Tiger Bridge 5.0.1 Administration Guide

30 March 2023

THIRD-PARTY TRADEMARKS

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

Title: Tiger Bridge Administration Guide

Software version: 5.0.1

Date: March 30, 2023 7:01 PM

Manual Revision and Control

Revision Record

Date	Description	Page	Version
27 Jan. 2022	Initial Draft for version 5.0		

15 Nov. 2022	Additional step for verifying versioning is enabled on the target when enabling versioning in Tiger Bridge.	5.0.1
15 Nov. 2022	Added support for Azure target authentication with SAS connection string and SAS token.	5.0.1
15 Nov. 2022	Retrieving data from target tray icon status added.	5.0.1
15 Nov. 2022	Choosing virtual-hosted–style or path-style URLs for access to an S3-compatible bucket.	5.0.1
15 Nov. 2022	Selecting between protocol signature version 2 or 4 on S3-compatible targets.	5.0.1
15 Nov. 2022	Retrieving only recently accessed data command added to the command-line interface.	5.0.1
15 Nov. 2022	Fine-tune scanning of NAS sources by increasing the number of threads used steps added.	5.0.1
15 Nov. 2022	Preserving the security descriptor of retrieved files per source steps added.	5.0.1
15 Nov. 2022	Manually clearing the Windows icons cache steps added.	5.0.1

Table of Contents

Tiger Bridge 5.0.1 Administration Guide

1

Introduction to Tiger Bridge

How It Works

Tiger Bridge Interfaces

Tiger Bridge Licensing

System Requirements

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:
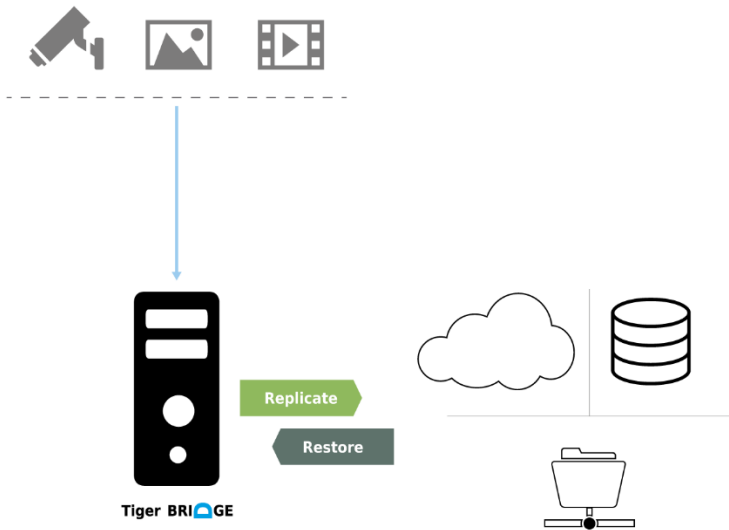
Data replication - Tiger Bridge copies a file from the source to the target. You can configure a policy, which instructs which files need to be copied to the target automatically and transparently,

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.

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 on 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 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.

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 Configure Automatic Archiving.

Active 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 Active Sync.

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.

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.

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
- lowering the costs for block storage in the cloud
- interfacing object storage
- geo replication

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

Data Protection

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

- To gain access to any Tiger Bridge functions you need to authenticate yourself as the administrator of the computer on which Tiger Bridge runs. For more information, refer to Tiger Bridge Interfaces.
- The Tiger Bridge workflow supports applying any Windows techniques for controlling access to and protecting data at rest at source level.
- Tiger Bridge does not require maximum privileges of the credentials used for access to the target and adopts the target provider's own mechanisms for ensuring credentials protection is not compromised.
- 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.

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

Tiger Bridge Interfaces

Tiger Bridge Configuration
Use the graphic user interface of the product, the Tiger Bridge Configuration to create pairs of source and target and to 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:

- Double-click the Tiger Bridge Configuration shortcut on the desktop.
- Right-click the Tiger Bridge tray icon and click "Open Tiger Bridge Configuration" in the menu.

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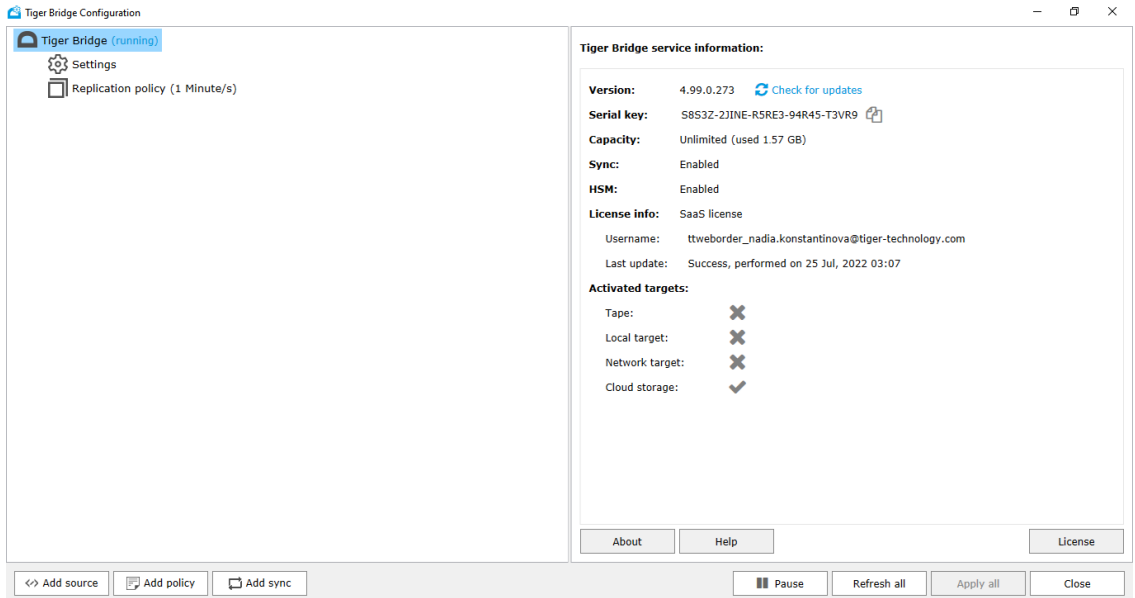
Tiger Bridge Explorer

A graphic interface browser allowing you to explore the contents of your sources filtering the results displayed 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 the Tiger Bridge .

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

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

Tiger Bridge 5.0.1 Administration Guide

- Click "Show failed files" to load the Tiger Bridge Explorer with pre-defined filter showing you all files that have failed to replicate on all sources.
- Click "Show pending files" to load the Tiger Bridge Explorer with pre-defined filter showing you all files queued for replication on all sources.
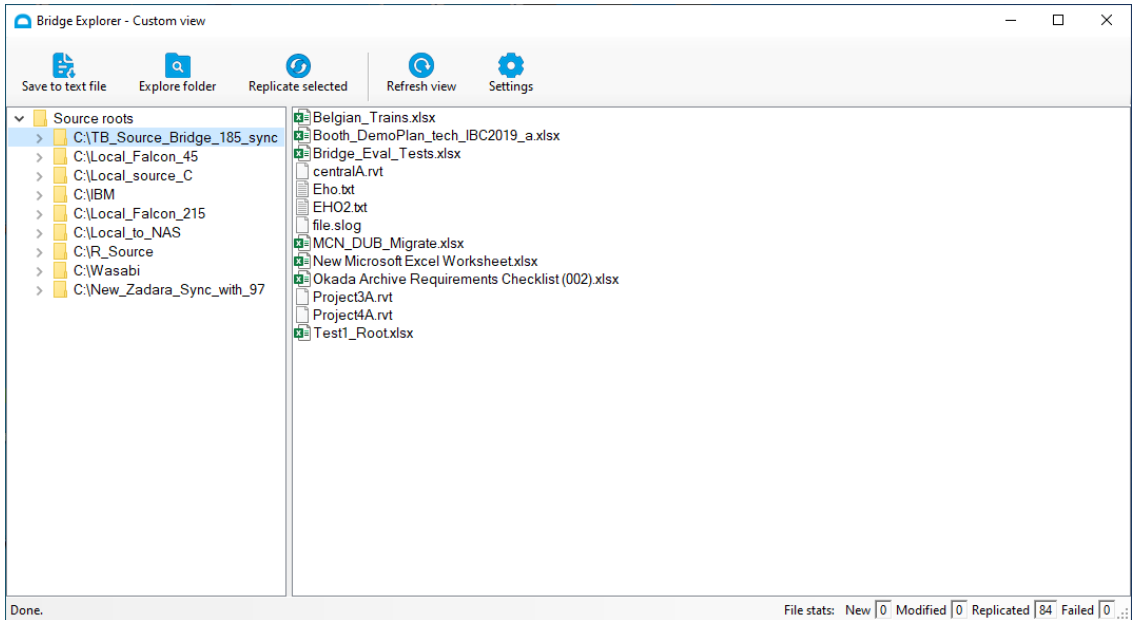
Command-line Interface

The command-line interface 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 Appendix 1: Tiger Bridge Command-line Interface.

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.

You can use the Tiger Bridge shell extension on the computer running Tiger Bridge as well as on any other remote Windows computer having access to a NAS source or to a local source exported as an SMB share. For the purpose, a Tiger Bridge administrator must allow remote shell extension access to the sources. For more information, refer to Enable Remote Shell Extension Access.

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 source or to the local control folder of a NAS source on the Tiger Bridge computer.

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

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

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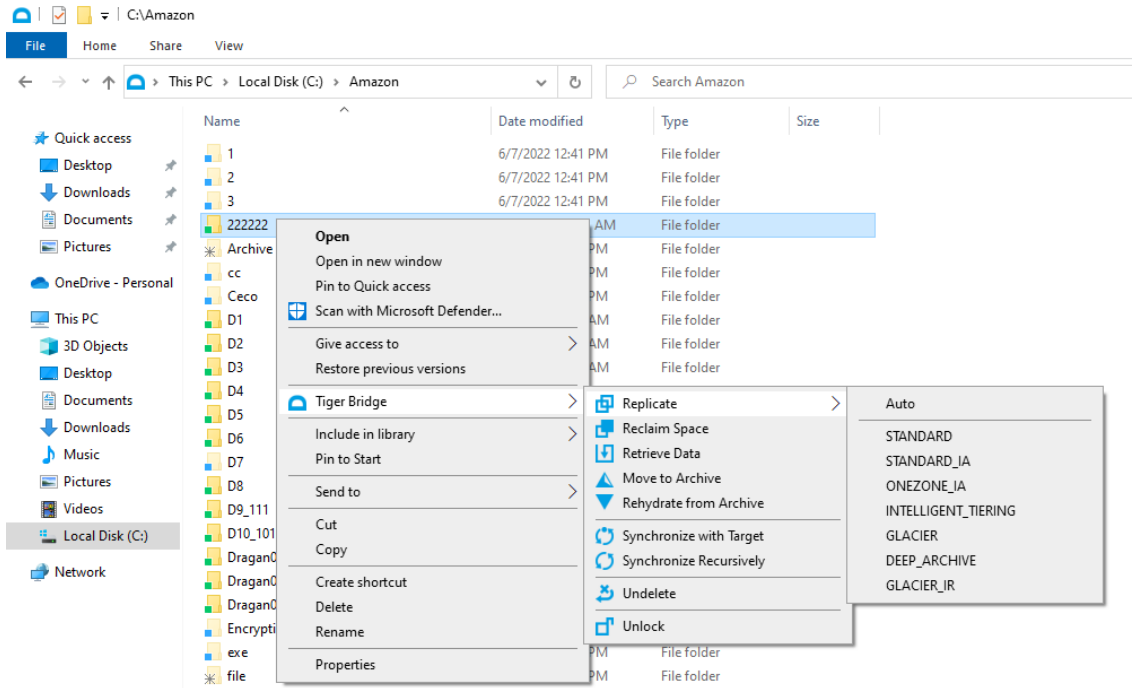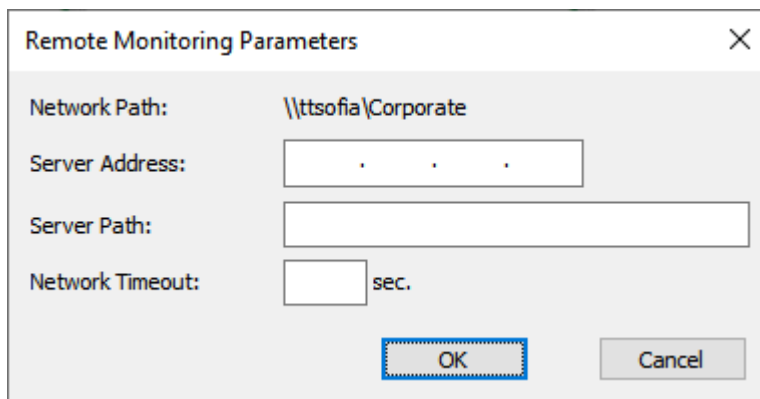
3. On remote computers, before gaining access to the Tiger Bridge shell extension commands, you need to click Remote Monitoring ▣ under Tiger Bridge:
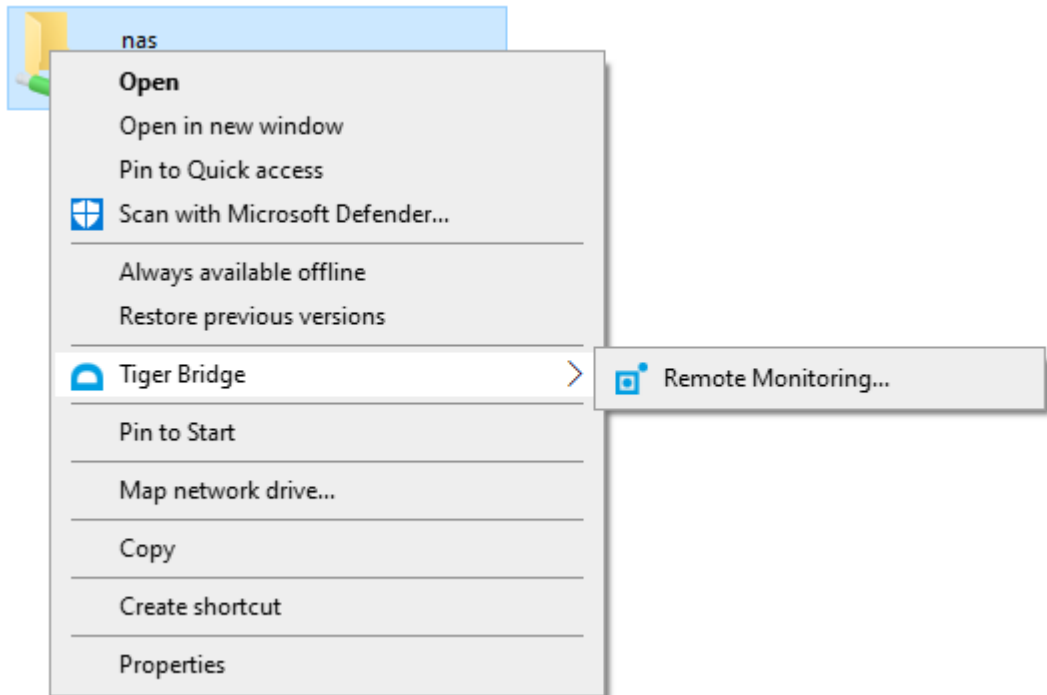
4. In Remote Monitoring Parameters, enter the following details to authorize your access to the source:

- Server address - the IP address of the computer running Tiger Bridge.

- Server path (local 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 source folder "Source", which is a sub-folder of folder "Documents" in the root of drive D on the Tiger Bridge computer, enter the following in server path: D:\Documents\Source
- 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 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 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, when 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 Event Viewer.

To access the Tiger Bridge logs in the Event Viewer:

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

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.

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 2TB of data, even if only 1TB of its files are currently replicated or replaced by stub files, the overall capacity of this source will be calculated as 2TB. 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, following the steps in Monitor Tiger Bridge in the Configuration.

System Requirements

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

- PC with 64-bit (x64) processor.
  Note: Tiger Bridge actively uses the APIs provided by the target provider. These APIs may take significant amount of CPU depending on connection and the amount of data moved. Please, refer to the minimum CPU requirements of your target provider.
- 64-bit Microsoft Windows® 7/Server 2008 R2/Windows® 8/Server 2012/Server 2012 R2/Windows® 10/Server 2016/Server 2019, 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 is approximately 100MB. Unless there's enough free space for the database, Tiger Bridge is unable to operate.

