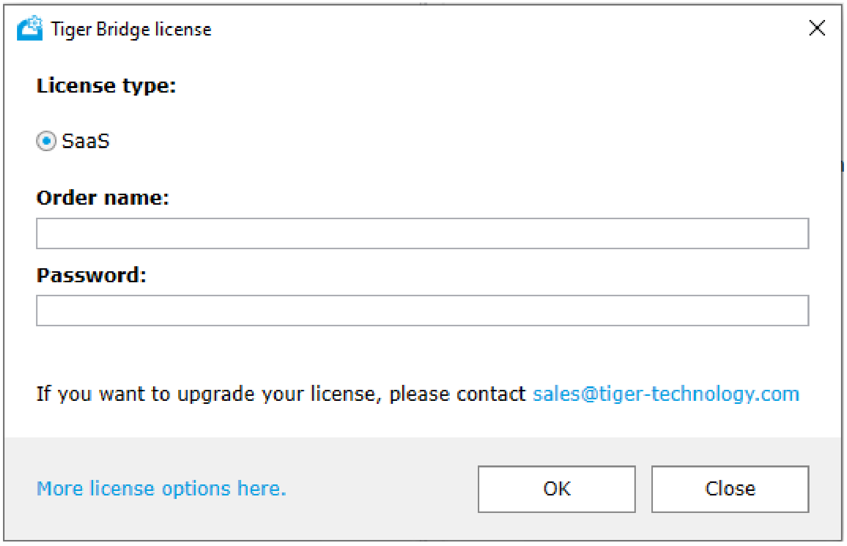
Tape: ✗

Local target: ✗

Network target: ✗

Cloud storage: ✓

6. In the Tiger Bridge License dialog, click on “More license options here”.



License type:

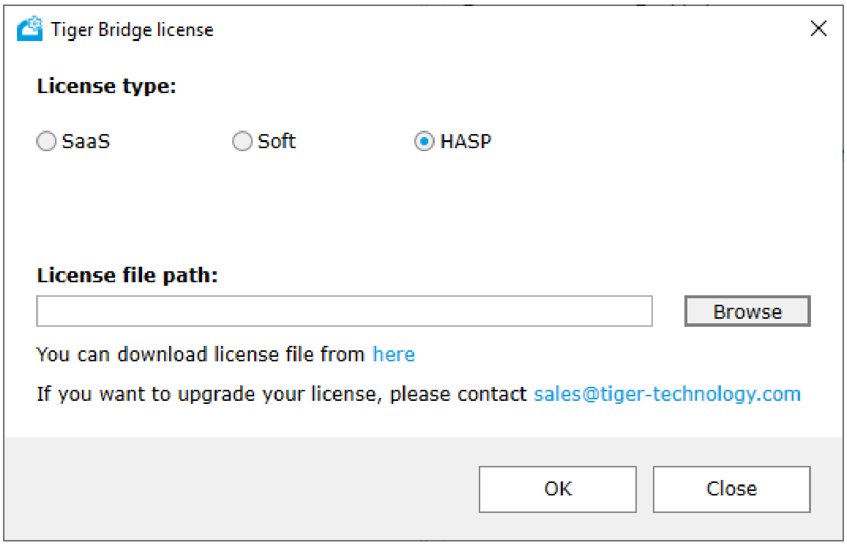
● SaaS

Order name:

Password:

If you want to upgrade your license, please contact sales@tiger-technology.com

7. Select HASP and then click Browse.



Tiger Bridge license

License type:

○ SaaS ○ Soft ● HASP

License file path:

You can download license file from here

If you want to upgrade your license, please contact sales@tiger-technology.com

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

Pair a Source with the Target

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 a source allows you to pair folders on one and the same volume/share with different targets, and thus define different criteria for automatic data replication, space reclaiming, data archiving, etc. Once you select the path to be used as a source, you can further refine, which data in it should be automatically managed by Tiger Bridge, by following the steps in Refine the List of Automatically Managed Source Locations on page 71.

You can add as many sources as you wish. 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.

Before pairing a source with a target of your choice, check the NAS source prerequisites (see NAS Source Prerequisites and Setup below). When pairing a source with a target in the Tiger Bridge Configuration you will be prompted to select how to synchronize the source with data already existing on the target. For more information, refer to Manage Existing Data on the Target on the next page,

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 the local volume source, when the Tiger Bridge space reclaiming 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 Sync mechanism unless you have configured the mechanism to automatically retrieve to the source synchronized data from other sources. When you need to manually synchronize the contents of the source and the target, you need to perform the operation on the control folder and all restored data will appear there in the form of stub files 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 an 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.

Manage Existing Data on the Target

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 to your source. You can import it later on, by following the steps in Recover Data from The Target on page 131.

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.

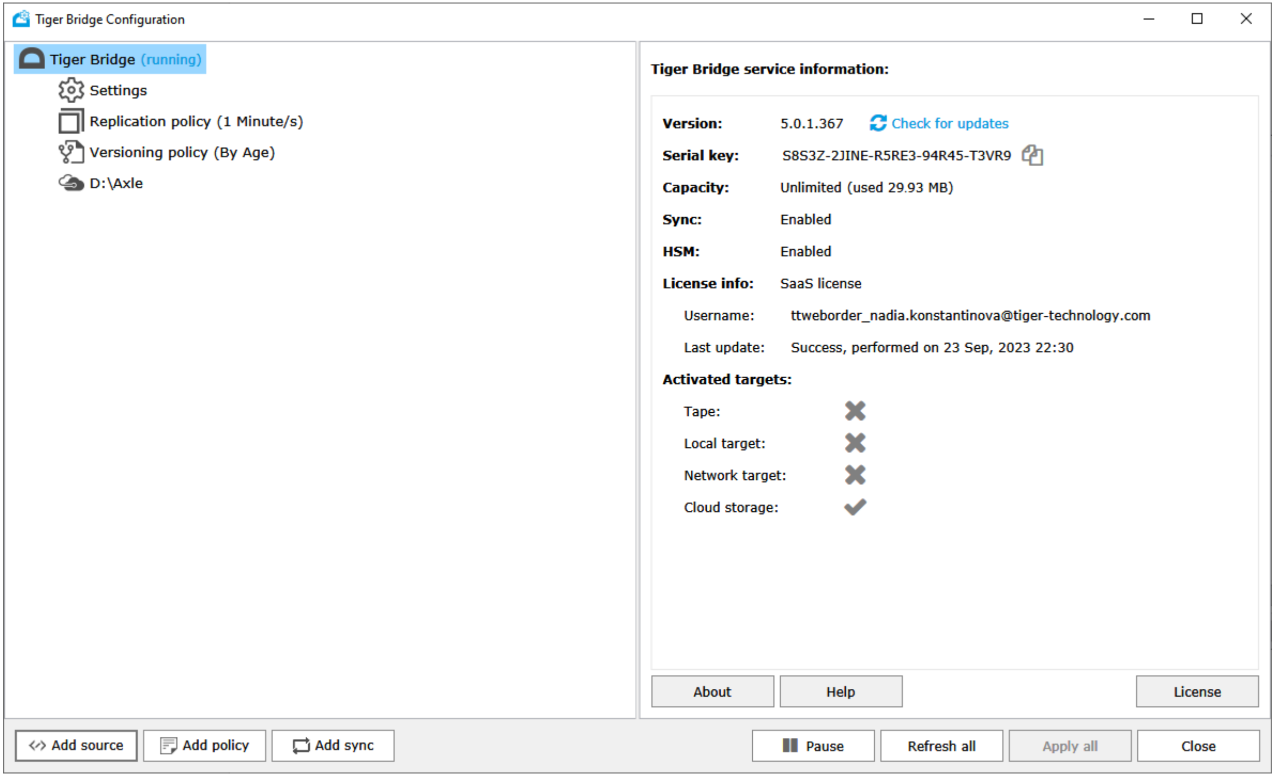
Restore all data — Tiger Bridge retrieves on your source all files and folders from the target, keeping their hierarchical structure. All retrieved files will be with replicated status.

Important: The operation may take time and the free space on your source must be enough to accommodate all data found 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). In the Target dialog, click either Public Cloud or On-Premises, then select the target type and click OK.

To pair a source with a target:

1. In the Tiger Bridge Configuration, click Tiger Bridge in the left pane and then click Add source.



Tiger Bridge Configuration

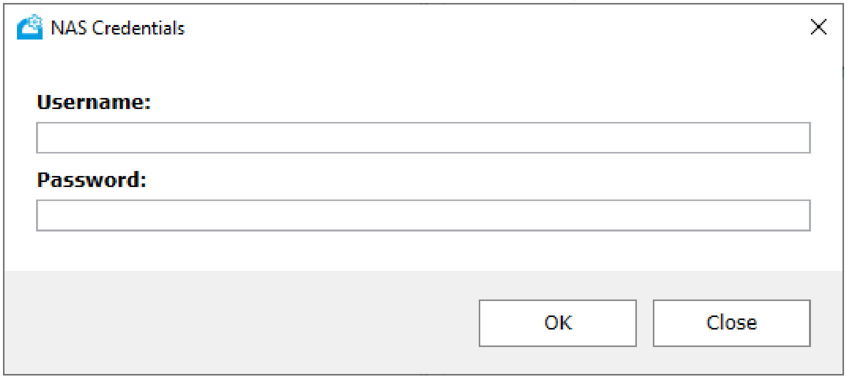
Tiger Bridge (running)
- Settings
- Replication policy (1 Minute/s)
- Versioning policy (By Age)
- D:\Axle

Tiger Bridge service information:

Version: 5.0.1.367 Check for updates
Serial key: S8S3Z-2JINE-R5RE3-94R45-T3VR9
Capacity: Unlimited (used 29.93 MB)
Sync: Enabled
HSM: Enabled
License info: SaaS license
Username: ttweborder_nadia.konstantinova@tiger-technology.com
Last update: Success, performed on 23 Sep, 2023 22:30
Activated targets:
Tape: ✗
Local target: ✗
Network target: ✗
Cloud storage: ✓

2. Browse to and select a location on the local NTFS/ ReFS or SMB/NFS share you want to add as a source or enter the path manually, then click Select Folder.

3. (SMB share only) In the NAS Credentials dialog, enter the username and password of a user with Full Control over the network share in the respective fields.



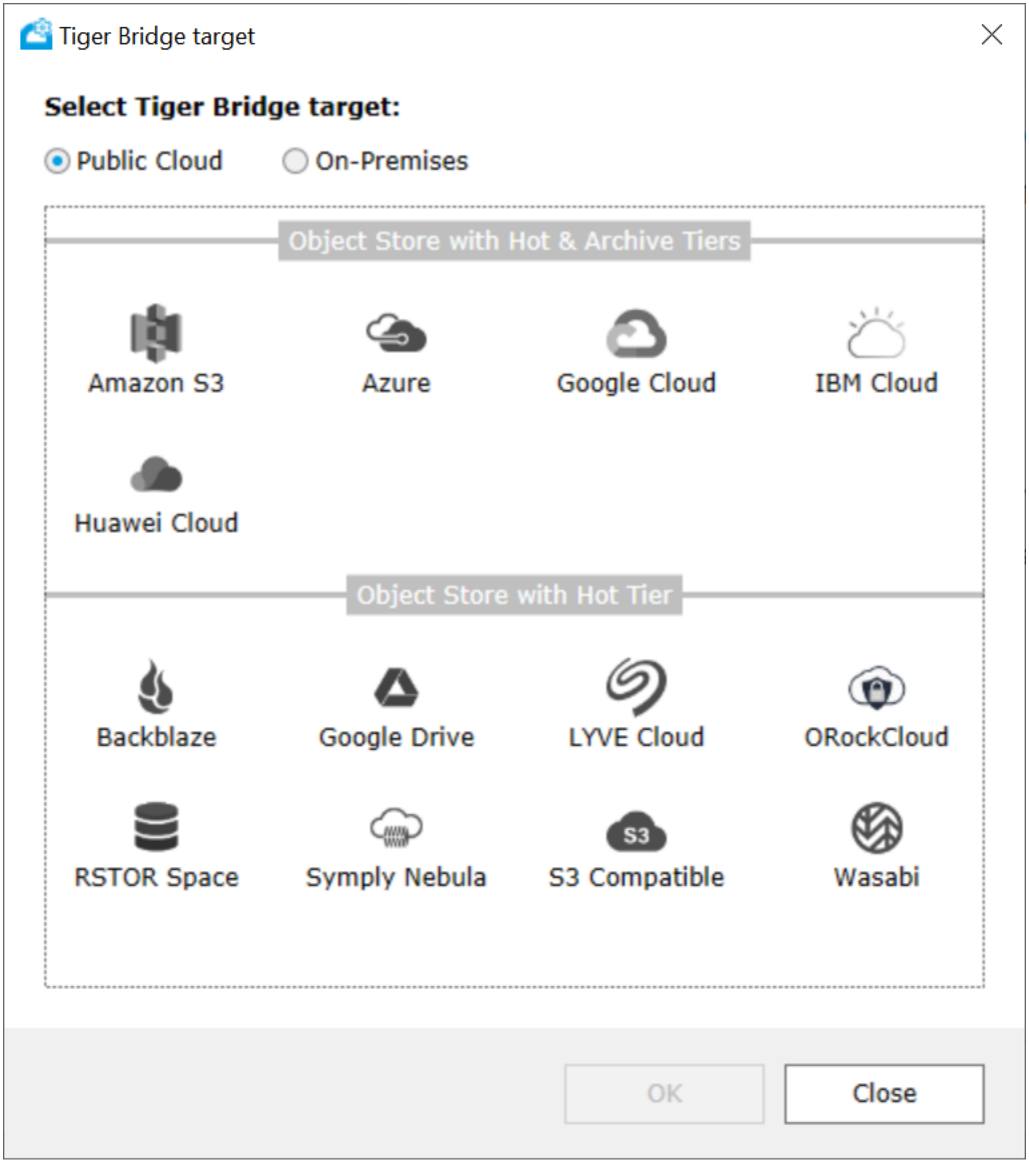
NAS Credentials

Username:

Password:

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

4. In the Tiger Bridge Target dialog, click either Public Cloud or On-Premises, then select the target type and click OK.

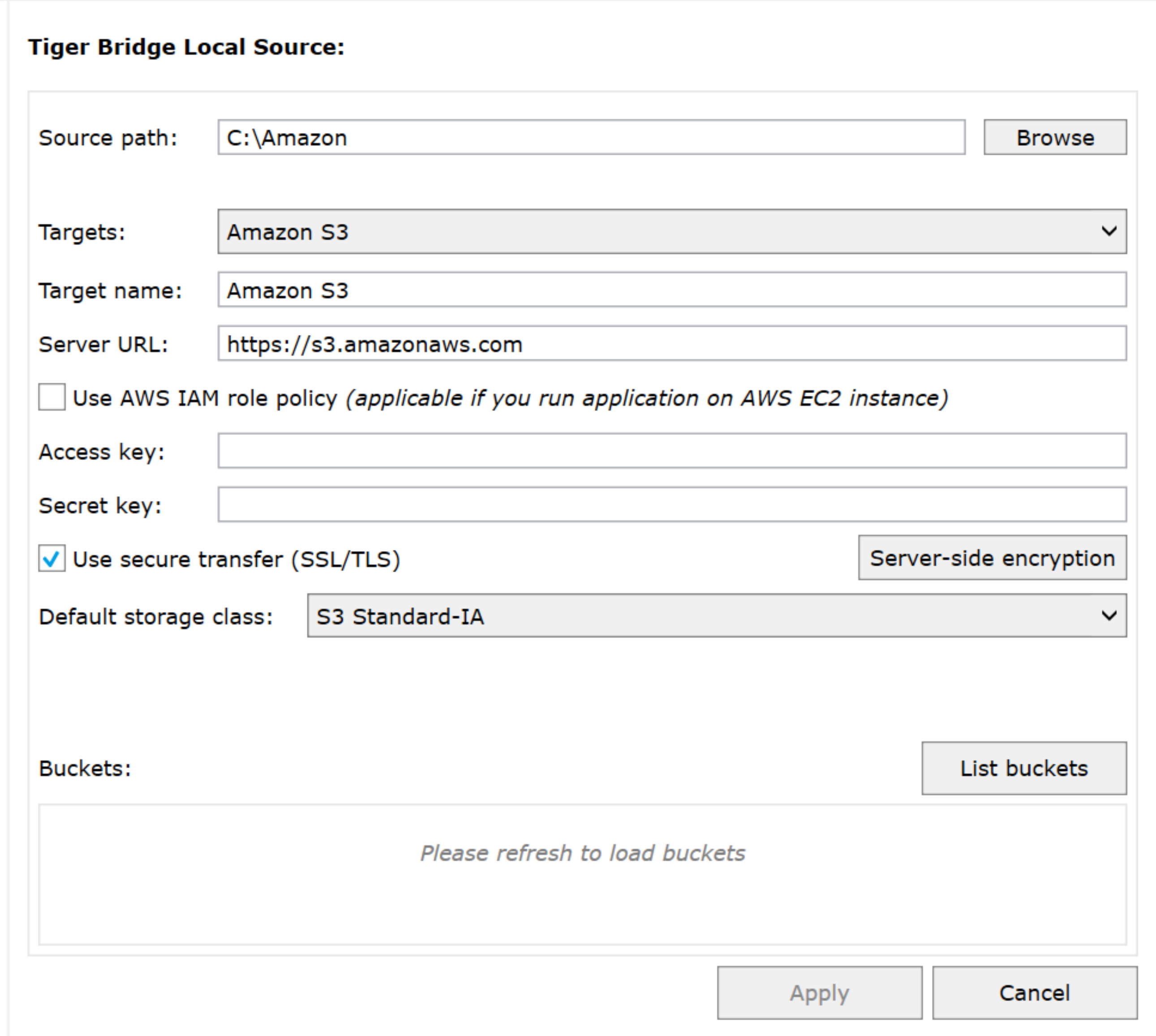


Tiger Bridge target

Select Tiger Bridge target:

● Public Cloud ○ On-Premises

5. (NAS source only) In the right pane of the Configuration, click Browse and browse to and select the control folder or alternatively enter the path to it.



Tiger Bridge Local Source:

Source path: C:\Amazon

Targets: Amazon S3

Target name: Amazon S3

Server URL: https://s3.amazonaws.com

□ Use AWS IAM role policy *(applicable if you run application on AWS EC2 instance)*

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)

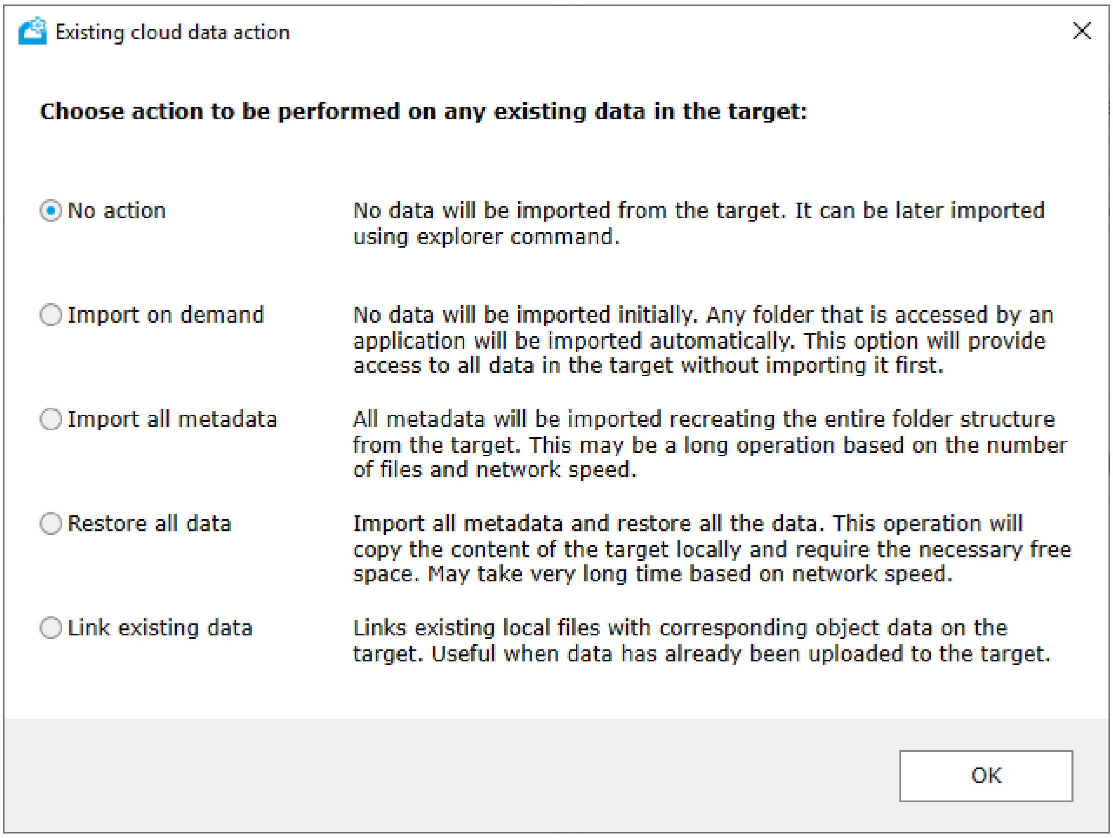
Default storage class: S3 Standard-IA

Buckets:

Please refresh to load buckets

6. In the right pane of the Configuration, fill in the requested target details as outlined in Target Storage Prerequisites on page 20 and click Apply.

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



Existing cloud data action

Choose action to be performed on any existing data in the target:

● 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.

8. Click Apply.

Note: By default, each time you change the Tiger Bridge configuration, all automatic operations are paused. To resume them, follow the steps in Pause/Resume Automatic Tiger Bridge Operations below.

Tip: If you have configured a folder as a source, Windows Explorer displays it with this icon ☁ on the Tiger Bridge computer.

Pause/Resume Automatic Tiger Bridge Operations

By default, all automatic data lifecycle operations are initially paused. Tiger Bridge also pauses them each time you introduce a change in its configuration. You can manually pause and resume the automatic Tiger Bridge operations at any time either using the tray icon or the Configuration.

Tip: The tray application icon color designates whether automatic operations are paused or running. For more information refer to Monitor Tiger Bridge Status and Activity Using the Tray Icon on page 144.

To pause/resume automatic Tiger Bridge operations using the tray icon:

Right-click the Tiger Bridge tray icon and do one of the following:

- Click “Resume operation” to resume automatic Tiger Bridge operations.
- Click “Pause operation” to pause automatic Tiger Bridge operations.

To pause/resume automatic Tiger Bridge operations in the Configuration:

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 lower part of the Configuration.

- To pause all automatic Tiger Bridge operations, click Pause in the lower part of the Configuration.

Refine the List of Automatically Managed Source Locations

By default, Tiger Bridge automatically manages all data on your source, except encrypted files and the following files and folders that are ignored by default:

- RECYCLER
- System Volume Information
- Recycled
- $RECYCLE.BIN
- SANConfig.san
- .san_config.cfg
- .DS_Store
- .Spotlight-V100
- .TemporaryItems
- .Trashes
- .VolumeIcon.icns
- .com.apple.timemachine.supported
- .com.apple.timemachine.donotpresent
- .fseventsd
- .metadata_never_index
- .san_alive.dmn
- .tt_rt_guid
- Thumbs.db
- TIER_SYNC_PRIVATE_DIR_NAME
- .tt_rt
- DfsrPrivate
- not replicated files with offline attribute

Note: You can manually replicate all files that are ignored by default.

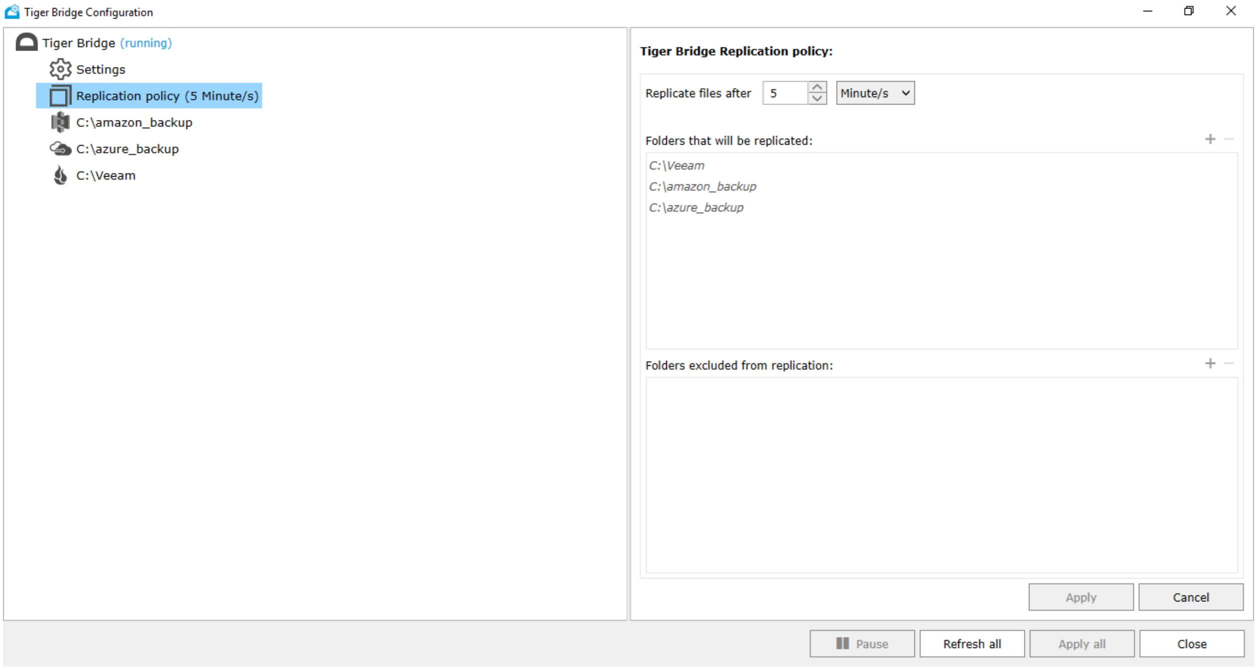
In addition to the files ignored by default, you can also configure Tiger Bridge to manage automatically only data in certain paths on your sources and omit other data, allowing you to replicate, archive, or reclaim it only manually. `For this purpose, you should configure lists of included and excluded locations on all sources. When you pair a source with a target in the Configuration Tiger Bridge automatically adds the root of each source to the list of included locations meaning that by default all data on the source is automatically managed. To refine the list of automatically managed locations, add or remove paths in the two lists, adhering to these rules:

- The root of the source is in the included locations list and the excluded locations list is empty - all data on a source is automatically managed.
- The root of the source is in the included locations list and the excluded locations list contains the paths of some sub-folders – all data on the source is automatically managed except data in the excluded sub-folders.
- The root of the source is in the excluded locations list and the included locations list contains the paths of some sub-folders - only data in the sub-folders is managed and all other data is excluded.
- The included locations list is empty – no data is automatically managed.

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

To refine the list of automatically managed locations on all sources:

1. In the left pane of the Configuration, under Settings, click Replication policy.



Tiger Bridge Replication policy:

Replicate files after 5 Minute/s

Folders that will be replicated:

C:\Veeam
C:\amazon_backup
C:\azure_backup

Folders excluded from replication:

2. In the right pane, 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, browse to and select the respective folder, then click OK.

Tip: 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.

3. Click Apply and optionally resume automatic Tiger Bridge operations.

Configure Automatic Data Replication

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 for Tiger Bridge to queue it for replication. You can configure the global data replication policy (created during the initial configuration of Tiger Bridge), which is valid for all pairs of 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 assigning a data replication policy to a given pair of source and target and thus specify different parameters.

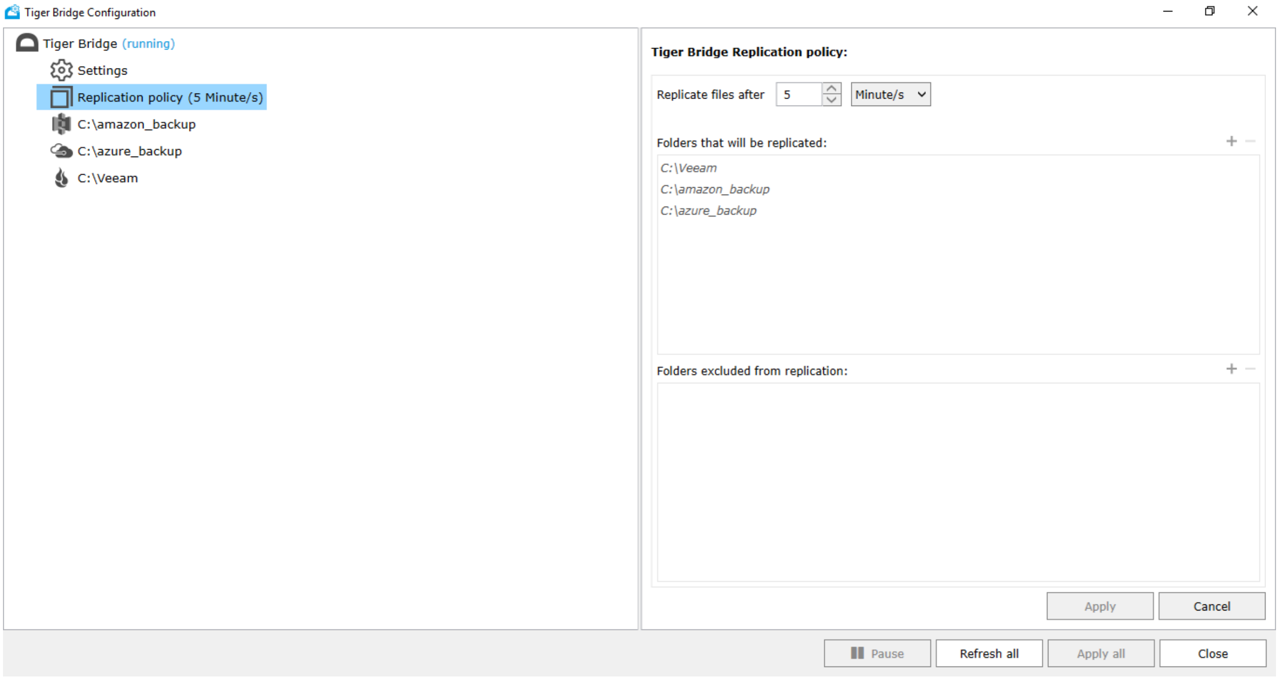
You can disable automatic data replication both globally or just for a specific pair of source and target. For this purpose, you need to configure it to replicate files when they have not been modified for 0 minutes. In this case, you can replicate files only manually.

When configuring the global data replication policy, you can also refine the list of automatically managed locations on all sources and exclude some paths from automatic replication, archiving, and/or space reclaiming. For more information, refer to Refine the List of Automatically Managed Source Locations on page 71.

You can also fine-tune your data replication workflow by configuring several advanced settings. For more information, refer to Fine-Tune Data Replication on page 107.

To configure global data replication policy:

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



Tiger Bridge Replication policy:

Replicate files after 5 Minute/s

Folders that will be replicated:

C:\Veeam
C:\amazon_backup
C:\azure_backup

Folders excluded from replication:

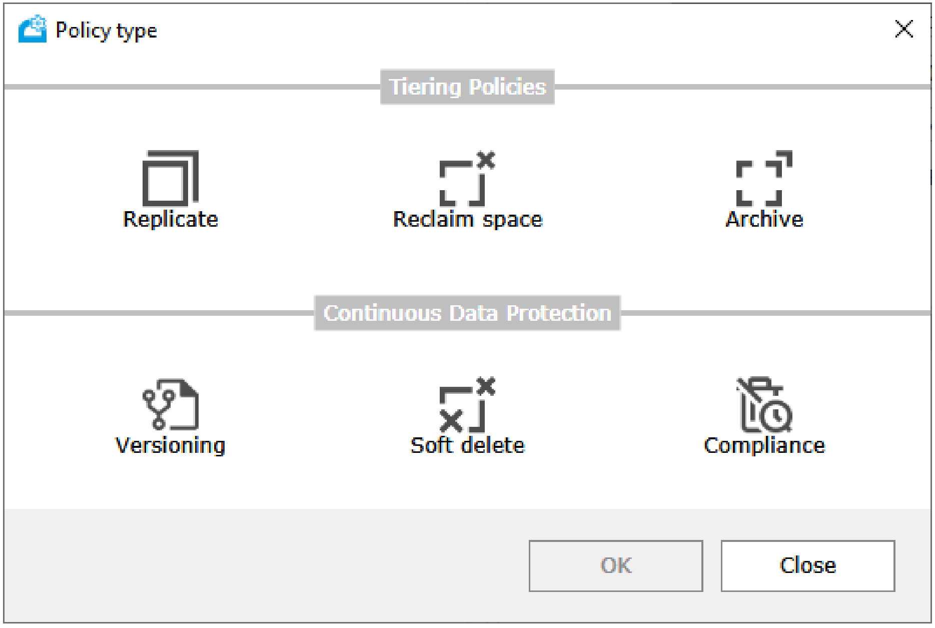
2. In the right pane, specify for how long a file should not have been modified for Tiger Bridge to replicate it, by entering the desired number and selecting the unit of measure in the drop-down box beside it.

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

3. Click Apply and optionally resume automatic Tiger Bridge operations.

To overwrite the global replication policy for a specific pair:

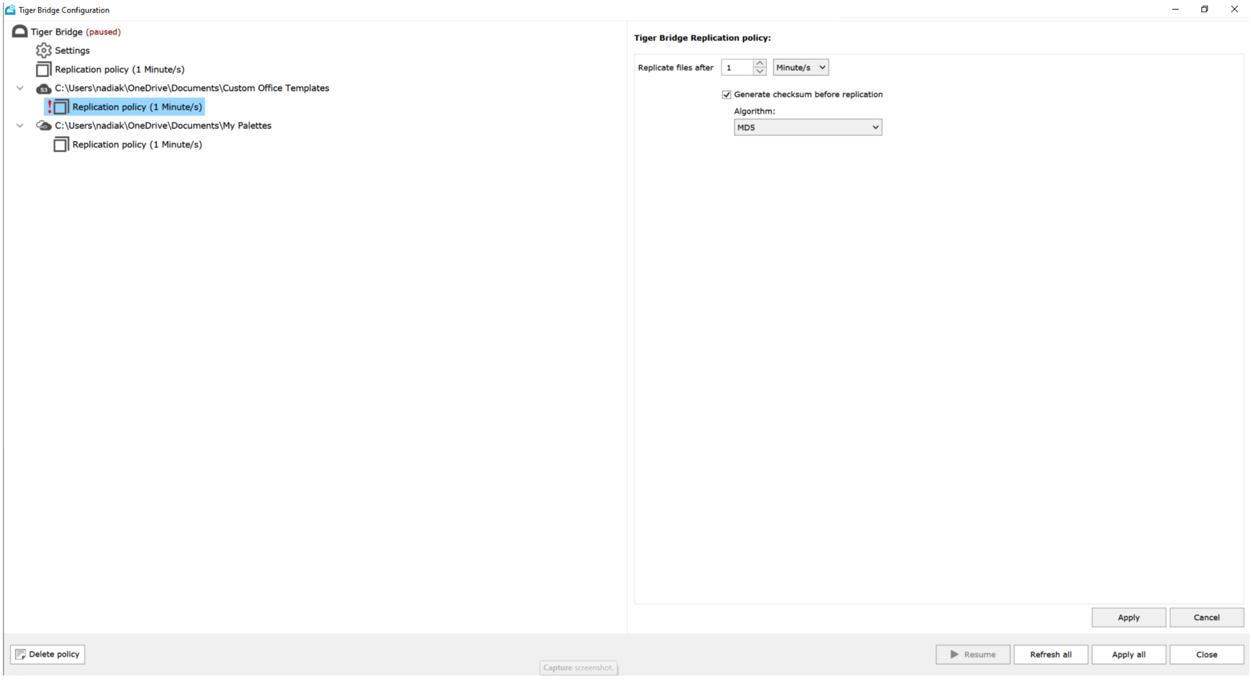
1. In the Tiger Bridge Configuration, select the source in the left pane and click Add policy.



2. In the Policy Type dialog, select Replicate and click OK.

Tip: 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.

2. In the right pane, do the following:



Tiger Bridge Configuration

- Tiger Bridge (paused)
  - Settings
  - Replication policy (1 Minute/s)
  - C:\Users\nadiak\OneDrive\Documents\Custom Office Templates
    - Replication policy (1 Minute/s)
  - C:\Users\nadiak\OneDrive\Documents\My Palettes
    - Replication policy (1 Minute/s)

Tiger Bridge Replication policy:

Replicate files after 1 Minute/s

☑ Generate checksum before replication

Algorithm: MD5

- 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.

- Select the "Generate checksum before replication" check box to instruct Tiger Bridge to generate a checksum for each file before it replicates itand in the Algorith drop-down box select the algorithm that is also running on the target.

Note: On Microsoft Azure, the Algorithm drop-down box is not present as Tiger Bridge is configured to automatically use the default target algorithm .