- The following TCP ports must not be blocked by the firewall on the Tiger Bridge computer or the computer managing the inbound and outbound traffic on your network:
  - o (for communication with object storage target over http connection) 80 - outbound rule only
  - o (for SaaS activation and/or communication with object storage target over https) 443 - outbound rule only
  - o (for communication with SMB network share target) 445 - outbound rule only
  - o 8536 – remote shell extension access
  - o 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.
- 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 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 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 and install them yourself, before installing Tiger Bridge. In addition, you must ensure that the "Code Signing" purpose of each 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 also set up for high availability (for more information, refer to the latest Tiger Store Administration Guide).
- All your source locations must be on Tiger Store-managed volumes, accessible with Read & Write permissions by both server nodes.
- Both server nodes must have identical access to all targets.
- The Tiger Bridge configuration must be identical on both server nodes.

Storage Requirements

Source Storage Requirements
Tiger Bridge supports the following sources:

- NTFS or ReFS volume, mounted on the computer running Tiger Bridge as a local volume with Read & Write permissions and on which the System account is granted Full Control.
  Note: You can use as a source the whole volume or just a folder on it. You cannot use as a source a folder whose parent folder is already paired with a target i.e., is set as a source itself.
- SMB or NFS share accessible on the same network as the computer, running Tiger Bridge:
  - SMB share - you need to provide a dedicated account (Active Directory domain or local account on the NAS appliance), which has Full Control (on

Windows) or Read & Write permissions (on Linux) over each share, which will be used as a source.

- o 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.

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.

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

Target Storage Requirements
Note: Refer to Target Storage Prerequisites for specific requirements about each storage type.

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

- Public cloud storage:
  - o Amazon S3 object storage (with support for all available storage classes)
  - o Microsoft Azure Blob Storage
  - o Google cloud storage
  - o IBM Cloud Object Storage
  - o Backblaze B2 Cloud Storage
  - o Google drive storage
  - o LYVE Cloud
  - o ORockCloud
  - o RSTOR Space
  - o Symply NEBULA

- o Wasabi Hot Cloud Storage
  - o S3-compatible object storage (using protocol signature version 2 or 4)
- On-premises object store with hot tier:
  - o Hitachi Content Platform (HCP)
  - o IBM COS
  - o OpenStack Swift
  - o S3-compatible object storage (using protocol signature version 2)
  - o Seagate CORTX
- On-premises object store for archive:
  - o Spectra BlackPearl Deep Storage Gateway
  - o Coeus managed digital content library
  - o FujiFilm Object Archive
- On-premises non-object store:
  - o NTFS or ReFS volume mounted on the Tiger Bridge computer with Read & Write permissions
  - o 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:	D:\Adobe Scripts [Browse]
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)   [Server-side encryption]

Default storage class:	S3 Standard-IA
Archive retrieval option:	Standard

Buckets: [List buckets]

Please refresh to load buckets

[Apply]   [Cancel]

- 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 an 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 that Tiger Bridge operates normally, if you grant the IAM user full permissions over objects in the bucket. Still, if the security policies of your organization are more restrictive, you can use the following bucket policy as a sample for granting the minimum required permissions for a bucket "bucket-name" to user "bridge_user":

```json
{
  "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 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 to replicate data directly, omitting any intermediate tiers.

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

- Select the method for retrieving data from the archival tier of your S3 object storage.

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

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

- To benefit from Tiger Bridge versioning, you must enable versioning on the target, following these instructions:
  https://docs.aws.amazon.com/AmazonS3/latest/user-guide/enable-versioning.html
- Amazon S3 Object Lock is supported under the following conditions:
    - versioning is enabled on each bucket with Object Lock enabled.
    - Tiger Bridge is configured to replicate files' data and metadata to different buckets, following the steps in Replicate File's Metadata to a Different Bucket/Container.

4

Tiger Bridge 5.0.1 Administration Guide

- o 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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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:

- 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.
- Provide credentials for access to the designated Azure Blob endpoint:
  - account name and account key/SAS token
    Note: To use a SAS token as an authentication method for access to Azure, it must have all permissions enabled. Additionally, you must manually enter the name of the container designated for the selected source.
  - SAS connection string

> **Note:** Currently, you can pair a source with an Azure target using SAS connection string only through the command-line interface of Tiger Bridge, following [these steps](#).

- Select whether to access the target using secure transfer (SSL/TLS).
- Select whether to use the Hot, Cool or Archive tier of Azure as default tier for Tiger Bridge replication.
- Select whether offline files should be rehydrated using the Standard or the High option.
- 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 use the same container for two or more sources on the same computer. You must use the same container for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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:	Browse
Targets:	Google Cloud
Target name:	Google Cloud
Project ID:	
Service account:	
Private key:	
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 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

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

  > **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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). Do not change the name of the bucket as this may prevent Tiger Bridge replication from operating.

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

IBM Cloud Object Storage

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

- 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 public IBM cloud 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 IBM cloud.
- 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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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

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

Source path:		Browse

Targets: Backblaze

Target name: Backblaze

KeyID:

Application key:

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.
- 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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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 a Google Drive storage, you must provide the following information:

Source path:	C:\Users\Administrator\Documents\haga	Browse
Targets:	Google Drive	
Target name:	Google Drive	
Username:		
Prefix:		

- 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 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 use the same Google Drive folder for two or more sources on the same computer. You must use the same folder for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). Do not change the name of the folder as this may prevent Tiger Bridge replication from operating.

![LYVE Cloud logo] *LYVE Cloud*

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

- 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.

- 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.
  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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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).

ORockCloud

To pair a source with an ORockCloud target, you must provide the following information:

Source path:			Browse

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: 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 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.

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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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).

 RSTOR Space

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

| Source path: | C:\Users\Administrator\Documents\haga | Browse |

Targets: RSTOR Space

Target name: RSTOR Space

Server URL:

Access key:

Secret key:

☑ Use secure transfer (SSL/TLS)   Server-side encryption

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 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 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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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

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

Tiger Bridge Local Source:

Source path: [   ] [Browse]

Targets: [Symply Nebula   ⌄]

Target name: [Symply Nebula   ]

Server URL: [   ]

Access key: [   ]

Secret key: [   ]

☑ Use secure transfer (SSL/TLS)   [Server-side encryption]

Buckets: [List buckets]

Please refresh to load buckets

[Apply]   [Cancel]

- 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 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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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 *S3-Compatible Object Storage*

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

- 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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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

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

Source path:	C:\Users\Administrator\Documents\haga	Browse

Targets:	Wasabi
Target name:	Wasabi
Server URL:	https://s3.wasabisys.com
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 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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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)

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

• 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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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

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

• 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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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*

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

• 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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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

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

• 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 an 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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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).

BlackPearl Object Storage

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

Source path:		Browse

Targets: BlackPearl

Target name: BlackPearl

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 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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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

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

Source path:		Browse
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, port through which it is accessible from the computer running Tiger Bridge and API key.

FujiFilm Object Archive

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

• 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 use the same bucket for two or more sources on the same computer. You must use the same bucket for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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

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

Source path:		Browse
Target name:	Local storage	
Target path:		Browse

• 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 use the same path for two or more sources on the same computer. You must use the same path for multiple sources each on a different computer, only when you deploy Tiger Bridge for geo replication (active sync). 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

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

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

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 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.

2

Tiger Bridge Installation

Install Tiger Bridge

Uninstall Tiger Bridge

Install Tiger Bridge

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

• Tiger Bridge - installs the product, the graphic and command-line interfaces for configuring the product.

• Shell Extension - provides integration with Windows Explorer, allowing you to view the status of files and folders on your source through icon overlays, and to manually manage data through the Windows Explorer context menu.

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 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.
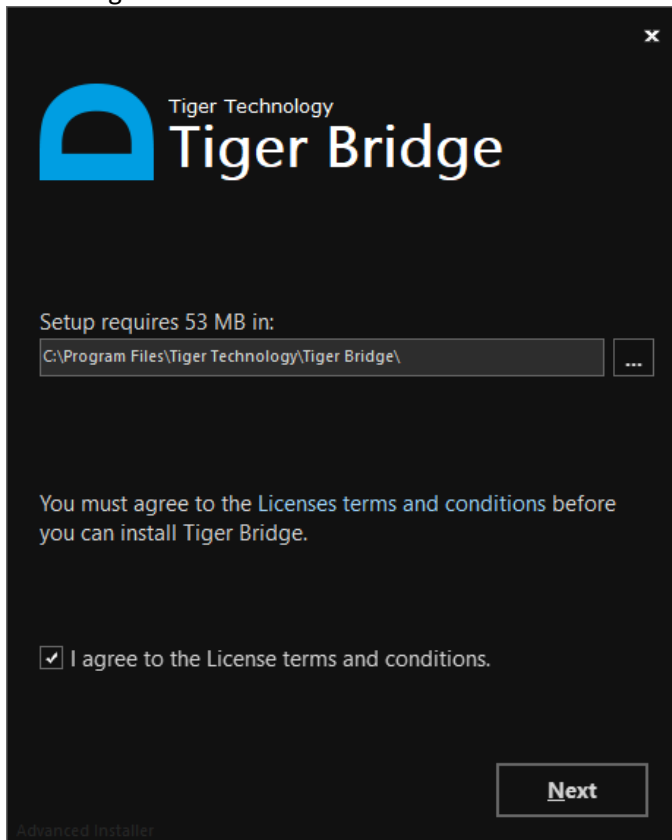
3. Make sure the check boxes of the Tiger Bridge components you want to install are selected and then click Install.
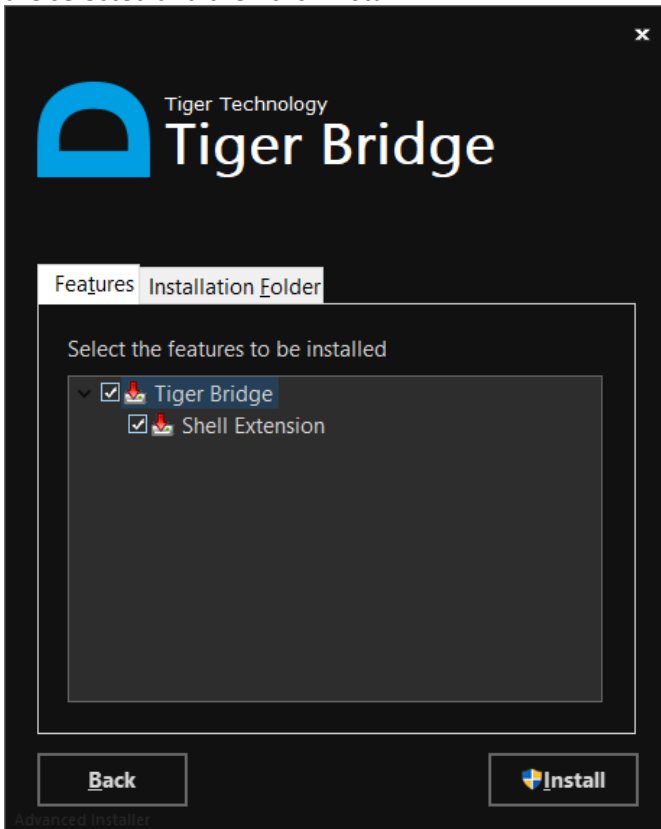
Note: If you clear the check box of a component, you can install it later, following the same installation steps.

- 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.
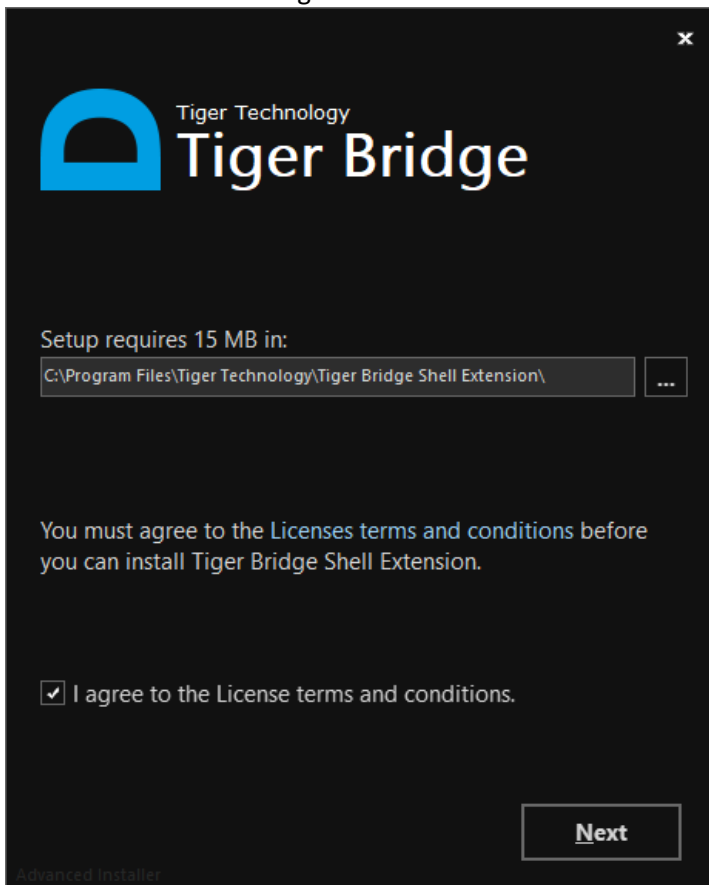
3. Make sure the check box of the Tiger Bridge shell extension is selected and click Install.

4. When the installation is complete, click Finish.

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

Uninstall Tiger Bridge

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

To uninstall Tiger Bridge or any of its components:

1. In Control Panel, go to Programs and Features.

2. Right-click Tiger Bridge or any of its components and select Uninstall.

3. When prompted to confirm that you want to remove Tiger Bridge or any of its components from the computer, click Yes.

Update Tiger Bridge

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

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

1. In the left pane of the Configuration, click Tiger Bridge.
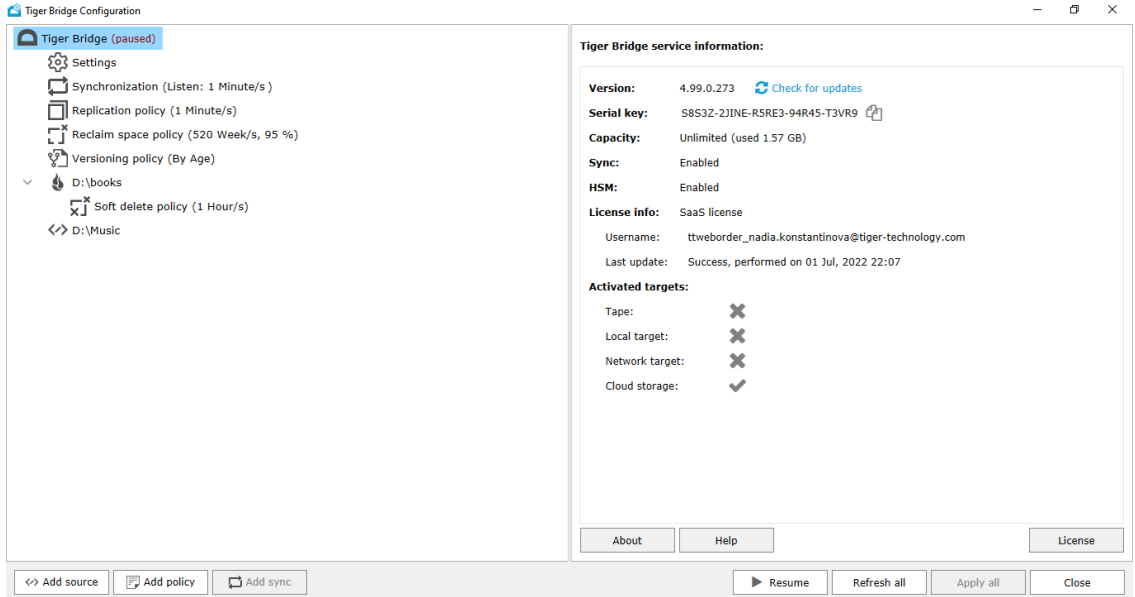
2. In the right pane, click Check for updates.

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

3

Get Started with Tiger Bridge