3. Click Apply and optionally resume automatic Tiger Bridge operations.

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

Checksum Verification of Replicated Data

To support workflows that require checksum verification for data integrity, you can configure Tiger Bridge to generate a checksum for each file before replicating it manually or automatically to the target. The generated checksum is stored on the source in the file's metadata, even if space is reclaimed and the file is replaced by a stub file. This checksum is used for data integrity verification by comparing it with the checksum generated by an algorithm running on the target, if such an algorithm exists.

On an Azure target, verification is performed automatically by comparing the checksum generated on the source with the one generated by Azure's algorithm. If the file's integrity has been compromised during transit to the target (for example, if SSL/TLS is not used for transfer), replication will fail due to a checksum mismatch. If the data on the target has been tampered with, resulting in a checksum that differs from the one stored on the source, retrieving the file from the target will fail. You can also manually verify the integrity of a file replica without retrieving it from the source by executing the following command:

```
    tiercli op verify <path to file or folder> --logfile <path where .txt log should
be created>
```

For other targets that support checksums, manual verification is required by comparing the checksum generated on the source with the one generated on the target. To view the checksum of a source file, use the following command:

```
    tiercli op info <path to a source file>
```

Currently, checksum generation is supported on both cloud and local storage targets. You can enable it through the replication policy of a specific source-target pair. Once enabled, the system generates a checksum for each file before replicating it, either automatically or manually. Refer to Configure Automatic Data Replication on page 73 for instructions on how to add a source-specific replication policy and enable automatic checksum generation.

Configure Automatic Space Reclaiming

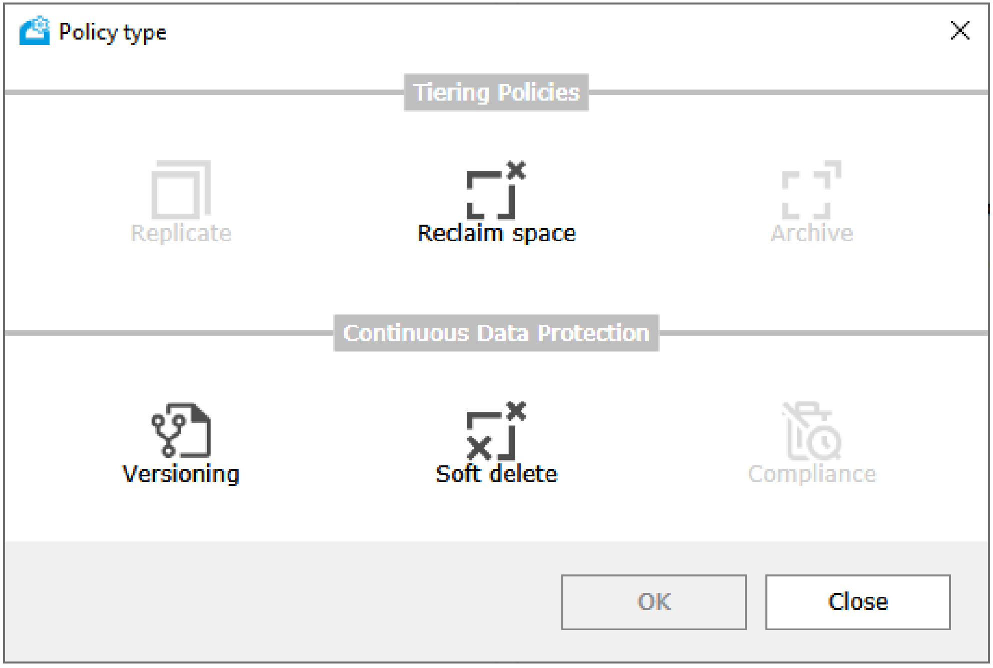
To let Tiger Bridge automatically reclaim space on your sources, you must add a Reclaim Space policy. The policy instructs Tiger Bridge which files must be replicated (if not already replicated) and then replaced by stubs on the source. Once you add a Reclaim Space policy, unless you configure its parameters, it uses the default ones:

- Regardless of their size all files in the included locations on the source are replicated (if not already replicated) and then replaced by stubs if they have not been accessed for more than 4 weeks.
- Files matching the above criteria are replaced by stubs regardless of the used space on the source.
- When the used space on the source exceeds 90% all files subject to replication are also queued for replacement with stub files regardless of their size and time of last access. In this, Tiger Bridge processes the queue of files scheduled for replacement with stubs, starting from the ones that are least recently accessed and proceeds with the reclaiming of space on the source until the used space falls below 90%.

You can add a global Reclaim Space policy, valid for all sources. You can also add and enable a Reclaim Space policy valid for just a specific pair of a source and a target, and thus use different parameters. Keep in mind that the global policy is valid only for sources that do not have a Reclaim Space policy of their own. Thus, even if you have configured a Reclaim Space policy for a pair of source and target, but it is disabled, Tiger Bridge assumes that the pair has a policy of its own and does not apply the global policy and does not reclaim any space on that source.

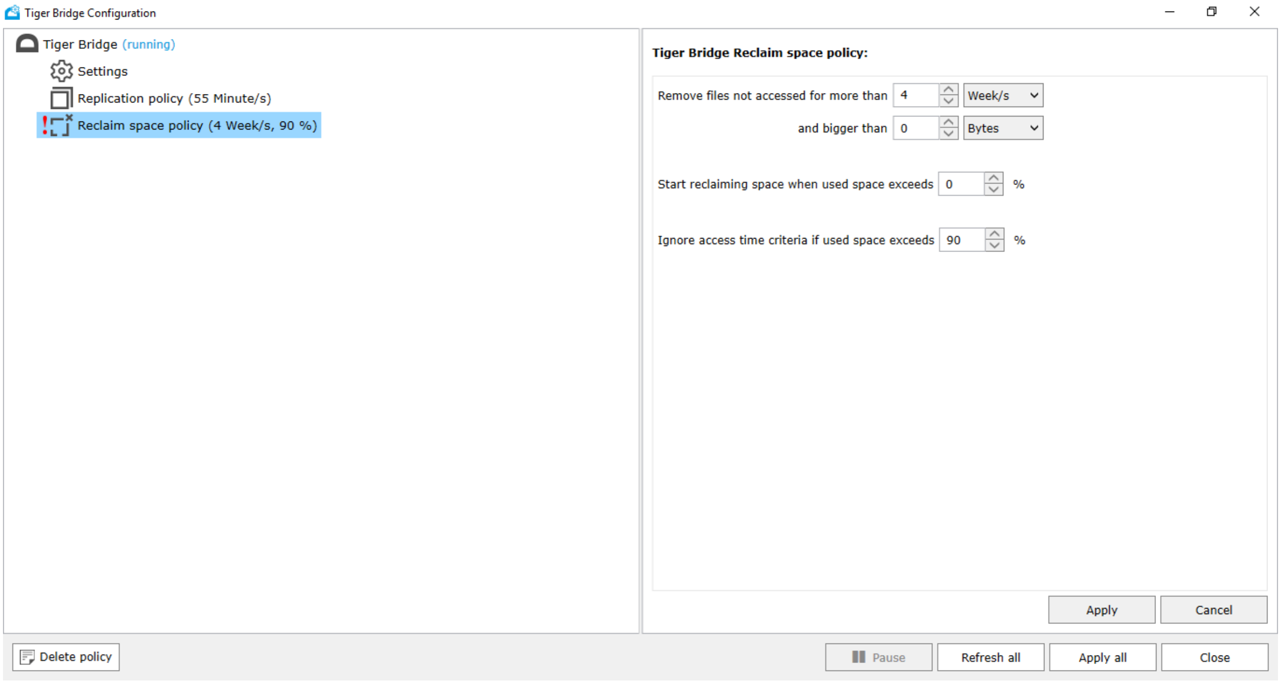
To configure the global Reclaim Space policy:

1. In the Tiger Bridge Configuration, select Tiger Bridge in the left pane and click Add policy.



2. In the Policy Type dialog, click ”Reclaim space” and click OK.

3. In the right pane, configure the following parameters:


Tiger Bridge Configuration
Tiger Bridge (running)
Settings
Replication policy (55 Minute/s)
Reclaim space policy (4 Week/s, 90 %)
Apply
Cancel
Delete policy
Pause
Refresh all
Apply all
Close

Tiger Bridge Reclaim space policy:

Remove files not accessed for more than 4 Week/s

and bigger than 0 Bytes

Start reclaiming space when used space exceeds 0 %

Ignore access time criteria if used space exceeds 90 %

- In “Remove files not accessed for more than” specify for how long a file must not have been accessed for Tiger Bridge to replace it with a stub on the source.
- In “Bigger than” specify how big a file should be for Tiger Bridge to replace it with a stub. To allow the replacement of all files regardless of their size, leave the default value of 0 Bytes.
- In “Start reclaiming space when used space exceeds” specify the used space threshold, which when exceeded triggers Tiger Bridge to reclaim space. To let Tiger Bridge reclaim space regardless of the used space, leave the value to 0%.

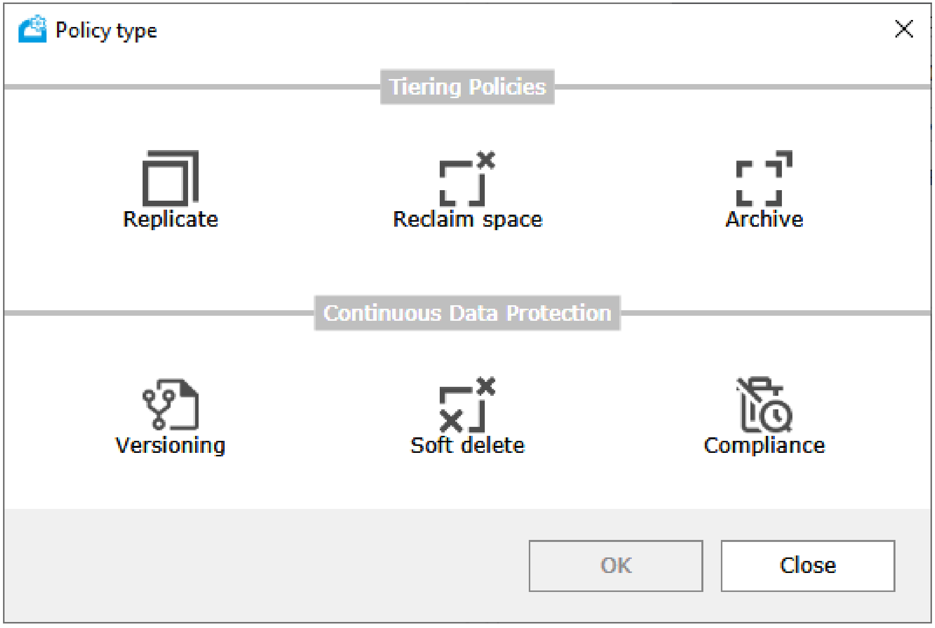
- In “Ignore access time criteria if used space exceeds” specify the used space threshold, which when exceeded triggers the replacement of replicated files with stubs even if they do not yet meet the access time criteria.

4. Click Apply and optionally resume automatic Tiger Bridge operations.

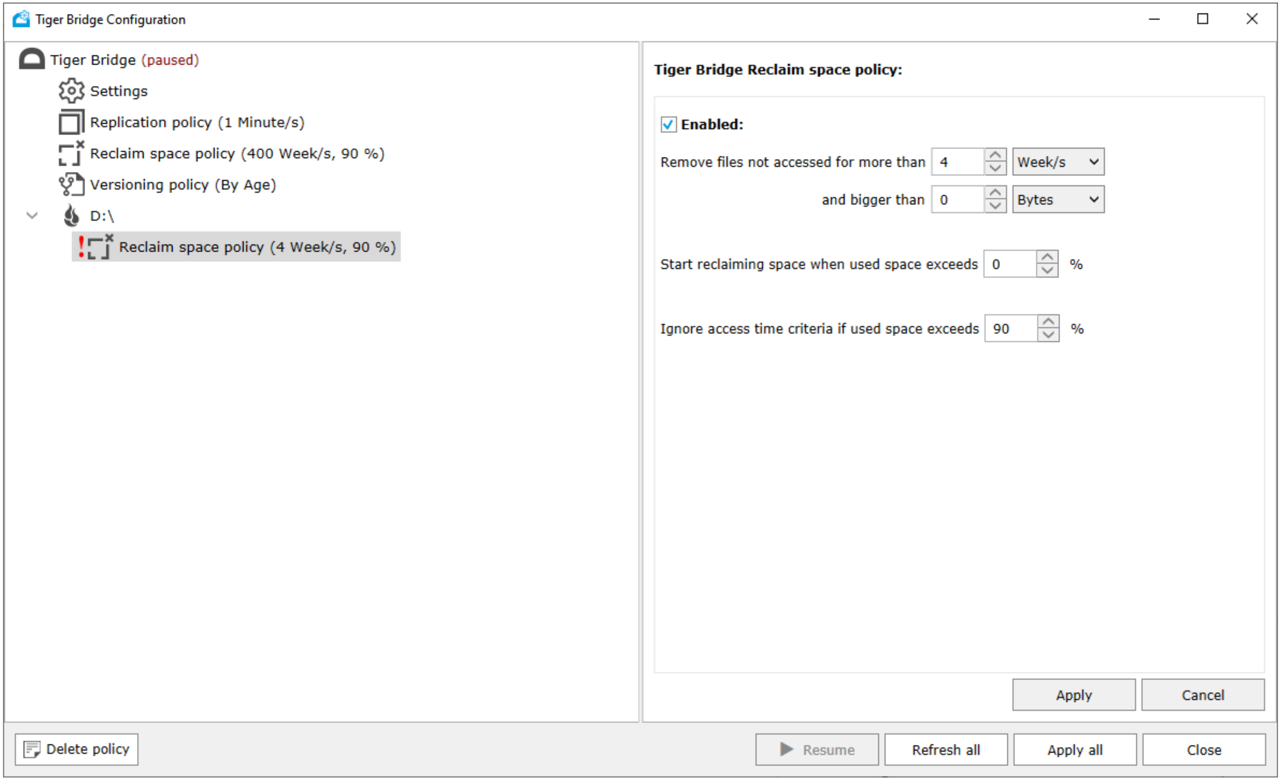
Note: To edit the global policy, simply select it in the left pane, edit the desired parameter, and click Apply. To delete the global policy, select it in the left pane and click Delete policy.

To overwrite the global Reclaim Space 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 "Reclaim space" and click OK.


Tiger Bridge Configuration
Tiger Bridge (paused)
Settings
Replication policy (1 Minute/s)
Reclaim space policy (400 Week/s, 90 %)
Versioning policy (By Age)
D:\
Reclaim space policy (4 Week/s, 90 %)
Apply
Cancel
Delete policy
Resume
Refresh all
Apply all
Close

Tiger Bridge Reclaim space policy:

☑ Enabled:

Remove files not accessed for more than 4 Week/s

and bigger than 0 Bytes

Start reclaiming space when used space exceeds 0 %

Ignore access time criteria if used space exceeds 90 %

3. In the right pane, select the Enabled check box, to enable the policy.
4. To change the default parameters of the Reclaim Space policy, do the following:

- In “Remove files not accessed for more than” specify for how long a file must not have been accessed for Tiger Bridge to replace it with a stub on the source.
- In “Bigger than” specify how big a file should be for Tiger Bridge to replace it with a stub. To allow the replacement of all files regardless of their size, leave the default value of 0 Bytes.
- In “Start reclaiming space when used space exceeds” specify the used space threshold, which when exceeded triggers Tiger Bridge to reclaim space. To let Tiger Bridge reclaim space regardless of the used space, leave the value to 0%.
- In “Ignore access time criteria if used space exceeds” specify the used space threshold, which when exceeded triggers the replacement of replicated files with stubs even if they do not yet meet the access time criteria.

5. Click Apply and optionally resume automatic Tiger Bridge operations.

Note: To edit the policy, simply select it in the left pane, edit the desired parameter, and click Apply. To delete the policy, select it in the left pane and click Delete policy. To disable the policy without deleting it, select it in the left pane and clear the “Enable” check box, then click Apply.

Automatic Archiving

In Tiger Bridge, data archiving means moving already replicated files from the tier/storage class for direct replication of your cloud storage target to the archival tier/storage class. If you have set up Tiger Bridge to replicate directly to an archival tier/storage class of the target, there is no need to enable data archiving as all replicated data is already archived.

The available storage classes differ from target to target. Also, each different target allows or disallows the possibility for a third-party software to move data to the archive. Thus, the archiving options provided by Tiger Bridge depend on the target you are using:

- As long as your target allows third-party policies to manage the moving of data from their hot/cool tier to the archival tier, you can use Tiger Bridge to archive data both manually and automatically. To archive data automatically, you must add a Tiger Bridge archiving policy to your source. Note that Tiger Bridge's Archive policy does not overwrite the target provider's own archiving rule and if both are enabled, they operate concurrently.
- On targets like IBM Cloud storage you can enable, configure, or delete the target provider's own archiving rule from within Tiger Bridge.
- On targets that do not allow third-party software to move data to the archive, you can synchronize Tiger Bridge with the target's own archive rule and thus let it check for archived files. This can be useful when space reclaiming is also enabled as Tiger Bridge can update the status of reclaimed files on the source to offline.

Configure Tiger Bridge Archiving Policy

Tiger Bridge’s archiving policy allows you to specify which already replicated files must be moved to the archival tier/storage class of the target. If the files are replaced with stubs on the source by the space reclaiming mechanism, Tiger Bridge updates their status to offline when they are moved to the archive. Currently, you can add a Tiger Bridge archive policy on the following targets:

- Microsoft Azure
- Amazon S3
- Google Cloud
- Huawei Cloud
- any S3-compatible object storage provider that allows third-party software to move data to the archival tier

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 10 MB and the time interval to 2 weeks, Tiger Bridge moves to the archive all replicated files with size 10 MB or above that have not been accessed for at least 2 weeks. By default, Tiger Bridge moves to the archive replicated files that are bigger than 10 MB if they have not been accessed for more than 50 weeks. Tiger Bridge processes the queue of replicated files scheduled for automatic archiving starting from the ones that are least recently accessed.

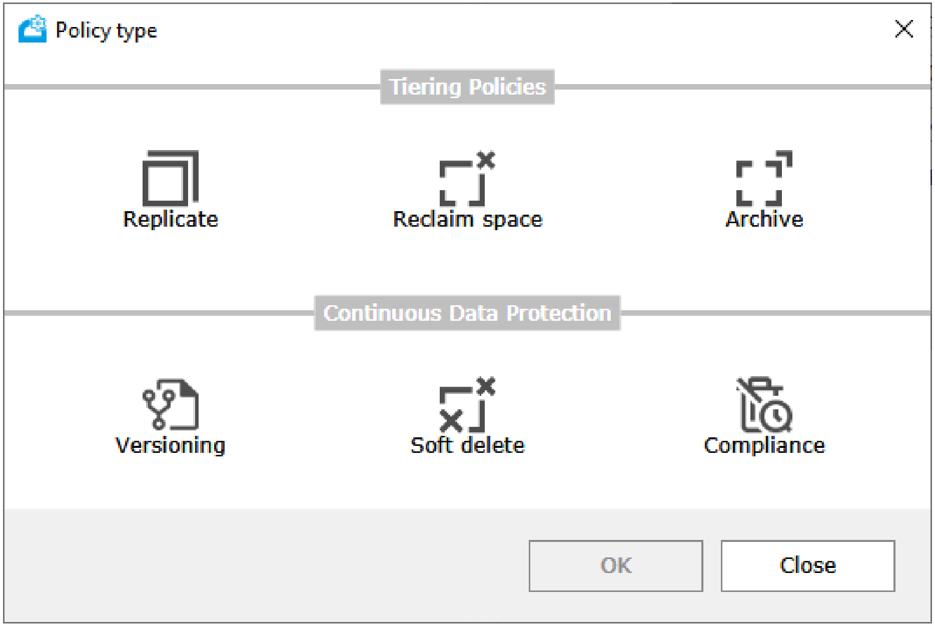
Additionally, on Microsoft Azure, Amazon S3, and Huawei targets you can select the exact archival tier/storage class to which a file is moved by the archiving policy and specify the method for retrieving data from the archive. On all other targets, you need to select the archival storage class that is supported by your provider. Should you select an unsupported storage class while configuring the Archive policy, no data will be archived and Tiger Bridge will report an error, but only after the first attempt to move a file to the selected storage class.

Note: Before configuring these options, make sure that you are acquainted with your target provider's pricing model, to avoid incurred costs.

As automatic archiving differs from target to target, 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.

To configure Tiger Bridge archiving policy:

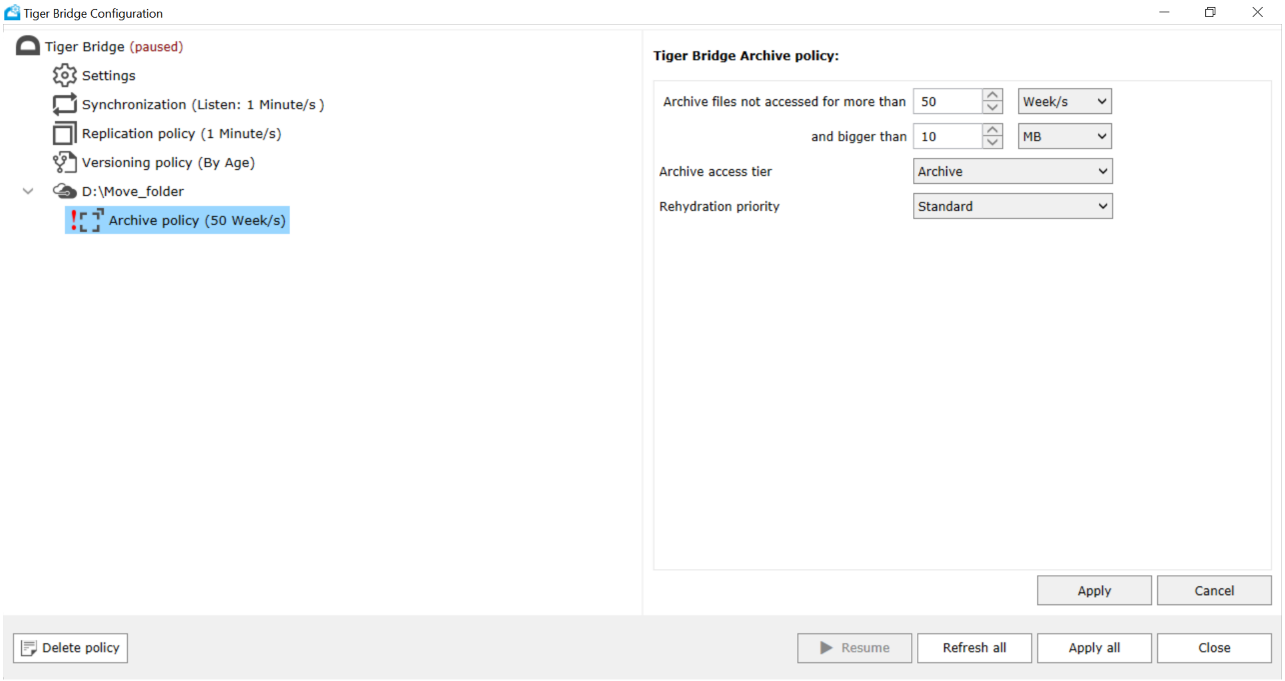
1. In the Tiger Bridge Configuration, select the source in the left pane and click Add policy.



2. In the Policy Type dialog, select Archive and click OK.

Note: If the Archive policy is greyed out, your target does not provide an archive.

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 archive.



Tiger Bridge Configuration
Tiger Bridge (paused)
Settings
Synchronization (Listen: 1 Minute/s)
Replication policy (1 Minute/s)
Versioning policy (By Age)
D:\Move_folder
Archive policy (50 Week/s)
Apply
Cancel
Delete policy
Resume
Refresh all
Apply all
Close

Tiger Bridge Archive policy:

Archive files not accessed for more than 50 Week/s

and bigger than 10 MB

Archive access tier: Archive

Rehydration priority: Standard

4. Select the target tier/storage class, to which files should be archived.

Note: You cannot use the same tier/storage class for both direct data replication and data archiving. You can check the tier/storage class designated for direct replication by clicking the source in the left pane and then checking the target details in the right pane.

5. Select the rehydration priority/archive retrieval option.

Note: You cannot select a rehydration priority/archive retrieval option, which is not supported on the selected archival tier/storage class. On Amazon S3 target, if at the time of data retrieval there is insufficient capacity to process the selected rehydration method, Tiger Bridge automatically switches to Standard.

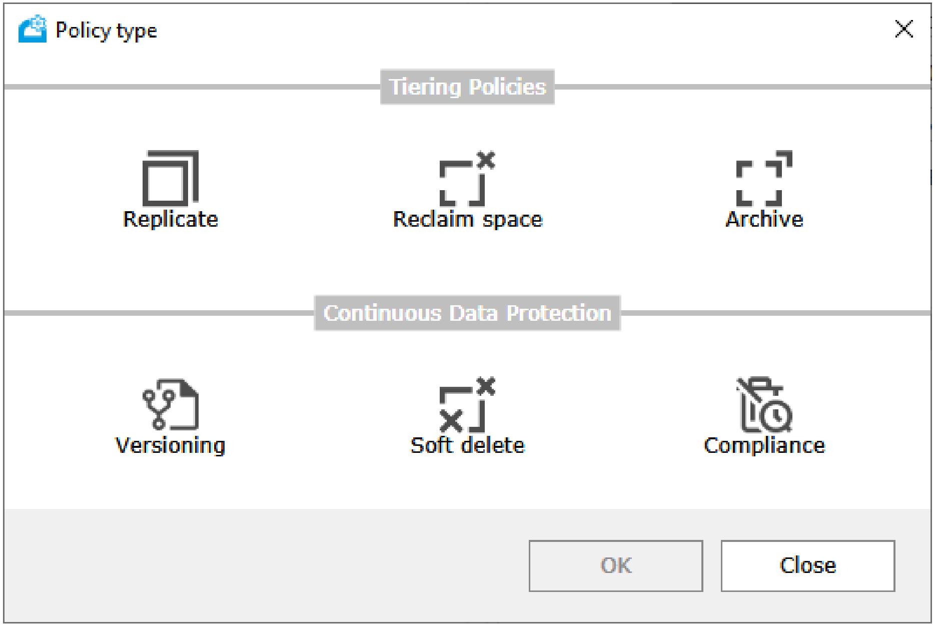
6. Click Apply and optionally resume automatic Tiger Bridge operations.

Manage IBM Cloud Object Storage Archive Policy Through Tiger Bridge

If you use IBM cloud object storage as a target, you can add, modify, or delete the archive policy of the target provider for the bucket used with a Tiger Bridge source using the Configuration. Thus, if no archive policy is specified in the cloud, you can configure it through Tiger Bridge. If an archive policy is already specified for the bucket paired with a source, you can synchronize it locally and let Tiger Bridge use the same parameters to verify the archive status of files or you can modify it in the Configuration and update the rule in the cloud. You can also delete the existing archive policy in the cloud by deleting the source's archive policy in the Configuration.

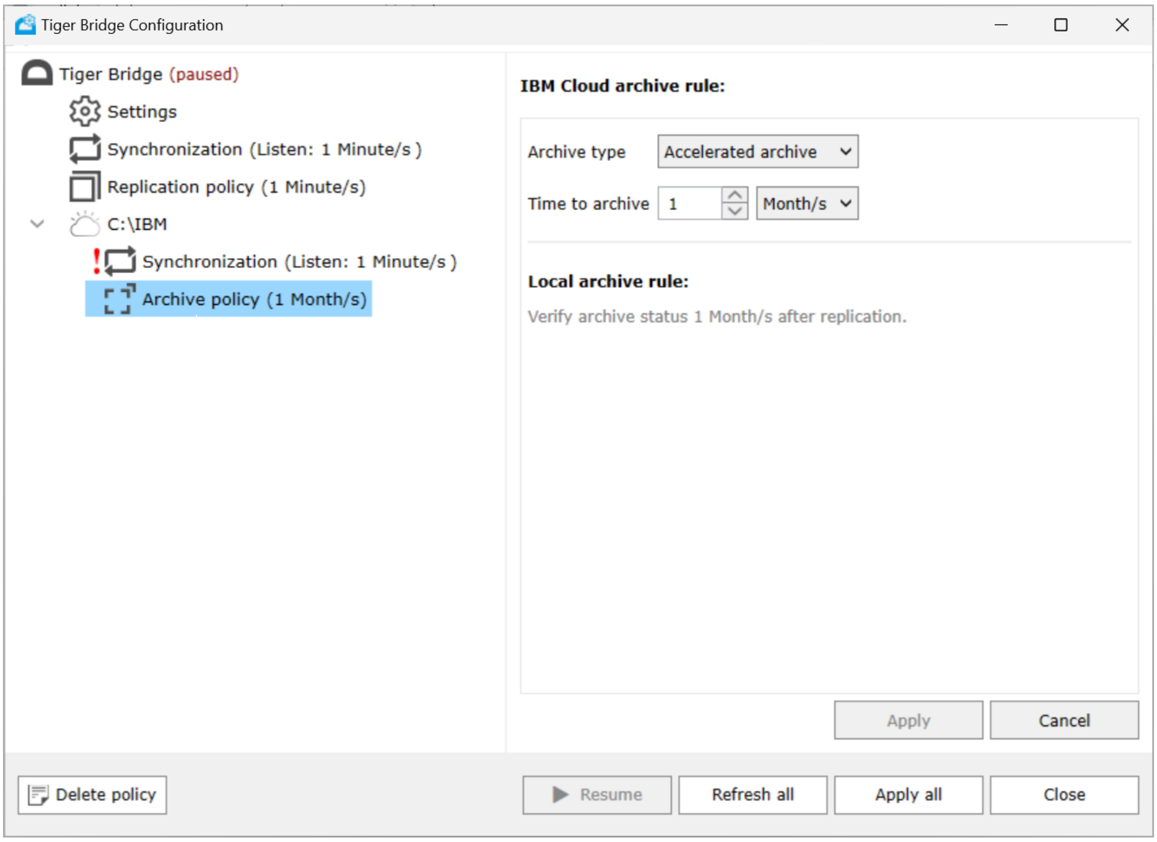
To manage IBM cloud object storage Archive policy through Tiger Bridge:

1. In the Tiger Bridge Configuration, select the source in the left pane and click Add policy.



2. In the Policy Type dialog, select Archive and click OK.

The right pane of the Configuration displays the current Archive policy as applied both in the cloud and locally. If no policy is configured in the cloud, the Configuration displays the default Archive policy settings and the Local archive rule is empty. If changes to the Archive policy have been introduced in the cloud after the last time you synchronized it locally, the Local archive rule is displayed in red. If Tiger Bridge cannot receive the Archive policy configuration from the target provider, the pane displays an error.


Tiger Bridge Configuration
Tiger Bridge (paused)
Settings
Synchronization (Listen: 1 Minute/s)
Replication policy (1 Minute/s)
C:\IBM
Synchronization (Listen: 1 Minute/s)
Archive policy (1 Month/s)
Delete policy
Resume
Refresh all
Apply all
Close
Apply
Cancel

IBM Cloud archive rule:

Archive type: Accelerated archive

Time to archive: 1 Month/s

Local archive rule:

Verify archive status 1 Month/s after replication.

3. Do one of the following:

- (if "Local archive rule" is empty) Click Apply, to add an archive policy with its default settings both in the cloud and locally.

Note: You can also modify the default parameters and then click Apply to add an Archive policy in the cloud.

- (if "Local archive rule" displays the same parameters as the policy) Modify the parameters of the Archive policy and click Apply to change them both locally and in the cloud.
- (If "Local archive rule" parameters are in red) Either accept locally the changes introduced in the cloud (the ones displayed above) or modify them above to overwrite them in the cloud, then click Apply.
- To delete the Archive policy both locally and in the cloud, select it in the left pane and then click Delete policy.

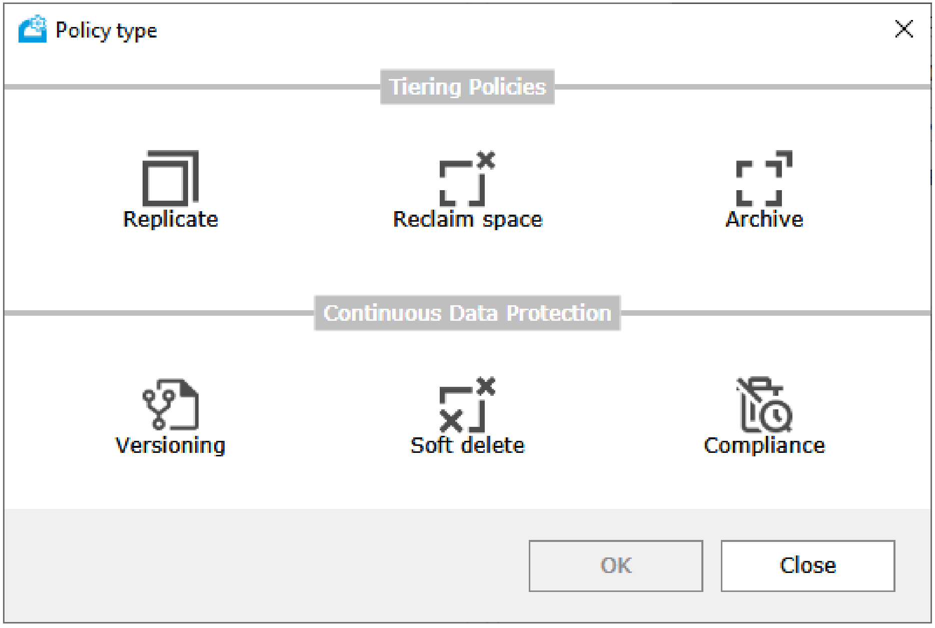
Synchronize Tiger Bridge with the Target's Own Archiving Policy

On targets that provide an archive, but do not allow third-party policies to move files to it, you can synchronize Tiger Bridge with the target's own archiving policy. This way Tiger Bridge can check the status of reclaimed stub files and update it to offline for files moved to the archive. For instant synchronization, it is advisable to set the time interval at which Tiger Bridge checks for files moved to the archive to the same value as the target's archiving policy.

Currently, you can synchronize Tiger Bridge with the target's own archiving policy only on Spectra BlackPearl and FujiFilm targets.

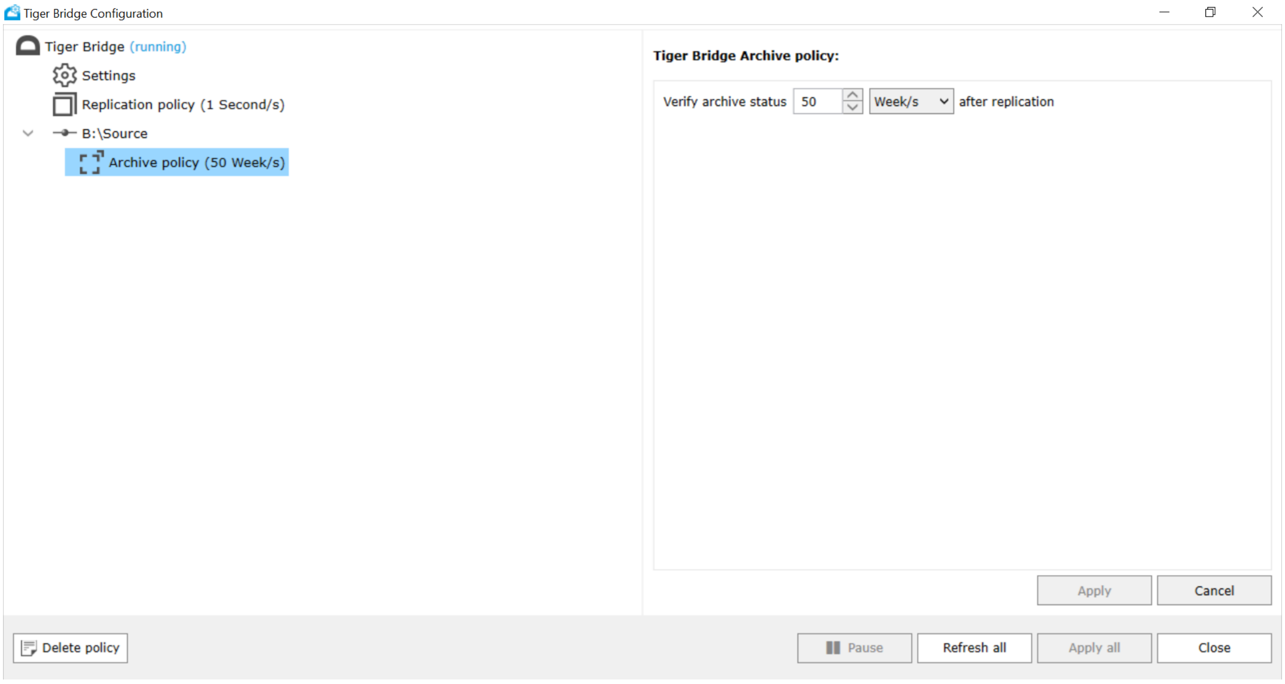
To synchronize Tiger Bridge with the target's own archiving policy:

1. In the Tiger Bridge Configuration, select the source in the left pane and click Add policy.



2. In the Policy Type dialog, select Archive and click OK.

3. In the right pane, specify the time interval at which Tiger Bridge should check for files moved to the archive.



Tiger Bridge Archive policy:

Verify archive status 50 Week/s after replication

4. Click Apply and optionally resume automatic Tiger Bridge operations.

Configure Multi-Site Sync

Tiger Bridge’s multi-site sync allows you to synchronize the contents of two or more sources, each on a separate computer, through a common target. When enabled, each synchronized computer receives a notification about newly replicated or modified data from sources on other synchronized computers and updates its own source(s) accordingly. The synchronization concerns not only newly created data but also modifications (modified content or file/folder renaming) to already synchronized data.