Activate Tiger Bridge

Pair a Source with the Target

Pause/Resume Automatic Tiger Bridge Operations

Refine the List of Automatically Managed Locations

Configure Automatic Data Replication

Configure Automatic Space Reclaiming

Configure Automatic Archiving

Configure Active Sync

Configure Versioning

Configure File Operation Mode

Configure Soft Delete Policy

Tiger Bridge 5.0.1 Administration Guide

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, which 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 settings or configure a separate replication policy for a specific pair of source and target, following the steps in Configure Automatic Data Replication. You can also manually replicate data to the target, following the steps in Perform Manual Data Lifecycle Operations.

Space reclaiming – until you configure a global space reclaiming 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, following the steps in Perform Manual Data Lifecycle Operations. For more information about configuring a space reclaiming policy, refer to Configure Automatic Space Reclaiming.

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, following the steps in Configure Automatic Archiving. Even without a configured policy, you can manually archive data, following the steps in Perform Manual Data Lifecycle Operations.

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

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.

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 Delete Mode.

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 Retrieve Mode.

Soft delete policy – specify by how long after a file is deleted from the source it should also be deleted from 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.

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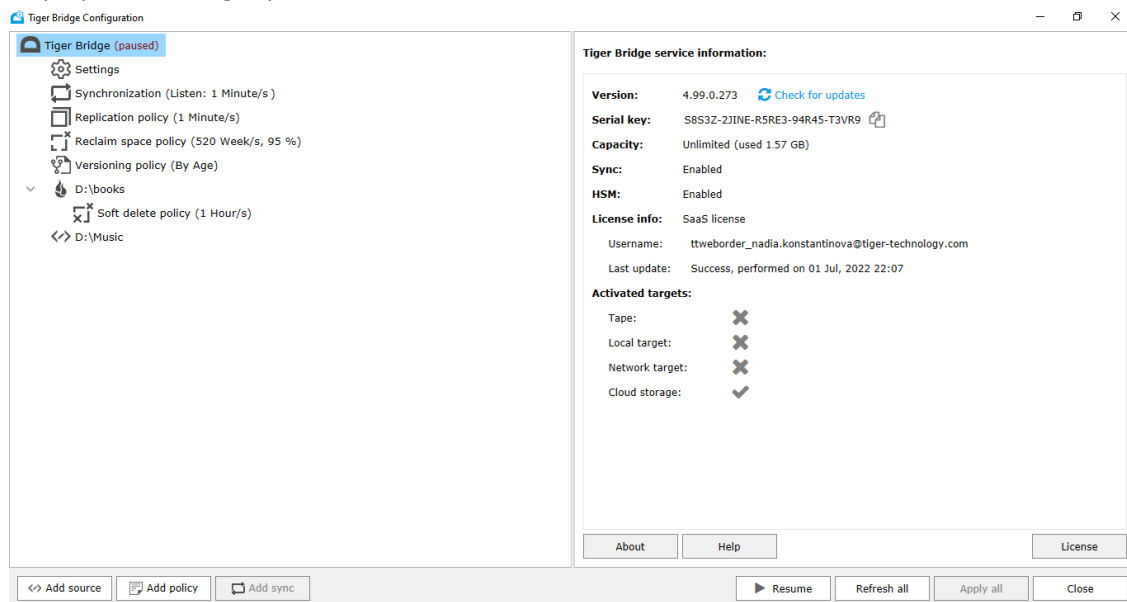
You can activate Tiger Bridge using one of the following:

• 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.

To activate a Tiger Bridge SaaS license:

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

2. In the Tiger Bridge License dialog, enter the username and password for your software subscription and then click OK.
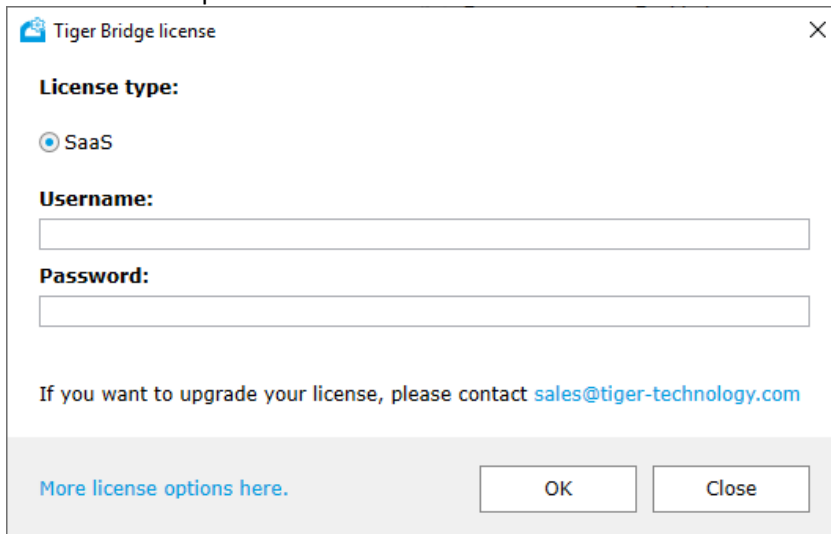
Tiger Bridge 5.0.1 Administration Guide

To activate Tiger Bridge with a software activation key:

1. In the Tiger Bridge Configuration, click Tiger Bridge in the left pane and click License in the right pane.
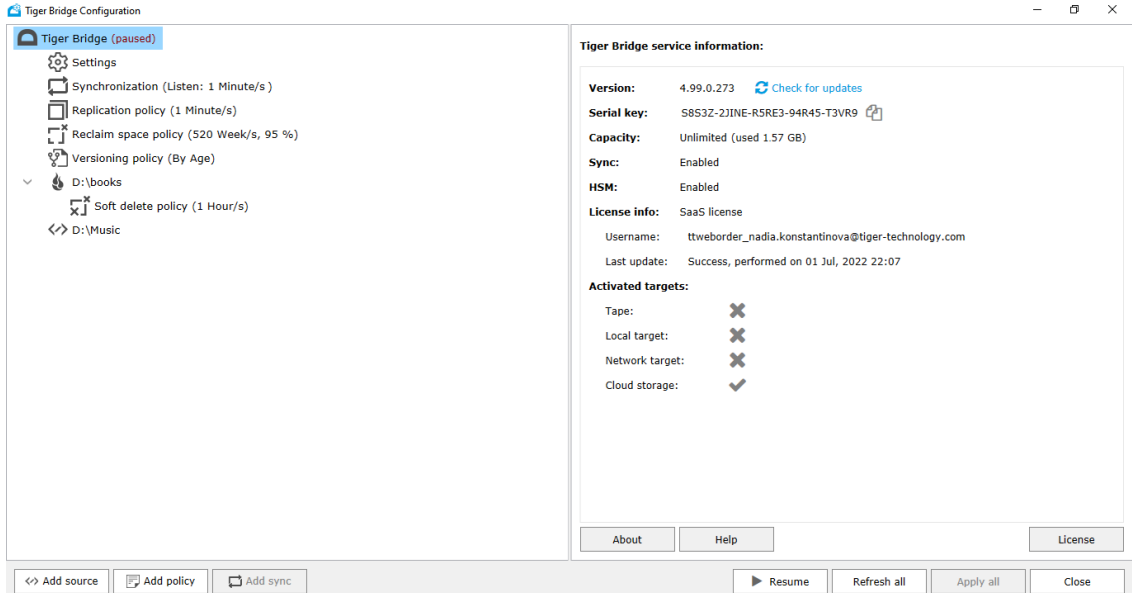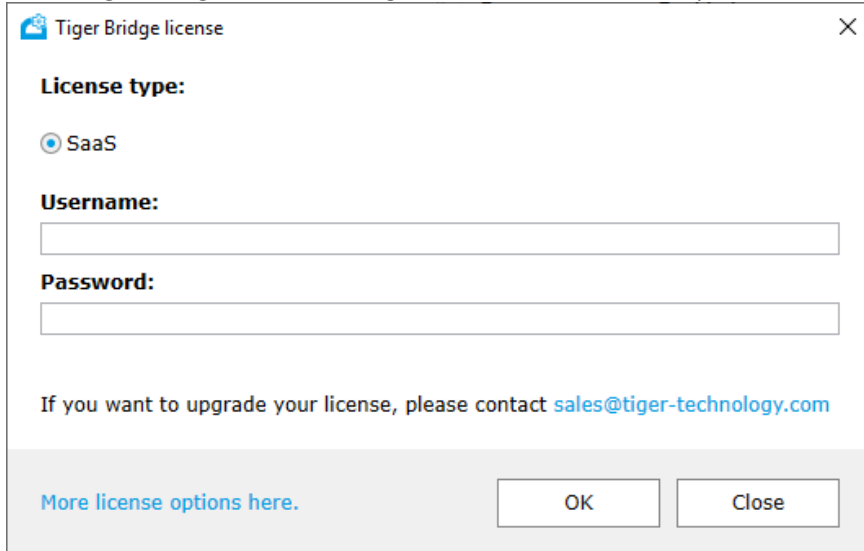
2. In the Tiger Bridge License dialog, click on "More license options here".

3. Select Soft and then copy the product serial key, by clicking the Copy button.
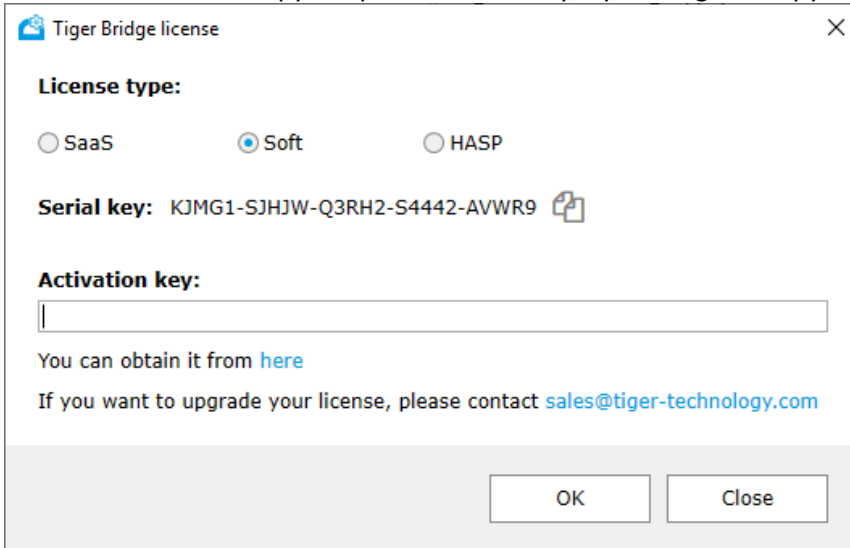
4. In a web browser go to:
   https://license.tiger-technology.com
   Tip: Click the link below the Activation key field, to automatically load the URL in your default web browser.
5. In the home page of the licensing server, enter your name and password in the corresponding fields, and click Log in.
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. In the home page of the licensing server, enter your name 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.
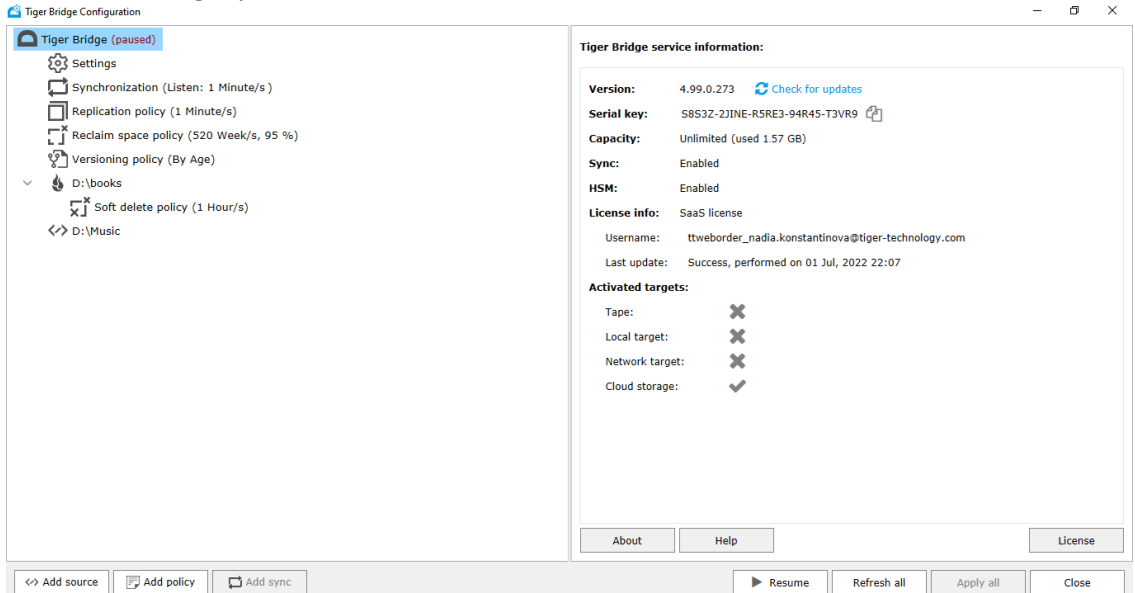
6. In the Tiger Bridge License dialog, click on More license options here.
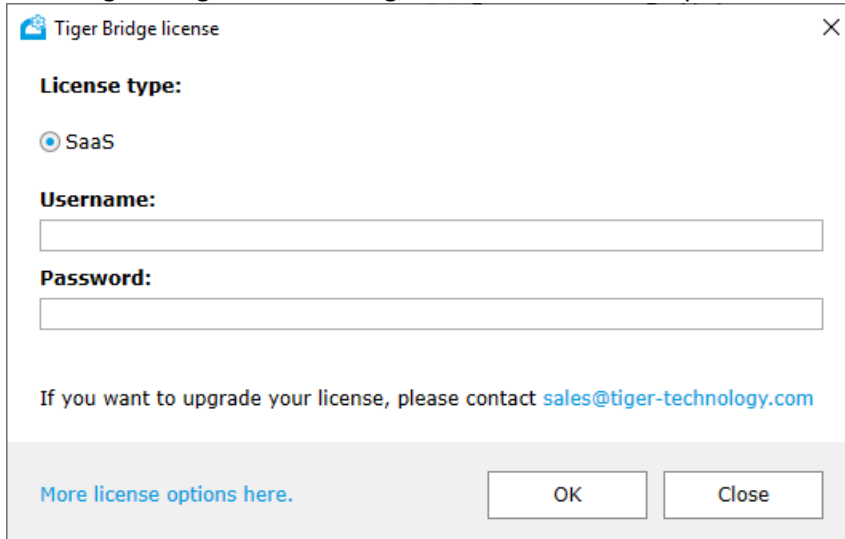
7. Select HASP and then click Browse.

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 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, following the steps in Refine the List of Automatically Managed Locations.

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.

NAS Source Prerequisites and Setup

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

While with data replication there is no difference from local volume source, when the Tiger Bridge space reclaiming mechanism needs to replace the actual file on the NAS source with a stub file, it actually creates the stub file only in the control folder, but creates a placeholder

file with .reclaimed extension on the NAS source, to let you identify that the stub counterpart is in the control folder. If you want to retrieve a nearline file or rehydrate an offline file manually, you need to perform the operation on the stub file located in the control folder. The same goes for the active sync mechanism, unless you have configured the mechanism to automatically retrieve on the source synchronized data from other sources. When you need to manually synchronize the contents of source and target, you need to perform the operation on the control folder and all restored data will appear there in the form of stub files and placeholder files on the NAS source itself. You can then manually retrieve the stub files on the NAS source.

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

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

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

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).
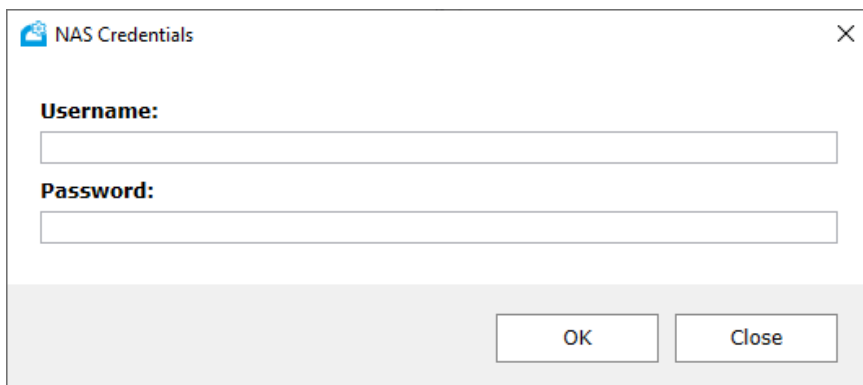
To pair a source with a target:

1. In the Tiger Bridge Configuration, click Tiger Bridge in the left pane and then click Add source.
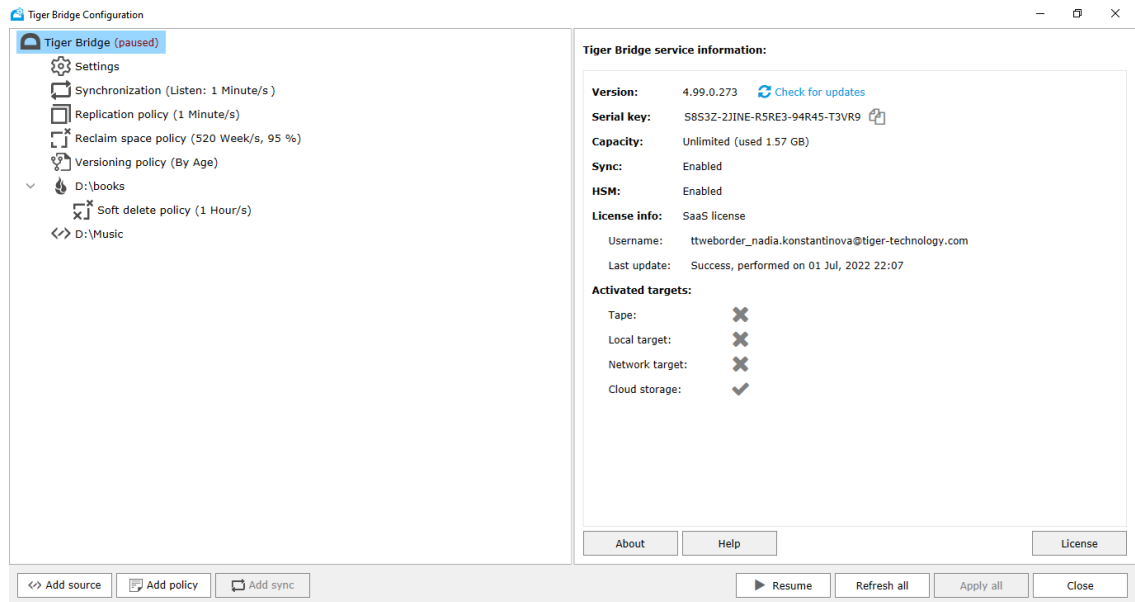
2. Browse to and select location on the local NTFS/ ReFS or SMB/NFS share you want to add as a source or enter the path manually, then click Select Folder.
3. (SMB share only) In the NAS Credentials dialog, enter username and password of a user with Full Control over the network share in the respective fields.

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

4. In the Tiger Bridge Target dialog, click either Public Cloud or On-Premises, then select the target type and click OK.
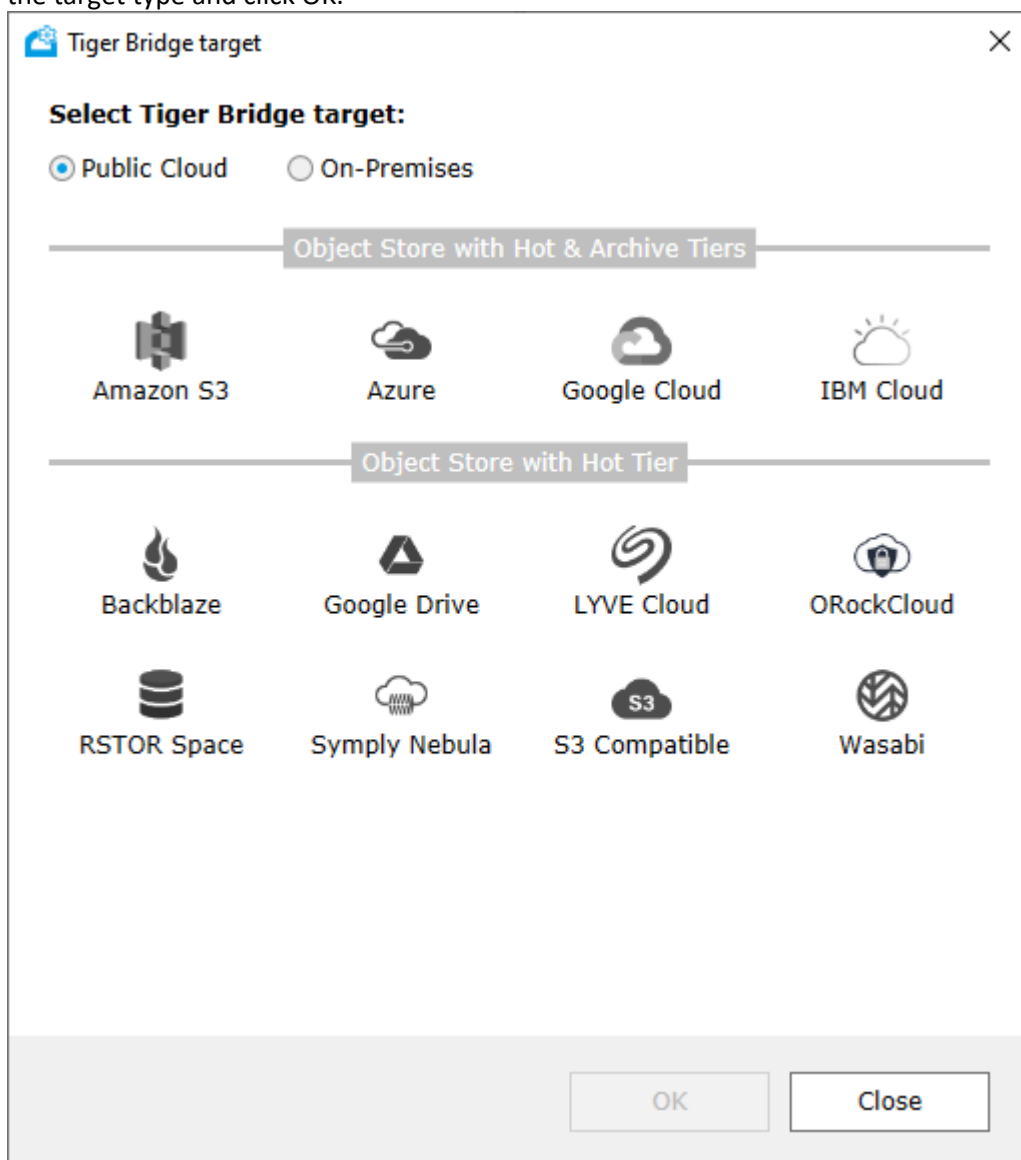
5. (NAS source only) In the right pane of the Configuration, click Browse and browse to and select the control folder or alternatively enter the path to it.

Tiger Bridge Local Source:

Source path:	D:\Adobe Scripts	Browse

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)   Server-side encryption

Default storage class: S3 Standard-IA

Archive retrieval option: Standard

Buckets: List buckets

Please refresh to load buckets

Apply   Cancel

6. In the right pane of the Configuration, fill in the requested target details as outlined in Target Storage Prerequisites 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.
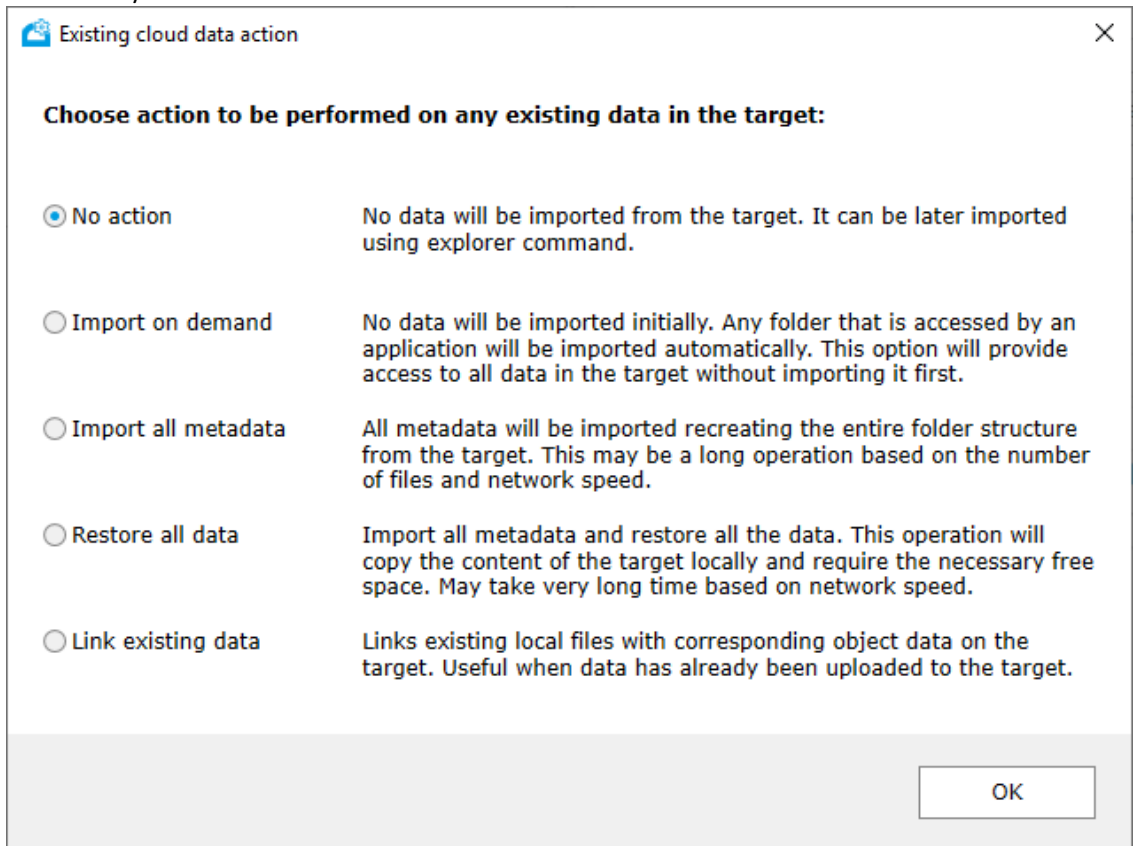
8. Click Apply.

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.

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 Using the Tray Icon.

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

1. 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.
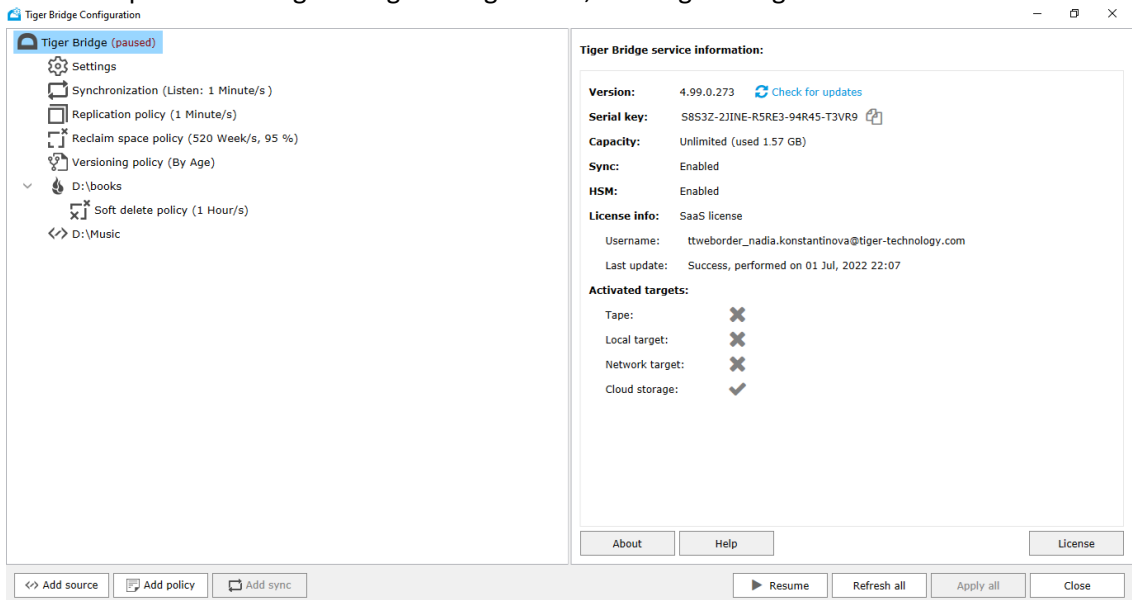
2. Do one of the following:
   - To resume all automatic Tiger Bridge operations, click Resume in the taskbar.
   - To pause all automatic Tiger Bridge operations, click Pause in the taskbar.

Refine the List of Automatically Managed Locations

By default, Tiger Bridge automatically manages all data on your source, except

the following files and folders:

- 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
> - encrypted files

You can also configure Tiger Bridge to manage automatically only data in certain paths on your sources and omit other data, allowing you replicate, archive or reclaim it only manually. For the 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, 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.
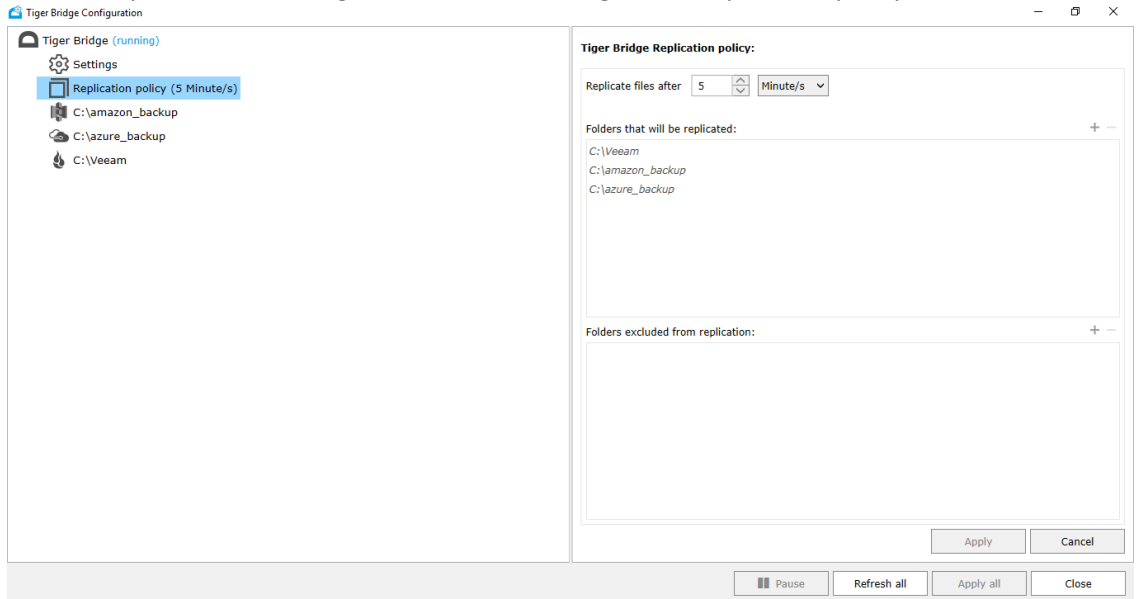
2. In the right pane, refine the list of automatically managed locations on all sources, by doing one of the following:
   • To add a folder to the list of included or excluded locations, click the + next to the respective list and browse to and select the respective folder, then click OK.
   Tip: You 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 in order 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 the 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 Locations.

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

To configure global data replication policy:

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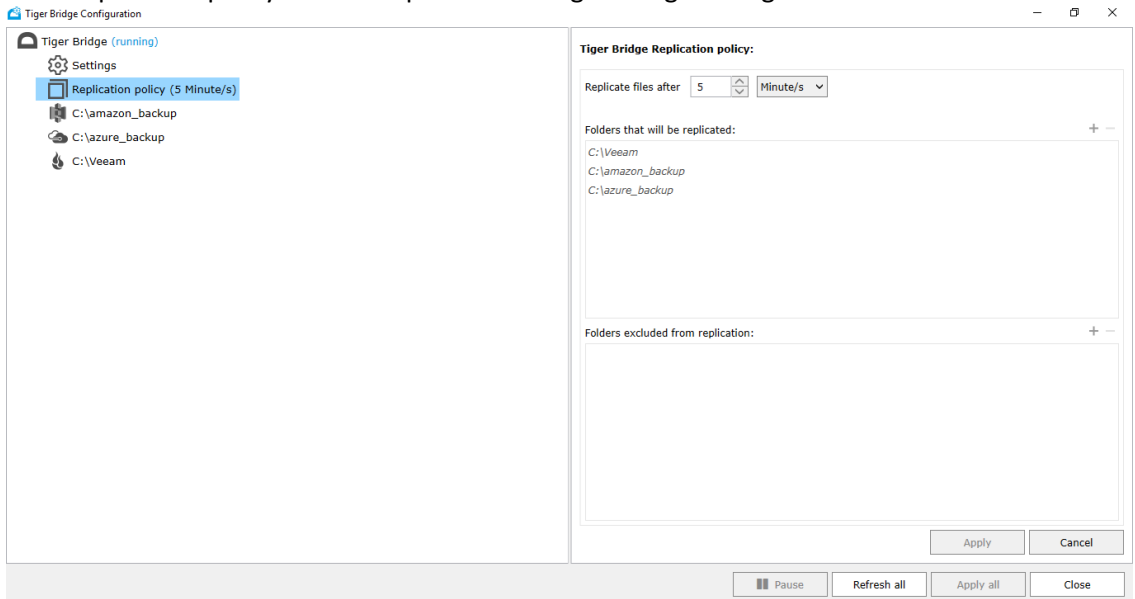
2. In the right pane, specify for how long a file should not have been modified for Tiger Bridge to replicate it, by entering the desired number and selecting the unit of measure in the drop-down box beside it.

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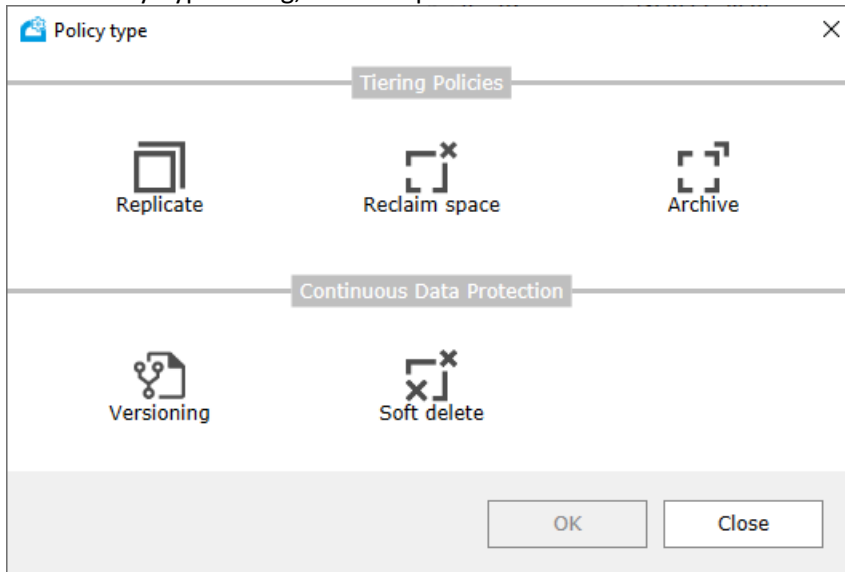
> **Tip:** To make the source use the global replication policy set for all pairs, simply delete its own policy by selecting it and clicking Delete policy.

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

Configure Automatic Space Reclaiming

To let Tiger Bridge automatically reclaim space on your sources, you must add a Space reclaiming 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 Space reclaiming 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, which 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 space reclaiming policy, valid for all sources. You can also add and enable a space reclaiming policy valid for just a specific pair of source and target, and thus use different parameters. Keep in mind that the global space reclaiming policy is valid only for sources that do not have a space reclaiming policy of their own. Thus, even if you have configured a space reclaiming 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 global space reclaiming policy:

1. Select Tiger Bridge in the left pane and then click Add policy.

2. In the Policy Type dialog, click "Reclaim space" and click OK.
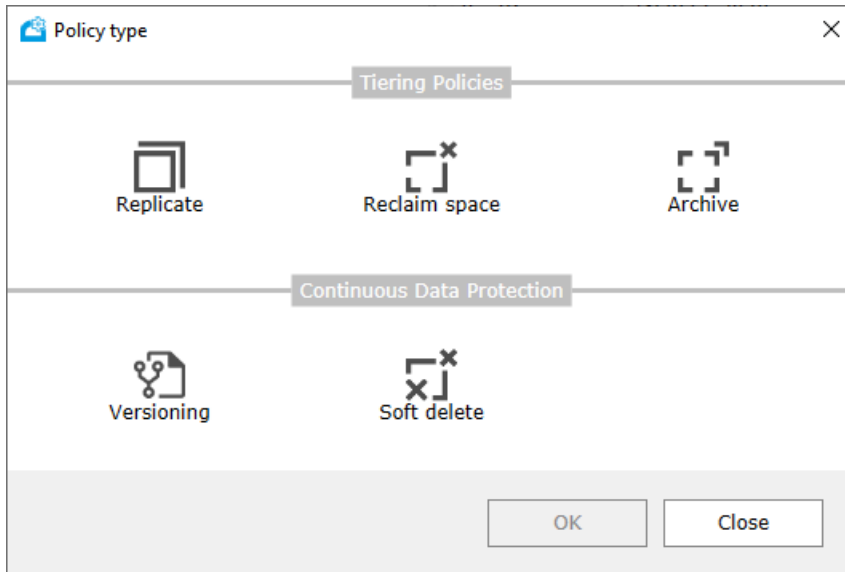
Note: If you have not deleted the global space reclaiming policy, created during the initial configuration of Tiger Bridge, you can only edit its settings. To do so, select "Reclaim space policy" under Tiger Bridge in the left pane and then proceed with the steps below.

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

- 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 space reclaiming policy for a specific source:

1. In the Tiger Bridge Configuration, select the source in the left pane and then click Add policy.
2. In the Policy Type dialog, click "Reclaim space" and then click OK.
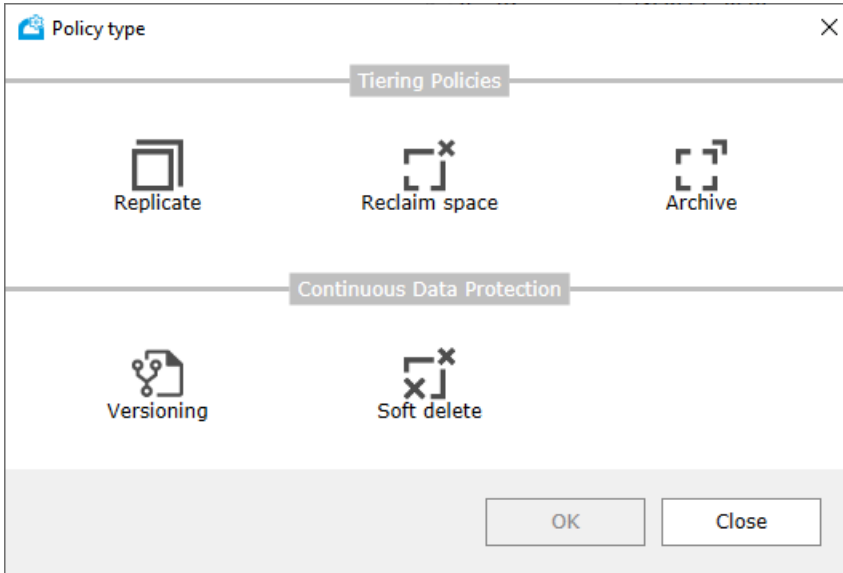
3. In the right pane, select the Enabled check box, to enable the policy.
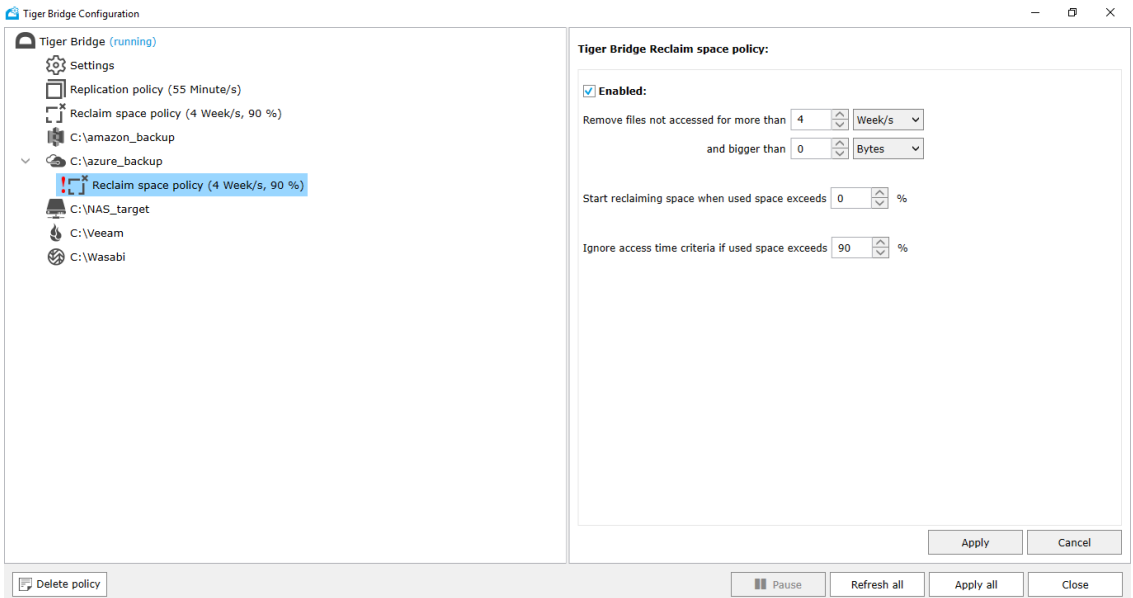
4. To change the default parameters of the space reclaiming policy, do the following:
    - In "Remove files not accessed for more than" specify for how long a file must not have been accessed for Tiger Bridge to replace it with a stub on the source.
    - In "Bigger than" specify how big a file should 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.

Configure Automatic Archiving

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

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 enable automatic archiving of data on a source, you must add a Tiger Bridge archiving policy to it.

On targets that do not support third-party policies for moving of data from their hot/cool tier to the archival tier, you can enable the target's own archiving policy through Tiger Bridge and synchronize Tiger Bridge to check for archived files at the time the policy archives them. 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 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. Currently, you can add a Tiger Bridge archive policy on the following targets:

- Microsoft Azure
- Amazon S3
- Google Cloud

The policy uses two parameters - minimal file size and time interval for which the file has not been accessed on the source. For example, if you set the file size threshold to 10MB and the time interval to 2 weeks, Tiger Bridge will move to the archival tier all replicated files with size 10MB or above that have not been accessed for at least 2 weeks. By default, Tiger Bridge moves to the archive replicated files that are bigger than 10MB and if they have not been accessed for more than 50 weeks. Tiger Bridge processes the queue of replicated files scheduled for automatic archiving starting from the ones, which are least recently accessed.

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 then click Add policy.

2. In the Policy Type dialog, select Archive and click OK.
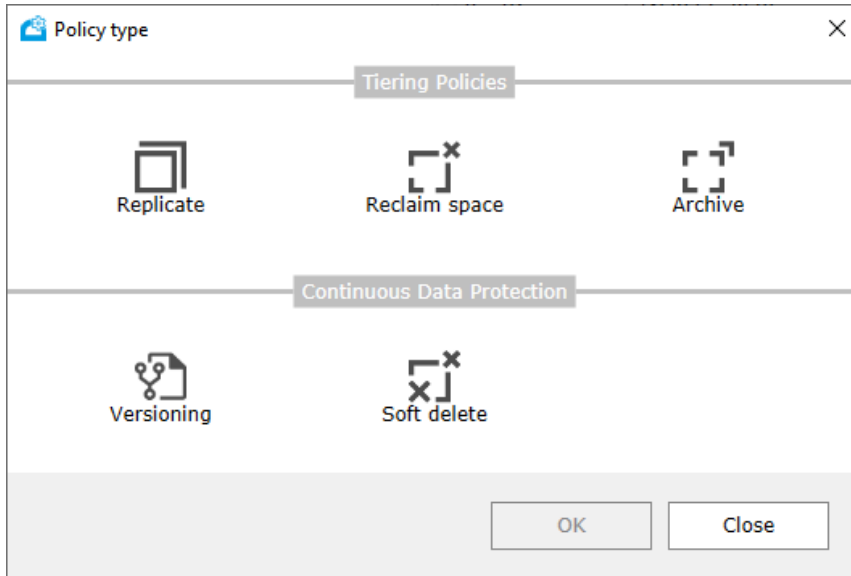
Note: Archive policy is greyed out, when the target does not provide an archival tier.

3. In the right pane, specify the minimum file size and for how long a file should not have been accessed on the source in order to be moved to the archival tier.

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

Synchronize Tiger Bridge with the Target's Own Archiving Policy

On targets that provide an archival tier, but do not allow third-party policies to move files to it, you can synchronize Tiger Bridge with the target's own archiving policy. You can do this in the following ways:

> • (if the target's own archiving policy is enabled) Specify at what intervals after a file has been replicated Tiger Bridge must check if it has been archived. This can be useful when Tiger Bridge checks the status of reclaimed stub files and updates it to offline for files moved to the archive. For more effective synchronization, it is advisable to adjust this value to the same value as the one used by the target's archiving policy. For example, if the policy is configured to move to the archive files that have not been accessed for 40 days, configure Tiger Bridge to check whether they are archived 40 days after their replication.

• (if the target's own archiving policy is not enabled) Enable the target's policy through Tiger Bridge by creating a corresponding rule on the target, which uses the same parameters as the parameters for synchronizing Tiger Bridge. Thus, if you configured Tiger Bridge to verify the archive status on the target 20 days after they have been replicated and select to create a corresponding archiving rule on the target, the target provider will move to the archive files which have not been accessed for 20 days.

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

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

1. In the Tiger Bridge Configuration, select the source in the left pane and then click Add policy.
2. In the Policy Type dialog, select Archive and click OK.
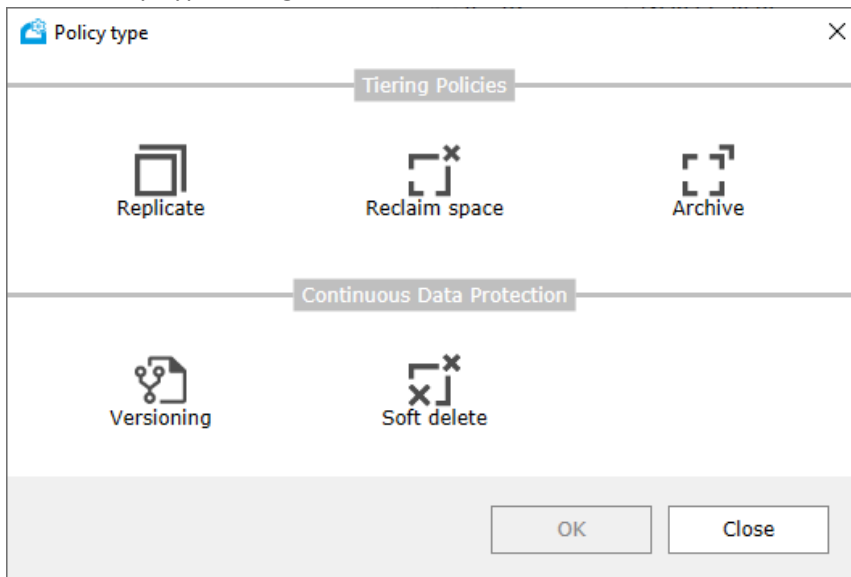
Note: Archive policy is greyed out, when the target does not provide archival tier.

3. In the right pane, specify the time interval at which Tiger Bridge should check for files moved to the archival tier and if n archiving policy is enabled on the target, select the "Create corresponding Glacier Transition rule" check box to enable it and make it use the same time interval for archiving files.
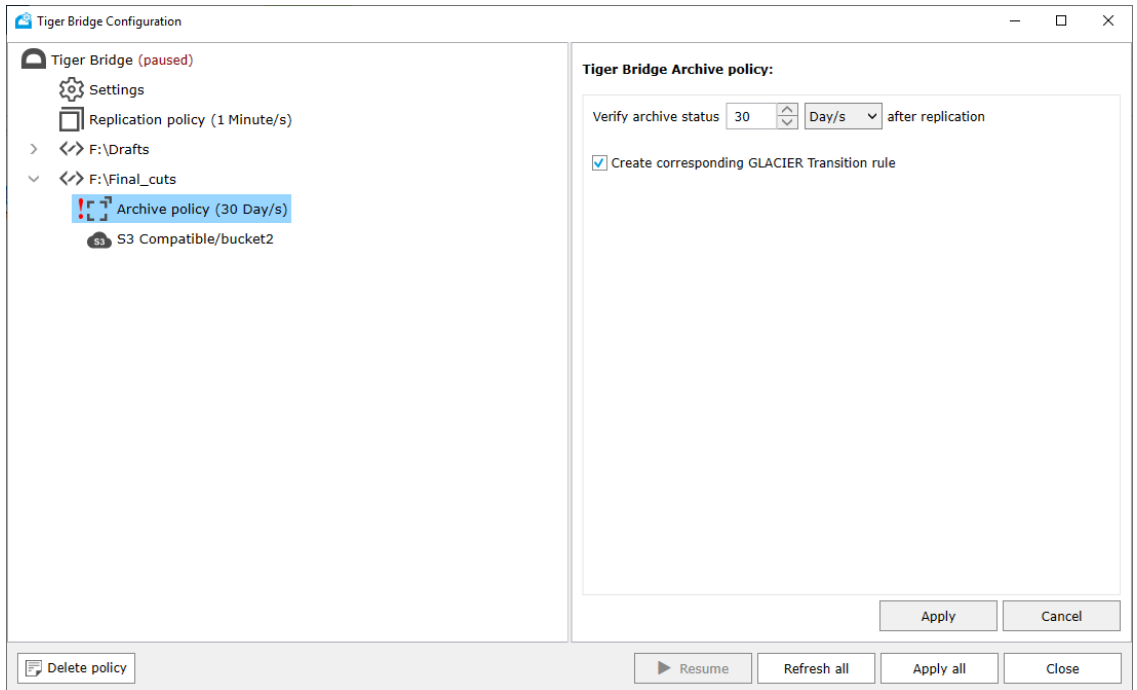
4. Click Apply and optionally resume automatic Tiger Bridge operations.

Configure Active Sync

Tiger Bridge's Active Sync allows you to synchronize the contents of two or more sources, each on a separate computer, through a common target. With Active Sync, 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.

Important: To allow for the proper contents synchronization, it is advisable on all sources to set up Tiger Bridge operation mode parameters in such a way that a file on the target is not

deleted when it is retrieved on one of the sources and also not to delete the file from the target, if it is deleted on any of the sources. Otherwise, other sources may fail to retrieve the respective file, even though the retrieve mode and delete mode on them are set to keep the replica. For more information, refer to Configure File Delete Mode.

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 Active Sync policy.

The Active 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 on 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 contents of the synchronized sources is updated with offline files instead of nearline files.

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

To configure the global Active Sync policy:

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

2. In the right pane, do the following:
   • 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 restore files on the synchronized source" check box, to let Tiger Bridge begin retrieving the files immediately after contents is synchronized.
   • Clear the "Automatically restore 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 Active Sync policy for a specific source:

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

2. In the right pane, do the following:
- 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 restore files on the synchronized source" check box, to let Tiger Bridge begin retrieving the files immediately after contents is synchronized.
- Clear the "Automatically restore 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 active sync policy for this source, simply select it in the left pane, edit the desired parameter and click Apply. To delete the policy and let the source use the global active sync policy, select it in the left pane and then click Delete sync.

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.

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.

To enable/disable versioning during replication:

1. In the left pane of the Tiger Bridge Configuration, click Settings.
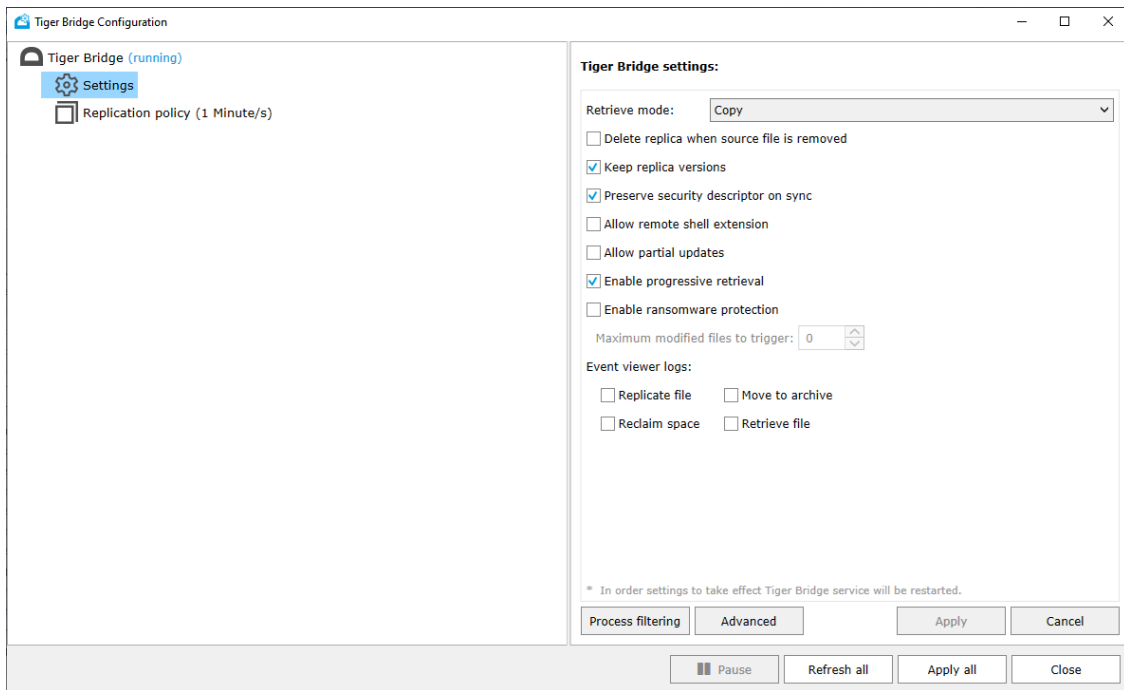
2. Do one of the following:
- Select the "Keep replica versions" check box, to enable versioning in Tiger Bridge.
- Clear the "Keep replica versions" check box, to disable versioning in Tiger Bridge.
3. When prompted, verify that versioning is enabled on the buckets/containers of the target(s), and click 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, which 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 source and 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. Select Tiger Bridge in the left pane and then click Add policy.

2. In the Policy Type dialog, click Versioning and click OK.
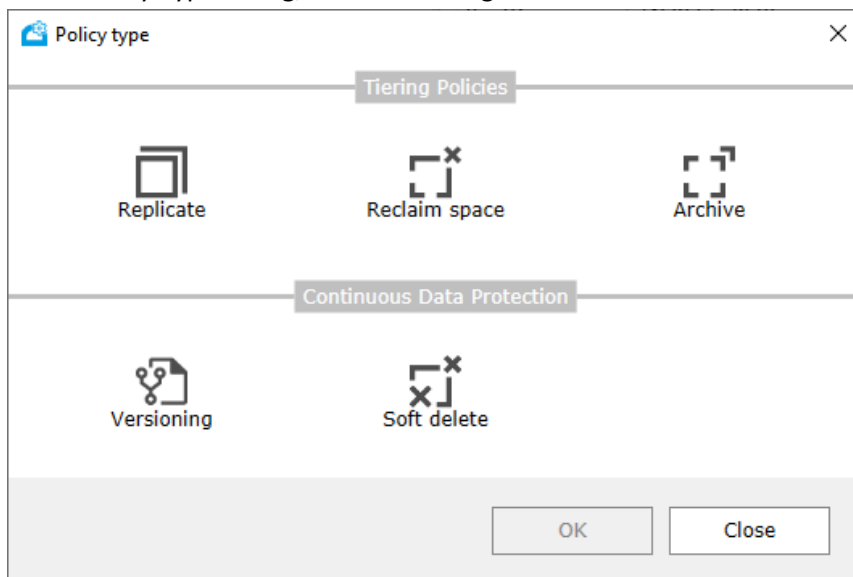
Note: Versioning policy is greyed if you have not enabled the "Keep replica versions" check box in the Tiger Bridge settings.

3. In the right pane, do one of the following:
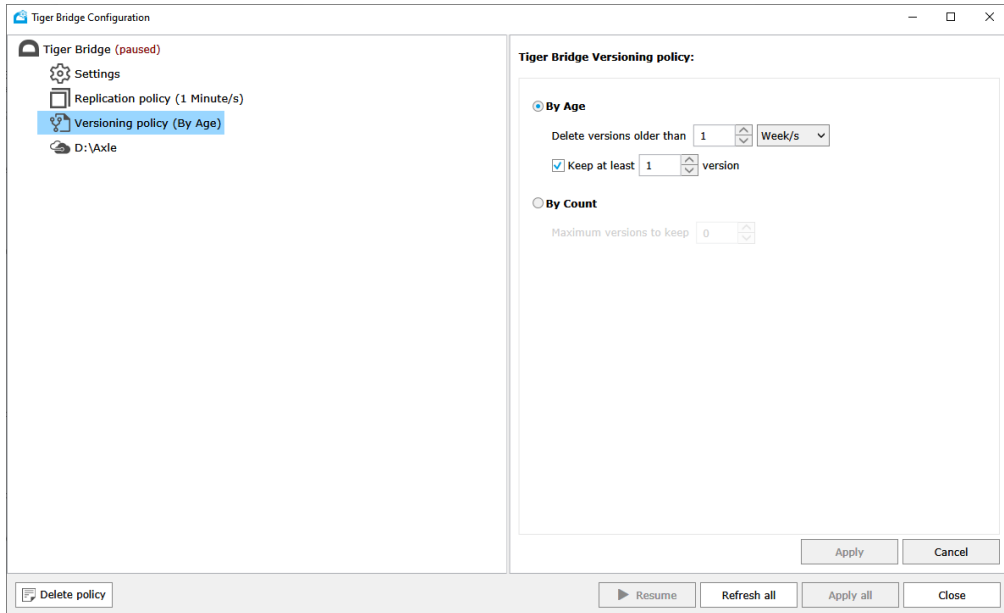
- Select "By Age" and in "Delete versions older than" specify how old a version should be for Tiger Bridge to delete it from the target.
- Select the "Keep at least" check box and specify the maximum number of versions of the same file, which when exceeded triggers the "By Age" rule.
- Clear the "Keep 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 then click Add policy.
2. In the Policy Type dialog, click Versioning and then click OK.
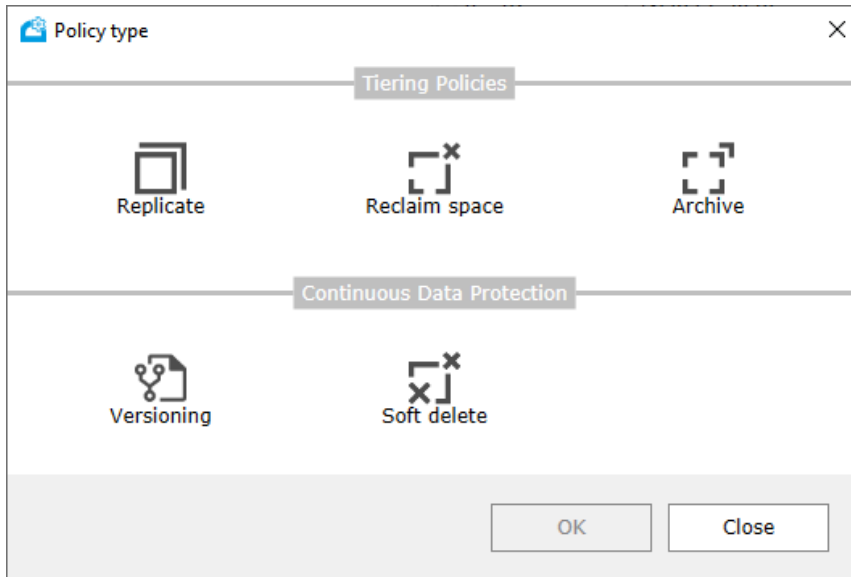
Note: Versioning policy is greyed if you have not enabled the "Keep replica versions" check box in the Tiger Bridge settings.

3. In the right pane, select the Enabled check box, to enable the policy.
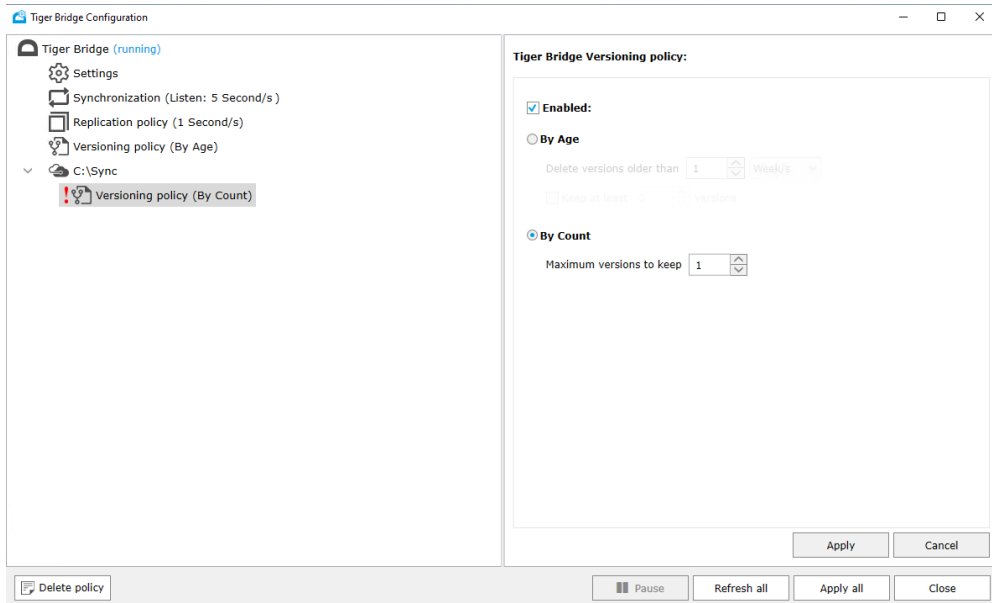
4. To change the default parameters of the versioning policy, do one of the following:
- Select "By Age" and in "Delete versions older than" specify how old a version should be for Tiger Bridge to delete it from the target.
    - Select the "Keep at least" check box and specify the maximum number of 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 on the first source as the files are no longer available on the target.

You can set Tiger Bridge to remove file replica from target when it is successfully retrieved on 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.

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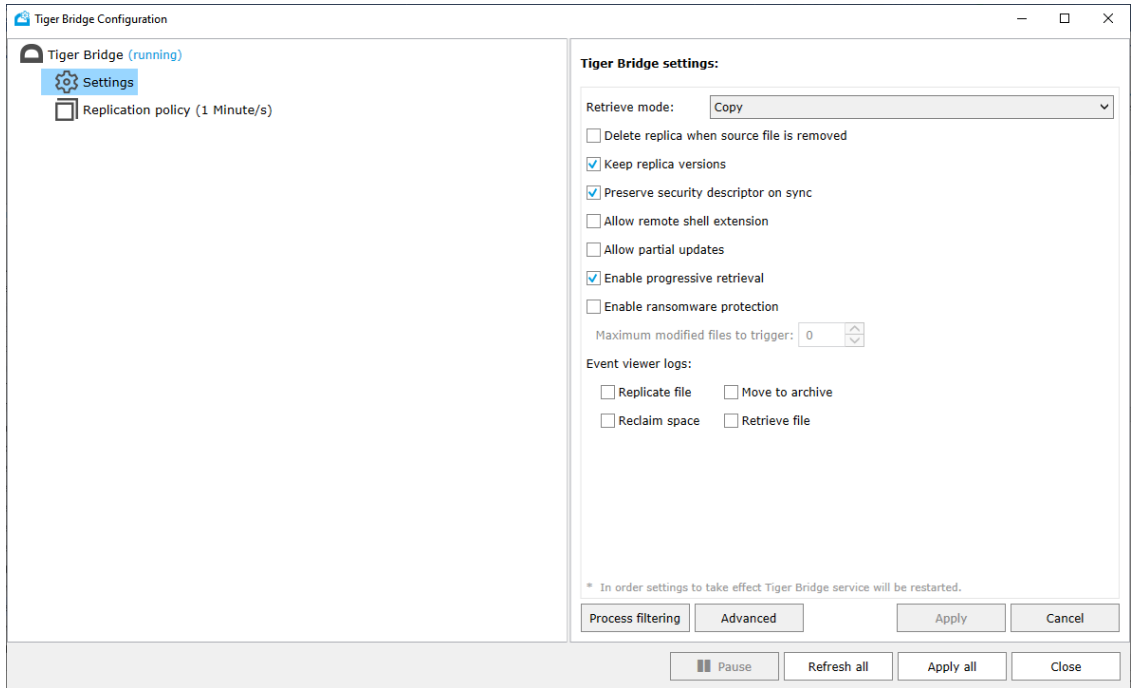
- To let Tiger Bridge keep the replica on the target, when the file is successfully retrieved on the source volume, select Copy.
- To let Tiger Bridge remove the replica from the target, when the file is successfully retrieved on the source volume, select Move.

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, following the steps in "Undelete Data on the Source". 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 on Configure Soft Delete Policy.

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 on 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.
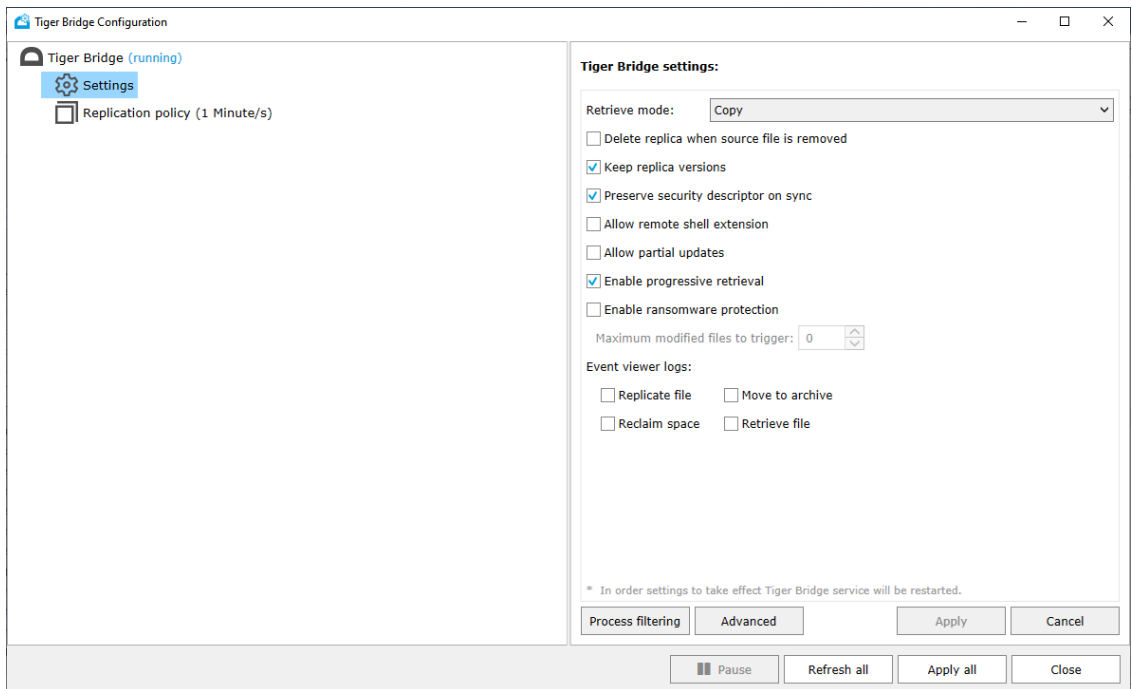
2. Do one of the following:
- Select the "Delete replica when source file is removed" check box, to let Tiger Bridge remove the replica from the target, upon deleting the file from the source volume.

- 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 to simply specify by how much time the synchronization of the deletion of the file on the target is delayed. Thus, if you use the default setting – 1 hour, should you delete a file from your source its deletion from the target is offset with 1 hour and meanwhile you can manually undelete the file, following the steps in Undelete Data from the Source.

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. Select Tiger Bridge in the left pane and then click Add policy.

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

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

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 then click Add policy.
2. In the Policy Type dialog, click "Soft delete" and then click OK.

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

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.

4

Fine-tune Tiger Bridge

Enable Remote Shell Extension Access

Define the Tiers of Your Object Storage Target

Configure Interaction with Windows Explorer

Use Proxy Server for Access to the Target

Set Startup Scan Wait Time

Disable NFS Locking on the Tiger Bridge Computer

Manage The Number of Threads Scanning a NAS Source

Fine-Tune Data Replication

Fine-Tune Space Reclaiming

Fine-tune Active Sync

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 on a local 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.
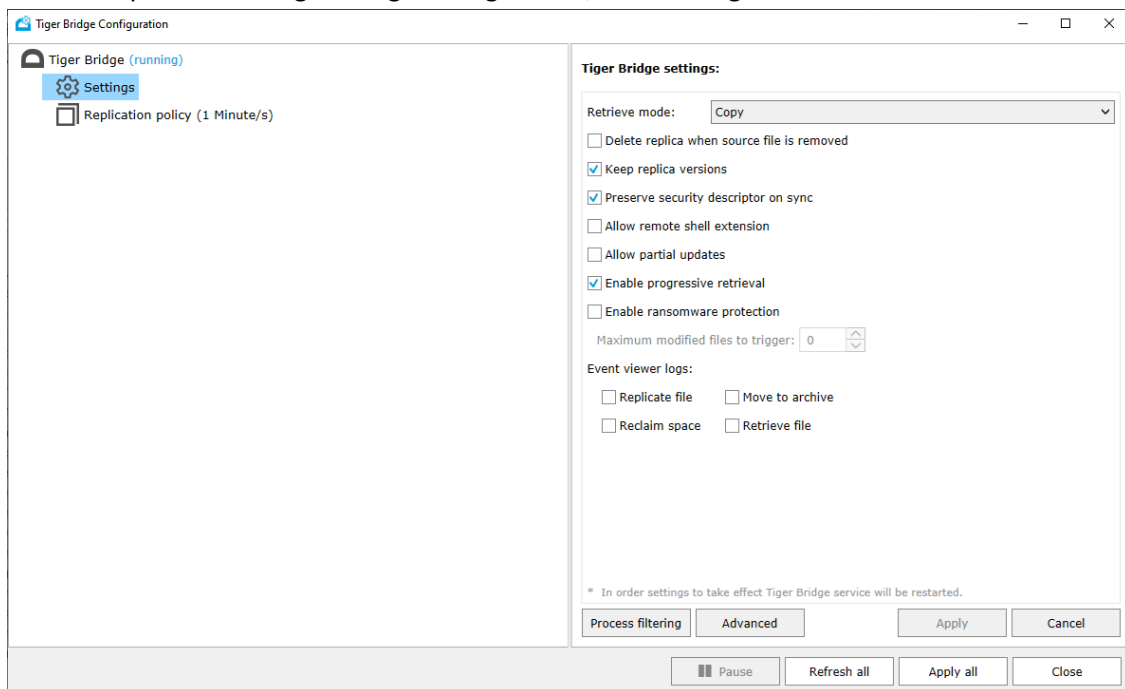
2. In the right pane, do one of the following:
- Select the "Allow remote shell extension" check box to enable the execution of shell extension commands from remote computers.
- Clear the "Allow remote shell extension" check box to prevent users on remote computers from executing Tiger Bridge shell extension 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 replicates data to the hot tier of your cloud object storage target and archives it to the archival tier. For the purpose, Tiger Bridge uses the equivalents to the hot, cool and archive tiers or storage classes as defined by your target provider. Thus, for example, on Amazon S3 object storage it replicates data to the S3 Standard-IA and archives it to S3 Glacier. As most cloud object storage providers offer more than three storage classes or tiers, you can manually define which ones should be used for replication (hot) and for archiving (archive). The tiers are defined per pair of source and target.

To define the hot and archive tiers of your 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> tiers <hot> <cool> <archive>
   ```
   For example, to configure Tiger Bridge to use the Google Cloud Nearline storage class for replication and Coldline storage class for archiving, execute the following:
   ```
   tiercli config <path to source> tiers nearline "" 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
   ```