With multi-site sync, a synchronized file can be opened for editing on two or more computers at the same time. In this case, the changes that are kept are the ones bearing the latest modification timestamp. Changes introduced on other computers are overwritten once the file is synchronized again.

Important: For proper content synchronization, it is advisable to configure Tiger Bridge operation mode parameters on all sources, ensuring that files are not deleted from the target when retrieved to any source, and likewise, that files are not deleted from the target if they are deleted on any source. 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 File Operation Mode on page 91.

To benefit from the feature each computer must run Tiger Bridge activated for multi-site sync. Additionally, you must pair the source on each computer with the same target, then add and configure the Sync policy.

The Sync policy uses two parameters:

- 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. The smallest the interval, the faster changes on different sources are synchronized.

- Enable or disable the automatic retrieval to the source of newly replicated data from other sources. In case you do not configure the policy to automatically retrieve files, newly created files from other sources appear as nearline stub files that you can retrieve on demand or manually.

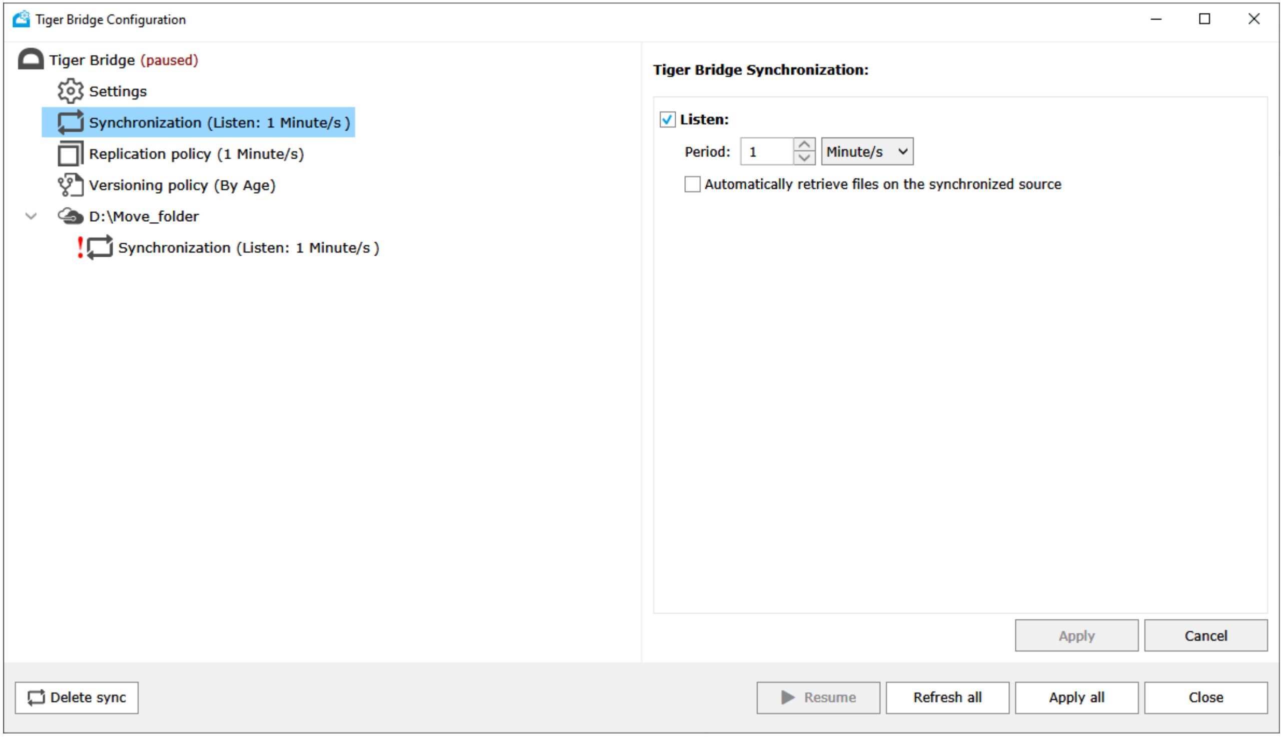
Note: If you have configured Tiger Bridge to use as a target an archival tier (Amazon S3 Glacier/S3 Glacier Deep Archive or Azure Archive), the content of the synchronized sources is updated with offline files instead of nearline files.

You can add a global Sync policy, valid for all sources. You can also add and enable a Sync policy valid for just a specific pair of a source and a target, and thus use different parameters.

To configure the global 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:


Tiger Bridge Configuration
Tiger Bridge (paused)
Settings
Synchronization (Listen: 1 Minute/s)
Replication policy (1 Minute/s)
Versioning policy (By Age)
D:\Move_folder
Synchronization (Listen: 1 Minute/s)
Apply
Cancel
Delete sync
Resume
Refresh all
Apply all
Close

Tiger Bridge Synchronization:

☑ Listen:

Period: 1 Minute/s

□ Automatically retrieve files on the synchronized source

- Enable the “Listen” check box and below it, specify the time interval at which the computer should check for notifications from other computers about changes in the contents of their sources.

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

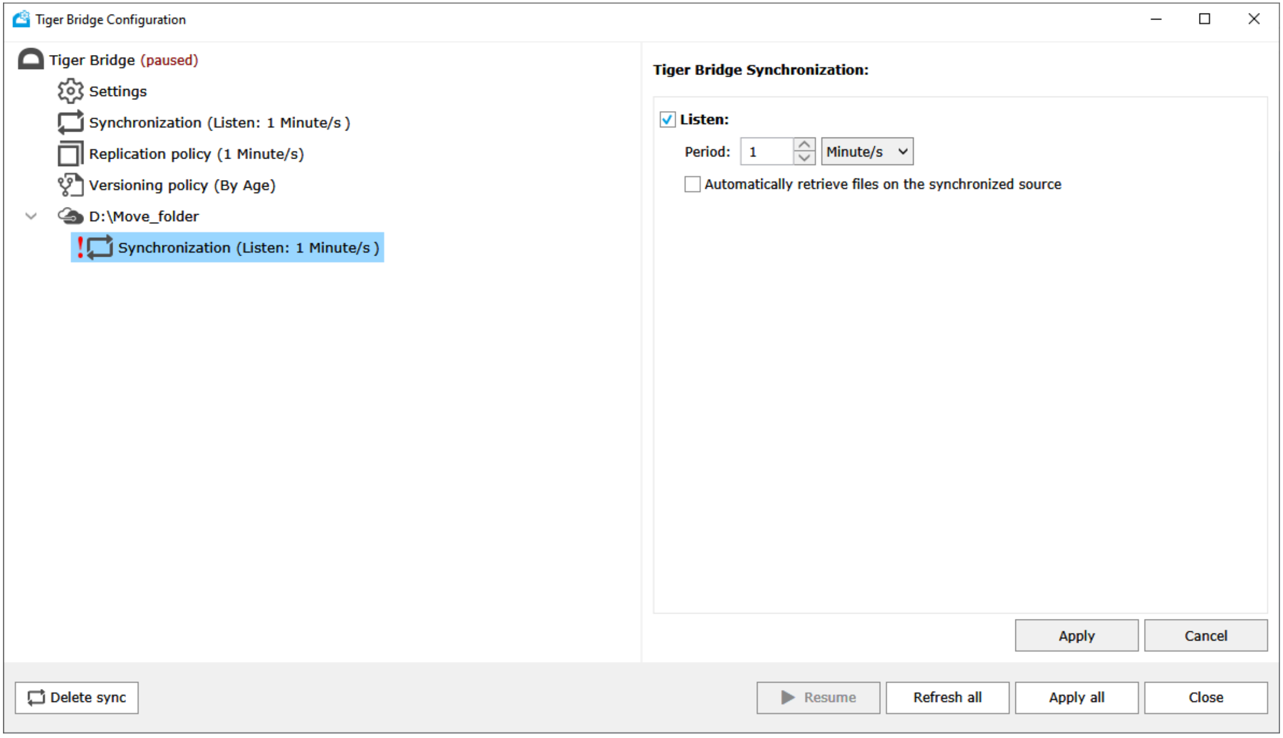
- Clear the “Automatically retrieve files on the synchronized source” check box, to update your source with newly replicated files from other sources in the form of nearline files that can be retrieved manually or on demand.

3. Click Apply and optionally resume automatic Tiger Bridge operations.

Note: 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. To disable it without deleting it, clear the “Listen” check box.

To overwrite the global 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:



Tiger Bridge Configuration

Tiger Bridge (paused)
- Settings
- Synchronization (Listen: 1 Minute/s)
- Replication policy (1 Minute/s)
- Versioning policy (By Age)
- D:\Move_folder
  - Synchronization (Listen: 1 Minute/s)

Tiger Bridge Synchronization:

☑ Listen:

Period: 1 Minute/s

□ Automatically retrieve files on the synchronized source

- Enable the “Listen” check box and below it, specify the time interval at which the computer should check for notifications from other computers about changes in the contents of their sources.
- Select the “Automatically retrieve files on the synchronized source” check box, to let Tiger Bridge begin retrieving the files immediately after the content is synchronized.
- Clear the “Automatically retrieve files on the synchronized source” check box, to update your source with newly replicated files from other sources in the form of nearline files that can be retrieved manually or on demand.

3. Click Apply and optionally resume automatic Tiger Bridge operations.

Note: To edit the 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 Sync policy, select it in the left pane and then click "Delete sync".

Configure Versioning

Important: To allow keeping versions of replicated files, versioning must be enabled both on the target and in Tiger Bridge. If either one is disabled each new copy of a replicated file overwrites the previous one.

By default, until you enable versioning on the target and in Tiger Bridge, each new replica of the same file overwrites the previous one. Once you enable versioning in Tiger Bridge, each new replica of the same file is kept as a separate version on the target. Tiger Bridge provides you with the interface to manage versions, by selecting which one to be synchronized with the file on the source, deleting obsolete versions, etc. For more information refer to Manage Files and Folders Versions on page 134.

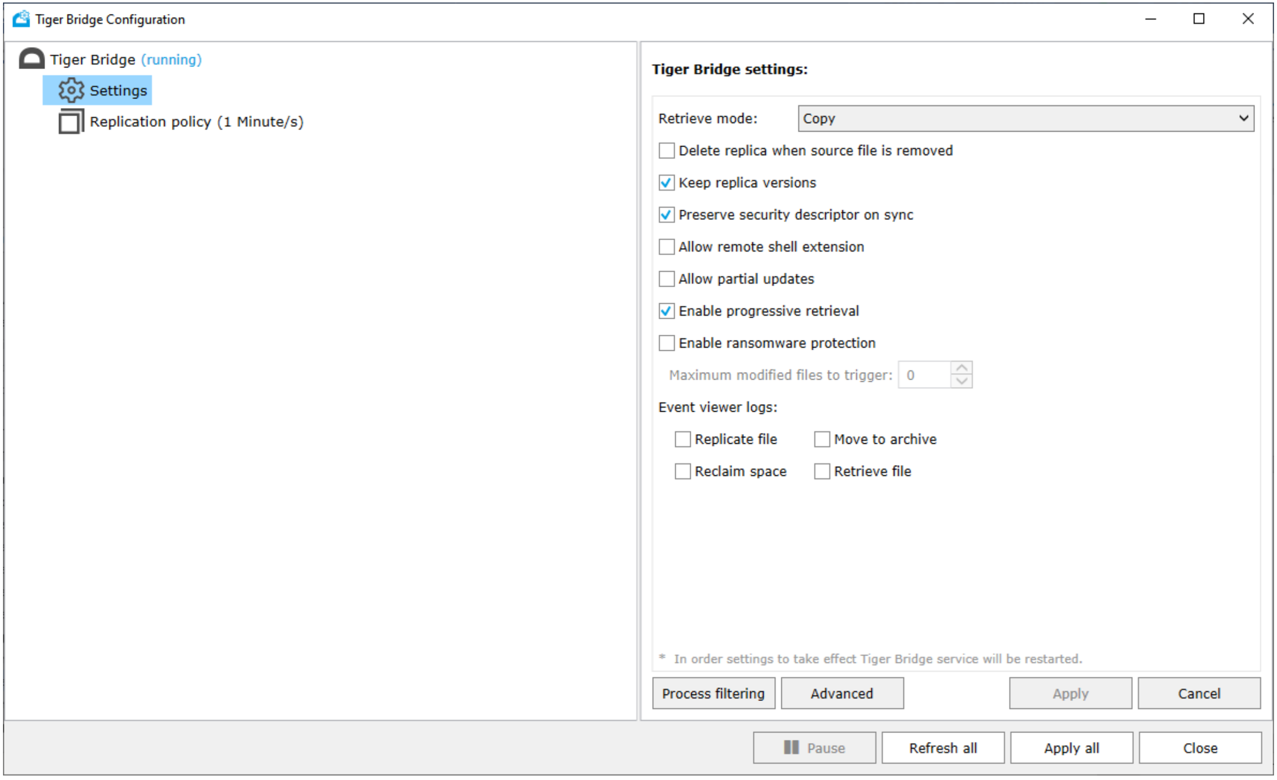
You can disable versioning in Tiger Bridge at any time, keeping in mind that:

- all already saved versions of a file are kept on the target, but you can retrieve a specific version only by using the target provider's own method.
- using Tiger Bridge you can retrieve only the latest version of a replicated file.
- any modifications of a file on the source overwrites only the latest version of the file on the target.

You can also limit the number of versions kept on the target, by adding a versioning policy. For more information, see Versioning Policy below

To enable/disable versioning during replication:

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



Tiger Bridge settings:

Retrieve mode: Copy

☐ Delete replica when source file is removed

☑ Keep replica versions

☑ Preserve security descriptor on sync

☐ Allow remote shell extension

☐ Allow partial updates

☑ Enable progressive retrieval

☐ Enable ransomware protection

Maximum modified files to trigger: 0

Event viewer logs:

☐ Replicate file ☐ Move to archive

☐ Reclaim space ☐ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

2. Do one of the following:

- Select the "Keep replica versions" check box, to enable versioning in Tiger Bridge.
- Clear the "Keep replica versions" check box, to disable versioning in Tiger Bridge.

3. When prompted, verify that versioning is enabled on the buckets/containers of the target(s), and click Confirm.

4. Click Apply and optionally resume automatic Tiger Bridge operations.

Versioning Policy

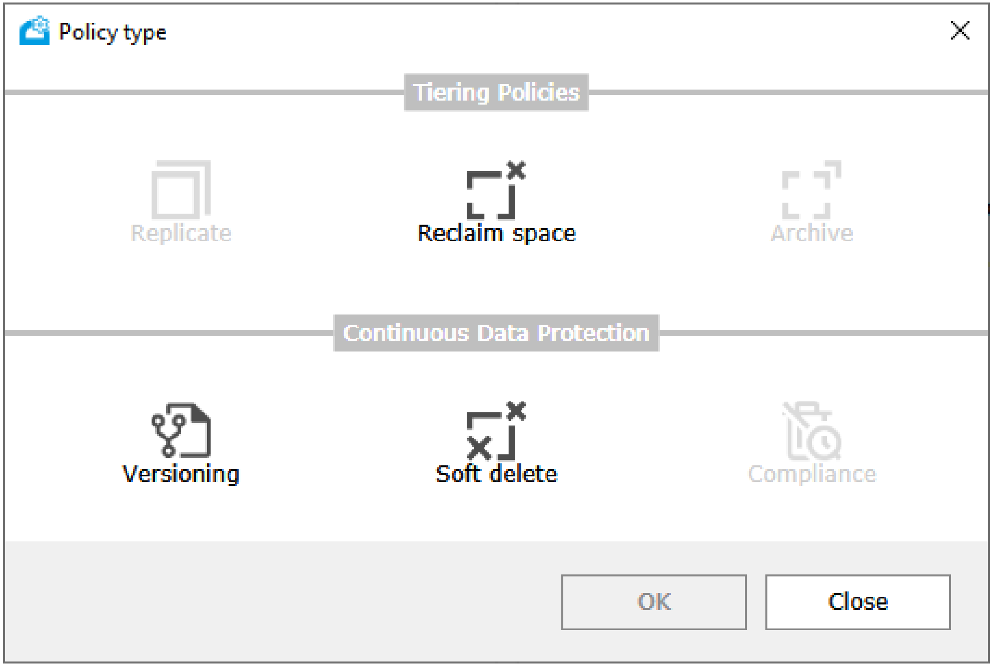
As long as versioning is enabled in Tiger Bridge, each new replica of a file is kept as a separate version on the target. To help you limit the number of replicas of the same file, Tiger Bridge allows you to add a versioning policy. When you add a versioning policy without modifying its parameters, it uses the default ones – all versions of the same file that are older than one week are automatically deleted from the target, regardless of their number. You can modify the policy in the following ways:

- Specify a different time interval after which a version must be deleted from the target.
- Specify that the above rule must be applied only if the number of versions exceeds a specified number. For example, if you have configured the versioning policy to delete replicas older than 1 month, but only if the overall number of replicas of the same file is 5, Tiger Bridge deletes the version of the file that has been replicated 2 months ago, only when a sixth version is replicated on the target.
- Specify the maximum number of versions, which should be kept on the target. When this number is exceeded, Tiger Bridge automatically deletes the oldest version.

You can add a global policy, valid for all sources. You can also add and enable a versioning policy valid for just a specific pair of a source and a target, and thus use different parameters. Keep in mind that the global versioning policy is valid only for sources that do not have a versioning policy of their own. Thus, even if you have configured a versioning policy for a pair of source and target, but it is disabled, Tiger Bridge assumes that the pair has a policy of its own and does not apply the global versioning policy.

To add and configure global versioning policy:

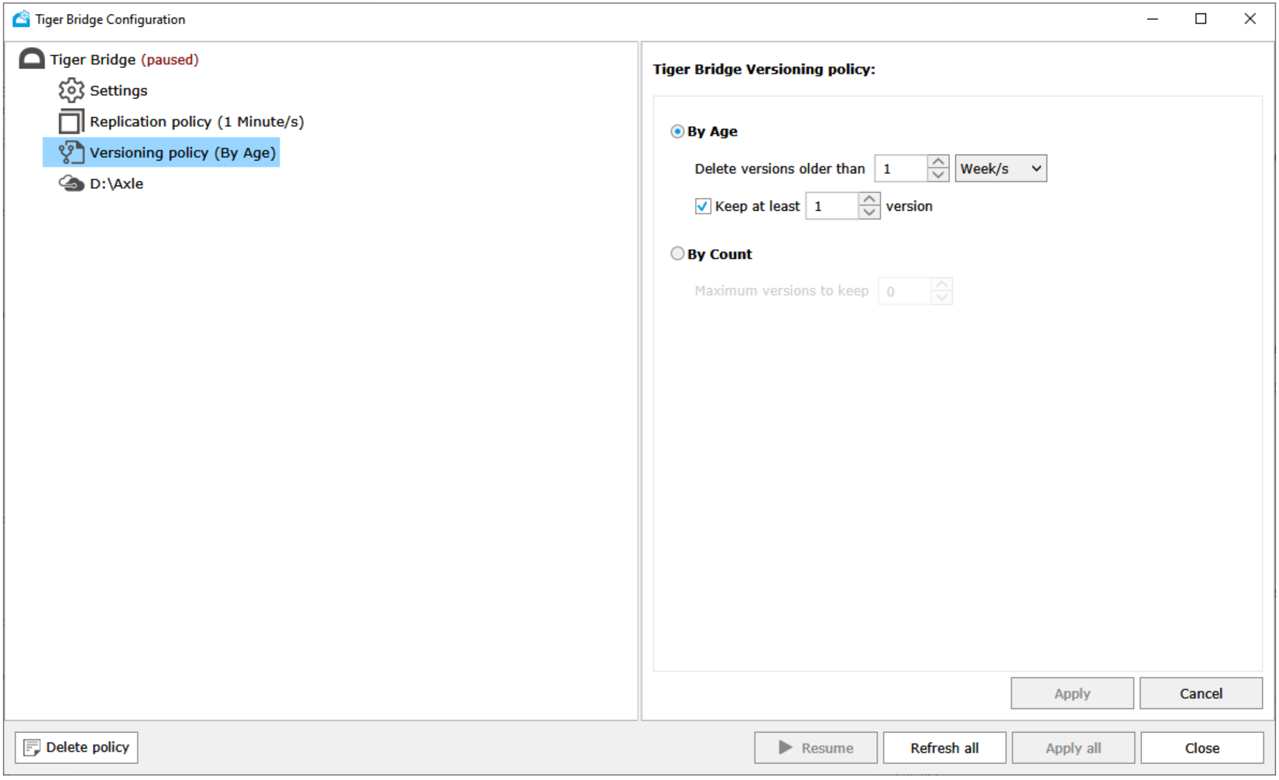
1. In the Tiger Bridge Configuration, select Tiger Bridge in the left pane and click Add policy.



2. In the Policy Type dialog, click Versioning and click OK.

Note: Versioning policy is greyed if you have not enabled the “Keep replica versions” check box in the Tiger Bridge settings.

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



Tiger Bridge Configuration

Tiger Bridge (paused)

Settings

Replication policy (1 Minute/s)

Versioning policy (By Age)

D:\Axle

Tiger Bridge Versioning policy:

● By Age

Delete versions older than 1 Week/s

☑ Keep at least 1 version

○ By Count

Maximum versions to keep 0

- Select “By Age” and in “Delete versions older than” specify how old a version should be for Tiger Bridge to delete it from the target.
- Select the “Keep at least” check box and specify the maximum number of versions of the same file, which when exceeded triggers the “By Age” rule.
- Clear the “Keep at least” check box, to apply the “By Age” rule regardless of the number of versions on the target.
- Select “By Count” and in “Maximum versions to keep” specify the maximum number of versions kept on the target. When this number is exceeded, Tiger Bridge deletes any version of the same file above the limit, starting with the oldest ones.

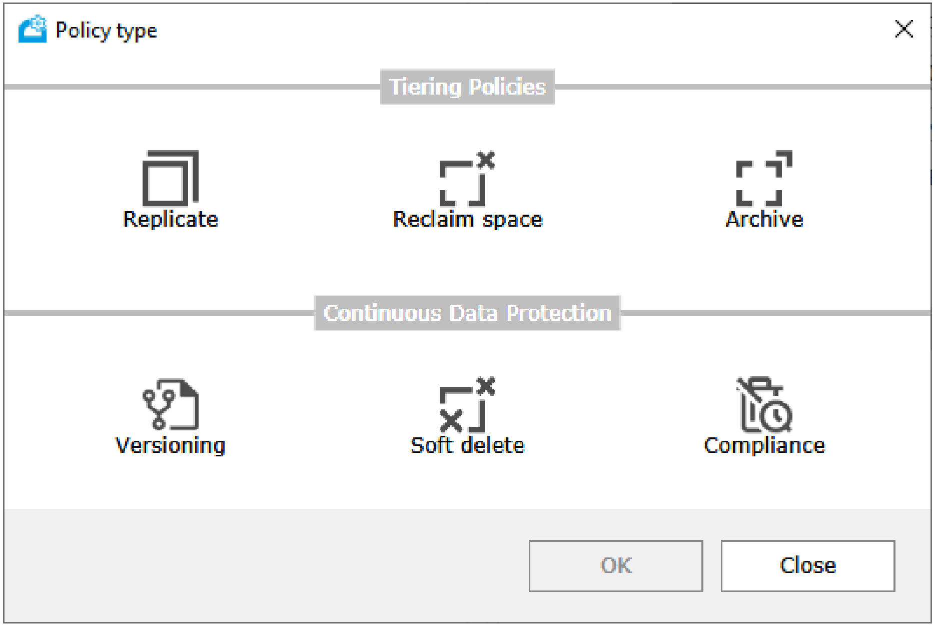
4. When prompted, verify that versioning is enabled on the buckets/containers of the target(s), and click Confirm.

5. Click Apply and optionally resume automatic Tiger Bridge operations.

Note: 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.

To overwrite the global versioning policy for a specific source:

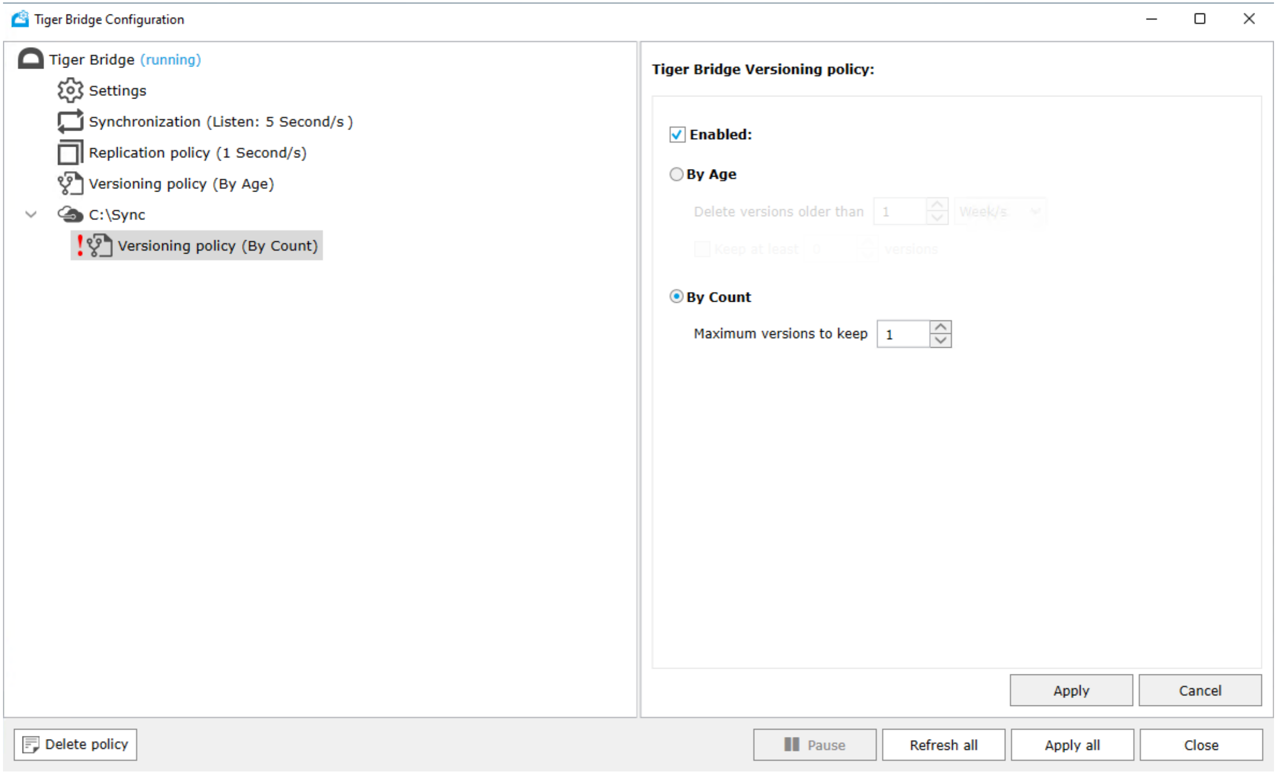
1. In the Tiger Bridge Configuration, select the source in the left pane and click Add policy.



2. In the Policy Type dialog, click Versioning and then click OK.

Note: Versioning policy is greyed if you have not enabled the “Keep replica versions” check box in the Tiger Bridge settings.

3. In the right pane, select the Enabled check box, to enable the policy.



Tiger Bridge Configuration

Tiger Bridge (running)
Settings
Synchronization (Listen: 5 Second/s)
Replication policy (1 Second/s)
Versioning policy (By Age)
C:\Sync
! Versioning policy (By Count)

Tiger Bridge Versioning policy:

☑ Enabled:

○ By Age

Delete versions older than 1 Week/s

□ Keep at least 0 versions

● By Count

Maximum versions to keep 1

4. To change the default parameters of the versioning policy, do one of the following:

- Select “By Age” and in “Delete versions older than” specify how old a version should be for Tiger Bridge to delete it from the target.

- Select the “Keep at least” check box and specify the maximum number of versions of the same file, which only when exceeded triggers the “By Age” rule.
- Clear the “Keep at least” check box, to apply the “By Age” rule regardless of the number of versions on the target.
- Select “By Count” and in “Maximum versions to keep” specify the maximum number of versions kept on the target. When this number is exceeded, Tiger Bridge deletes any version of the same file above the limit, starting with the oldest ones.

5. When prompted, verify that versioning is enabled on the bucket/container of the target, and click Confirm.
6. Click Apply and optionally resume automatic Tiger Bridge operations.

Note: To edit the policy, simply select it in the left pane, edit the desired parameter, and click Apply. To delete the policy, select it in the left pane and click Delete policy. To disable the policy without deleting it, select it in the left pane and clear the “Enable” check box, then click Apply.

Configure File Operation Mode

Depending on the purpose you deploy Tiger Bridge for, configuring the behavior of the following two file operations is vital for achieving the desired result:

Retrieve file – specify whether retrieving a stub file back on the source deletes the replica from the target.

Delete file – specify whether deleting a file from the source also deletes the replica from the target.

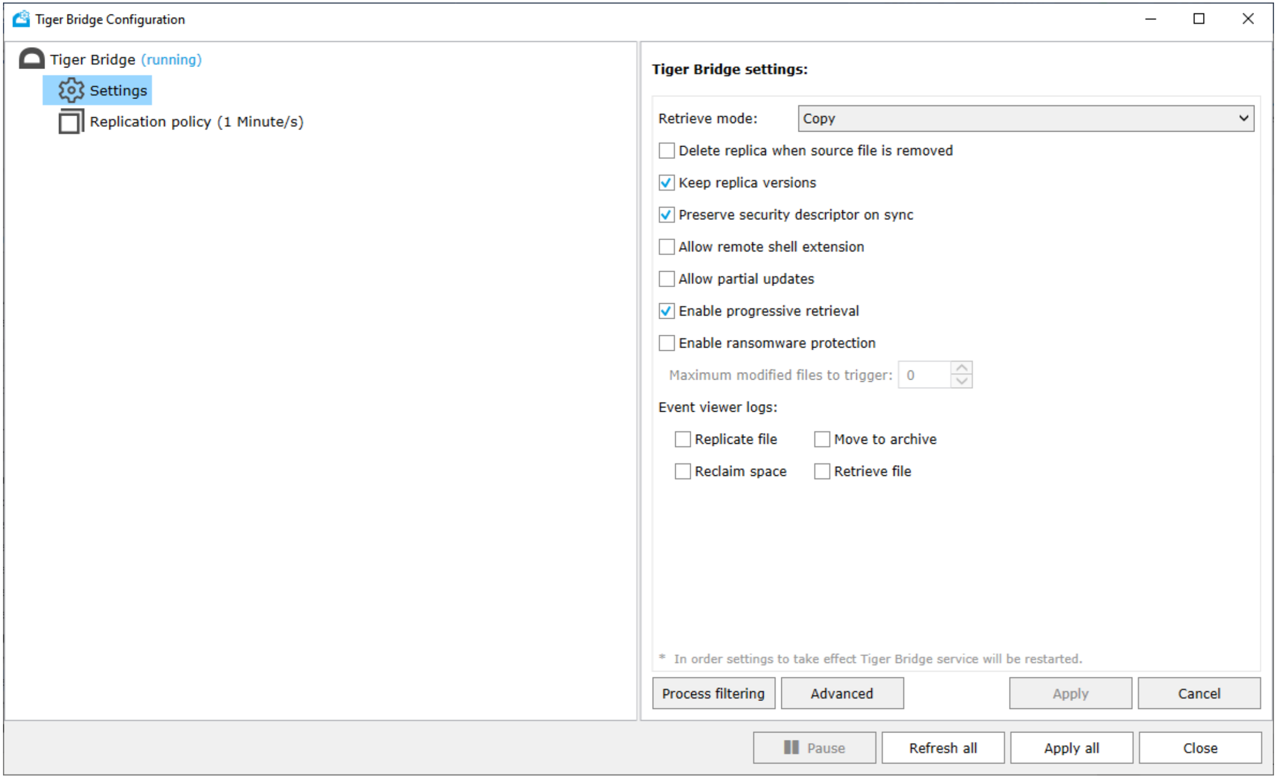
Configure File Retrieve Mode

By default, Tiger Bridge is set up to keep the replica on the target when you retrieve a stub file on the source. This setting is useful when you deploy Tiger Bridge for data backup and disaster recovery as it keeps your backup intact. It is also advisable to keep the default setting when deploying Tiger Bridge for geo-replication. Otherwise, if data is being synchronized between three or more machines, synchronized sources may fail to update their contents with newly replicated files once they are retrieved to the first source as the files are no longer available on the target.

You can set Tiger Bridge to remove the file replica from the target when it is successfully retrieved to the source. This behavior is useful when you want to configure the target as an extension to your source as it reduces file duplication.

To configure file retrieve mode:

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



Tiger Bridge Configuration

Tiger Bridge (running)

Settings

Replication policy (1 Minute/s)

Tiger Bridge settings:

Retrieve mode: Copy

☐ Delete replica when source file is removed

☑ Keep replica versions

☑ Preserve security descriptor on sync

☐ Allow remote shell extension

☐ Allow partial updates

☑ Enable progressive retrieval

☐ Enable ransomware protection

Maximum modified files to trigger: 0

Event viewer logs:

☐ Replicate file ☐ Move to archive

☐ Reclaim space ☐ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

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 to the source volume, select Copy.
- To let Tiger Bridge remove the replica from the target when the file is successfully retrieved to the source volume, select Move.

3. Click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

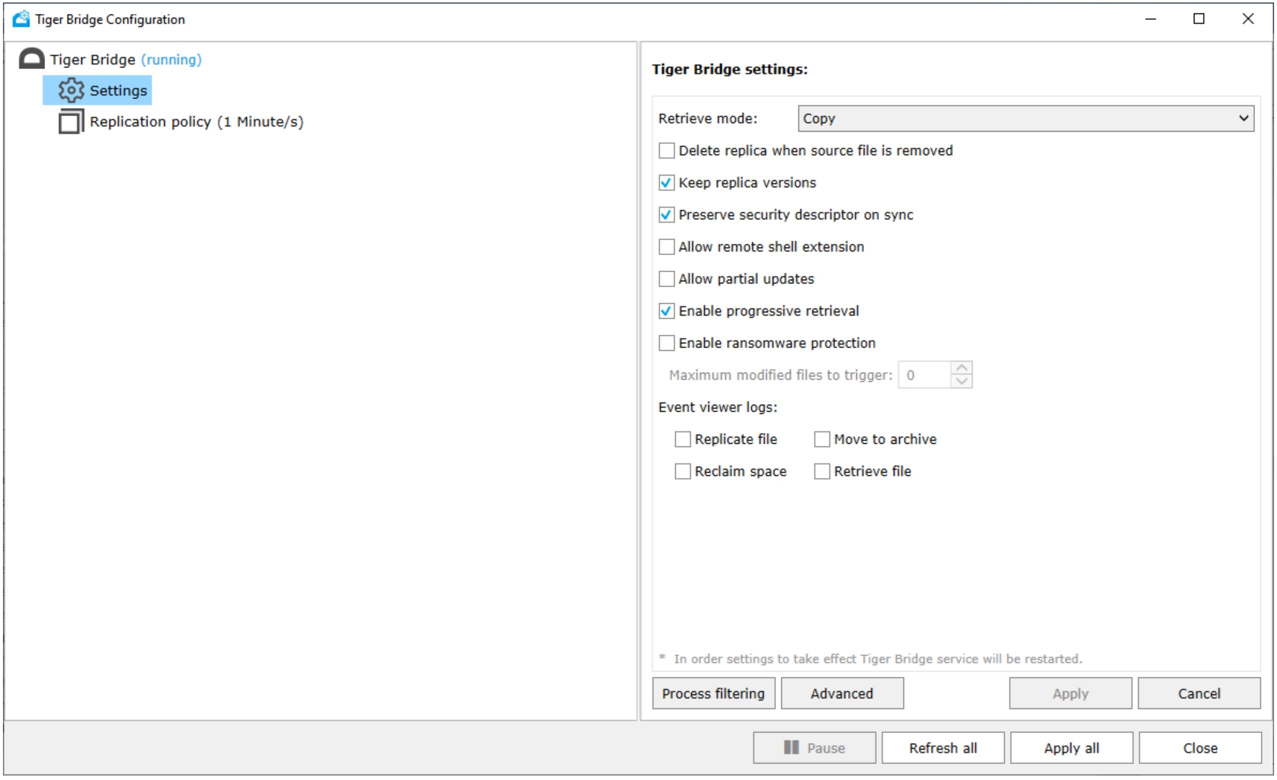
Configure File Delete Mode

By default, Tiger Bridge is configured to delete the replica of a file from the target as soon as it is deleted from the source. This behavior is designed to enhance scenarios in which the target is meant to act as an extension of your source i.e., both tiers of the unity are treated as a whole and a file operation on the source is valid for the same file on the target. As long as soft delete is supported and enabled on your target, you can restore a deleted file, by following the steps in Undelete Data from the Source on page 133. On targets that do not support soft delete, you can ensure against accidental deletion of data by configuring a Soft Delete policy, which offsets the synchronization of the file deletion on the target by a time interval you specify. Until the soft delete policy interval elapses you can undelete the file on your source by retrieving the replica from the target. You can find more information about configuring and using the Soft Delete policy in Configure Soft Delete Policy on the facing page.

When you deploy Tiger Bridge for disaster recovery or geo synchronization, it is advisable to change this default behavior and configure Tiger Bridge to keep the replica on the target even if the file is deleted from the source. In this case, to delete it from the target as well you should access the target and manually delete the file.

To configure file delete mode:

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



Tiger Bridge settings:

Retrieve mode: Copy

☐ Delete replica when source file is removed

☑ Keep replica versions

☑ Preserve security descriptor on sync

☐ Allow remote shell extension

☐ Allow partial updates

☑ Enable progressive retrieval

☐ Enable ransomware protection

Maximum modified files to trigger: 0

Event viewer logs:

☐ Replicate file ☐ Move to archive

☐ Reclaim space ☐ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

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 and when prompted, confirm that you want to restart the Tiger Bridge service.

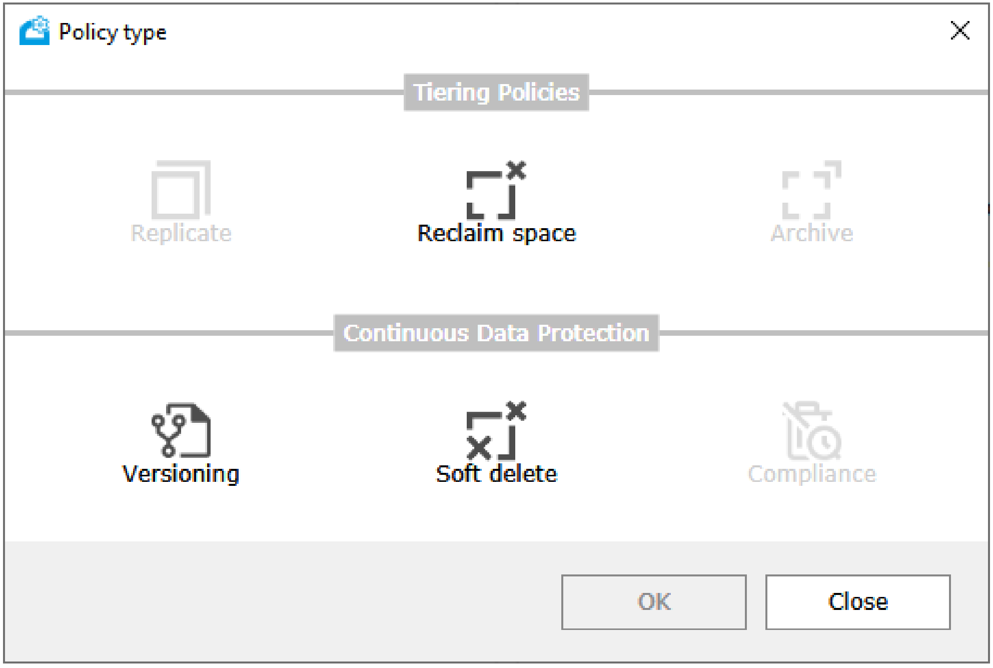
Configure Soft Delete Policy

The Soft Delete policy provides you with a safety net against accidental deletion of files from the source if you have set up Tiger Bridge’s operation mode to delete the replica from the target when a file is deleted file from the source. Configuring the Soft Delete policy means specifying how long to delay the synchronization of the deletion of the file on the target. Thus, if you use the default setting of 1 hour, when you delete a file from your source, its deletion from the target is delayed by 1 hour. During this time, you can manually undelete the file by following the steps outlined in Undelete Data from the Source on page 133.

You can add a global Soft Delete policy, valid for all pairs of source and target that do not have a Soft Delete policy of their own. You can also overwrite the global Soft Delete policy for a pair of source and target, by adding and configuring a Soft Delete policy of its own. In case you have a global policy, but you want to configure a pair of source and target to not delay the deletion of the file from the target, simply add a policy for that pair and configure it to remove files from the target after 1 second.

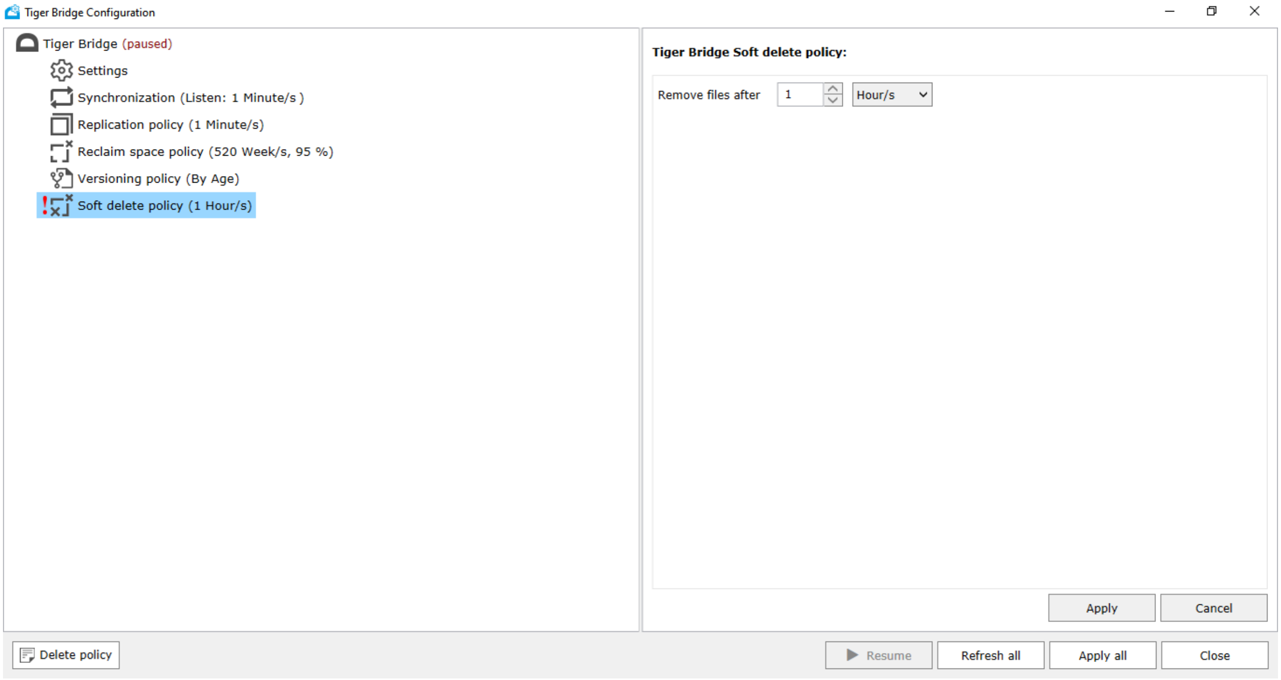
To add and configure the global Soft Delete policy:

1. In the Tiger Bridge Configuration, select Tiger Bridge in the left pane and click Add policy.



2. In the Policy Type dialog, click “Soft delete” and then click OK.

3. In the right pane, specify how long Tiger Bridge should delay the deletion of the file from the target.


Tiger Bridge Configuration
Tiger Bridge (paused)
Settings
Synchronization (Listen: 1 Minute/s)
Replication policy (1 Minute/s)
Reclaim space policy (520 Week/s, 95 %)
Versioning policy (By Age)
Soft delete policy (1 Hour/s)
Apply
Cancel
Delete policy
Resume
Refresh all
Apply all
Close

Tiger Bridge Soft delete policy:

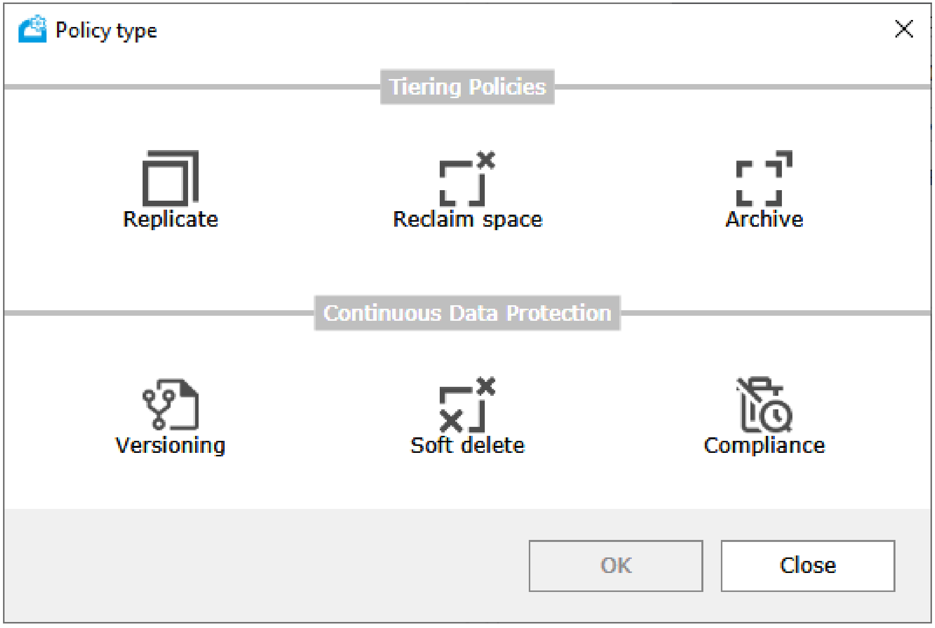
Remove files after 1 Hour/s

4. Click Apply and optionally resume automatic Tiger Bridge operations.

Note: 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.

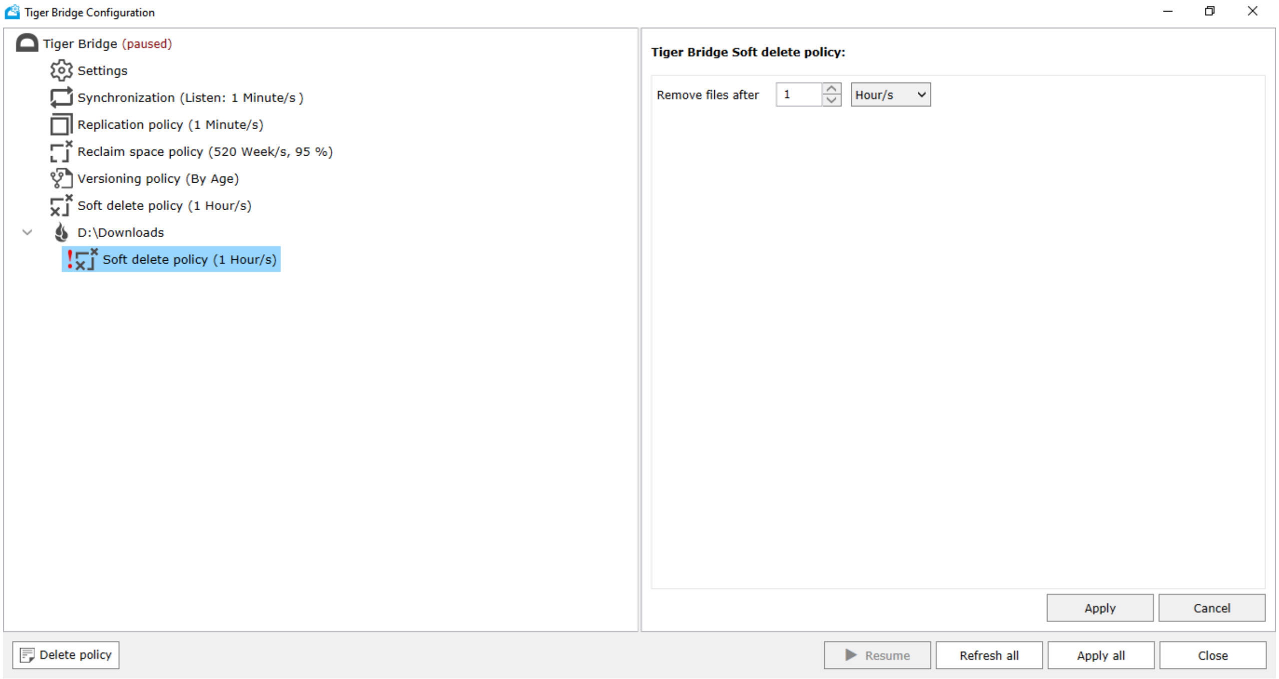
To overwrite the global Soft Delete policy for a specific source:

1. In the Tiger Bridge Configuration, select the source in the left pane and click Add policy.



2. In the Policy Type dialog, click “Soft delete” and then click OK.

3. In the right pane, specify how long Tiger Bridge should delay the deletion of the file from the target.


Tiger Bridge Configuration

- Tiger Bridge (paused)
  - Settings
  - Synchronization (Listen: 1 Minute/s)
  - Replication policy (1 Minute/s)
  - Reclaim space policy (520 Week/s, 95 %)
  - Versioning policy (By Age)
  - Soft delete policy (1 Hour/s)
  - D:\Downloads
    - Soft delete policy (1 Hour/s)

Tiger Bridge Soft delete policy:

Remove files after 1 Hour/s

4. Click Apply and optionally resume automatic Tiger Bridge operations.

Note: To edit the policy, simply select it in the left pane, edit the desired parameter, and click Apply. To delete the policy, select it in the left pane and click Delete policy.

Configure Compliance Mode

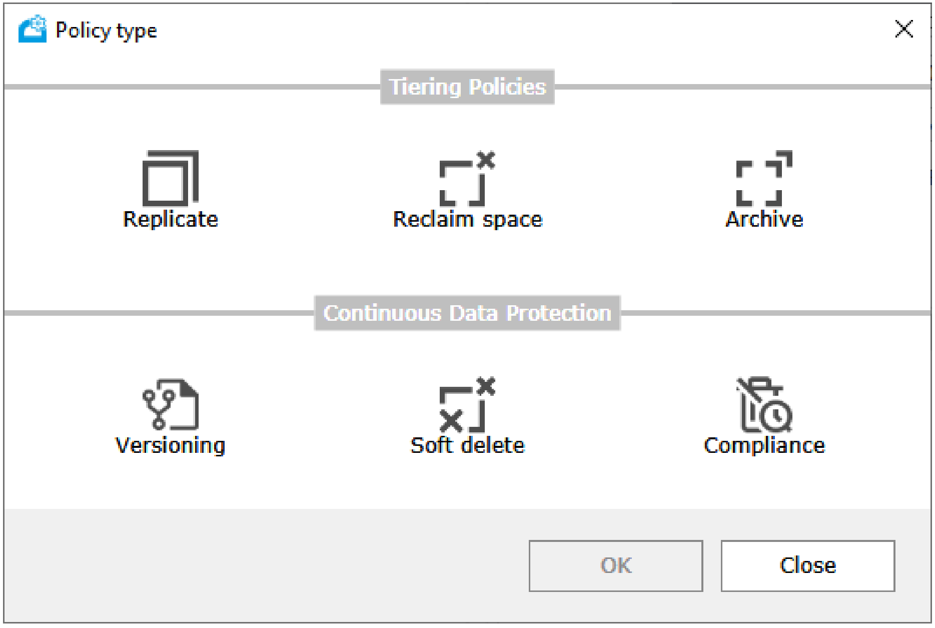
For workflows requiring strict data integrity and retention, you can add and configure a Compliance policy in Tiger Bridge. The policy prevents files from being deleted or renamed on the source after replication for a set retention period. The retention period for each file starts from the time it is replicated. Modifications during this period are allowed only if the "Keep replica versions" setting is enabled (see Configure Versioning on page 86).

Important: "Keep replica versions" is a global setting valid for all pairs of sources and targets. If the setting is enabled but versioning is not enabled or supported on the target of a source with Compliance policy added, each modification of the file will overwrite the previous one.

Compliance mode is configurable per source. To ensure full data immutability, the compliance policy should be used alongside the target’s compliance settings with matching retention periods. Enabling just Tiger Bridge's compliance policy guarantees data immutability only on the source.

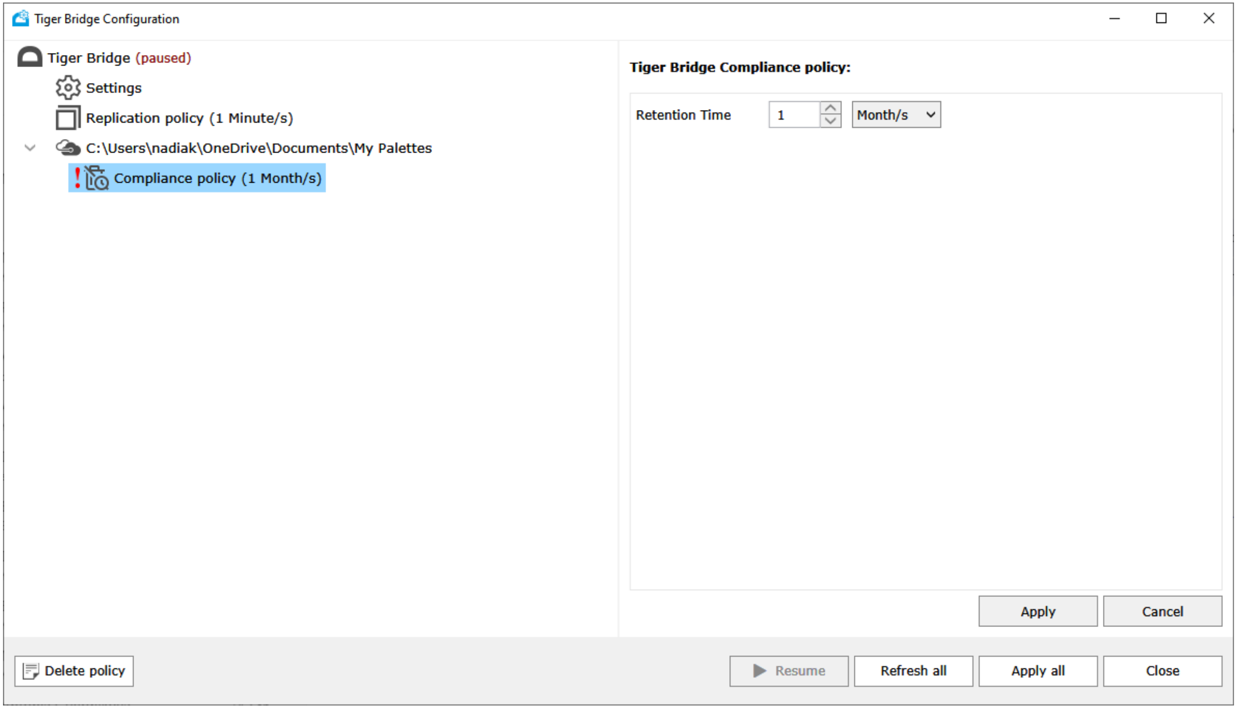
To add and configure a Compliance policy for a specific source:

1. In the Tiger Bridge Configuration, select the source in the left pane and click Add policy.



2. In the Policy Type dialog, click Compliance and then click OK.

3. In the right pane, specify how long Tiger Bridge should prevent the renaming, deletion and optionally modifying a source file after it has been replicated.



Tiger Bridge Configuration
Tiger Bridge (paused)
Settings
Replication policy (1 Minute/s)
C:\Users\nadiak\OneDrive\Documents\My Palettes
Compliance policy (1 Month/s)
Tiger Bridge Compliance policy:
Delete policy
Resume
Refresh all
Apply all
Close
Apply
Cancel

Retention Time 1 Month/s

4. Click Apply and optionally resume automatic Tiger Bridge operations.

Note: To edit the policy, simply select it in the left pane, edit the desired parameter, and click Apply. To delete the policy, select it in the left pane and click Delete policy.

Fine-Tune Tiger Bridge

In this chapter, you will find information about fine-tuning Tiger Bridge to best serve the needs of your workflow.

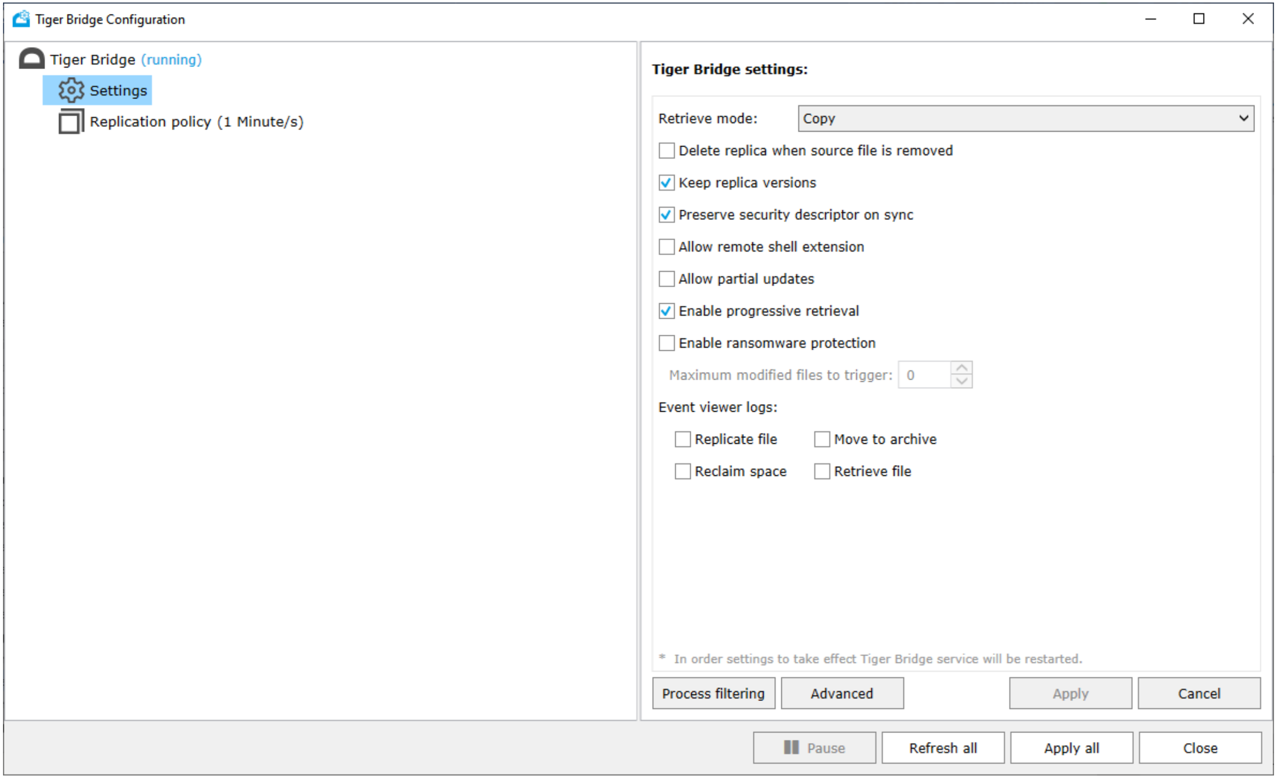
Enable Remote Shell Extension Access

You can install the Tiger Bridge shell extension as a standalone component on a remote computer and thus allow users with administrative privileges to perform manual Tiger Bridge operations on a NAS source or a local storage source exported as an SMB 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: Keep in mind that 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.



Tiger Bridge settings:

Retrieve mode: Copy

☐ Delete replica when source file is removed
☑ Keep replica versions
☑ Preserve security descriptor on sync
☐ Allow remote shell extension
☐ Allow partial updates
☑ Enable progressive retrieval
☐ Enable ransomware protection

Maximum modified files to trigger: 0

Event viewer logs:

☐ Replicate file ☐ Move to archive
☐ Reclaim space ☐ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

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. In the Settings pane, click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

Note: For Remote shell extension to work, TCP port 8536 must not be blocked in the configuration of your firewall.

Define the Tiers of Your Object Storage Target

By default, Tiger Bridge uses the default tiers/storage classes as specified by your object storage provider to replicate, rehydrate, and archive data. You can use the command-line interface of Tiger Bridge to instruct it where you want it to archive and rehydrate data. Note that the command defines the tier/storage classes per pair of a source and a target.

To define where data should be archived:

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <path to source> tiers "" "" <archival storage class name>
```

For example, to configure Tiger Bridge to use the Google Cloud Coldline storage class for archiving, execute the following:

```
tiercli config <path to source> tiers "" "" coldline
```

Note: To let Tiger Bridge use the default tiers/storage classes as defined by the target provider, execute the following:

```
tiercli config <path to source> tiers "" "" ""
```

3. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc
```

```
net start tiersvc
```

To define where data should be rehydrated:

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <path to source> tiers "" <rehydration storage class name> ""
```

For example, to configure Tiger Bridge to use the hot tier of Azure for rehydration of archived files, execute the following:

```
tiercli config <path to source> tiers "" hot ""
```

Note: To let Tiger Bridge use the default tiers/storage classes as defined by the target provider, execute the following:

```
tiercli config <path to source> tiers "" "" ""
```

3. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc

net start tiersvc
```

Fine-Tune Metadata Tracking

To keep track of what data it manages Tiger Bridge scans the file system of each source and stores the collected metadata in a database. The database is stored in the system memory of the Tiger Bridge computer for faster access. The database is regenerated on each restart of the computer or the Tiger Bridge service. If the database size exceeds 200 MB, the database is automatically stored locally in each source and persists across restarts of the computer or the Tiger Bridge service.

Currently, you can fine-tune the source metadata tracking in the following ways:

- Configure where the database is stored - in the system memory, locally, or switch from in-memory to locally stored when a specific database size threshold is reached.
- Configure how many CPU threads are used for the scanning of a NAS source to speed up the scan.
- Configure for how long Tiger Bridge should wait when it scans its sources before it begins processing data on them.

Manage the Tracked Metadata Database

Tiger Bridge scans the file system of the sources it manages to determine what data on them needs to be processed. The collected metadata is stored in a database. Until the database size reaches 200 MB, it is stored in the system memory and regenerated on each restart of the computer or the Tiger Bridge service. To reduce the need for full file system scans , if the database size exceeds the 200 MB threshold, Tiger Bridge stores it locally for each source and it persists across restarts.

You can change where the database is stored (in the system memory only, locally only, or locally if its size exceeds a specified threshold) as well as specify the threshold that triggers the saving of the database locally.

To specify where the tracked metadata database is stored:

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\fstrack_settings

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

4. Rename the new REG_SZ value to **database_mode**.

5. Right-click the **database_mode** value and select Modify.

6. Do one of the following:

- To let Tiger Bridge store the database in the system memory regardless of its size, change the value to memory and click OK.

- To let Tiger Bridge store the database locally regardless of its size, change the value to disk and click OK.

- To let Tiger Bridge store the database locally only if its size exceeds a specified threshold, change the value to memory-with-disk-fallback and click OK.

Note: By default, the threshold is set to 200 MB. You can change this threshold by creating and managing the memory_limit string value in the Tiger Bridge registry.

7. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc

net start tiersvc
```

To change the threshold switching to persistent local database:

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\fstrack_settings

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

4. Rename the new REG_SZ value to **memory_limit**.

5. Right-click the **memory_limit** value and select Modify.

6. Enter the maximum size threshold in bytes and click OK.

7. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc

net start tiersvc
```

Set Source Scan Wait Time

Tiger Bridge scans the file system of the sources it manages to determine what data on them needs to be processed. The collected metadata is stored in a database. The scan is performed in the following cases:

- When you add a source.
- When you restart the computer or the Tiger Bridge service as long as the database is stored in the system memory (by default, until its size reaches 200 MB).
- When the database is stored locally (by default, when its size is 200 MB or more) and it is deleted or gets corrupted.

By default, Tiger Bridge is set to wait until the file system scan finishes, before it begins processing data, thus ensuring maximum precision of the scheduled file operations. On sources 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 source scan wait time:

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 in the right pane and select New | String Value.

4. Rename the new REG_SZ value to:
step_ready_wait_time

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

6. Do one of the following:

- to set Tiger Bridge to wait until the scan finishes, 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.

7. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

8. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc

net start tiersvc
```

Manage The Number of Threads Scanning a NAS Source

By default, when scanning a source's file system Tiger Bridge uses just two threads. For NAS sources containing a lot of data, the initial scan may take quite long. To increase the speed of the source scan, you can increase the number of threads used in the process, by modifying a string value in the Tiger Bridge registry.

To specify the number of threads used for scanning NAS sources:

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. In the right pane, right-click the “nas_scan_thread_count” REG_SZ and click Modify.

4. In Value data, enter the desired number of threads to be used and then click OK.

5. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

6. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc

net start tiersvc
```

Configure Interaction with Windows Explorer

Manage Shell Extension Icon Overlays

By default, as long as the Tiger Bridge shell extension is installed when browsing a source in Windows Explorer, Tiger Bridge displays the icons of files and folders with an overlay showing you their status. For more information about the icon overlays, refer to Monitor Data Status Using the Tiger Bridge Icon Overlays on page 148. As you can access a source simultaneously from multiple computers using the remote shell extension, it is possible that the number of requests for files and folders status burdens performance and leads to delays in displaying the icon overlays. A workaround to this problem is to disable the display of icon overlays on computers that do not need to manually manage data on the source.

Additionally, you can fix icon overlays display in the following ways:

- should a third-party application overwrite the Tiger Bridge icon overlays, you can force the display of icon overlays.
- should Windows fail to display the new set of icons after upgrading Tiger Bridge, you can manually clear the Windows icon cache.

To enable/disable the display of Tiger Bridge icon overlays for a computer:

1. Right-click the Tiger Bridge tray icon.

2. Do one of the following:

- To display the Tiger Bridge icon overlays in Windows Explorer, select “Show status icons” in the context menu.
- To hide the Tiger Bridge icon overlays in Windows Explorer, clear “Show status icons” in the context menu.

3. When prompted, confirm that you want to restart Windows Explorer.

To force the display of Tiger Bridge icon overlays:

1. Right-click the Tiger Bridge tray icon.
2. Click “Fix status icons” in the context menu.

To clear the Windows icon cache:

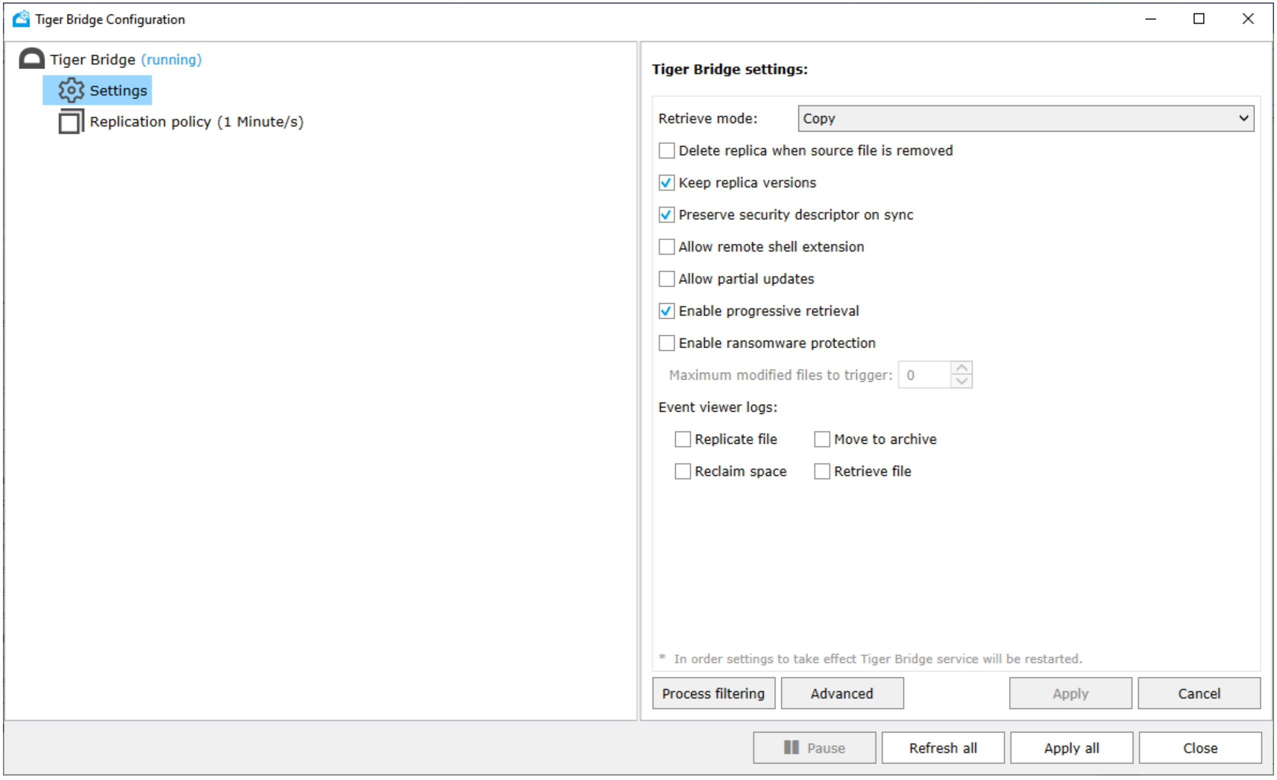
1. Right-click the Tiger Bridge tray icon.
2. Click “Clear Windows icon cache” in the context menu.

Configure How Stub Files Are Populated in a Folder During Synchronization

When you are synchronizing the contents of the source and the target, files present only on the target are populated on the source in the form of stub files. When recovering from a disaster, for example, if the number of files you need to recover from the target is too big, Windows Explorer may fail to correctly report the number of files that are already populated on your source as the process is still ongoing. To prevent you from having to constantly refresh the information about the number of files in a folder, Tiger Bridge allows you to enable synchronous folder population. When enabled, should you attempt to browse a folder on your source, which is being populated with data from the target, Windows Explorer will delay the opening of the folder until all data is completely populated. You can disable this option at any time and browse your source folders even if not all data in them is fully synchronized with the target.

To enable/disable synchronous folder population on all sources:

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



Tiger Bridge Configuration

Tiger Bridge (running)
Settings
Replication policy (1 Minute/s)

Tiger Bridge settings:

Retrieve mode: Copy

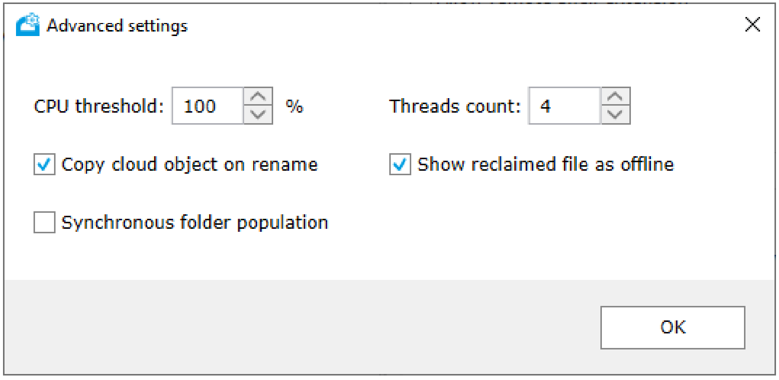
□ Delete replica when source file is removed
☑ Keep replica versions
☑ Preserve security descriptor on sync
□ Allow remote shell extension
□ Allow partial updates
☑ Enable progressive retrieval
□ Enable ransomware protection
Maximum modified files to trigger: 0

Event viewer logs:
□ Replicate file
□ Move to archive
□ Reclaim space
□ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

2. In the right pane, click Advanced.

3. In the Advanced Settings dialog, do one of the following:



CPU threshold: 100 %

Threads count: 4

☑ Copy cloud object on rename

☑ Show reclaimed file as offline

□ Synchronous folder population

- Select the “Synchronous folder population” check box, to let Windows Explorer open the currently browsed folder only after it has been fully populated with stub files from the target, then click OK

- Clear the “Synchronous folder population” check box, to browse folders in Windows Explorer even if they have not been fully populated with stub files from the target, then click OK

4. In the Settings pane, click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

Use Proxy Server for Access to the Target

You can let Tiger Bridge access Amazon S3 and Microsoft Azure targets using a proxy server, already set up on your network. `For this purpose, you need to specify the proxy server settings using the command-line interface of Tiger Bridge.