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 Tiger Bridge Shell Extension and Windows Explorer. As you can access a source simultaneously from multiple computers using the remote shell extension, it is possible the number of requests for files and folders status to burden performance and lead to delays in displaying the icon overlays. A

workaround to this problem is to disable the display of icon overlays on the 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.
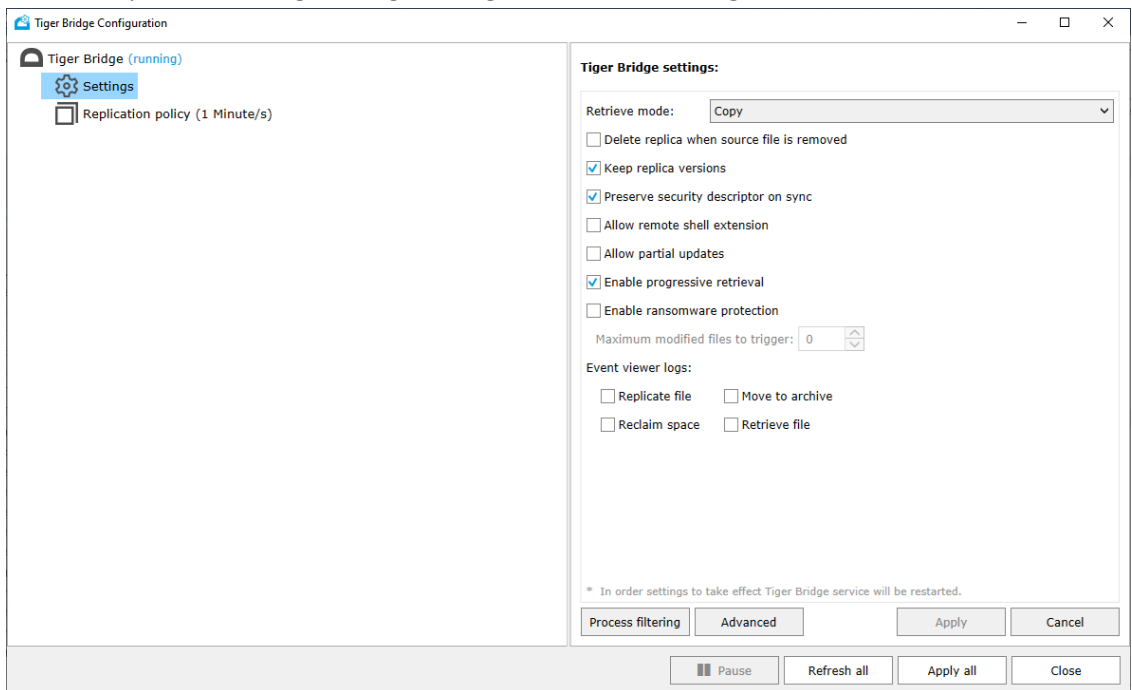
2. In the right pane, click Advanced.

3. In the Advanced Settings dialog, do one of the following:
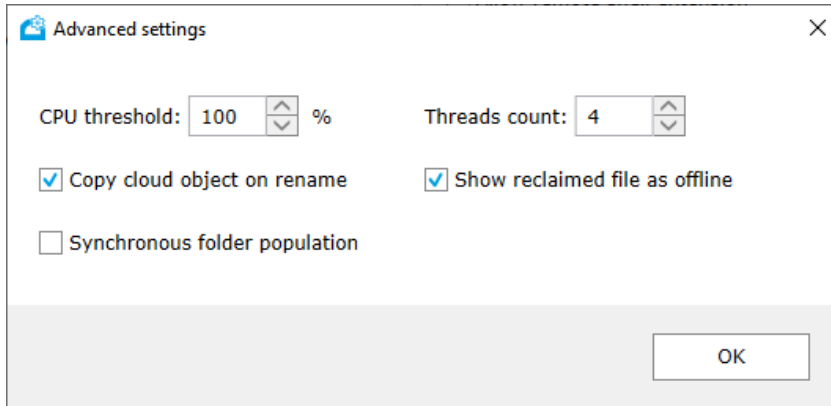
- Select the "Synchronous folder population" check box, to let Windows Explorer open the currently browsed folder only after it has been fully populated with stub files from the target, then click OK
- Clear the "Synchronous folder population" check box, to browse folders in Windows Explorer even if 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 the purpose, you need to specify the proxy server settings using the command-line interface of Tiger Bridge.