To specify proxy server settings:

1. 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 used for authentication on the proxy server;

<password> is the password used for authentication on the proxy server;

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 "" ""
```

2. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc
```

```
net start tiersvc
```

To disable access through a proxy server:

1. Execute the following:

   ```
   tiercli config global proxy ""
   ```

2. Restart the Tiger Bridge service, by executing the following:

   ```
   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.

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 by 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.

7. Click OK.

8. Restart the Tiger Bridge computer.

Fine-Tune Data Replication

Enable and Configure Ransomware Protection

Important: This feature protects only already replicated data and prevents Tiger Bridge from overwriting a healthy copy on the target with an encrypted version from the source. Tiger Bridge cannot prevent a ransomware attack on your source.

To prevent replication of files that have been encrypted on your source due to a ransomware attack, Tiger Bridge provides you with a fail-safe setting, which automatically pauses scheduled replication on a source, once specific conditions are present. As ransomware attacks usually result in an encryption of as many files as possible, Tiger Bridge lets you specify the maximum number of already replicated files, queued to be replicated again because they have been modified on a source. When the number of modified files queued for re-replication on a source exceeds the threshold you have specified, Tiger Bridge automatically pauses all its operations for that source and logs this in the Windows Event Viewer. After identifying the encrypted files on the source, you can retrieve from the target their unencrypted copies, and then resume normal operations. For more information about retrieving healthy copies of files from the target, seeRecover Data from The Target on page 131.

Using the Configuration, you can configure Tiger Bridge's ransomware protection parameter valid for each source. By default, once enabled the maximum number of files triggering the protection mechanism on any source is 600. You can change this number depending on your specific workload calculations. In the Tiger Bridge registry, you can overwrite this setting for a specific source by enabling/disabling ransomware protection for a specific source only or by specifying a different number of files that pause the automatic replication on that source.

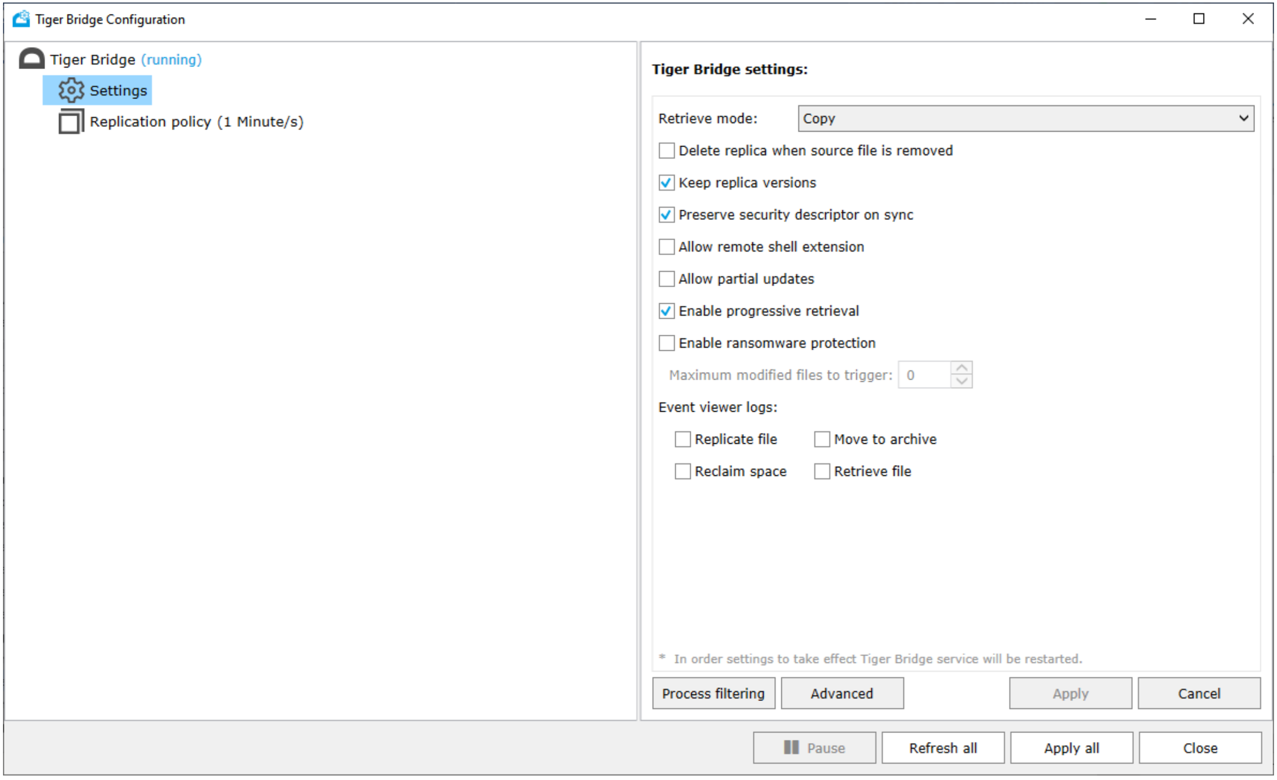
When enabling ransomware protection, use the statistics about modified files per source provided by the Tiger Bridge shell extension as a starting point (see Monitor Data Management Statistics on page 150). You should also keep in mind that:

- If the workload on your sources differs drastically, it is probably better to configure individual ransomware protection thresholds in the registry instead of setting a common threshold in the Configuration.
- 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 source's queue immediately after it has been modified i.e., the longer the time interval in the replication policy, the bigger the chance that healthy files stay in a source's 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 not automatically paused.

To enable/disable the ransomware protection mechanism for each source:

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



Tiger Bridge settings:

Retrieve mode: Copy

□ Delete replica when source file is removed

☑ Keep replica versions

☑ Preserve security descriptor on sync

□ Allow remote shell extension

□ Allow partial updates

☑ Enable progressive retrieval

□ Enable ransomware protection

Maximum modified files to trigger: 0

Event viewer logs:

□ Replicate file □ Move to archive

□ Reclaim space □ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

2. In the right pane, do one of the following:

- Select the “Enable ransomware protection” check box and in “Maximum modified files to trigger” enter the desired number.

- Clear the “Enable ransomware protection” check box to allow Tiger Bridge to re-replicate a file regardless of the number of files currently queued for re-replication on a source.

3. Click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

To overwrite the global ransomware protection setting for a source:

1. Start the Registry Editor.

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

1. Navigate to:
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tiger Technology\tiger-bridge\tiersvc\settings\sources\

2. In the left pane, click the node of a source, whose ransomware protection setting you want to configure.

Tip: You can identify the node of a source by the **source_vol_path REG_SZ** value if the source is a folder on a volume, or by the **source_vol_guid REG_SZ** value, which contains the serial number of the volume whose root is added as a source. You can get the serial number of the volume by executing the following in Command Prompt:

```
vol [drive letter]:
```

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

4. Rename the new REG_SZ value to:
replication_modified_files_threshold

5. Right-click the **replication_modified_files_threshold** value and select Modify.

6. Do one of the following:

- to disable ransomware protection for the source, change the value to 0 and click OK.

  to change the maximum number of files queued for re-replication, which should pause automatic replication when exceeded, enter the desired number and click OK.

7. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

8. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc
```

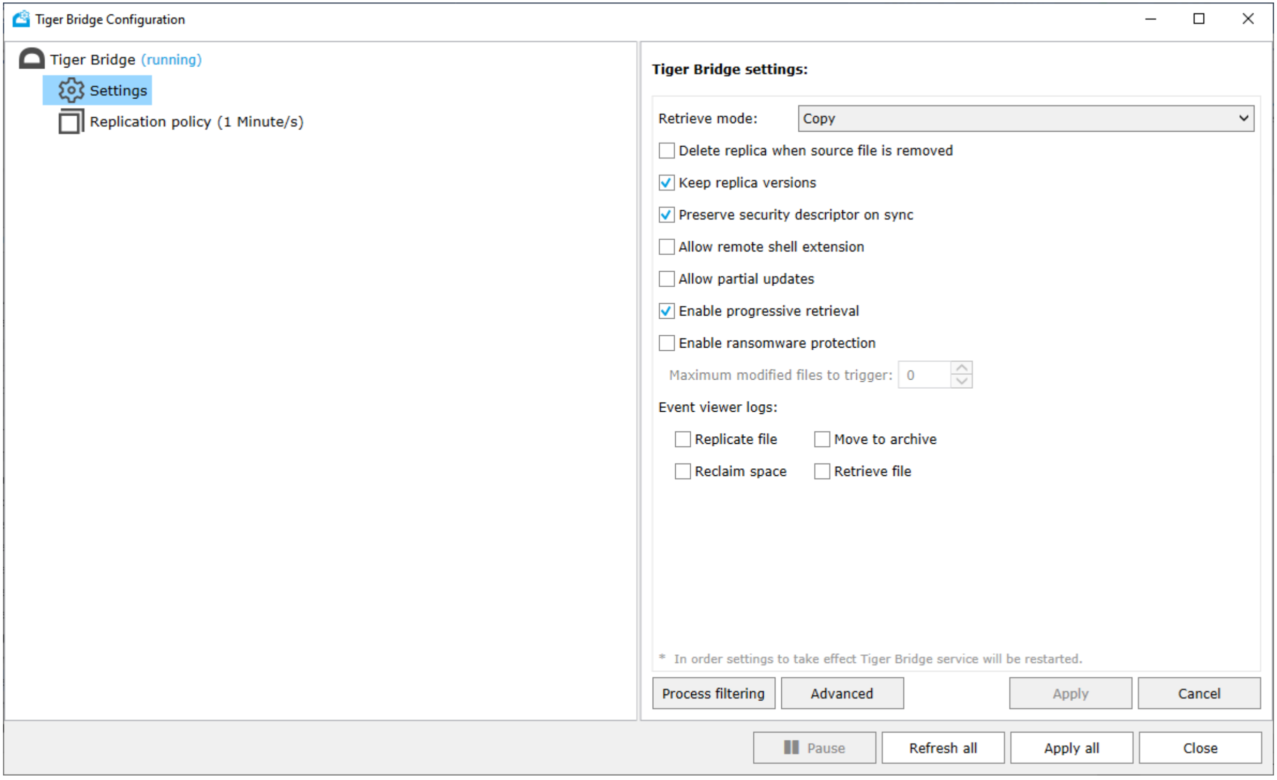
```
net start tiersvc
```

Synchronize the File Name and Path on the Cloud Target When You Rename or Move It on the Source

By default, when you rename an already replicated file or move it to another location within the source, Tiger Bridge also updates the object on the cloud target. To apply the changes on the cloud target Tiger Bridge copies the replicated file with its new name or path and then deletes the original replica. You can disable these operations on the cloud, while still maintaining the changes in the file metadata guaranteeing that when you retrieve the renamed/moved file on the same source or another computer it will be retrieved with its new name and path.

To configure the file name and path synchronization on rename or move:

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



Tiger Bridge Configuration

Tiger Bridge (running)
- Settings
- Replication policy (1 Minute/s)

Tiger Bridge settings:

Retrieve mode: Copy

☐ Delete replica when source file is removed

☑ Keep replica versions

☑ Preserve security descriptor on sync

☐ Allow remote shell extension

☐ Allow partial updates

☑ Enable progressive retrieval

☐ Enable ransomware protection

Maximum modified files to trigger: 0

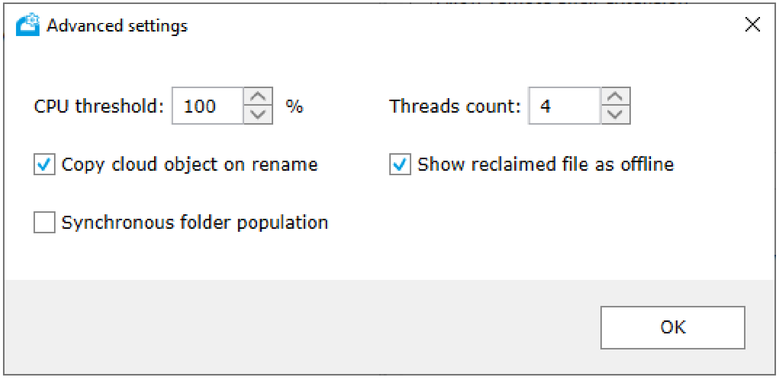
Event viewer logs:

☐ Replicate file ☐ Move to archive

☐ Reclaim space ☐ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

2. In the right pane, click Advanced.



Advanced settings

CPU threshold: 100 %

Threads count: 4

☑ Copy cloud object on rename

☑ Show reclaimed file as offline

☐ Synchronous folder population

3. Do one of the following:

- Select the “Copy cloud object on rename” check box to create a copy of a renamed/moved file on the target before deleting the replica, which uses the old name, then click OK.
- Clear the “Copy cloud object on rename” check box to preserve the changes to the file name and path without creating a new copy on the target, then click OK.

4. Click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

Optimize Processing During Replication

You can optimize the processing of data during file replication from the source to the target in the following ways:

- Set the number of parallel threads used when replicating files and thus increase or decrease the replication speed.

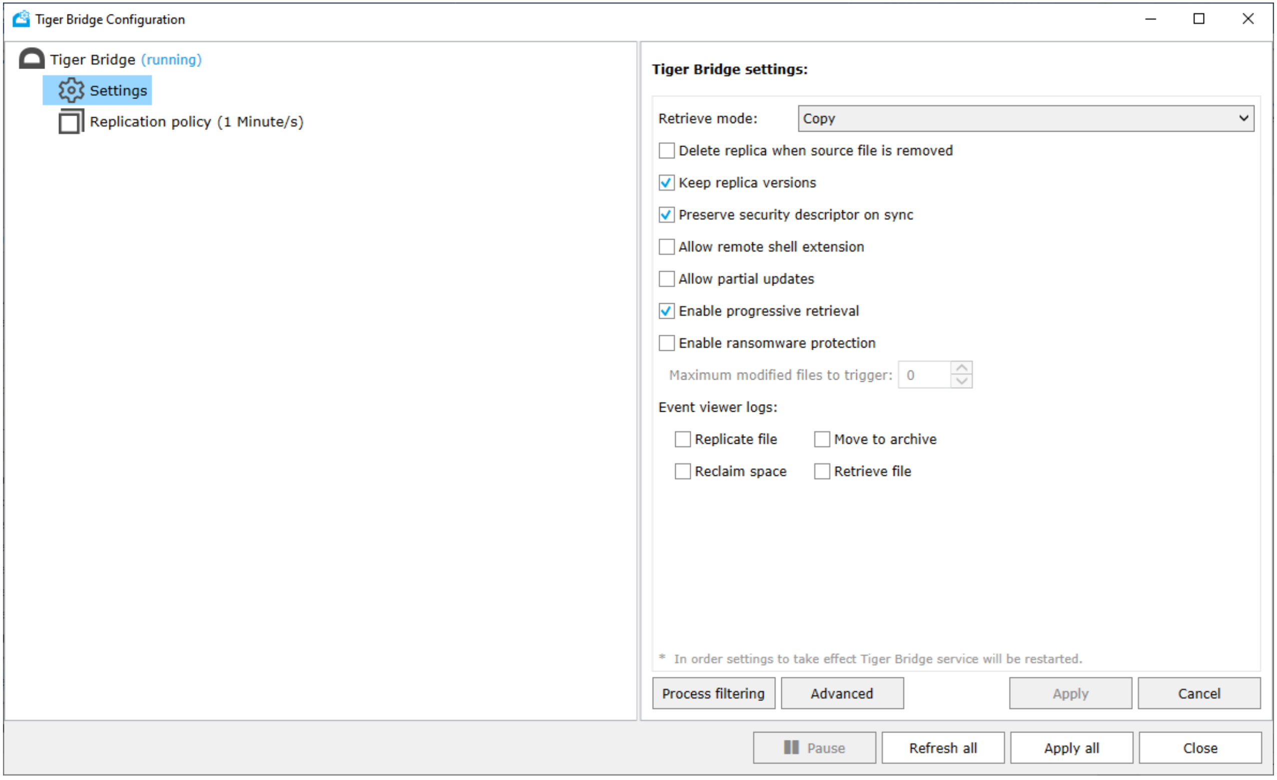
- Set the maximum percentage of CPU usage allowed for data replication, reserving CPU for other operations going on simultaneously.

Set the 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 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:

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



Tiger Bridge Configuration

Tiger Bridge (running)
Settings
Replication policy (1 Minute/s)

Tiger Bridge settings:

Retrieve mode: Copy

□ Delete replica when source file is removed
☑ Keep replica versions
☑ Preserve security descriptor on sync
□ Allow remote shell extension
□ Allow partial updates
☑ Enable progressive retrieval
□ Enable ransomware protection

Maximum modified files to trigger: 0

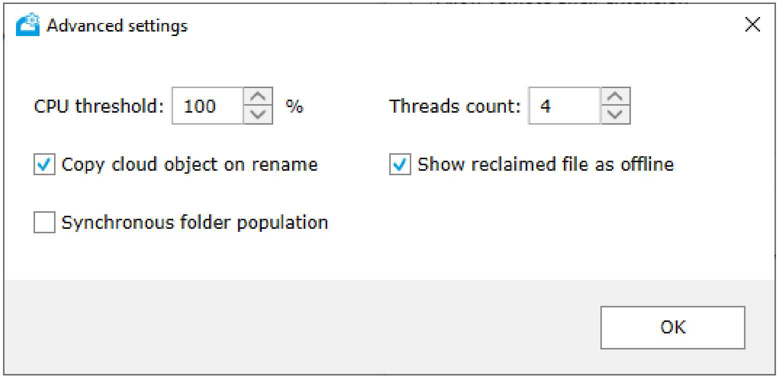
Event viewer logs:

□ Replicate file □ Move to archive
□ Reclaim space □ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

1. In the right pane, click Advanced.

2. In the “Threads count” field of the Advanced Settings dialog, specify the number of parallel threads used by Tiger Bridge during replication and then click OK



Advanced settings

CPU threshold: 100 %   Threads count: 4

☑ Copy cloud object on rename   ☑ Show reclaimed file as offline

□ Synchronous folder population

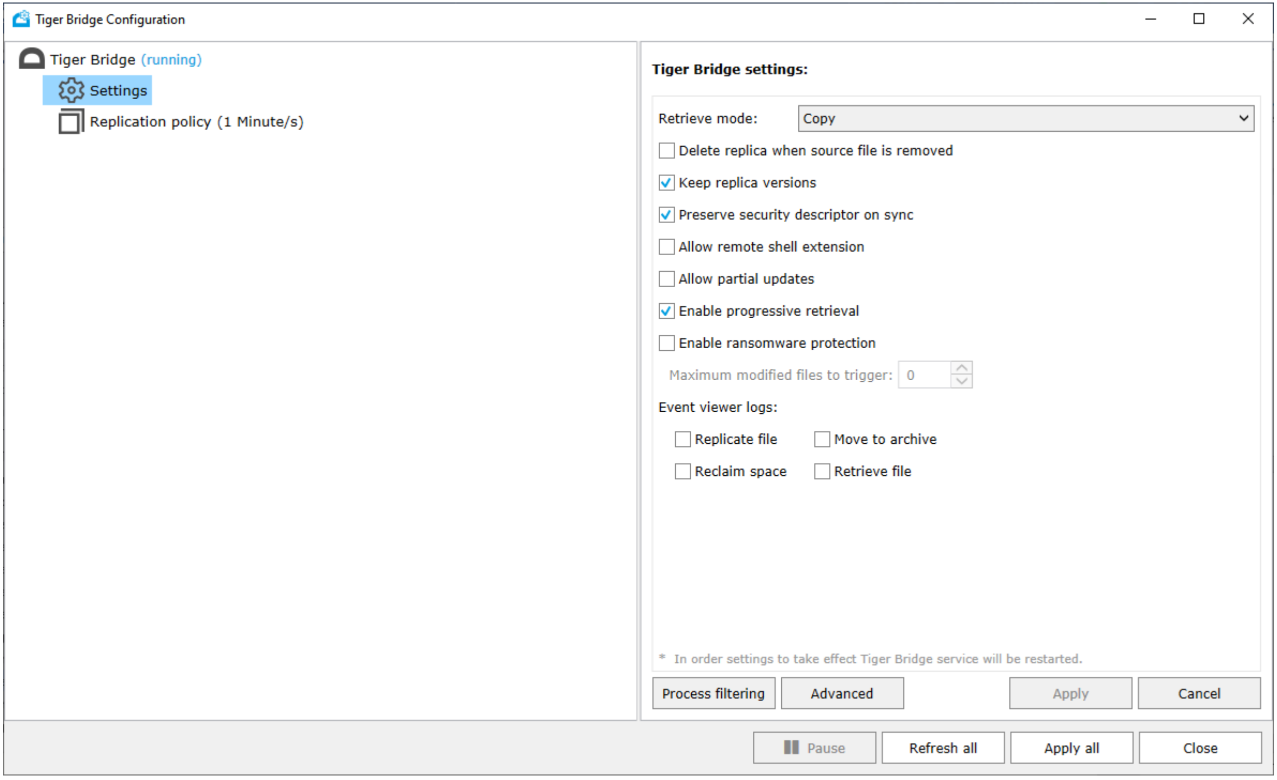
3. In the Settings pane, click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

Set CPU Threshold During Replication

By default, the replication is set to utilize 100% of the CPU resources available at any given moment. If you configure a smaller CPU threshold, when reached Tiger Bridge itself slows down the processing of files queued for replication, until the percentage falls below the one you have specified.

To set the CPU threshold for processing data replication:

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



Tiger Bridge settings:

Retrieve mode: Copy

□ Delete replica when source file is removed

☑ Keep replica versions

☑ Preserve security descriptor on sync

□ Allow remote shell extension

□ Allow partial updates

☑ Enable progressive retrieval

□ Enable ransomware protection

Maximum modified files to trigger: 0

Event viewer logs:

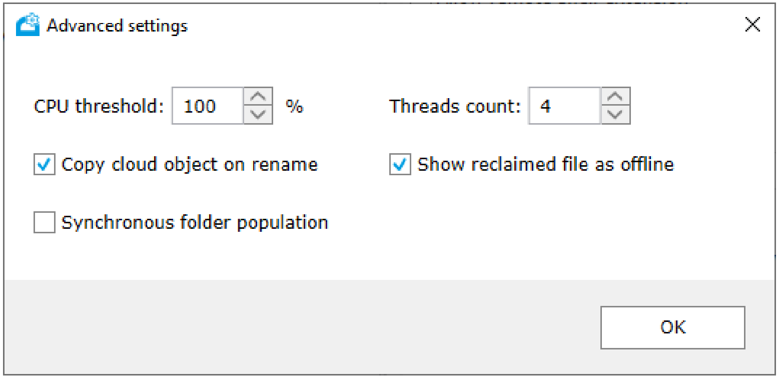
□ Replicate file □ Move to archive

□ Reclaim space □ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

1. In the right pane, click Advanced.

2. In the “CPU threshold” field of the Advanced Settings dialog, specify the percentage of CPU processing power data replication cannot exceed and then click OK.



CPU threshold: 100 %   Threads count: 4

☑ Copy cloud object on rename   ☑ Show reclaimed file as offline

□ Synchronous folder population

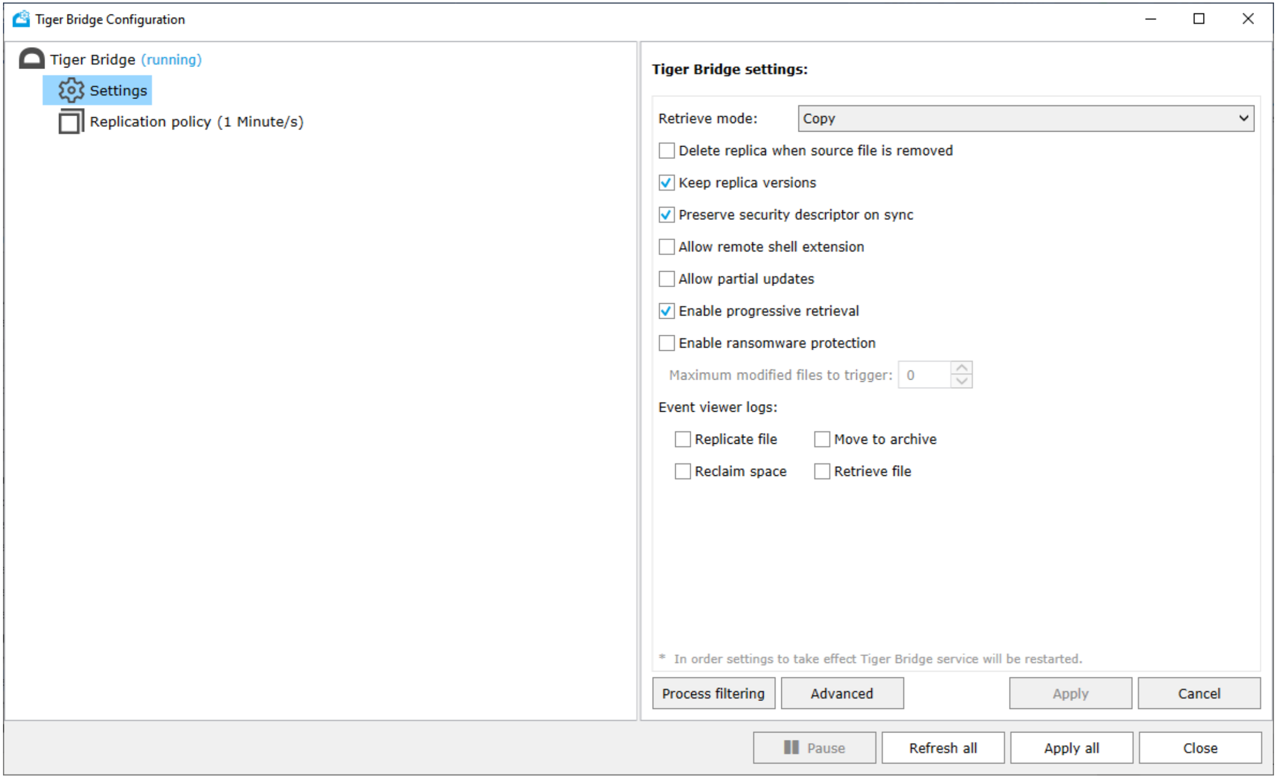
3. In the Settings pane, click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

Partial File Replication

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 that 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 storage sources. Even if you enable it on other targets or 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.



Tiger Bridge settings:

Retrieve mode: Copy

□ Delete replica when source file is removed

☑ Keep replica versions

☑ Preserve security descriptor on sync

□ Allow remote shell extension

□ Allow partial updates

☑ Enable progressive retrieval

□ Enable ransomware protection

Maximum modified files to trigger: 0

Event viewer logs:

□ Replicate file □ Move to archive

□ Reclaim space □ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

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 and when prompted, confirm that you want to restart the Tiger Bridge service.

Minimum File Size for Replication

By default, the only criteria for queuing a file for replication is for how long this file has not been modified. You can also set Tiger Bridge to only queue for replication 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 a size below this minimum, this file will be replicated.

To specify the 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 a 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. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

6. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc

net start tiersvc
```

Replicate File’s Metadata to a Different Bucket/Container

With Amazon S3, Microsoft Azure, and all S3-compatible targets you can configure Tiger Bridge to replicate files’ data and metadata to different buckets/containers of the same target.

Note: Currently, you cannot benefit from separating the replication of a file’s data and metadata on IBM cloud object storage target, if you have configured Tiger Bridge to work with the Accelerated Archive storage class.

With Amazon S3 target, 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 this purpose, you must designate another bucket for storing just replicated files’ metadata.

To configure a separate bucket/container for replication of a file’s metadata:

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <source> meta <bucket_name> [access_id] [access_key]
```

where:

- <source> is the full path to the source;
- <bucket_name> is the name of the bucket/container, designated for storing metadata from this source;

Optional parameters to use, if the credentials for access to the bucket differ from the credentials for access to the bucket/container designated for replicated data:

- [access_id] is the access key ID for access to the S3 or S3-compatible storage or the account name used for accessing your Azure Blob storage;
- [access_key] is the secret key for access to the S3 or S3-compatible storage, or the account key for access to the Azure Blob storage;

3. Repeat the above step for each source whose metadata should be replicated to a separate bucket/container.

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

```
tiercli config reload
```

Fine-Tune Space Reclaiming

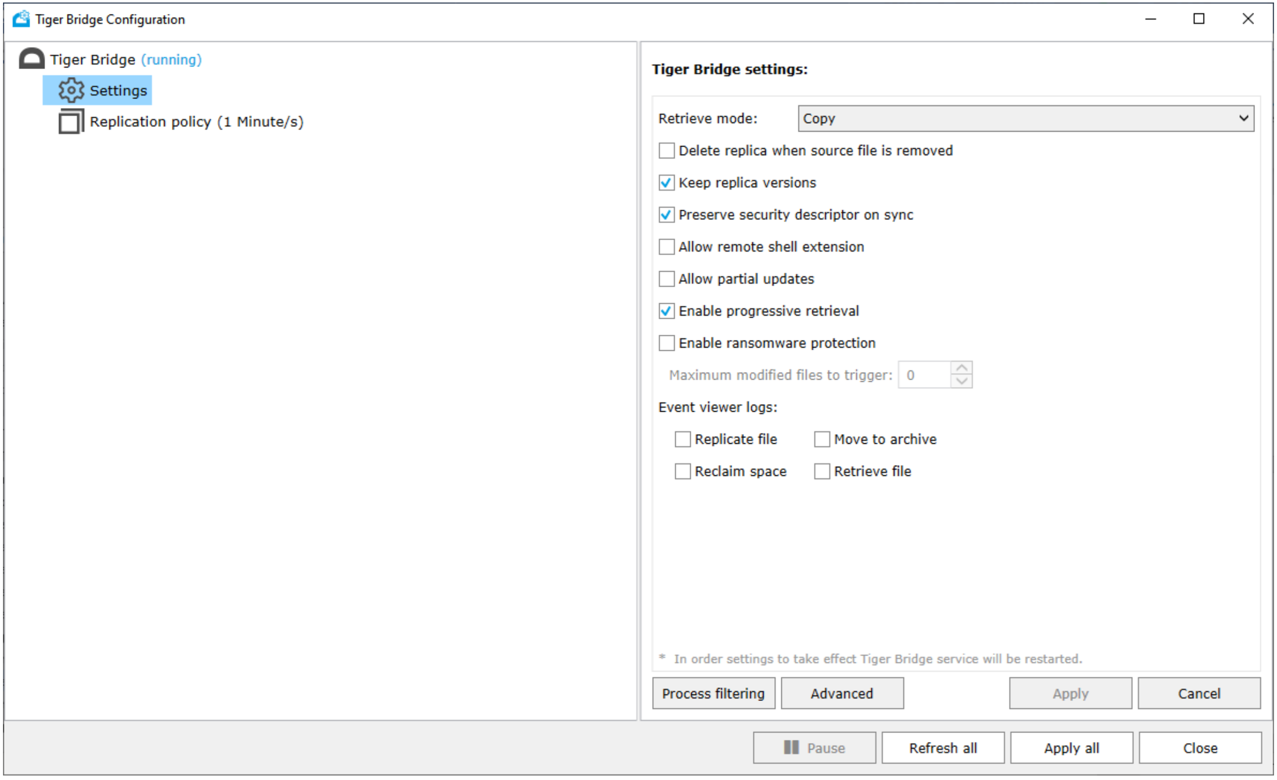
Configure the Applications Automatically Retrieving Nearline Files from the Target

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 a list of processes that cannot trigger the 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 nearline file. In case you decide to specify the processes that 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.

Note: 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.

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

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



Tiger Bridge Configuration

Tiger Bridge (running)
Settings
Replication policy (1 Minute/s)

Tiger Bridge settings:

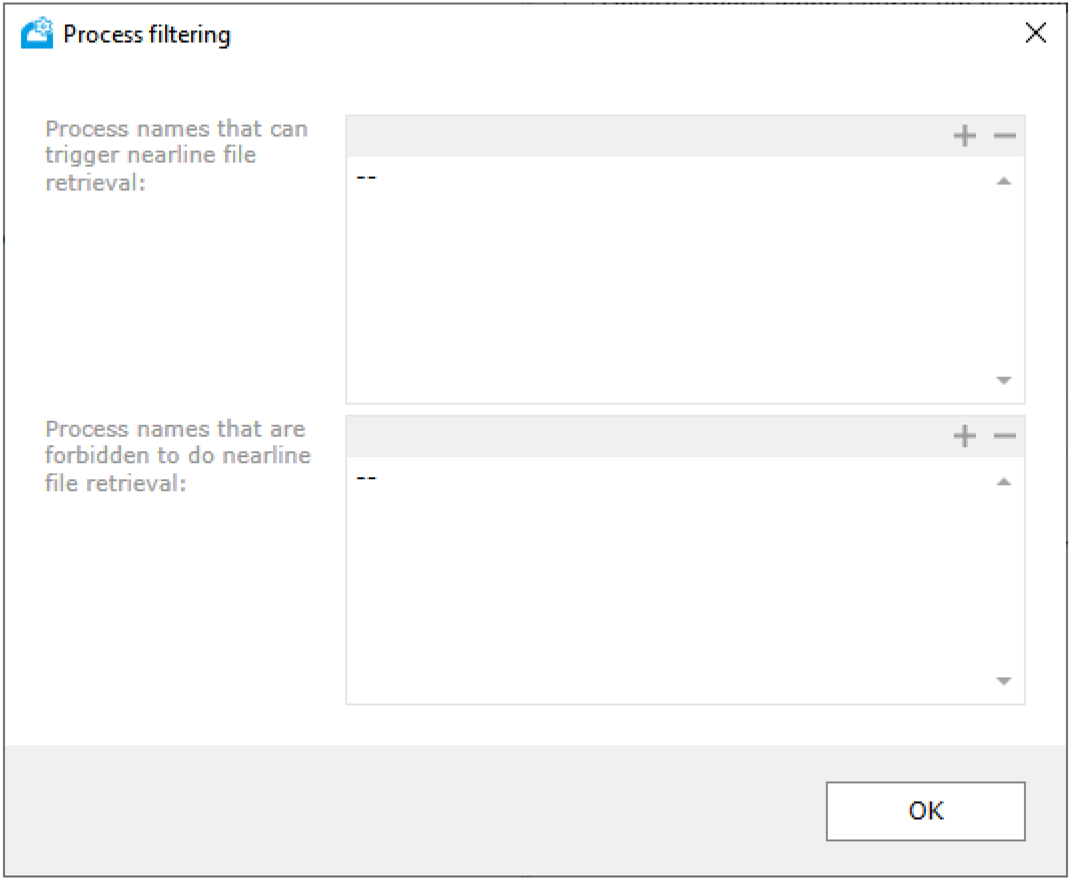
Retrieve mode: Copy

□ Delete replica when source file is removed
☑ Keep replica versions
☑ Preserve security descriptor on sync
□ Allow remote shell extension
□ Allow partial updates
☑ Enable progressive retrieval
□ Enable ransomware protection
Maximum modified files to trigger: 0

Event viewer logs:
□ Replicate file □ Move to archive
□ Reclaim space □ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

2. Click “Process filtering” and in the dialog, do one of the following:



Process filtering

Process names that can trigger nearline file retrieval: --

Process names that are forbidden to do nearline file retrieval: --

- 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.

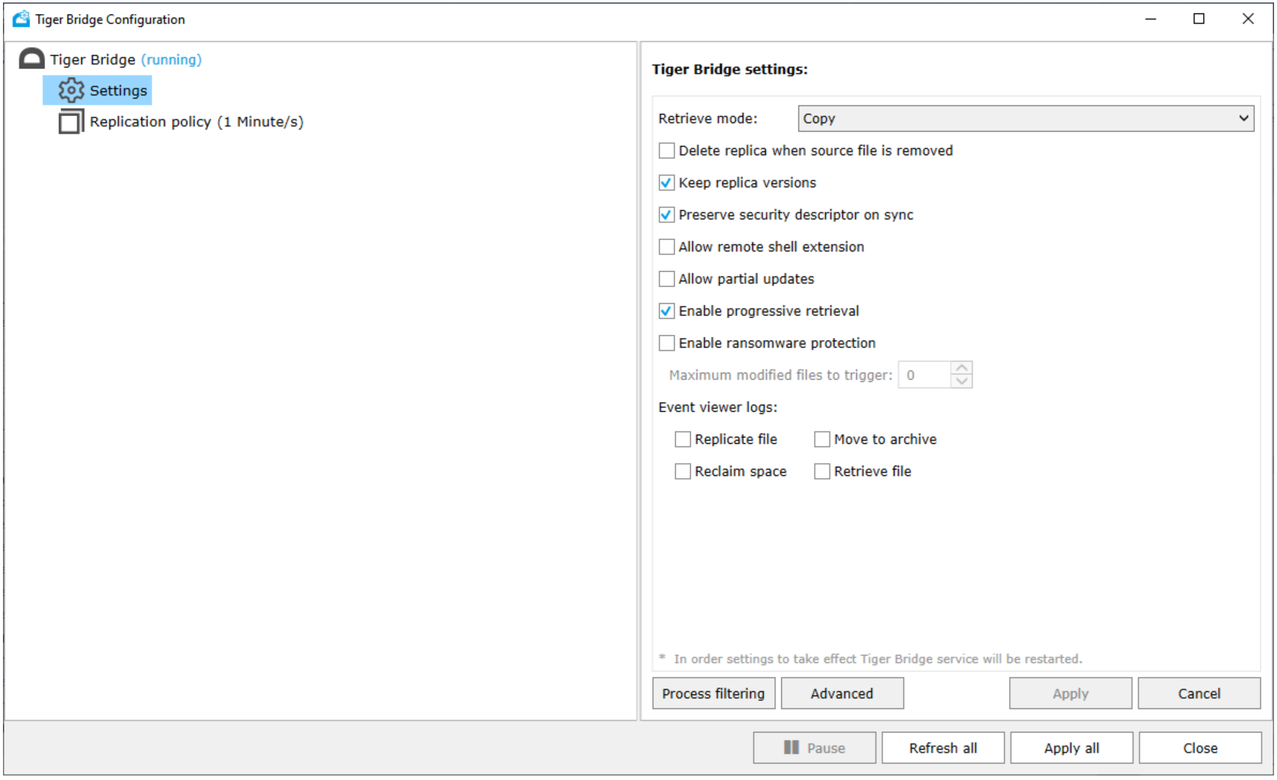
3. In the Configuration, click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

Hide Offline Attribute of Stub Files

While Tiger Bridge takes care to present stub files on the source as available, by default, it does not hide their “offline” attribute in the file system of your source. As this may prevent certain applications from even attempting to open a stub file, you can hide this attribute and allow their retrieval on demand i.e. when a user or an application attempts to open the stub file.

To show/hide the offline attribute of stub files on all sources:

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



Tiger Bridge settings:

Retrieve mode: Copy

□ Delete replica when source file is removed

☑ Keep replica versions

☑ Preserve security descriptor on sync

□ Allow remote shell extension

□ Allow partial updates

☑ Enable progressive retrieval

□ Enable ransomware protection

Maximum modified files to trigger: 0

Event viewer logs:

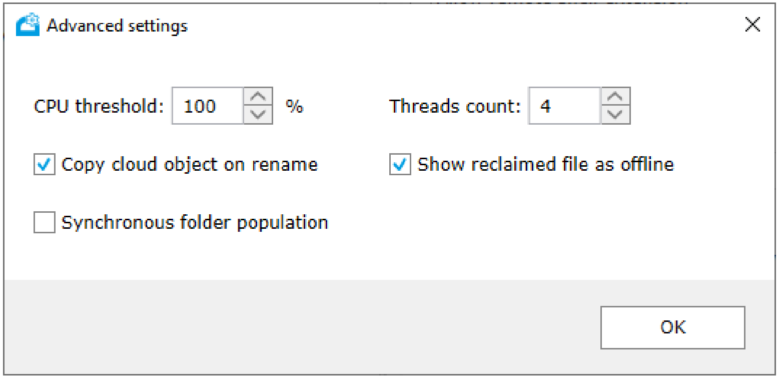
□ Replicate file □ Move to archive

□ Reclaim space □ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

2. In the right pane, click Advanced.

3. In the Advanced Settings dialog, do one of the following:



Advanced settings

CPU threshold: 100 %

Threads count: 4

☑ Copy cloud object on rename

☑ Show reclaimed file as offline

□ Synchronous folder population

- Select the “Show reclaimed file as offline" check box, to show the offline file attribute of stub files on all sources, then click OK.
- Clear the “Show reclaimed file as offline" check box, to hide the offline file attribute of stub files on all sources, then click OK.

4. In the Settings pane, click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

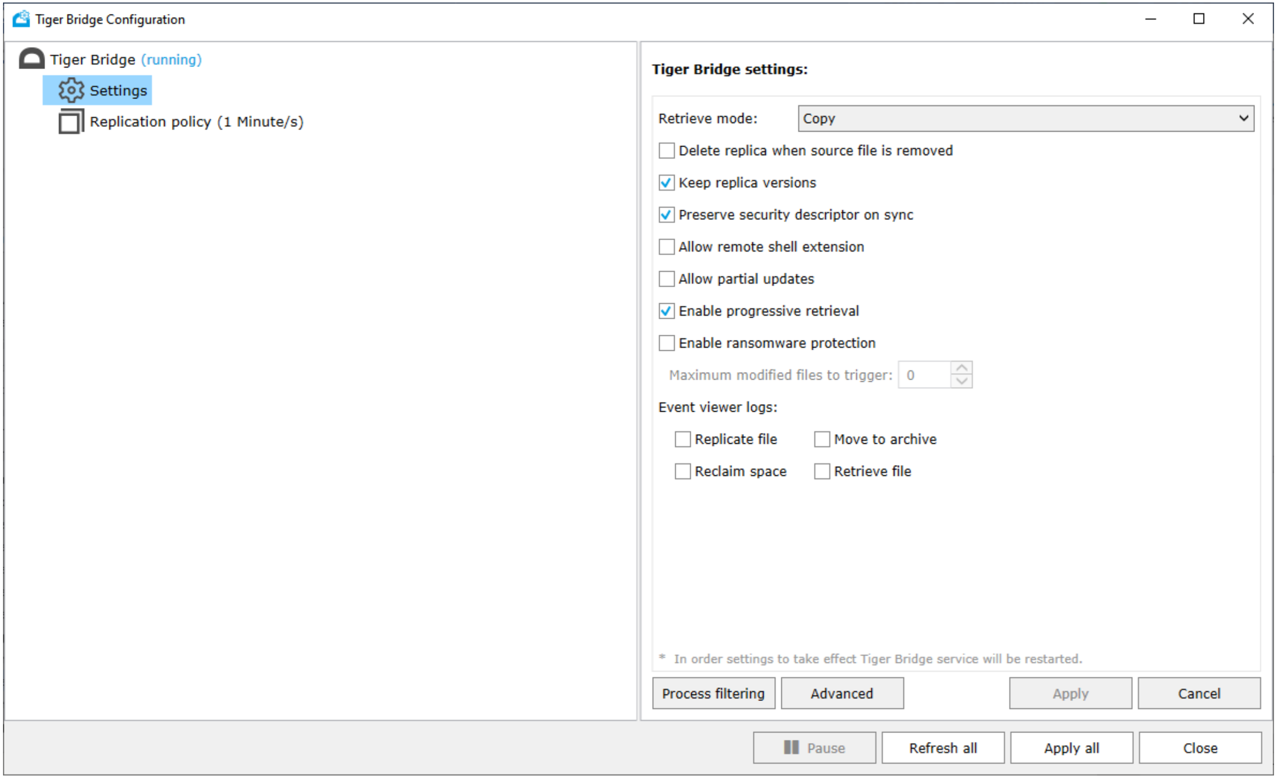
Progressive File Retrieval

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 applications 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, reading of partially retrieved files must not be disabled. For more information, refer to Reading of Partially Retrieved Files on page 122.

To enable/disable progressive file retrieval:

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



Tiger Bridge settings:

Retrieve mode: Copy

□ Delete replica when source file is removed

☑ Keep replica versions

☑ Preserve security descriptor on sync

□ Allow remote shell extension

□ Allow partial updates

☑ Enable progressive retrieval

□ Enable ransomware protection

Maximum modified files to trigger: 0

Event viewer logs:

□ Replicate file □ Move to archive

□ Reclaim space □ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

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. In the Settings pane, click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

Disable Automatic Retrieval of Nearline Files

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 behavior 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 retrieval behavior:

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 a manual retrieve operation is executed from the command-line interface or the shell extension, change the value to 0 and click OK.

5. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

6. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc
```

```
net start tiersvc
```

Automatic Rehydration of Offline Files

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 behavior 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 this 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, for example, that 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 that can trigger the 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. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

8. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc
```

```
net start tiersvc
```

To specify the processes allowed to trigger the 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.

- 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, by 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 that 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. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

6. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc
```

```
net start tiersvc
```

Reading of Partially Retrieved Files

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 to the source.

To specify whether applications can begin reading partially retrieved 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 in the right pane and select New | String Value.
4. Rename the new REG_SZ value to "active_restore_partial".
5. Right-click the "active_restore_partial" string value and select Modify.
6. 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.

7. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

8. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc
net start tiersvc
```

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 to 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. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

6. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc

net start tiersvc
```

Reclaim Space Based on File Modification Timestamp

By default, one of the parameters for replacing a replicated file with a stub file is how long this file has not been accessed. Tiger Bridge allows you to change this parameter of the Reclaim Space policy to the time interval for which a file has not been modified on the source. You can revert to the default policy parameter at any time.

Note: If you set Tiger Bridge to use the file modification time as Reclaim Space policy criteria, use the file last access time field to specify the value.

To change the Reclaim Space 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 a parameter, change the value to 0 and click OK.

- To use the file modification time as a parameter, change the value to 1 and click OK.

5. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

6. Restart the Tiger Bridge service, by executing the following:

```
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. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

6. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc
```

```
net start tiersvc
```

Keep Selected Part of Reclaimed File on the Source

By default, stub files keep none of the original file's data or metadata and take no space on the source. Tiger Bridge allows you to configure the space reclaiming mechanism in such a way that a portion of a reclaimed file remains on the source. This can be useful when you work with applications that need to regularly access a specific portion of the file containing information, which does not otherwise require retrieving the whole file from the target. As with different applications, this portion of the file may be located in different places of the file, Tiger Bridge allows you to add an entry for each file type and specify:

- the size of the portion of the file that is retained in the stub file on the source
- the offset from the beginning of the file at which this portion begins

You can edit the list of file types by adding or removing an entry for a specific file type. To edit the parameters of an already configured entry, you must first remove it from the list and then configure it anew. All file types for which there is no entry specifying which portion of the file should be kept on the source are replaced with stub files containing no actual data and metadata during space reclaiming.

You can create a global list, valid for all pairs of a source and a target that do not have a list of their own. You can also overwrite the list for a specific pair of source and target and specify different file types.

To view the list of file types with configured entries:

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. In Command Prompt, execute the following:

```
tiercli config policy reclaimspace ondisk show
```

Tiger Bridge lists all file type entries in order of configuring them and gives you information about the file type, the offset from the beginning of the file, and the length of the portion kept on the source in bytes.

Note: To view the list of configured entries for a specific pair of source and target, execute the command including the path to the source:

```
tiercli config <path to source> policy reclaimspace ondisk show
```

To add a file type entry:

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. In Command Prompt, execute the following:

```
tiercli config policy reclaimspace ondisk add <file extension> <offset> <length>
```

where:

- <file extension> is the extension used by the file type
- <offset> is the point from the beginning of the file in bytes at which the portion you want to keep on the source begins
- <length> is the size of the portion of the file you want to keep on the source

For example, to specify that when Tiger Bridge reclaims AVI files the stubs that replace them on the source must contain the 56-byte header, starting at offset 32 within the file, execute the following:

```
tiercli config policy reclaimspace ondisk add avi 32 56
```

Note: To add a file type entry to the list for a specific pair of source and target, execute the command including the path to the source:

```
tiercli config <path to source> policy reclaimspace ondisk add <file extension>
<offset> <length>
```

To remove a file type entry:

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. In Command Prompt, execute the following:

```
tiercli config policy reclaimspace ondisk clear <file extension>
```

where:

- <file extension> is the extension used by the file type

Tip: To remove all entries about file types keeping a portion of the original file, execute the command using an asterisk instead of a file extension:

```
tiercli config policy reclaimspace ondisk clear *
```

For example, to clear the entry of Microsoft Word files from the list of file types that keep a portion of the of the original file on the source, execute the following:

```
tiercli config policy reclaimspace ondisk clear docx
```

Note: To remove a file type entry from the list for a specific pair of source and target, execute the command including the path to the source:

```
   tiercli config <path to source> policy reclaimspace ondisk clear <file extension
 >
```

Fine-Tune Sync

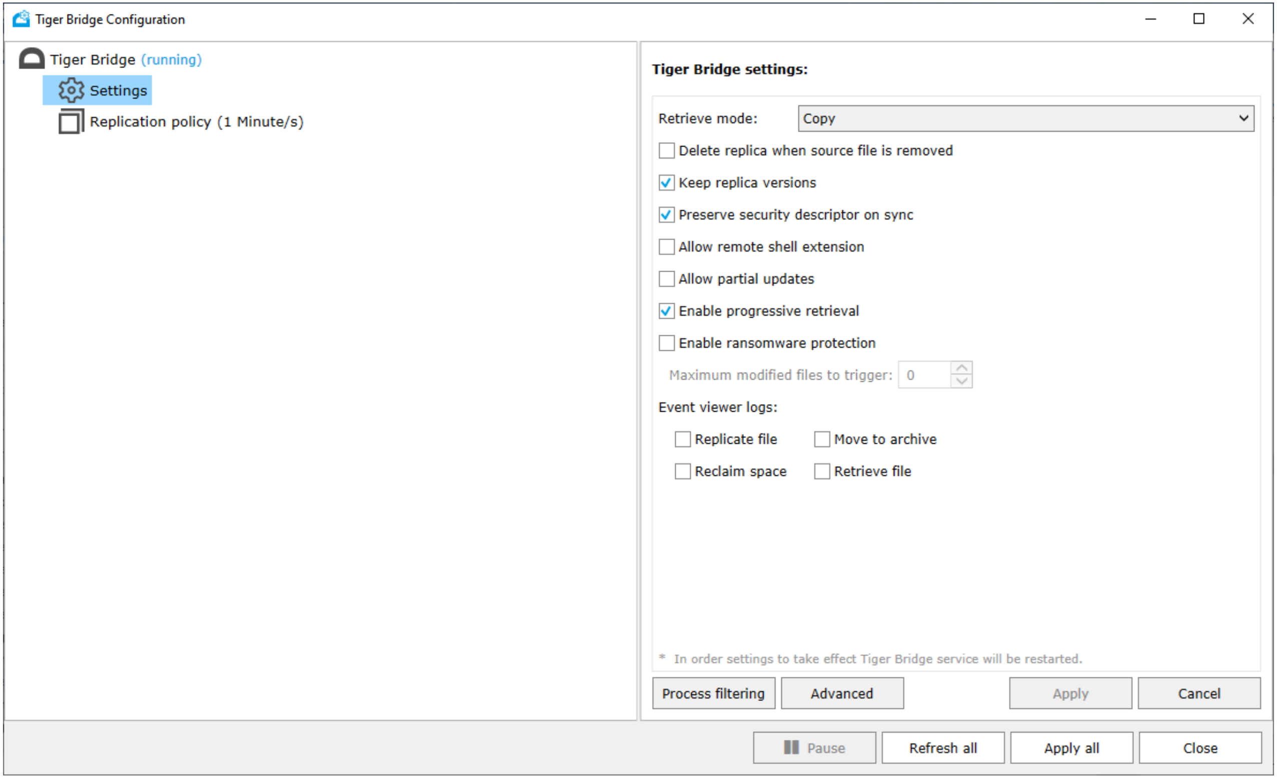
Preserve the Security Descriptor of Retrieved Files

You can configure Tiger Bridge to keep a file's security descriptor when it is being retrieved to other sources through Sync. In the Tiger Bridge Configuration, you can select whether to preserve or not the security descriptor of retrieved files on all sources. In the Tiger Bridge registry, you can configure specific sources on which the descriptor is kept.

It is advisable to preserve the security descriptor of retrieved files only on sources that are in the same Active Directory domain.

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

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



Tiger Bridge settings:

Retrieve mode: Copy

☐ Delete replica when source file is removed
☑ Keep replica versions
☑ Preserve security descriptor on sync
☐ Allow remote shell extension
☐ Allow partial updates
☑ Enable progressive retrieval
☐ Enable ransomware protection

Maximum modified files to trigger: 0

Event viewer logs:

☐ Replicate file ☐ Move to archive
☐ Reclaim space ☐ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

2. Do one of the following:

- Select the "Preserve security descriptor on sync" check box, to keep the security descriptor of all files on each source after contents synchronization.
- Clear the "Preserve security descriptor on sync" check box, to retrieve all files without their security descriptor on each source after contents synchronization.

3. Click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

To configure Tiger Bridge to preserve the files' security descriptor on a selected source:

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 Sources node in the left pane and select the node of the source for which you want to configure the security descriptor setting.

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

5. Rename the new REG_SZ value to "preserve_security_descriptor".

6. Right-click the "preserve_security_descriptor" value and select Modify.

7. Do one of the following:

- to set Tiger Bridge to preserve the security descriptor of files retrieved to this source from other sources, change the value to 1, and click OK.
- to retrieve files to this source without preserving their security descriptor, change the value to 0, and click OK.

8. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

9. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc

net start tiersvc
```

Manually Manage Data

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 Data Lifecycle Operations below.
- Manage files that have failed to replicate. For more information, see Manage Files That Have Failed to Replicate on the next page.
- Manually synchronize a source with other sources through a common target. For more information, see Manually Synchronize Sources Through a Common Target on page 131.
- Recover data from the target. For more information, see Recover Data from The Target on page 131.
- Revert file modifications to their last replicated state. For more information, see Revert File Modifications on the Source on page 132.
- Undelete files from the source. For more information, see Undelete Data from the Source on page 133.
- Manage files and folders versions. For more information, see Manage Files and Folders Versions on page 134.

Perform Manual Data Lifecycle Operations

As long as the Tiger Bridge shell extension is installed on the computer, you can use it to perform the following lifecycle operations on a single file, on multiple selected files, or on all data in a folder in either Windows Explorer or the Tiger Bridge Explorer:

Replicate data. On some cloud object storage targets, you can also choose to what tier to replicate the selected data.

Reclaim space on your source by replicating the selected files, if not already replicated, and then replacing them with stub files.

Retrieve data from the target, the command is available only when at least one stub file is selected.

Move the selected replicated file(s) from the nearline to the archival tier of the target, the command is available only on targets that support third-party policies to move files to the archive

Rehydrate a file from the archival tier of the target to the hot/cool tier

The context menu of the shell extension displays the respective commands only if they are applicable to the selected files/folders i.e., you cannot issue the “Reclaim space” command for a nearline file, for example.

Note: 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.

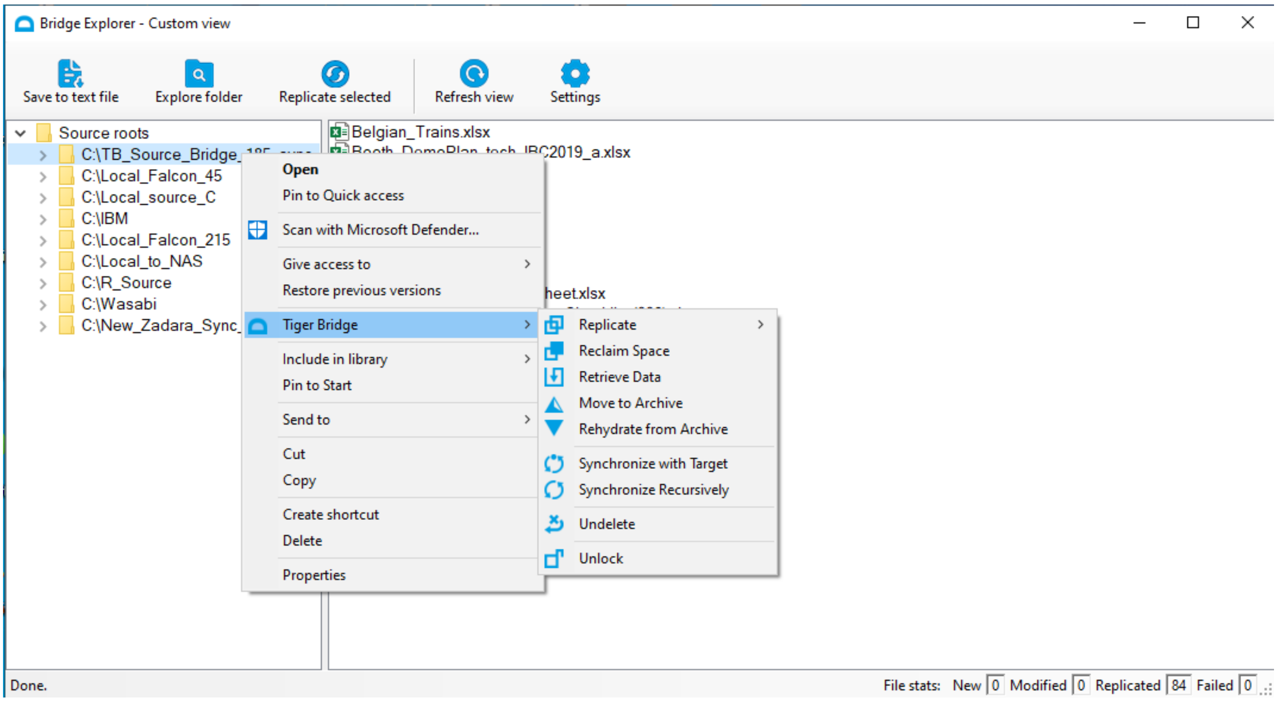
To perform data lifecycle management operations:

1. In the Tiger Bridge Explorer/Windows Explorer, do one of the following:

- Browse to and select a source or any of its sub-folders.
- Browse to and select one or more files in the right pane.

2. (Windows Explorer only) For access from a 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.

3. Right-click the selection and in the context menu, click Tiger Bridge and then click the respective command.



Manage Files That Have Failed to Replicate

Files that have failed to replicate if the connection to the target has been lost, for example, are not automatically added to the replication queue. To add them to the replication queue again, you should either restart the Tiger Bridge computer or its service, by following these steps:

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Restart the Tiger Bridge service, by executing the following:

```
net stop tiersvc

net start tiersvc
```

You can also easily replicate all failed files in the Tiger Bridge Explorer, without having to restart the Tiger Bridge computer or service.

To replicate files the replication of which has failed:

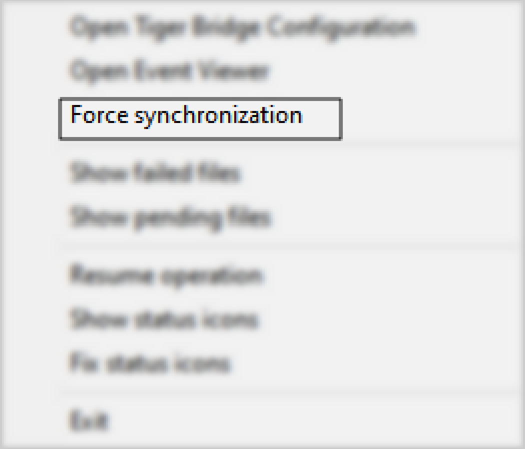
1. Right-click the Tiger Bridge tray icon and click “Show failed files”.
2. Click Settings and in the Settings dialog, clear the “Flat listing” check box to display all failed files, without having to browse your source’s folder structure.
3. In the left pane of the Tiger Bridge Explorer, select a source and click “Retry selected” in the toolbar.
4. Repeat the above step for each source, listed in the left pane.

Manually Synchronize Sources Through a Common Target

You can manually update your source’s contents with changes from other source(s) without having to wait for the Sync policy to check for updates. Force synchronizing data on your computer only updates your sources with new changes on other computers but does not force sources on other computers to update their contents with changes from your computer.

To force the synchronization of your sources with sources on other computers:

1. Right-click the Tiger Bridge tray icon.
2. Click “Force synchronization” in the context menu.



Recover Data from The Target

In contrast to retrieving reclaimed data that is available on the source only in the form of stub files, manually synchronizing the contents of the source and target allows you to recover data that is not present on the source. The method recovers data on the source as stub files that you can retrieve manually, or on demand by opening them. Use the functionality to:

- Recover data after a disaster, if you use a non-object storage target or if the source is intact i.e., there is no need to reformat the file system on which it is located. With object storage targets, in case of a disaster you can simply pair the source with the target again and import all data from the target, as described in Manage Existing Data on the Target on page 66.
- Retrieve from the target a healthy copy of a file encrypted on the source as a result of a ransomware attack.

Important: Unless versioning is enabled, do not delete the encrypted copies of replicated files from the source before making sure that the “Delete replica when source file is removed” option is disabled (see Configure File Operation Mode on page 91). If you must keep the option enabled, use the following Tiger Bridge command-line interface command to delete files only from the source:

```
tiercli op delete -l <path to a file or a whole folder>
```

- Migrate data from one source to another on the same computer (when you need to replace the volume of your initial source with a bigger one, for example). `For this purpose, before recovering data on your new source, you need to first delete the old source making sure beforehand that all needed data is replicated.

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 the Tiger Bridge Explorer/Windows Explorer, right-click the folder, whose contents you want to synchronize with the target.

2. (Windows Explorer only) For access from a 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.

3. In the context menu under Tiger Bridge, do one of the following:

- To synchronize just the contents of the folder with the target, click “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, click "Tiger Bridge | Synchronize Recursively”.

Revert File Modifications on the Source

If you have introduced changes to an already replicated file, you can revert them even if you have saved these changes and closed the file as long as the newly introduced changes are not replicated yet. The command in the Tiger Bridge context menu reverts the file to its last replicated state. You can execute it for a selected file or for all applicable files in a folder.

Important: After reverting the file modifications, all unreplicated changes to the file are lost.

To revert the modifications of a file to the last replicated state:

1. In the Tiger Bridge Explorer/Windows Explorer, right-click the file or folder.

Note: In Windows Explorer, to revert the modifications of a file from a NAS source, you need to perform the operation in its control folder.

2. (Windows Explorer only) For access from a 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.

3. In the context menu, select “Tiger Bridge | Revert”.

Undelete Data from the Source

Undeleting a file from your source means restoring back its copy from the target. Depending on the target tier the copy is located on, 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.

In case you have configured Tiger Bridge’s operation mode to delete the replica of a file from the target when it is deleted from the source, to undelete a file one of the following conditions must be present:

- (on targets that support versioning) Versioning is enabled in Tiger Bridge and versioning or soft delete is enabled on the target.
- (on all targets) There is a Soft Delete policy enabled and configured and the time for synchronizing the deletion on the target has not elapsed.

To undelete data on the source through the shell extension:

1. In the Tiger Bridge Explorer/Windows Explorer, right-click the folder, containing the file you want to undelete.

Note: In Windows Explorer, to undelete a file from a NAS source, you need to perform the operation in its control folder.

2. (Windows Explorer only) For access from a 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.

3. In the context menu, select “Tiger Bridge | Undelete”.

The Undelete Files dialog lists all files deleted from the selected folder that have copies on the target.

4. 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.

Manage Files and Folders Versions

As long as versioning is enabled on your cloud storage target and also in Tiger Bridge by following the steps in Configure Versioning on page 86, 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 of 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.)

Note: The grey icon is also displayed regardless of the tier/storage class the current version is stored on to notify you that there are changes to the file on the source that have not been replicated yet.

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 version or all older versions of a file from the target, discarding them as obsolete and thus freeing space on the target.
- Delete any selected version 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.

Note: You cannot delete a version of a file if it is the only one 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 can also select to automatically retrieve to thesource each restored version and to add the restored version as the newest copy on the target.

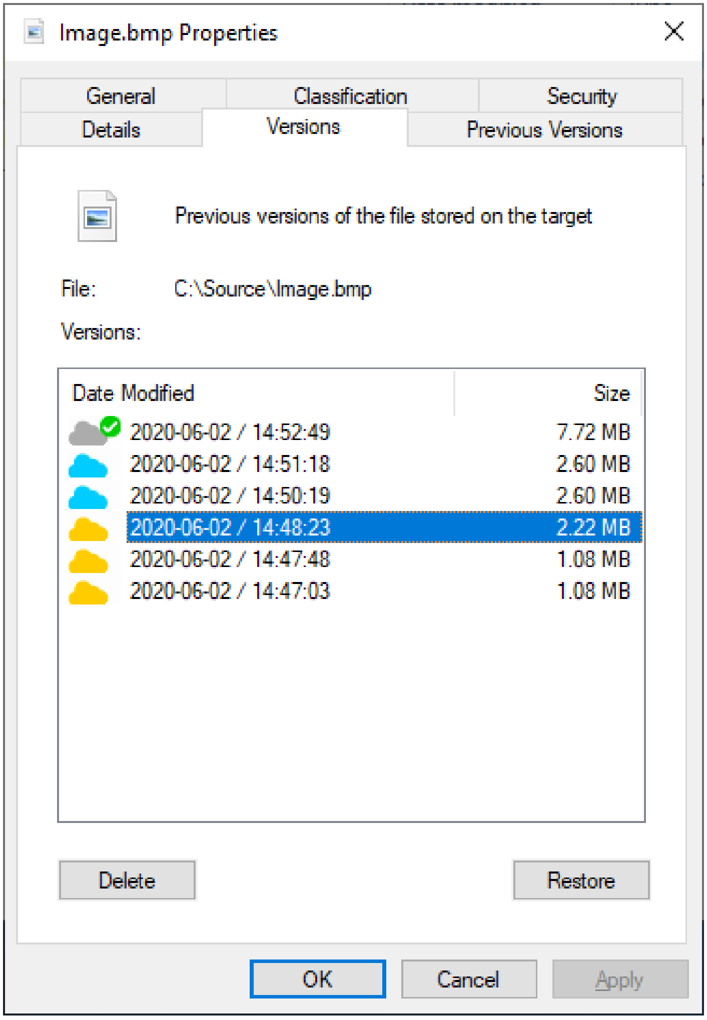
Important: You can manage the versions of files/folders on a NAS source in its control folder. The restored version of a file is automatically retrieved to theNAS source.

To restore a specific version of a file:

1. In Windows Explorer, right-click the file and select Properties.

2. In the Properties dialog, click 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.



Previous versions of the file stored on the target

File: C:\Source\Image.bmp

Versions:

Date Modified	Size
✓ 2020-06-02 / 14:52:49	7.72 MB
2020-06-02 / 14:51:18	2.60 MB
2020-06-02 / 14:50:19	2.60 MB
2020-06-02 / 14:48:23	2.22 MB
2020-06-02 / 14:47:48	1.08 MB
2020-06-02 / 14:47:03	1.08 MB

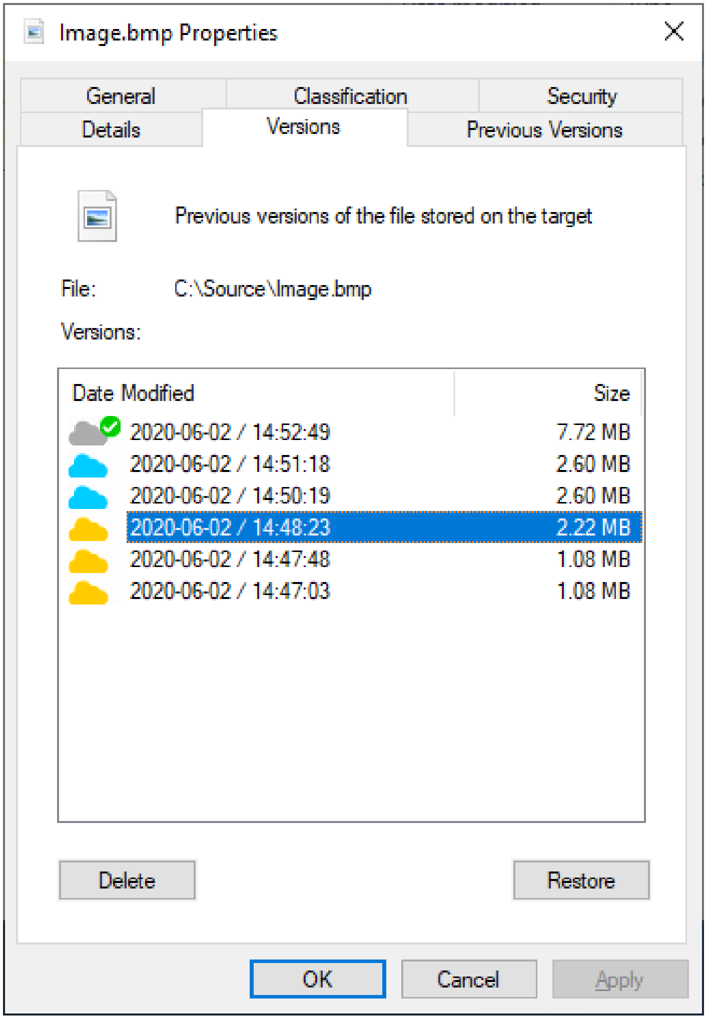
3. Select a file version in the list and click Restore.

To delete a specific version of a file:

1. In Windows Explorer, right-click the file and select Properties.

2. In the Properties dialog, click 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.



Previous versions of the file stored on the target

File: C:\Source\Image.bmp

Versions:

Date Modified	Size
✓ 2020-06-02 / 14:52:49	7.72 MB
2020-06-02 / 14:51:18	2.60 MB
2020-06-02 / 14:50:19	2.60 MB
2020-06-02 / 14:48:23	2.22 MB
2020-06-02 / 14:47:48	1.08 MB
2020-06-02 / 14:47:03	1.08 MB

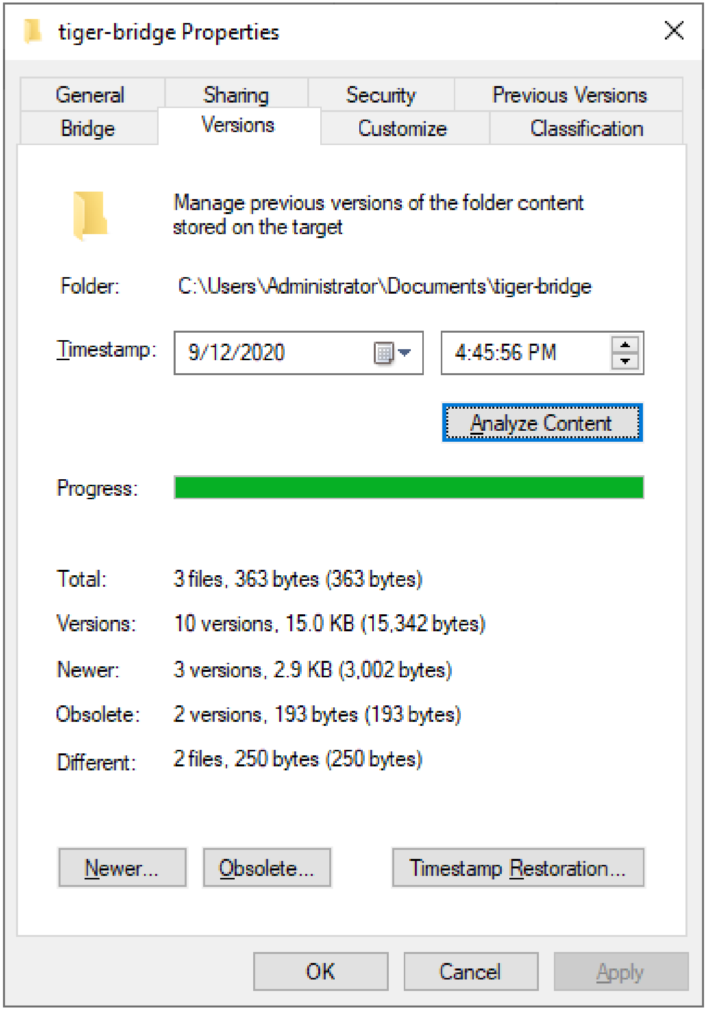
3. Select a file version in the list and click Delete to delete it from the target.

Note: You cannot delete the version, which is currently stored on your source i.e., the one with a check mark in its icon. First, restore another version on the source and then proceed with deleting the selected version.

To analyze the contents of a folder:

1. In Windows Explorer, right-click the folder and select Properties.
2. In the Properties dialog, click 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 the complete information.



Manage previous versions of the folder content stored on the target

Folder: C:\Users\Administrator\Documents\tiger-bridge

Timestamp: 9/12/2020 4:45:56 PM

Progress:

Total: 3 files, 363 bytes (363 bytes)

Versions: 10 versions, 15.0 KB (15,342 bytes)

Newer: 3 versions, 2.9 KB (3,002 bytes)

Obsolete: 2 versions, 193 bytes (193 bytes)

Different: 2 files, 250 bytes (250 bytes)

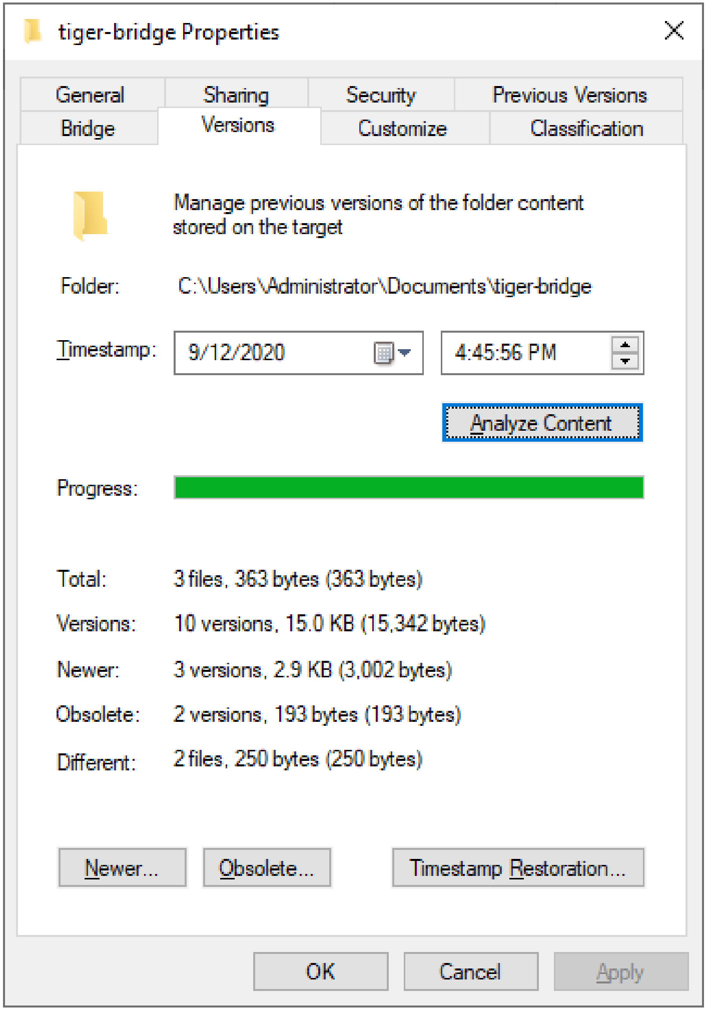
4. Tiger Bridge gives you the following information:

- 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.

To restore files in a folder to their state before the 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 the complete information.



Manage previous versions of the folder content stored on the target

Folder: C:\Users\Administrator\Documents\tiger-bridge

Timestamp: 9/12/2020 4:45:56 PM

Progress:

Total: 3 files, 363 bytes (363 bytes)

Versions: 10 versions, 15.0 KB (15,342 bytes)

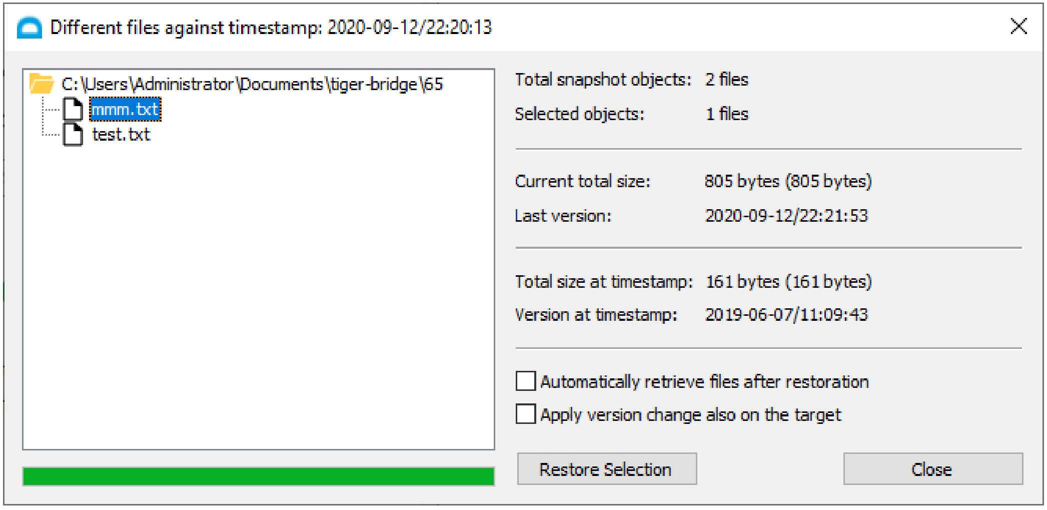
Newer: 3 versions, 2.9 KB (3,002 bytes)

Obsolete: 2 versions, 193 bytes (193 bytes)

Different: 2 files, 250 bytes (250 bytes)

4. Click “Timestamp Restoration...”.

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.



C:\Users\Administrator\Documents\tiger-bridge\65
- mmm.txt
- test.txt

Total snapshot objects: 2 files

Selected objects: 1 files

Current total size: 805 bytes (805 bytes)

Last version: 2020-09-12/22:21:53

Total size at timestamp: 161 bytes (161 bytes)

Version at timestamp: 2019-06-07/11:09:43

□ Automatically retrieve files after restoration

□ Apply version change also on the target

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 to thesource 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.

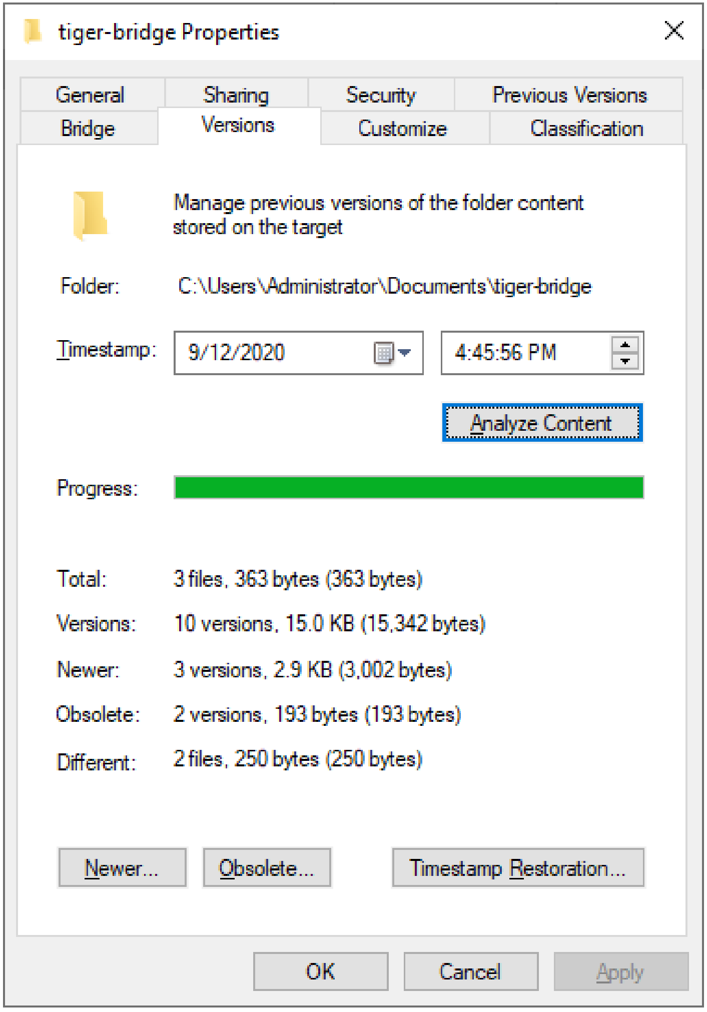
To delete obsolete versions of files in a folder:

1. In Windows Explorer, right-click the folder and select Properties.

2. In the Properties dialog, click 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 the complete information.



Manage previous versions of the folder content stored on the target

Folder: C:\Users\Administrator\Documents\tiger-bridge

Timestamp: 9/12/2020 4:45:56 PM

Total: 3 files, 363 bytes (363 bytes)

Versions: 10 versions, 15.0 KB (15,342 bytes)

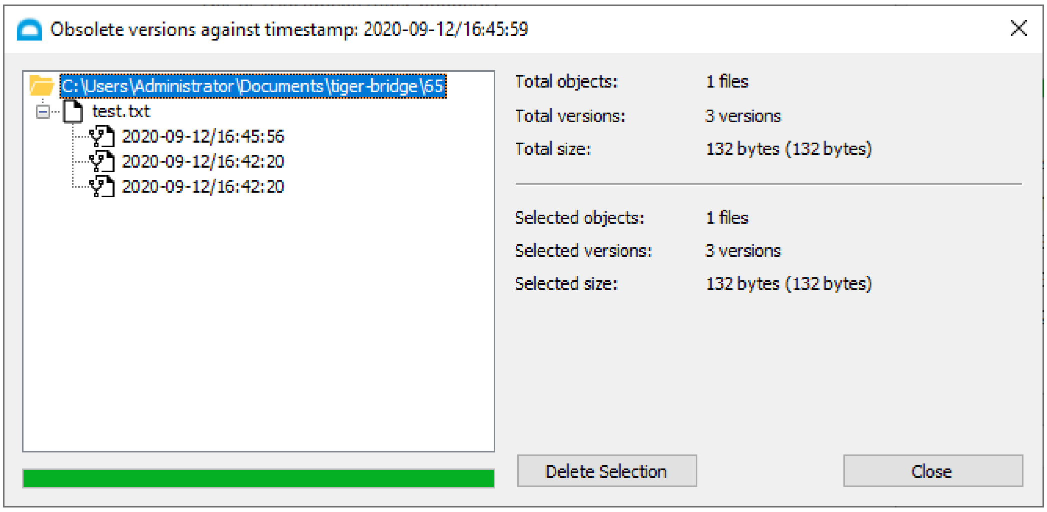
Newer: 3 versions, 2.9 KB (3,002 bytes)

Obsolete: 2 versions, 193 bytes (193 bytes)

Different: 2 files, 250 bytes (250 bytes)

4. Click Obsolete.

Tiger Bridge displays a dialog, listing all versions of a file that have been replicated before the selected time and date, giving you information about the size of each version as well as the total size of all versions.


Obsolete versions against timestamp: 2020-09-12/16:45:59

C:\Users\Administrator\Documents\tiger-bridge\65
test.txt
2020-09-12/16:45:56
2020-09-12/16:42:20
2020-09-12/16:42:20

Total objects: 1 files
Total versions: 3 versions
Total size: 132 bytes (132 bytes)

Selected objects: 1 files
Selected versions: 3 versions
Selected size: 132 bytes (132 bytes)

5. Do one of the following:

- Select a whole folder, to delete all versions of all its files that have been replicated before the selected date and time.
- Select a file, to delete all its versions that have been replicated before the selected date and time.
- Select a file version, to delete just this version of the file.

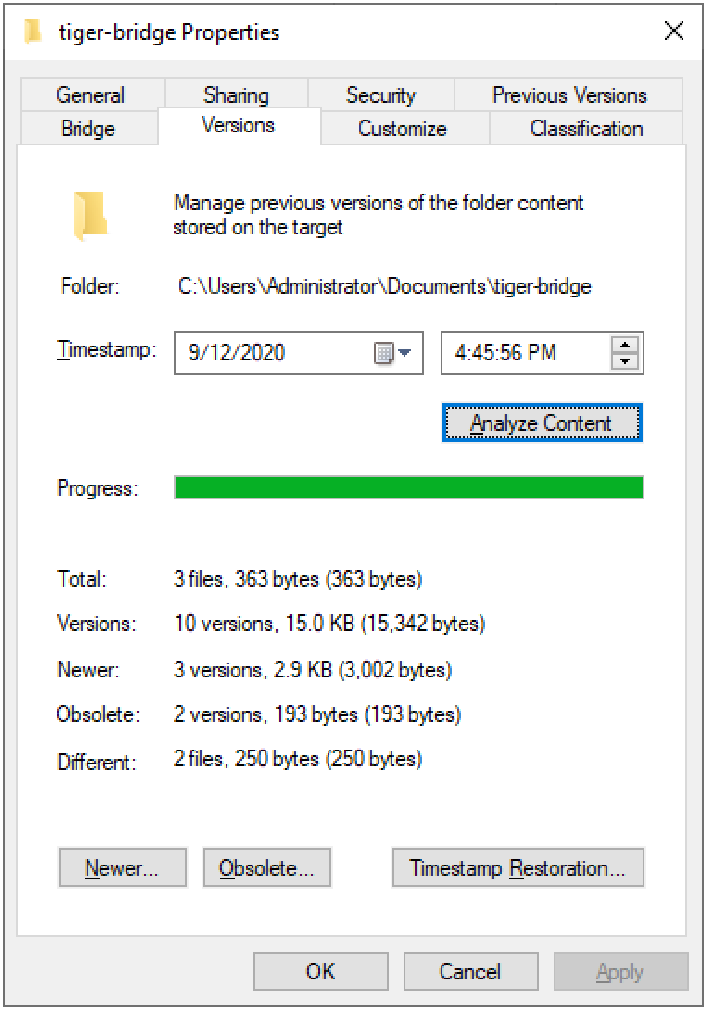
Important: You cannot delete a file version, which is currently linked to the file on the source. To do this you need to link the source file to another version. Also, you cannot delete a version of a file if it is the only one on the target.

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, click 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 the complete information.



tiger-bridge Properties

Manage previous versions of the folder content stored on the target

Folder: C:\Users\Administrator\Documents\tiger-bridge

Timestamp: 9/12/2020 4:45:56 PM

Total: 3 files, 363 bytes (363 bytes)

Versions: 10 versions, 15.0 KB (15,342 bytes)

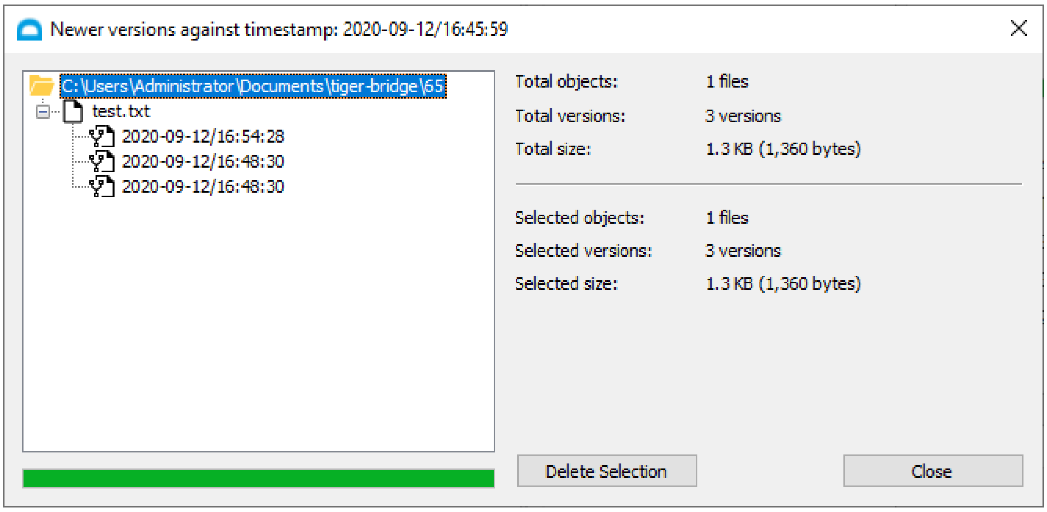
Newer: 3 versions, 2.9 KB (3,002 bytes)

Obsolete: 2 versions, 193 bytes (193 bytes)

Different: 2 files, 250 bytes (250 bytes)

4. Click Newer.

Tiger Bridge displays a dialog, listing all versions of a file that have been replicated before the selected time and date, giving you information about the size of each version as well as the total size of all versions.



Newer versions against timestamp: 2020-09-12/16:45:59

C:\Users\Administrator\Documents\tiger-bridge\65
test.txt
2020-09-12/16:54:28
2020-09-12/16:48:30
2020-09-12/16:48:30

Total objects: 1 files

Total versions: 3 versions

Total size: 1.3 KB (1,360 bytes)

Selected objects: 1 files

Selected versions: 3 versions

Selected size: 1.3 KB (1,360 bytes)

5. Do one of the following:

- Select a whole folder, to delete all versions of all its files that have been replicated after the selected date and time.
- Select a file, to delete all its versions that have been replicated after the selected date and time.
- Select a file version, to delete just this version of the file.

Important: You cannot delete a file version, which is currently linked to the file on the source. To do this you need to link the source file to another version. Also, you cannot delete a version of a file if it is the only one on the target.

6. Click Delete Selection.

Monitor Tiger Bridge

Each of the Tiger Bridge interfaces allows you to monitor the status of the product, the operations, and the managed data.

Use the Configuration and Tray Icon for Monitoring

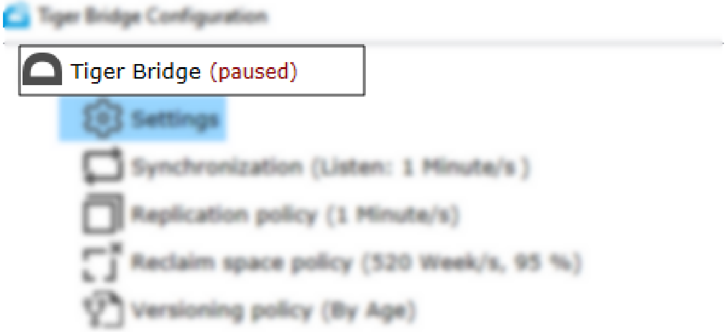
Monitor Tiger Bridge in the Configuration

You can use the Tiger Bridge Configuration to:

- monitor the status of Tiger Bridge (running or paused)
- view current used capacity per all sources
- view the percentage of replicated data per source.

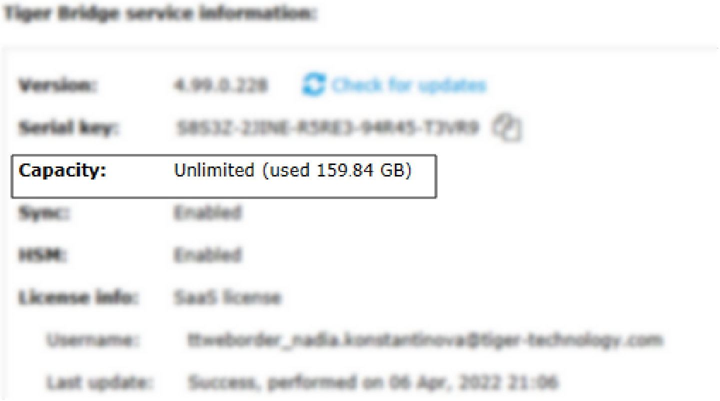
To monitor the status of Tiger Bridge:

In the left pane of the Configuration, check the status field next to Tiger Bridge.


Tiger Bridge Configuration
Tiger Bridge (paused)
Settings
Synchronization (Listen: 1 Minute/s)
Replication policy (1 Minute/s)
Reclaim space policy (520 Week/s, 95 %)
Versioning policy (By Age)

To monitor the license capacity usage:

1. In the left pane of the Configuration, click Tiger Bridge.
2. In the right pane, check the Capacity field.



Tiger Bridge service information:

Version: 4.99.0.228 Check for updates

Serial key: S8532-2JINE-R5RE3-94R45-T3VR9

Capacity: Unlimited (used 159.84 GB)

Sync: Enabled

HSM: Enabled

License info: SaaS license

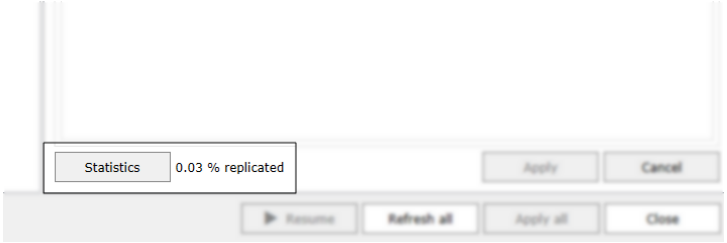
Username: ttweborder_nadia.konstantinova@tiger-technology.com

Last update: Success, performed on 06 Apr, 2022 21:06

To monitor the percentage of replicated data per source:

1. In the left pane of the Configuration, click a source.

2. In the bottom of the right pane, check the field next to the Statistics button.



Monitor Tiger Bridge Status and Activity Using the Tray Icon

Use the Tiger Bridge tray icon to monitor the status of Tiger Bridge and the automatic data replication queue.

Icon	Tiger Bridge Status
🟦	Tiger Bridge is activated, and automatic operations are running.
🟦	The queue with files scheduled for replication is being processed. Right-click the tray icon and then click “Show pending files” to view the full list.
🟦🔴	Replication of some files in the queue has failed. Refer to the Tiger Bridge logs for more detailed information. Right-click the tray icon and then click “Show failed files” to view the full list.
🟦▶	Tiger Bridge is retrieving files from the target or rehydrating offline files from the archival tier.
🟥	The Tiger Bridge service is not running.
🟨	Tiger Bridge is either not activated or your license has expired.
⬜	Automatic Tiger Bridge operations are paused.

Monitor Data in Tiger Bridge Explorer

Tiger Bridge Explorer allows you to browse your data filtering it by source, data status, and target tier. Once you apply the filters you want to use, the right pane of Tiger Bridge Explorer displays all files in the browsed path that match the filters you have applied. The files are listed alphabetically in descending order. You can save the list of any browsed path as a text file. You also perform bulk operations on a selected file or all files in a selected source/folder, by following the steps in Perform Manual Data Lifecycle Operations on page 129.

Additionally, you can open any browsed path directly in Windows Explorer and manage the files there.

By default, you can use two predefined filters:

- “Show failed files” - opens Tiger Bridge Explorer displaying all files on all sources the replication of which has failed.
- “Show pending files” - opens Tiger Bridge Explorer displaying all files on all sources queued for replication.

By default, these predefined filters use “Flat Listing” meaning that to view all failed or pending files in a selected source you need to browse its hierarchical structure. If you remove the “Flat listing” filter, selecting a source in the left pane displays all failed or pending files from all sub-folders of the source in the right pane.

You can filter data displayed in Tiger Bridge Explorer, by applying any of the following combinations:

- Source – select to display data on just one source, just selected sources, or all sources.
- Data status:

  ✓ Unprocessed – displays all files that are not yet replicated or queued for replication, and not in an excluded location on the source

  ✓ Pending – displays all files queued for automatic replication, but without any copy on the target

  ✓ Modified – displays all files queued for automatic replication that have a copy on the target, but are modified on the source

  ✓ Replicated – displays all files that have copies both on the source and the target, except reclaimed files and files in excluded locations

  ✓ Reclaimed – displays all files that have copies only on the target i.e. replicated files replaced by stubs on the source

  ✓ Excluded – displays all files that are not automatically managed by Tiger Bridge and that you can replicate and reclaim only manually

  ✓ Failed – displays all files that could not be replicated. These files are not automatically queued for replication until you restart Tiger Bridge (for more information, refer to Manage Files That Have Failed to Replicate on page 130).
- Target tiers:

  ✓ Unknown – displays the files having copies on a non-object storage target

  ✓ Hot – displays the files having copies on the equivalent of the hot tier of the target

  ✓ Cool – displays the files having copies on the equivalent of the cool tier of the target

  ✓ Archive – displays the files having copies on the equivalent of the archival tier of the target
- **Note:** When no tier check box is selected, Tiger Bridge Explorer displays data on all available tiers.
- Flat listing:

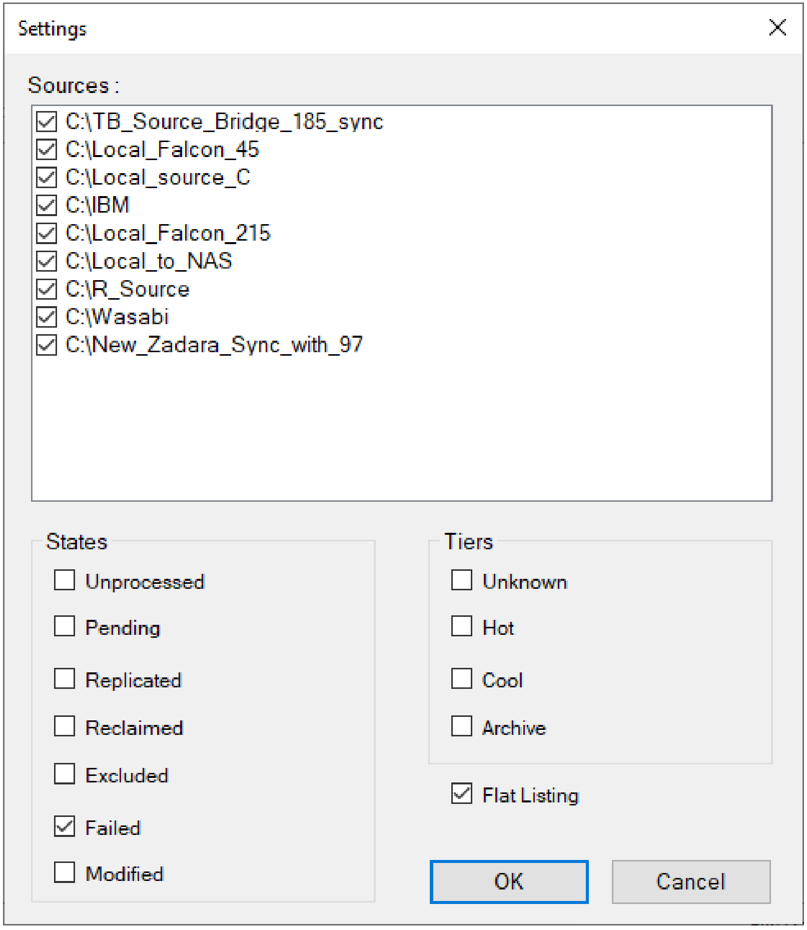
  ✓ Selected – displays just the files in the root of the selected folder. To view files in any of the sub-folders you need to browse them in the left pane.

✓ Cleared – displays all files in the selected folder and all its sub-folders in the right pane, without having to browse the hierarchical structure of the source.

Note: The statistics about the number of new, modified, replicated, and failed files in the status bar at the bottom of Tiger Bridge Explorer displays the total numbers about a selected source.

To filter data displayed in Tiger Bridge Explorer:

1. Double-click the Tiger Bridge tray icon.
2. In Tiger Bridge Explorer, click Settings.



Settings

Sources :

☑ C:\TB_Source_Bridge_185_sync
☑ C:\Local_Falcon_45
☑ C:\Local_source_C
☑ C:\IBM
☑ C:\Local_Falcon_215
☑ C:\Local_to_NAS
☑ C:\R_Source
☑ C:\Wasabi
☑ C:\New_Zadara_Sync_with_97

States

☐ Unprocessed
☐ Pending
☐ Replicated
☐ Reclaimed
☐ Excluded
☑ Failed
☐ Modified

Tiers

☐ Unknown
☐ Hot
☐ Cool
☐ Archive

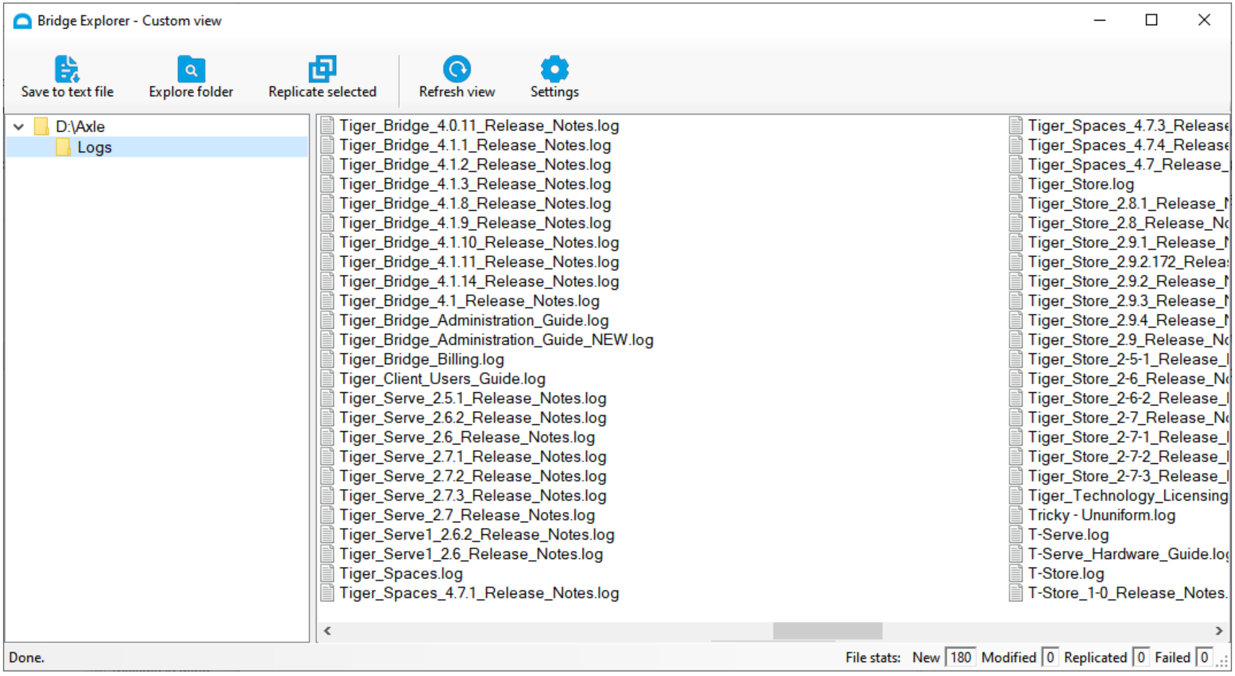
☑ Flat Listing

3. Select or clear the desired check boxes and click OK.

To save a list of the filtered results:

1. Double-click the Tiger Bridge tray icon.
2. In Tiger Bridge Explorer, click Settings and apply the desired filters.

3. In the left pane of Tiger Bridge Explorer, navigate to the desired source or any of its sub-folders to display the filtered results in the right pane.



```
Tiger_Bridge_4.0.11_Release_Notes.log
Tiger_Bridge_4.1.1_Release_Notes.log
Tiger_Bridge_4.1.2_Release_Notes.log
Tiger_Bridge_4.1.3_Release_Notes.log
Tiger_Bridge_4.1.8_Release_Notes.log
Tiger_Bridge_4.1.9_Release_Notes.log
Tiger_Bridge_4.1.10_Release_Notes.log
Tiger_Bridge_4.1.11_Release_Notes.log
Tiger_Bridge_4.1.14_Release_Notes.log
Tiger_Bridge_4.1_Release_Notes.log
Tiger_Bridge_Administration_Guide.log
Tiger_Bridge_Administration_Guide_NEW.log
Tiger_Bridge_Billing.log
Tiger_Client_Users_Guide.log
Tiger_Serve_2.5.1_Release_Notes.log
Tiger_Serve_2.6.2_Release_Notes.log
Tiger_Serve_2.6_Release_Notes.log
Tiger_Serve_2.7.1_Release_Notes.log
Tiger_Serve_2.7.2_Release_Notes.log
Tiger_Serve_2.7.3_Release_Notes.log
Tiger_Serve_2.7_Release_Notes.log
Tiger_Serve1_2.6.2_Release_Notes.log
Tiger_Serve1_2.6_Release_Notes.log
Tiger_Spaces.log
Tiger_Spaces_4.7.1_Release_Notes.log
Tiger_Spaces_4.7.3_Release
Tiger_Spaces_4.7.4_Release
Tiger_Spaces_4.7_Release_
Tiger_Store.log
Tiger_Store_2.8.1_Release_
Tiger_Store_2.8_Release_N
Tiger_Store_2.9.1_Release_
Tiger_Store_2.9.2.172_Relea
Tiger_Store_2.9.2_Release_
Tiger_Store_2.9.3_Release_
Tiger_Store_2.9.4_Release_
Tiger_Store_2.9_Release_N
Tiger_Store_2-5-1_Release_
Tiger_Store_2-6_Release_N
Tiger_Store_2-6-2_Release_
Tiger_Store_2-7_Release_N
Tiger_Store_2-7-1_Release_
Tiger_Store_2-7-2_Release_
Tiger_Store_2-7-3_Release_
Tiger_Technology_Licensing
Tricky - Ununiform.log
T-Serve.log
T-Serve_Hardware_Guide.lo
T-Store.log
T-Store_1-0_Release_Notes.
```

Done. File stats: New 180 Modified 0 Replicated 0 Failed 0

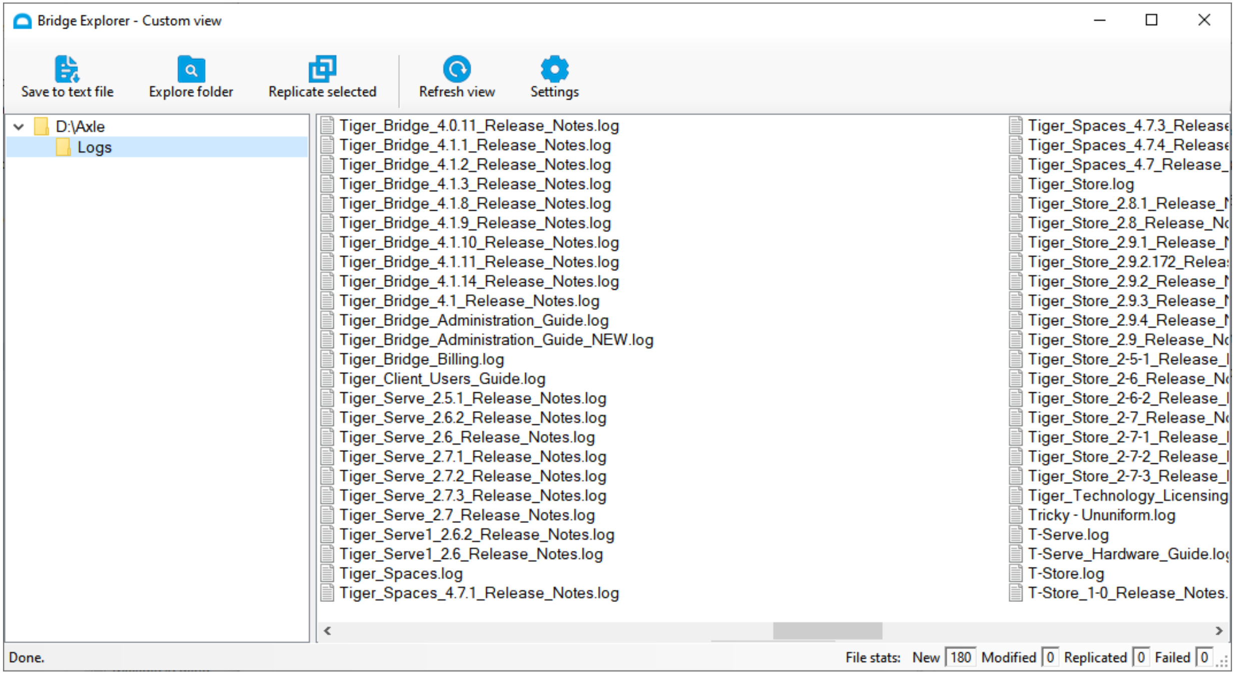
4. Click “Save to text file” and choose where to save the list.

To open the browsed path in Windows Explorer:

1. Double-click the Tiger Bridge tray icon.

2. In Tiger Bridge Explorer, click Settings and apply the desired filters.

3. In the left pane of Tiger Bridge Explorer, navigate to the desired source or any of its sub-folders to display the filtered results in the right pane.



```
Tiger_Bridge_4.0.11_Release_Notes.log
Tiger_Bridge_4.1.1_Release_Notes.log
Tiger_Bridge_4.1.2_Release_Notes.log
Tiger_Bridge_4.1.3_Release_Notes.log
Tiger_Bridge_4.1.8_Release_Notes.log
Tiger_Bridge_4.1.9_Release_Notes.log
Tiger_Bridge_4.1.10_Release_Notes.log
Tiger_Bridge_4.1.11_Release_Notes.log
Tiger_Bridge_4.1.14_Release_Notes.log
Tiger_Bridge_4.1_Release_Notes.log
Tiger_Bridge_Administration_Guide.log
Tiger_Bridge_Administration_Guide_NEW.log
Tiger_Bridge_Billing.log
Tiger_Client_Users_Guide.log
Tiger_Serve_2.5.1_Release_Notes.log
Tiger_Serve_2.6.2_Release_Notes.log
Tiger_Serve_2.6_Release_Notes.log
Tiger_Serve_2.7.1_Release_Notes.log
Tiger_Serve_2.7.2_Release_Notes.log
Tiger_Serve_2.7.3_Release_Notes.log
Tiger_Serve_2.7_Release_Notes.log
Tiger_Serve1_2.6.2_Release_Notes.log
Tiger_Serve1_2.6_Release_Notes.log
Tiger_Spaces.log
Tiger_Spaces_4.7.1_Release_Notes.log
Tiger_Spaces_4.7.3_Release
Tiger_Spaces_4.7.4_Release
Tiger_Spaces_4.7_Release_
Tiger_Store.log
Tiger_Store_2.8.1_Release_
Tiger_Store_2.8_Release_N
Tiger_Store_2.9.1_Release_
Tiger_Store_2.9.2.172_Relea
Tiger_Store_2.9.2_Release_
Tiger_Store_2.9.3_Release_
Tiger_Store_2.9.4_Release_
Tiger_Store_2.9_Release_N
Tiger_Store_2-5-1_Release_
Tiger_Store_2-6_Release_N
Tiger_Store_2-6-2_Release_
Tiger_Store_2-7_Release_N
Tiger_Store_2-7-1_Release_
Tiger_Store_2-7-2_Release_
Tiger_Store_2-7-3_Release_
Tiger_Technology_Licensing
Tricky - Ununiform.log
T-Serve.log
T-Serve_Hardware_Guide.lo
T-Store.log
T-Store_1-0_Release_Notes.
```

Done. File stats: New 180 Modified 0 Replicated 0 Failed 0

4. Click “Explore folder” to open the browsed path in Windows Explorer.

Monitor Data Status Using the Shell Extension and Windows Explorer

Monitor Data Status Using the Tiger Bridge Icon Overlays

The Tiger Bridge icon overlays provide you with visual means for monitoring managed data status while you browse it in Windows Explorer. You can enable or disable the overlays, by following the steps in Manage Shell Extension Icon Overlays on page 103.

Tiger Bridge allows you to adapt the icon overlays to the needs of your workflow. Thus, you can choose to use the overlays with their legacy statuses, used in Tiger Bridge versions before 5.0, or use the full set of icon overlays, which covers more states of data including transitional ones (queued for replication, failed to replicate, currently inaccessible, etc.). The full set of icon overlays also distinguishes between the expected monitoring purposes depending on whether you have configured your sources with automatic replication (allowing you to easily locate data that is not yet replicated) or without automatic replication (allowing you to easily locate data that you have manually replicated).

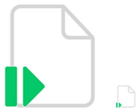
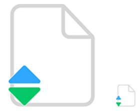
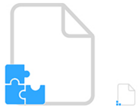
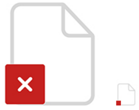
To select the icon overlays statuses that you will use:

1. Right-click the Tiger Bridge tray icon.
2. Do one of the following:

- Select the “Use legacy status icons” check box to use the icon overlays with their legacy statuses.
- Clear the “Use legacy status icons” check box to use the full set.

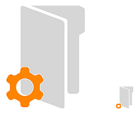
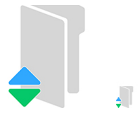
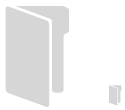
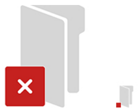
File Icon Overlays

File Icon	With replication policy	Without replication policy	Legacy status
🗋	This is a replicated file, which has a copy on both the source and the target.	The file is not replicated and has a copy only on the source.	
🗋 ✓	-	This is a replicated file, which has a copy on both the source volume and the target.	
🗋 +	This is a nearline file, reclaimed from your source and with a copy on the hot/cool tier of the target i.e., it can be retrieved on demand from the target by attempting to open it on the source.		
🗋 ❄	This file has a copy only on the target and cannot be retrieved immediately for one of the following reasons: • This is an offline file (its copy is on the archival tier of the target) and to retrieve it on the source you must first rehydrate it. • This is a nearline file (its copy is on the hot/cool tier of the target), but at the moment the		This is an offline file (its copy is on the archival tier of the target) and to retrieve it on the source you must first rehydrate it.

File Icon	With replication policy	Without replication policy	Legacy status
	target is inaccessible, and you cannot retrieve it to the source.		
	The file is queued for automatic replication. This can be an already replicated file, which has been modified and needs to be replicated again.	-	-
	A Tiger Bridge operation is being performed on the file at the moment. As some operations like "Make file nearline" or "Make file offline" are executed momentarily, this icon overlay is usually displayed when the file is being replicated or retrieved.		
	This is a nearline file, which has been retrieved to the source only partially. For more information about partial data retrieval, refer to Progressive File Retrieval on page 118.		-
	Replication of the file has failed.		-

Folder Icon Overlays

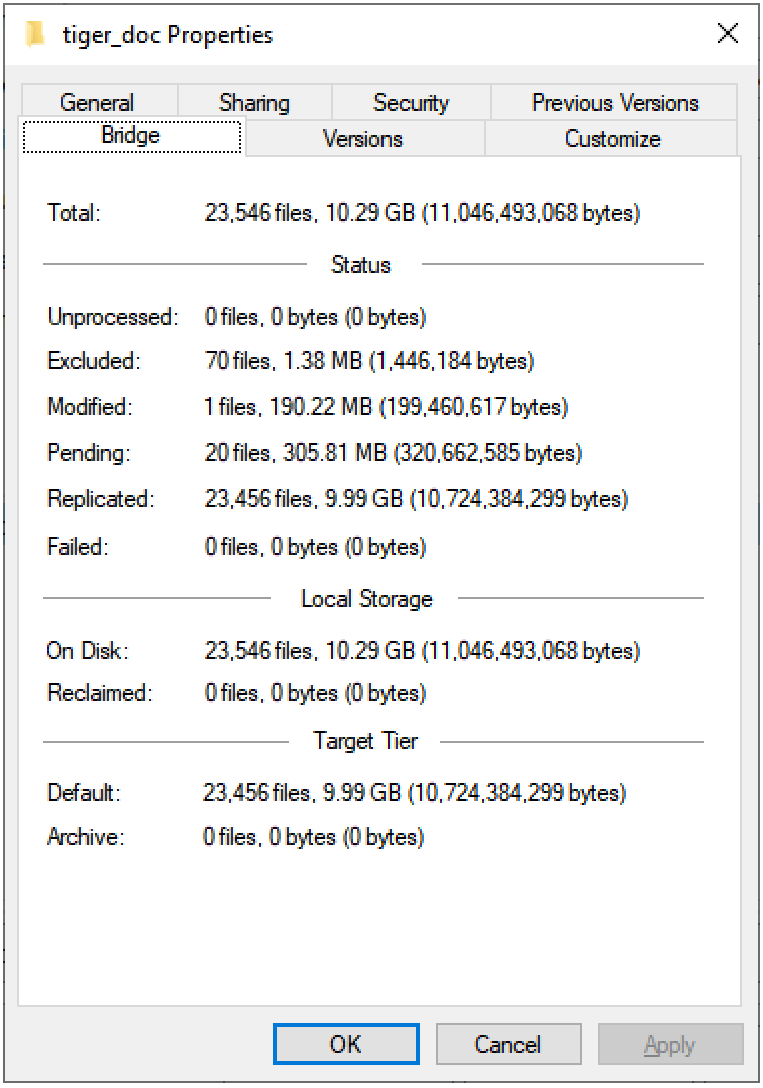
Folder status unlike file status often designates a combination of statuses as it may contain heterogeneous files.

Icon	With replication policy	Without replication policy	Legacy status
	Tiger Bridge is currently scanning the contents of the folder and is unable to display its status. After the scan finishes it will display any of the icon overlays below.		
	A Tiger Bridge operation is being performed on at least one file in the folder at the moment. After the scheduled operations are finished it will display any of the icon overlays below.		
	All files in the folder are replicated and have copies both on the source and the target, or the folder is empty.	All files in the folder are available only on the source.	
	The replication of at least one file in the folder has failed.		-

Icon	With replication policy	Without replication policy	Legacy status
❄	The folder contains at least one file, which has a copy only on the target and cannot be retrieved immediately for one of the following reasons: • This is an offline file (its copy is on the archival tier of the target) and to retrieve it on the source you must first rehydrate it. • This is a nearline file (its copy is on the hot/cool tier of the target), but at the moment the target is inaccessible, and you cannot retrieve it to the source.		The folder contains at least one offline file.
▶	The folder contains at least one file queued for replication – either a file, which has never been replicated, or a replicated file, which has been modified.	-	-
🧩	The folder contains both replicated and nearline files.	The folder contains at least one nearline file and at least one file with normal, replicated or with pending operations status.	-
⊞	All files in the folder are nearline i.e., they have copies only on the hot/cool tier of the target and can be retrieved to the source on demand. This icon overlay is also displayed for a folder containing only empty files i.e. indicating that no storage needs to be reclaimed.		
✓	-	All files in the folder are replicated and have copies both on the source and the target, or the folder is empty.	

Monitor Data Management Statistics

The Bridge tab of the Properties dialog of a source folder or any of its sub-folders displays detailed statistics about the number of files and their size. The statistics are updated dynamically, allowing you to keep track of data retrieval from the target, for example. You can display the Bridge tab of the Properties dialog of a source folder directly from the Tiger Bridge Configuration by selecting the source and then clicking Statistics in the right pane.



Total: 23,546 files, 10.29 GB (11,046,493,068 bytes)

Status

Unprocessed: 0 files, 0 bytes (0 bytes)

Excluded: 70 files, 1.38 MB (1,446,184 bytes)

Modified: 1 files, 190.22 MB (199,460,617 bytes)

Pending: 20 files, 305.81 MB (320,662,585 bytes)

Replicated: 23,456 files, 9.99 GB (10,724,384,299 bytes)

Failed: 0 files, 0 bytes (0 bytes)

Local Storage

On Disk: 23,546 files, 10.29 GB (11,046,493,068 bytes)

Reclaimed: 0 files, 0 bytes (0 bytes)

Target Tier

Default: 23,456 files, 9.99 GB (10,724,384,299 bytes)

Archive: 0 files, 0 bytes (0 bytes)

The statistics are divided into the following categories:

Total – the total number of files and their size

Unprocessed – the number and size of files not yet queued for replication

Excluded – the number and size of files excluded from automatic replication – files Tiger Bridge does not manage by default as well as files from locations on your source you have specified as excluded.

Tip: Deduct the size of excluded files on the source from the total size of the files to calculate the size of managed data for the source.

Modified – the number and size of already replicated files that have been modified and need to be replicated again

Pending – the number and size of files currently queued for replication

Replicated – the number and size of replicated files

Failed – the number and size of files the replication of which has failed

Local storage:

On disk – the number and size of files located on the local storage

Reclaimed – the number and size of reclaimed files available only on the target

Target Tier:

Default – the number and size of files available on the nearline tier of the target

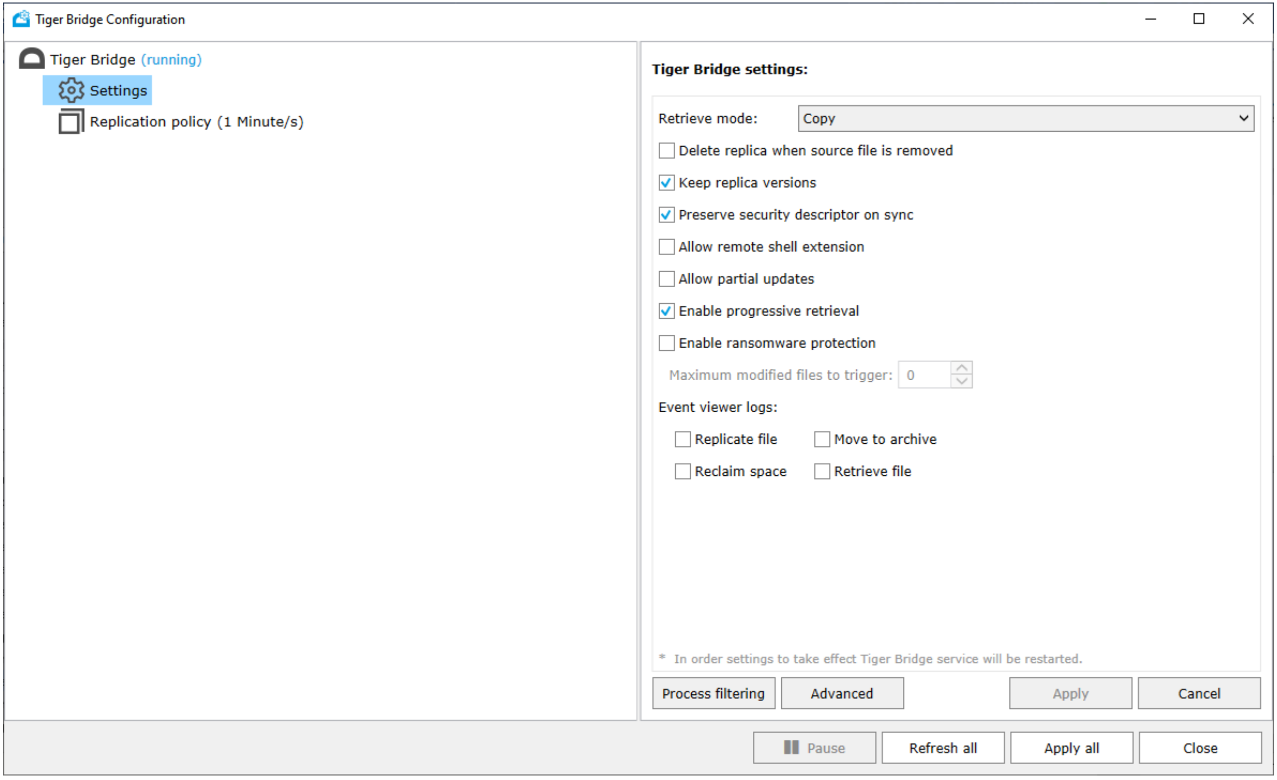
Archive – the number and size of files available from the archival tier of the target

Monitor Tiger Bridge in the Event Viewer

To let you monitor its activity, Tiger Bridge logs all target/source connectivity events in the Windows Event Viewer.

You can also configure Tiger Bridge to log an event each time a data lifecycle operation is performed, by following these steps:

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



Tiger Bridge Configuration

Tiger Bridge (running)

Settings

Replication policy (1 Minute/s)

Tiger Bridge settings:

Retrieve mode: Copy

☐ Delete replica when source file is removed

☑ Keep replica versions

☑ Preserve security descriptor on sync

☐ Allow remote shell extension

☐ Allow partial updates

☑ Enable progressive retrieval

☐ Enable ransomware protection

Maximum modified files to trigger: 0

Event viewer logs:

☐ Replicate file ☐ Move to archive

☐ Reclaim space ☐ Retrieve file

* In order settings to take effect Tiger Bridge service will be restarted.

2. In the right pane, 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.
- Clear the check box of an operation, to prevent Tiger Bridge from outputting logs for it in Windows Event Viewer.

3. Click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

You can easily navigate to the logs in the Event Viewer by right-clicking the Tiger Bridge tray icon and selecting “Open Event Viewer” in the context menu. Tiger Bridge logs three types of events in the Windows Event Viewer:

Information — logs information about successfully performed operations.

Success - logs information about successfully performed operations.

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.

All of the above are also displayed as pop-up notifications by the system.

You can find a detailed description of the logs generated by Tiger Bridge in Appendix 2: Tiger Bridge Logs on page 198.

Appendix 1: Tiger Bridge Command-line Interface

Activate Tiger Bridge

View Activation Status

To view the activation status of Tiger Bridge

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli license info
```

Activate Tiger Bridge Using a SaaS License

To activate Tiger Bridge using a SaaS license

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli license saas <order name> <password>
```

Example:

```
tiercli license saas 710637_user@company.com p@sSwOrd
```

Reactivate Tiger Bridge with New SaaS License Credentials

To re-activate Tiger Bridge with new SaaS license credentials

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli license saas deconfigure

tiercli license saas <order name> <password>
```

Example:

```
tiercli license saas deconfigure

tiercli license saas 810636_user@company.com dOrwSs@p
```

Activate Tiger Bridge with a Software Activation Key

To activate Tiger Bridge with a software activation key

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

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

Example:

```
tiercli license soft 5ZRPF-ALZ8D-ZV7WZ-S271N-VNTCW
```

Activate Tiger Bridge with a Software-protection Dongle

To activate Tiger Bridge with a software-protection dongle

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli license hasp <path to lic file >
```

Example:

```
tiercli license hasp C:\Users\user\Downloads\license.lic
```

Configure Tiger Bridge

View Current Tiger Bridge Configuration

To view the current Tiger Bridge configuration

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config show
```

Add a NAS Source

To add a NAS source

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <control folder path> naas <sharepath> <username> <password>
```

Example:

```
tiercli config D:\NasSource naas \\testsrv\share test 1234
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Pair Source and Target

Pair Source with a Microsoft Azure Target

Using Account Key or SAS Token

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
   tiercli config <source or control folder path> target azure <account_name>
<account_key or SAS token> <blob_endpoint>

   tiercli config <source or control folder path> container <container name>
```

Example:

```
   tiercli config F: target azure rwaccount
OPEkmf7v9ZHZPvNy2HWoxhDZu6QSFw0llCxam+ltoPegcAyw9YoJu8suuA/QvDPQ4WdbekaTuoDn0wmDwoZ
6pg== https://test.blob.core.windows.net/
```

```
   tiercli config F: container bridge
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
   tiercli config reload
```

Using Connection String

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following

```
   tiercli config target azure "" "" "" <connection_string>

   tiercli config <source or control folder path> container <container name>
```

Example:

```
   tiercli config F: target azure "" "" ""
DefaultEndpointsProtocol=https;AccountName=TTtests;AccountKey=LDYFUJ3gYaTT3fxnEpiq4
2buUof79pVgpnd2QLujrQ83aFTyeVbz988V4LMF1CbpAlWM7ip2SnizRRrgsmKaWj==;EndpointSuffix=
core.windows.net

   tiercli config F: container bridge
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
   tiercli config reload
```

Pair a Source with an AWS S3 Target

To pair a source with an AWS S3 target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
   tiercli config <source or control folder path> target s3 <access_id> <secret_
key> <server>

   tiercli config <source or control folder path> container <bucket name>
```

Example:

```
   tiercli config F: target s3 AKIAI633LOZJPNTZUIBA
Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4LfF s3.amazonaws.com
```

```
tiercli config F: container bridge
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Pair a Source with a Wasabi Target

To pair a source with a Wasabi target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli config <source or control folder path> target wasabi <access_id> <secret_key> <server>

tiercli config <source or control folder path> container <bucket name>
```

Example:

```
tiercli config F: target wasabi AKIAI633LOZJPNTZUIBA Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4LfF s3.eu-central-2.wasabisys.com

tiercli config F: container bridge
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Pair a Source with IBM Cloud Object Storage

To pair a source with an IBM Cloud Object Storage target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli config <source or control folder path> target icos <access_id> <secret_key> <accesser ip>

tiercli config <source or control folder path> container <bucket name>
```

Example:

```
   tiercli config F: target icos AKIAI633LOZJPNTZUIBA
Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4LfF 10.200.4.10

   tiercli config F: container bridge
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
   tiercli config reload
```

Pair a Source with a Backblaze Target

To pair a source with a Backblaze target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
   tiercli config <source or control folder path> target b2 <account_id>
<application_key>

   tiercli config <source or control folder path> container <bucket name>
```

Example:

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

   tiercli config F: container bridge
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
   tiercli config reload
```

Pair a Source with an S3-compatible Object Storage Target

To pair a source with an S3-compatible object storage target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
   tiercli config <source or control folder path> target s3compat <account_id>
<application_key>

   tiercli config <source or control folder path> container <bucket name>
```

Example:

```
   tiercli config F: target s3compat 63cd7057483d
000d6f3065670683d6250863c0746278cbbad71771

   tiercli config F: container bridge
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
   tiercli config reload
```

Pair a Source with a BlackPearl Object Storage Target

To pair a source with a Blackpearl Object Storage target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
   tiercli config <source or control folder path> target blackpearl <access_id>
<secret_key> <endpoint>

   tiercli config <source or control folder path> container <bucket name>
```

Example:

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

   tiercli config F: container bridge
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
   tiercli config reload
```

Pair a Source with a Coeus Managed Digital Content Library Target

To pair a source with a Coeus managed digital content library target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
   tiercli config <source or control folder path> target era <username> <password>
"<share path>;<archive folder>;<address>;<port>;<API Key>"
```

```
   tiercli config <source or control folder path> container <watch folder name>
```

Example:

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

   tiercli config F: container incoming
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
   tiercli config reload
```

Pair a Source with an SMB/NFS Network Share Target

To pair a source with an SMB/NFS network share target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
   tiercli config <source or control folder path> target network <sharepath>
<username> <password>

   tiercli config <source or control folder path> container <folder name>
```

Example:

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

   tiercli config F: container bridge
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
   tiercli config reload
```

Pair a Source with an NTFS or ReFS Volume Target

To pair a source with an NTFS or ReFS volume target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
   tiercli config <source or control folder path> target local set
```

```
tiercli config <source or control folder path> container <full path to folder>
```

Example:

```
tiercli config F: target local set

tiercli config F: container G:\Projects
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Configure Target Settings

Configure Target Server-side Encryption

To disable server-side encryption on the target:

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <source> sse None
```

Example:

```
tiercli config D:\test-source sse None
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To enable encryption with Amazon S3 Key (SSE-S3)

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <source> sse SSE-S3
```

Example:

```
tiercli config D:\test-source sse SSE-S3
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To enable encryption with AWS Key Management Service Key (SSE-KMS)

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <source> sse SSE-KMS [AWS KMS key ARN]
```

Example:

```
tiercli config D:\test-source sse SSE-KMS 0987dcba-09fe-87dc-65ba-ab0987654321
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To enable encryption with a customer-provided encryption key (SSE-C)

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <source> sse SSE-C <encryption key>
```

Example:

```
tiercli config D:\test-source sse SSE-C <encryption key>
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Configure the Target Hot, Cool, and Archive Tiers

To customize target tiers

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <path to source> tiers <hot> <cool> <archive>
```

Example:

```
tiercli config D:\test-source tiers "" coldline archive
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To reset to default target tiers

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config D:\test-source tiers "" "" ""
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Configure a Proxy Server for Access to the Target

To enable proxy server access to the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config global proxy <server:port> <username> <password>
```

Example:

```
tiercli config global proxy 10.200.9.16:3128 john.smith@domain.com p@33w0rD
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To disable proxy server access to the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config global proxy ""
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Configure Data Format on the Cloud

To display files with name and path in the cloud browser

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config global cloudfmt path
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To display files with object IDs in the cloud browser

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config global cloudfmt id
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Refine the List of Automatically Managed Source Locations

To configure included locations

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli config include <folder path> ... [folder path]
```

Example:

```
tiercli config include D:\test-source\new G:\source I:\projects\finished
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To clear the list of included locations

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli config include ""
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure excluded locations

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli config exclude<folder path> ... [folder path]
```

Example:

```
tiercli config include D:\test-source\temp G:\Drafts H:\
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To clear the list of excluded locations

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli config exclude ""
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Configure Data Replication

To configure the global replication policy

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli config policy replicate < interval in seconds [s], minutes [m], hours [h], days [d], weeks[w]>
```

Example:

tiercli config policy replicate 12h

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To overwrite the global replication policy for a source

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
   tiercli config <path to source> policy replicate <interval in seconds [s],
minutes [m], hours [h], days [d], weeks[w]>
```

Example:

```
   tiercli config D:\test-source policy replicate 12h
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
   tiercli config reload
```

To configure a different container for metadata replication

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
   tiercli config <path to source> meta <bucket_name> [access_id] [access_key]
```

Example:

```
   tiercli config D:\test-source meta metadata-only AKIAI633LOZJPNTZUIBA
Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4LfF
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
   tiercli config reload
```

Configure Space Reclaiming

Configure Global Reclaim Space Policy

To enable global space reclaiming

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

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

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
   tiercli config reload
```

To disable global space reclaiming

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

tiercli config policy reclaimspace turn off

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure the Reclaim Space policy File Access parameter

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config policy reclaimspace <interval in seconds [s], minutes [m], hours [h], days [d], weeks[w]>
```

Example:

```
tiercli config policy replicate 12h
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure the Reclaim Space policy Minimum File Size parameter

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config policy reclaimspace size <size in bytes [b], kilobytes [k], megabytes [m], gigabytes [g], terabytes [t]>
```

Example:

```
tiercli config policy reclaimspace size 1m
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure the Reclaim Space policy Minimum Used Space Threshold parameter

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

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

Example:

```
tiercli config policy reclaimspace minused 50
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure the Reclaim Space policy Maximum Used Space Threshold parameter

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

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

Example:

tiercli config policy reclaimspace maxused 90

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Configure Unreclaimed Portion of a File Type

To view the list of configured file types

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config policy reclaimspace ondisk show
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To add and configure a file type

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
   tiercli config policy reclaimspace ondisk add <file-extension> <offset from
beginning of the file> <length of unreclaimed portion>
```

Example:

```
tiercli config policy reclaimspace ondisk add jpg 0 1024
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To remove a file type

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config policy reclaimspace ondisk clear <file-extension>
```

Example:

```
tiercli config policy reclaimspace ondisk clear jpg
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To remove all file types

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config policy reclaimspace ondisk clear *
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Overwrite the Global Space Reclaiming for a Source

To enable Space Reclaiming for a pair of source and target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <path to source> policy reclaimspace turn on
```

Example:

```
tiercli config D:\test-source policy reclaimspace turn on
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To disable Space Reclaiming for a pair of source and target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <path to source> policy reclaimspace turn off
```

Example:

```
tiercli config D:\test-source policy reclaimspace turn off
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure a pair’s Reclaim Space policy File Access parameter

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <path to source> policy reclaimspace < interval in seconds [s], minutes [m], hours [h], days [d], weeks[w]>
```

Example:

```
tiercli config D:\test-source policy reclaimspace 1h
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure a pair’s Reclaim Space policy Minimum File Size parameter

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <path to source> policy reclaimspace size <size in bytes [b], kilobytes [k], megabytes [m], gigabytes [g], terabytes [t]>
```

Example:

```
tiercli config D:\test-source policy reclaimspace size 1m
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure a pair’s Reclaim Space policy Minimum Used Space Threshold parameter

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <path to source> policy reclaimspace minused <percentage>
```

Example:

```
tiercli config D:\test-source policy reclaimspace minused 50
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure a pair’s Reclaim Space policy Maximum Used Space Threshold parameter

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <path to source> policy reclaimspace maxused <percentage>
```

Example:

```
tiercli config D:\test-source policy reclaimspace maxused 90
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Configure Unreclaimed Portion of a File Type

To view the list of configured file types for the pair of source and target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <path to source> policy reclaimspace ondisk show
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To add and configure a file type in a pair's list

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli config <path to source> policy reclaimspace ondisk add <file-extension>
<offset from beginning of the file> <length of unreclaimed portion>
```

Example:

```
tiercli config D:\test-source policy reclaimspace ondisk add jpg 0 1024
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To remove a file type from a pair's list

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli config <path to source> policy reclaimspace ondisk clear <file-
extension>
```

Example:

```
tiercli config D:\test-source policy reclaimspace ondisk clear jpg
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To remove all file types from a pair's list

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli config <path to source> policy reclaimspace ondisk clear *
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Configure the Processes Allowed or Forbidden to Retrieve Files

To configure the processes allowed to retrieve files

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

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

Example:

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

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure the processes forbidden to retrieve files

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

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

Example:

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

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Configure Data Archiving

To enable Data Archiving

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <path to source> policy archive turn on
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To disable Data Archiving

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <path to source> policy archive turn off
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure the Data Archiving policy File Access parameter

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
   tiercli config <path to source> policy archive size <file access time in seconds
[s], minutes [m], hours [h], days [d], weeks [w]>
```

Example:

```
tiercli config D:\test-source policy archive age 12w
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure the Data Archiving policy File Size parameter

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
   tiercli config <path to source> policy archive <size in bytes [b], kilobytes
[k], megabytes [m], gigabytes [g], terabytes [t]>
```

Example:

```
tiercli config D:\test-source policy archive size 1g
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Configure Sync

Configure Global Sync Policy

Configure Global Sync Mode

To enable Listen Only Sync

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config sync mode listen
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To enable Notify Only Sync

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

tiercli config sync mode notify

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To enable both Listen and Notify Sync

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config sync mode both
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure the interval for checking for updates

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config sync listen <interval in seconds [s], minutes [m], hours [h], days [d], weeks [w]>
```

Example:

```
tiercli config sync listen 30m
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure the interval for sending notifications

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config sync notify <interval in seconds [s], minutes [m], hours [h], days [d], weeks [w]>
```

Example:

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

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To enable automatic retrieval of synchronized files

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config sync autorestore on
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To disable the automatic retrieval of synchronized files

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config sync autorestore off
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To disable Sync

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config sync mode off
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Overwrite the Sync Policy for a Source

Configure a Pair’s Sync Mode

To enable Listen Only Sync for a pair

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

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

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To enable Notify Only Sync for a pair

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

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

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To enable both Listen and Notify Sync for a pair

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

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

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To configure a pair’s Sync interval for checking for updates

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
   tiercli config <path to source> sync listen <interval in seconds [s], minutes
[m], hours [h], days [d], weeks [w]>
```

Example:

```
   tiercli config D:\test-source sync listen 30m
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
   tiercli config reload
```

To configure a pair’s Sync interval for sending notifications

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
   tiercli config <path to source> sync notify <interval in seconds [s], minutes
[m], hours [h], days [d], weeks [w]>
```

Example:

```
   tiercli config D:\test-source sync notify 1h
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
   tiercli config reload
```

To enable automatic retrieval of synchronized files for a pair

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
   tiercli config <path to source> sync autorestore on
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To disable the automatic retrieval of synchronized files for a pair

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config <path to source> sync autorestore off
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To disable Sync for a pair

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

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

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Configure File Retrieval Mode

To keep the file on the target when retrieving it on the source

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config global resmode copy
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To remove a file from the target when retrieving it on the source

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config global resmode move
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Configure File Deletion Mode

To keep a file on the target when deleting it from the source

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config global delmode off
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

To delete a file from the target when deleting it from the source

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli config global delmode on
```

Note: If you have finished editing the Tiger Bridge configuration, save your changes by executing the following:

```
tiercli config reload
```

Perform Manual Operations

To replicate data manually

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op replicate <path to a file or a whole folder>
```

Example:

```
tiercli op replicate d:\source\final-versions
```

To manually reclaim space on a source

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op offline <path to a file or a whole folder>
```

Example:

```
tiercli op offline d:\source\final-versions
```

To retrieve data from the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op restore <path to a file or a whole folder>
```

Example:

```
tiercli op restore d:\source\final-versions
```

To retrieve data from the target preserving the Last Access timestamp

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op restore -p <path to a file or a whole folder>
```

Example:

```
tiercli op restore -p d:\source\final-versions
```

To retrieve data skipping files accessed earlier than a specified time

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op restore --atime <seconds> <path to a file or a whole folder>
```

Example:

```
tiercli op restore --atime 3600 d:\source\final-versions
```

Delete Data

To delete data from both the source and the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op delete <path to a file or a whole folder>
```

Example:

```
tiercli op delete d:\source\final-versions
```

To delete data from the source keeping the replica on the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op delete -l <path to a file or a whole folder>
```

Example:

```
tiercli op delete -l d:\source\final-versions
```

To delete reclaimed files from both the source and the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op delete -o <path to a file or a whole folder>
```

Example:

```
tiercli op delete -o d:\source\final-versions
```

To delete reclaimed data from the source keeping the replica on the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

```
tiercli op delete -o -l <path to a file or a whole folder>
```

Example:

```
tiercli op delete -o -l d:\source\final-versions
```

To delete only replicated data from the source and the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

```
tiercli op delete --skip-normal yes <path to a file or a whole folder>
```

Example:

```
tiercli op delete --skip-normal yes d:\source\final-versions
```

To delete only replicated data from the source keeping the replica on the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

```
tiercli op delete -l --skip-normal yes <path to a file or a whole folder>
```

Example:

```
tiercli op delete -l --skip-normal yes d:\source\final-versions
```

Delete Data Using Time Criterion

To delete all data created, accessed, or modified before a specific timestamp

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
   tiercli op delete [-o] [-l] <path to a file or a whole folder> --end-time <Unix
epoch timestamp in seconds> --time-type <0 - Access time; 1 - Modify time; 2 -
Create time;>
```

Example (delete all reclaimed data accessed before 23 April 2022 from the source keeping the replicas on the target):

```
   tiercli op delete -o -l d:\source\final-versions --end-time 1650672000 --time-
type 0
```

To delete all data created, accessed, or modified after a specific timestamp

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
   tiercli op delete [-o] [-l] <path to a file or a whole folder> --start-time
<Unix epoch timestamp in seconds> --time-type <0 - Access time; 1 - Modify time; 2
- Create time;>
```

Example (delete all reclaimed files created after 23 April 2022 from both the source and the target):

```
   tiercli op delete -o d:\source\final-versions --start-time 1650672000 --time-
type 2
```

To delete all data created, accessed, or modified within a specific period

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
   tiercli op delete [-o] [-l] <path to a file or a whole folder> --start-time
<Unix epoch timestamp in seconds> --end-time <Unix epoch timestamp in seconds> --
time-type <0 - Access time; 1 - Modify time; 2 - Create time;>
```

Example (delete all reclaimed files modified between 23 April 2022 and 23 May 2022 from both the source and the target):

```
   tiercli op delete -o d:\source\final-versions –start-time 1650672000 --end-time
1684152601--time-type 1
```

Synchronize Source and Target Contents

To synchronize the contents of the current folder only

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op sync <path to folder>
```

Example:

```
tiercli op sync d:\source\final-versions
```

To synchronize the contents of the current folder only and retrieve data

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op sync -d <path to folder>
```

Example:

```
tiercli op sync -d d:\source\final-versions
```

To synchronize the content of the current folder and its sub-folders

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op sync -r <path to folder>
```

Example:

```
tiercli op sync -r d:\source\final-versions
```

To synchronize the content of the current folder and its sub-folders and retrieve data

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op sync -r -d <path to folder>
```

Example:

```
tiercli op sync -r -d d:\source\final-versions
```

To undelete data

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op sync -u <path to folder>
```

Example:

```
tiercli op sync -u d:\source\final-versions
```

To revert the modification on a source file to the last replicated state

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op revert <path to file or folder>
```

Example:

```
tiercli op revert d:\source\final-versions
```

Move Data Between Target Tiers

To move data to the hot tier

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op move_hot <path to file or folder>
```

Example:

```
tiercli op sync move_hot d:\source\test.txt
```

To move data to the hot tier and preserve the Last Access timestamp

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli op move_hot -p <path to file or folder>
```

Example:

```
tiercli op sync move_hot -p d:\source\test.txt
```

To move data to the cool tier

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli op move_cool <path to file or folder>
```

Example:

```
tiercli op sync move_cool d:\source\test.txt
```

To move data to the cool tier and preserve the Last Access timestamp

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli op move_cool -p <path to file or folder>
```

Example:

```
tiercli op sync move_cool -p d:\source\test.txt
```

To move data to the archive tier

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli op move_archive <path to file or folder>
```

Example:

```
tiercli op sync move_archive d:\source\test.txt
```

To move data to the archive tier and preserve the Last Access timestamp

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op move_archive -p <path to file or folder>
```

Example:

```
tiercli op sync move_archive -p d:\source\test.txt
```

Troubleshoot Data Replication and Space Reclaiming

To log missing replica and/or checksum mismatch

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op verify <path to file or folder> --logfile <path where .txt log should be created>
```

Example:

```
tiercli op verify d:\source --logfile d:\log.txt
```

To undelete a soft-deleted replica of a file from the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op verify <path to file or folder> --undelete yes
```

Example:

```
tiercli op verify d:\source\test.txt --undelete yes
```

To re-link a replicated source file to its replica on the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op verify <path to file or folder> --link yes
```

Example:

```
tiercli op verify d:\source\test.txt --link yes
```

To revert the replicated status of source file if the replica is missing from the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli op verify <path to file or folder> --clear yes
```

Example:

```
tiercli op verify d:\source\test.txt --clear yes
```

To check for the availability of reclaimed files on the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli op avail <path to file or folder>
```

Manage Manual Jobs

To list the IDs of pending jobs

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli op list p
```

To list the IDs of running jobs

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select "Run as administrator".

2. Execute the following:

```
tiercli op list a
```

To list the IDs of completed jobs

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op list c
```

To list the IDs of system jobs

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op list s
```

To specify the number of threads for executing a manual job on a file

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op verify <path to file or folder> --thread-count <threads number>
```

Example:

```
tiercli op verify d:\source\test.txt --thread-count 3
```

To view the status of a job

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op status <job ID>
```

To abort a job

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op abort <job ID>
```

Pause Operations

To pause all operations

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op pause all
```

To pause automatic policies

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op pause s
```

To pause retrieving data from the target on demand

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op pause a
```

To pause checking for updates in Sync

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op pause l
```

To pause notifying for updates in Sync

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op pause n
```

To pause replication

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op pause b
```

To pause space reclaiming

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op pause o
```

To pause data retrieval from the target

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op pause r
```

To pause data deletion

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op pause d
```

To resume all paused operations

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op pause none
```

Monitor Tiger Bridge

To monitor the data status and view checksum

1. Run Command Prompt as an administrator.

Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt, and select “Run as administrator”.

2. Execute the following:

```
tiercli op info <path to a file or a whole folder>
```

Example:

```
tiercli op info d:\source\final-versions
```

Appendix 2: 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 to 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`	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

Log Message	Description
`exceeded.`	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.
`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 a 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 a 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 a notification for a replicated file from another computer has failed. The reason for the failed operation may be a 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`	Tiger Bridge's attempt to synchronize the contents of two sources through

Log Message	Description
`<file name> failed.`	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 a 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.
`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 a 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 content on one computer when synchronizing it with the contents of another computer through a common target (Tiger BridgeSync) 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 content on one computer when synchronizing it with the contents of another computer through a common target (Tiger Bridge 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.	Check for the following: • Verify that the volume is mounted on the computer. • 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.
`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.	Check for the following: • Verify that the path to the folder added as a source is not changed (a folder is renamed or deleted, for example).

Log message	Description	Suggested action
		- 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.
`Source <path to source> cannot be loaded.`	Tiger Bridge failed to load a source because it was not meeting the source storage requirements anymore.	Check for the following: - Verify that the permissions for access to the source have not changed. Refer to Source Storage Requirements for more information. - Verify that a source on a Tiger Store-managed volume is not now mounted as a Tiger Client on the Tiger Bridge computer.
`Replication of file <path to file on source> failed.`	All attempts to replicate the specified file on the target have failed. Note: To let Tiger Bridge attempt to replicate the file again, you must restart Tiger Bridge.	Check for the following: - Make sure the file is not corrupted. - Make sure the target is still accessible and has not returned any errors.
`Retrieving file <path to file on source> <process name> from the target failed.`	All attempts to retrieve the specified file from the target have failed. **Note:** To let Tiger Bridge attempt to replicate the file again, you must restart Tiger Bridge .	Check for the following: - Make sure the target is accessible. - If the target is accessible, make sure the replicated file is not deleted from the target. - If the file is deleted and your target has versioning turned on, attempt to undelete it on the target.
`Modified files count threshold has been reached. Replication has been paused for source <path to source>.`	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. Note: Once the problem is resolved, to resume automatic Tiger Bridge operations, follow the steps in Pause/Resume Automatic	Check for the following: - Make sure that none of the files on your source is encrypted as part of a ransomware attack. - If one or more files are encrypted, restore their unencrypted versions, by following the steps in Manage Files and Folders Versions on page 134. - If none of the files is encrypted, change the ransomware protection

Log message	Description	Suggested action
	Tiger Bridge Operations on page 70.	threshold, by following the guidelines provided in Enable and Configure Ransomware Protection on page 107.
`License capacity exceeded.`	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.	Do one of the following: • Contact your Tiger Bridge reseller to exceed your license capacity. • Delete files on your source(s). For more information, refer to Tiger Bridge Licensing on page 15.