To specify proxy server settings:

1. Run Command Prompt as an administrator and restart the Tiger Bridge service, by executing the following:
```
net stop tiersvc
net start tiersvc
```
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>
   ```
   where:

   `<server:port>` is the proxy server IP address and the port through which it will access the targets;

   `<username>` is the user name with which for authentication on the proxy server;

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

   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 "" ""
   ```

3. Run Command Prompt as an administrator and restart the Tiger Bridge service, by executing the following:
   ```
   net stop tiersvc
   net start tiersvc
   ```
   Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt and select "Run as administrator".

To disable access through a proxy server:

1. Run Command Prompt as an administrator and restart the Tiger Bridge service, by executing the following:
   ```
   net stop tiersvc
   net start tiersvc
   ```
   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 ""
   ```

3. Restart the Tiger Bridge service, by executing the following:
   ```
   net stop tiersvc
   net start tiersvc
   ```

Set Startup Scan Wait Time

On startup Tiger Bridge scans the file systems of the source volumes it manages to determine what data on them needs to be processed. By default, Tiger Bridge is set to wait until this scan

finishes, before beginning with data lifecycle management operations, thus ensuring maximum precision of the scheduled file operations. On source volumes with much data this scan may take significant time and you can set up Tiger Bridge to reduce this wait time before the scan finishes.

To set Tiger Bridge startup scan wait time:

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 startup scan finishes completely, change the value to 0 and click OK.
   * enter the time in seconds, for which Tiger Bridge should wait before beginning to process data and click OK.
7. Run Command Prompt as an administrator and restart the Tiger Bridge service, by executing the following:
   ```
   net stop tiersvc
   net start tiersvc
   ```
   Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt and select "Run as administrator".

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 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 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.

Manage The Number of Threads Scanning a NAS Source

By default, when scanning a NAS source on startup Tiger Bridge uses just two threads. For NAS sources containing a lot of data, the initial scan may take up quite long. To increase the speed of the source scan each time the Tiger Bridge service starts, 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. 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. 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 replication, once specific conditions are present. As ransomware attacks usually result in encryption of as many files as possible, Tiger Bridge lets you specify the maximum number of already replicated files, queued to be replicated again because they have been modified on the source. When the number of modified files queued for re-replication reaches the threshold you have specified, Tiger Bridge automatically pauses all its operations and logs this in the Windows Event Viewer. You can then delete the encrypted files (if there are any), retrieve from the target their unencrypted copies, and then resume normal operations.

By default, when you enable Tiger Bridge's ransomware protection, the maximum number of files triggering the protection mechanism is 600. You can change this number depending on your specific workload calculations. You can use the statistics about modified files per source provided by the Tiger Bridge shell extension as a starting point (see Monitor Data Management Statistics). You should also keep in mind that:

*   the maximum number of files, which triggers the protection mechanism, is valid for each configured source i.e., the workload on one source may differ from that on another.
*   a replicated file, which has been modified on the source is replicated again once it meets the replication policy criteria but is added to the Tiger Bridge queue

immediately after it has been modified on the source i.e., the longer the time interval in the replication policy, the bigger the chance that healthy files stay in the queue, waiting to be replicated anew.

You can disable Tiger Bridge's ransomware protection mechanism at any time, thus guaranteeing that no matter how many replicated files are queued to be re-replicated, automatic Tiger Bridge operations are never paused.

To enable/disable the ransomware protection mechanism:

1. In the left pane of the Tiger Bridge Configuration, click Settings.
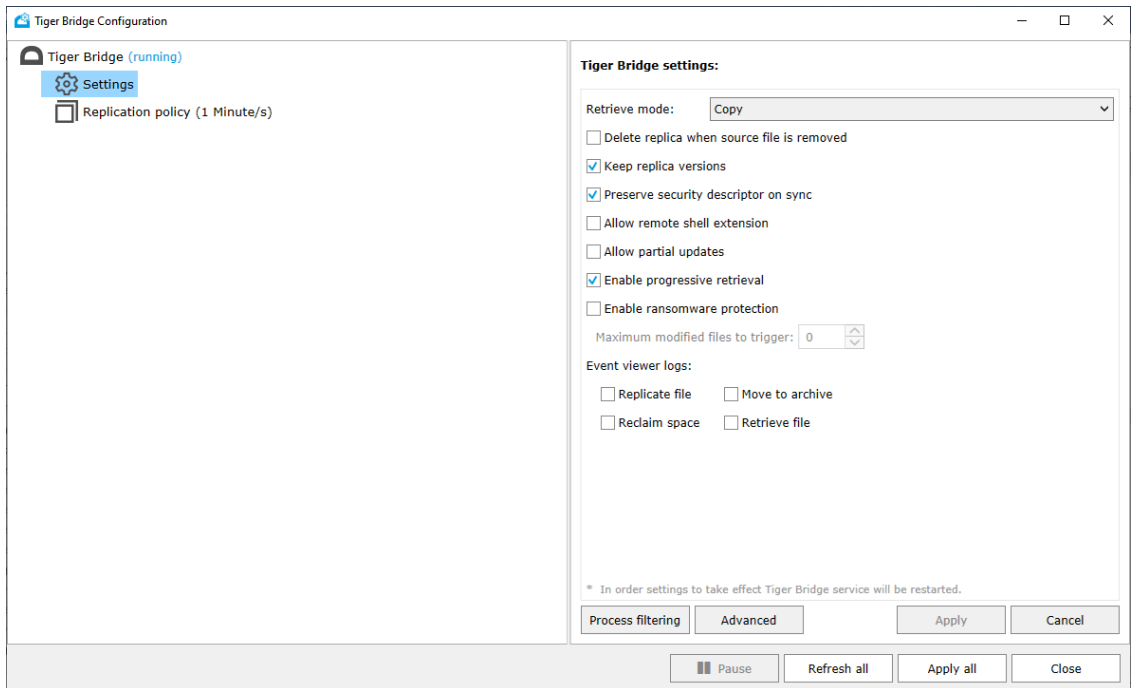
2. In the right pane, do one of the following:
- Select the "Enable ransomware protection" check box and in "Maximum modified files to trigger" enter the desired number.
- Clear the "Enable ransomware protection" check box to allow Tiger Bridge to re-replicate a file regardless of the number of files currently queued for re-replication.

3. 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 Number of Parallel Threads during Data Replication

By default, Tiger Bridge replicates files using four threads. You can increase or decrease the number of parallel threads in order to increase the replication speed, keeping in mind that using too many threads may hamper the performance of the Tiger Bridge computer.

To set the number of parallel threads during data replication:

1. In the left pane of the Tiger Bridge Configuration, click Settings.
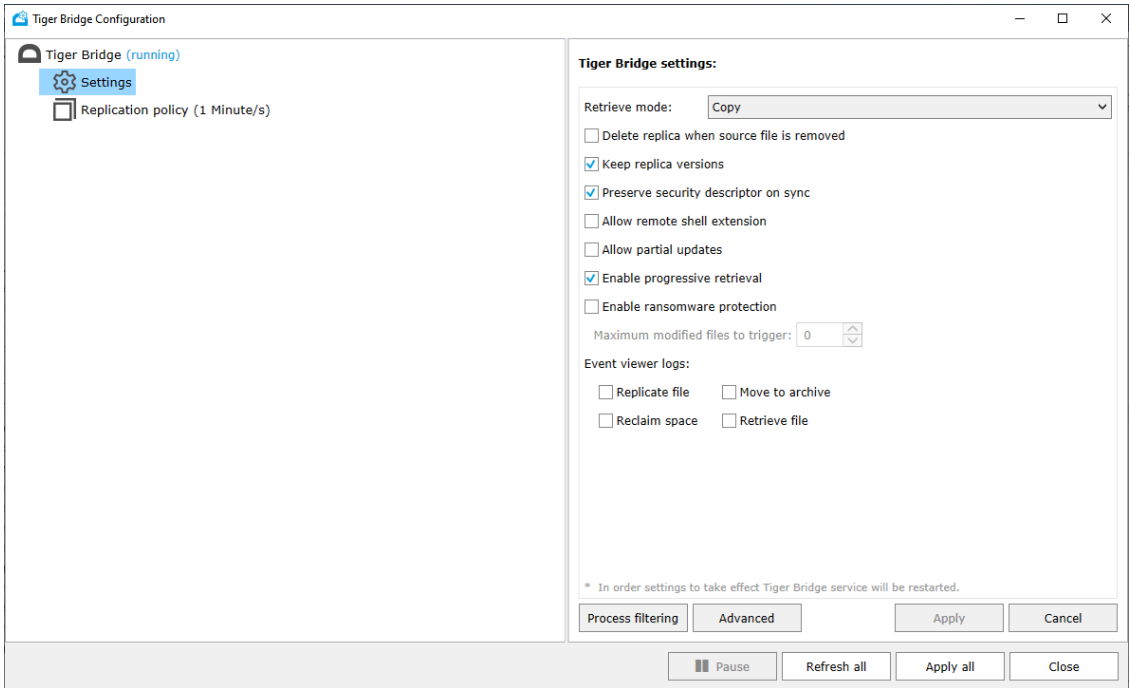
2. In the right pane, click Advanced.
3. In the "Threads count" field of the Advanced Settings dialog, specify the number of parallel threads used by Tiger Bridge during replication and then click OK
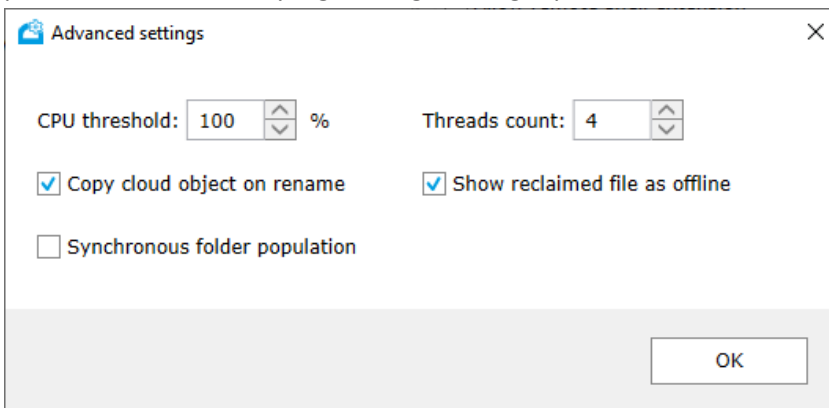
4. In the Settings pane, click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

Tiger Bridge 5.0.1 Administration Guide

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:

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

2. In the right pane, click Advanced.

134
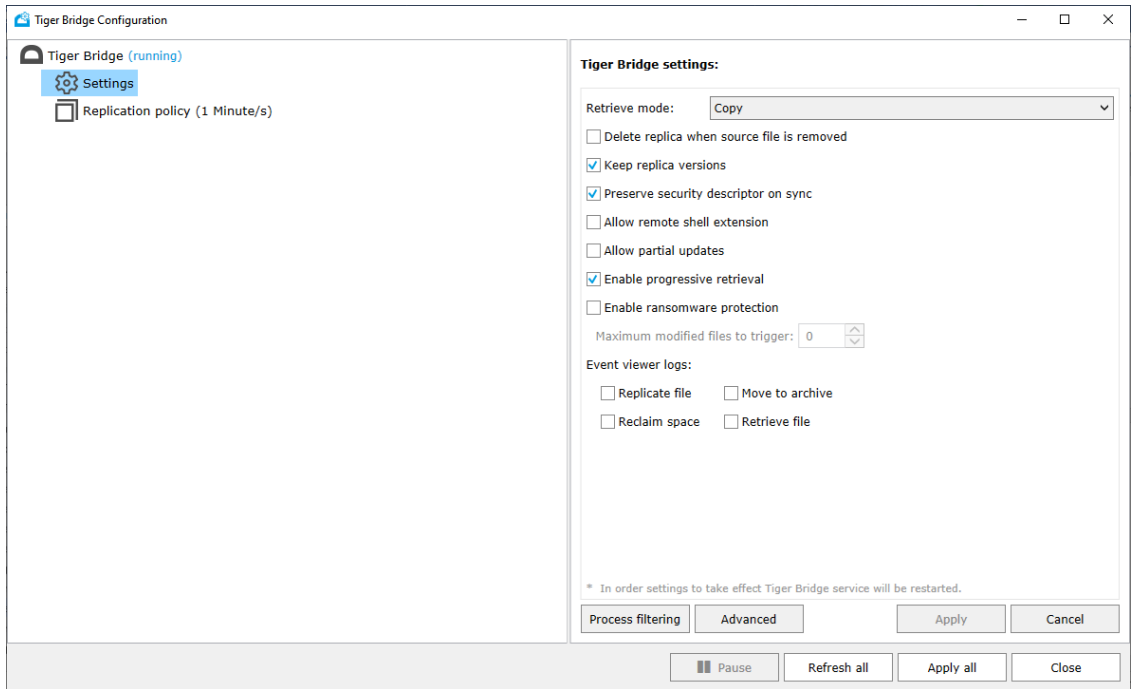
3. In the "CPU threshold" field of the Advanced Settings dialog, specify the percentage of CPU processing power data replication cannot exceed and then click OK.
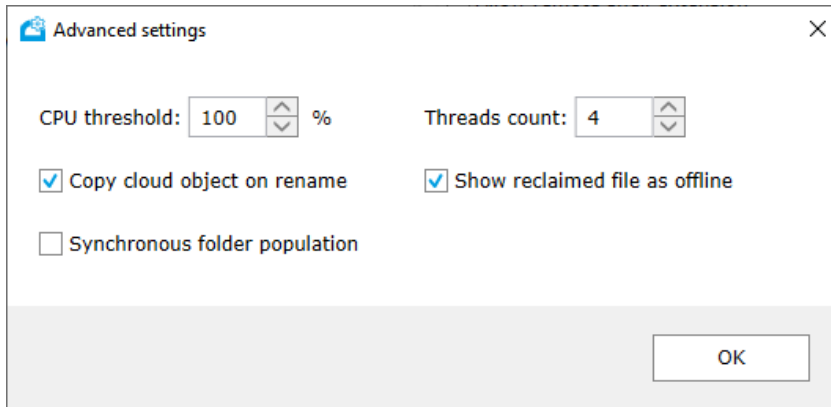
4. In the Settings pane, click Apply and when prompted, confirm that you want to restart the Tiger Bridge service.

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, which have been modified. Keep in mind that currently, partial file updates are supported only on Microsoft Azure, Backblaze B2 cloud storage, Amazon S3 object storage, Wasabi and IBM COS targets and on local volume source. Even if you enable it on other targets or on a NAS source, Tiger Bridge replaces the whole file and not just the modified parts of it.

To enable/disable partial file updates:

1. In the left pane of the Tiger Bridge Configuration, click Settings.
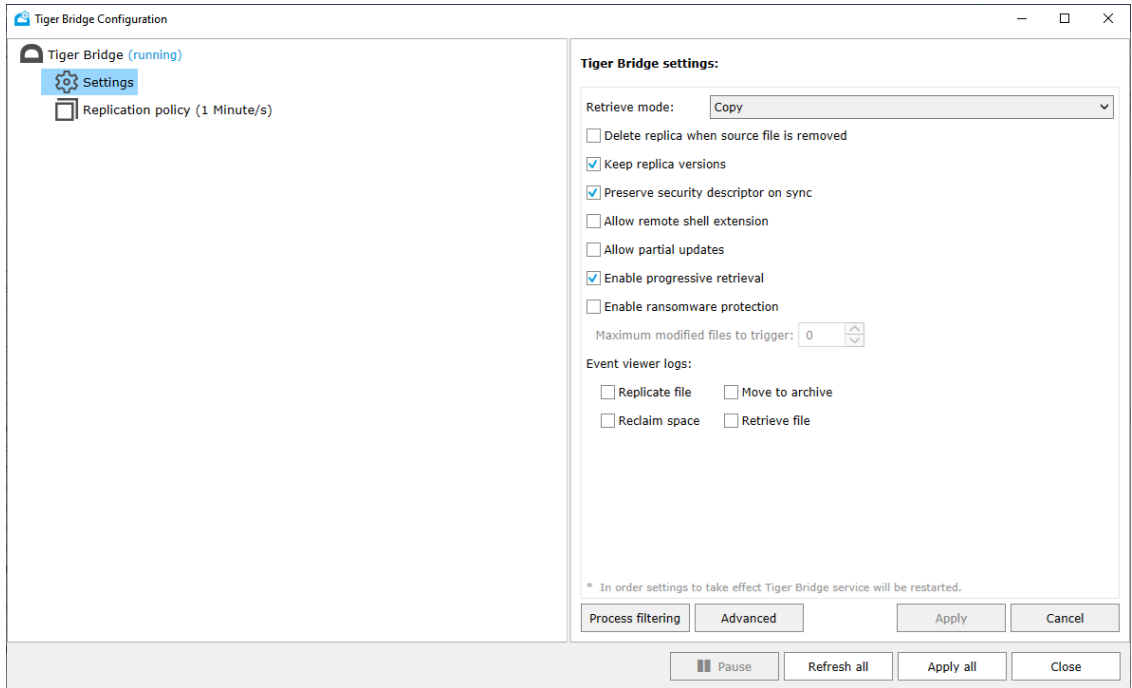
2. In the right pane, do one of the following:
- Select the "Allow partial updates" check box, to let Tiger Bridge upload on the target only the modified parts of an already replicated file.
- Clear the "Allow partial updates" check box, to replicate anew the whole file each time it is modified on the source.
3. Click Apply 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 have not been modified. You can also set Tiger Bridge to queue for replication only files whose size is above a given threshold, thus ignoring small files like log files, for example.

Note: The minimum file size for replication setting is valid only for files scheduled for automatic replication. Should you manually replicate a file with size below this minimum, this file will be replicated.

To specify minimum file size for it to be replicated:

1. Start the Registry Editor.
   Tip: To start Registry Editor, on the Start menu click Run and in the dialog type regedit.
2. Navigate to:
   HKEY_LOCAL_MACHINE\SOFTWARE\Tiger Technology\tiger-bridge\tiersvc\settings
3. Right-click the replication_min_filesize value and select Modify.
4. Do one of the following:
- To set Tiger Bridge to replicate any file regardless of its size, change the value to 0 and click OK.
- To set Tiger Bridge to schedule for automatic replication only files with size above the one you specify, enter the minimum file size in bytes and click OK.
   For example, to set Tiger Bridge to replicate only files whose size is above 100MB, enter 104857600 and click OK.
5. Run Command Prompt as an administrator and restart the Tiger Bridge service, by executing the following:
   ```
   net stop tiersvc
   net start tiersvc
   ```
   Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt and select "Run as administrator".

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

by creating a list of processes, which cannot trigger retrieval of nearline files. There is no need to create both lists. In case you create a list of processes allowed to trigger nearline file retrieval from the target, any process not included in the list will not trigger the operation when this process attempts to open the nearline file. In case you decide to specify the processes, which are not allowed to trigger file retrieval from the target, any process not mentioned in the list will trigger the nearline file retrieval when this process attempts to open that file.

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.
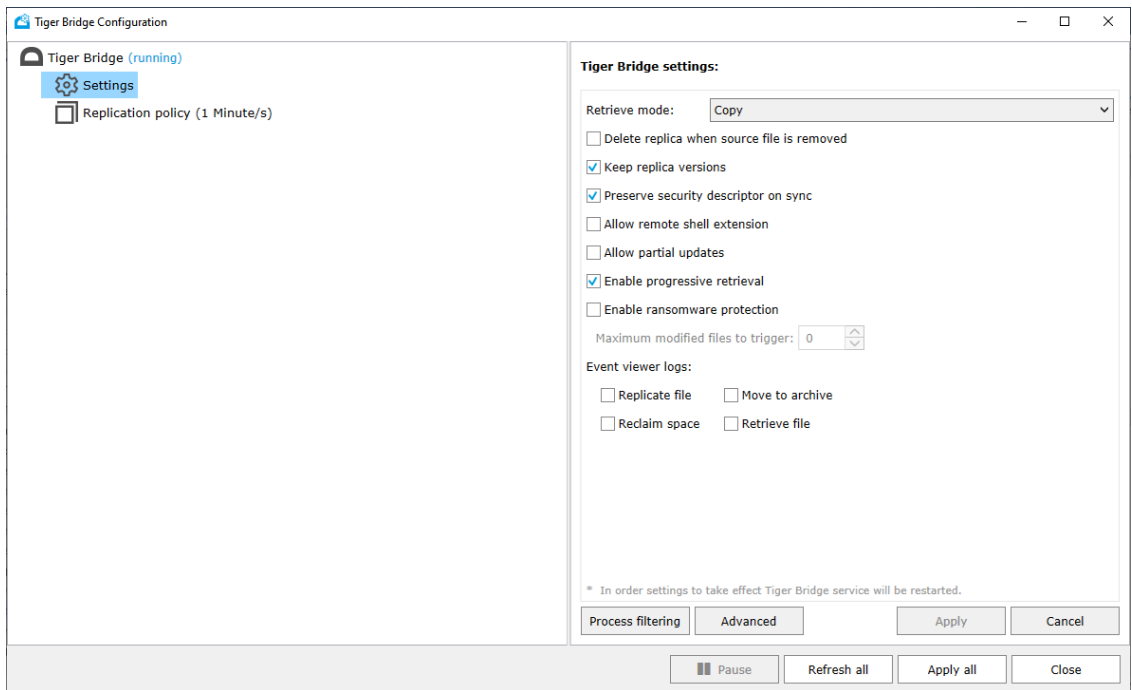
2. Click "Process filtering" and in the dialog, do one of the following:
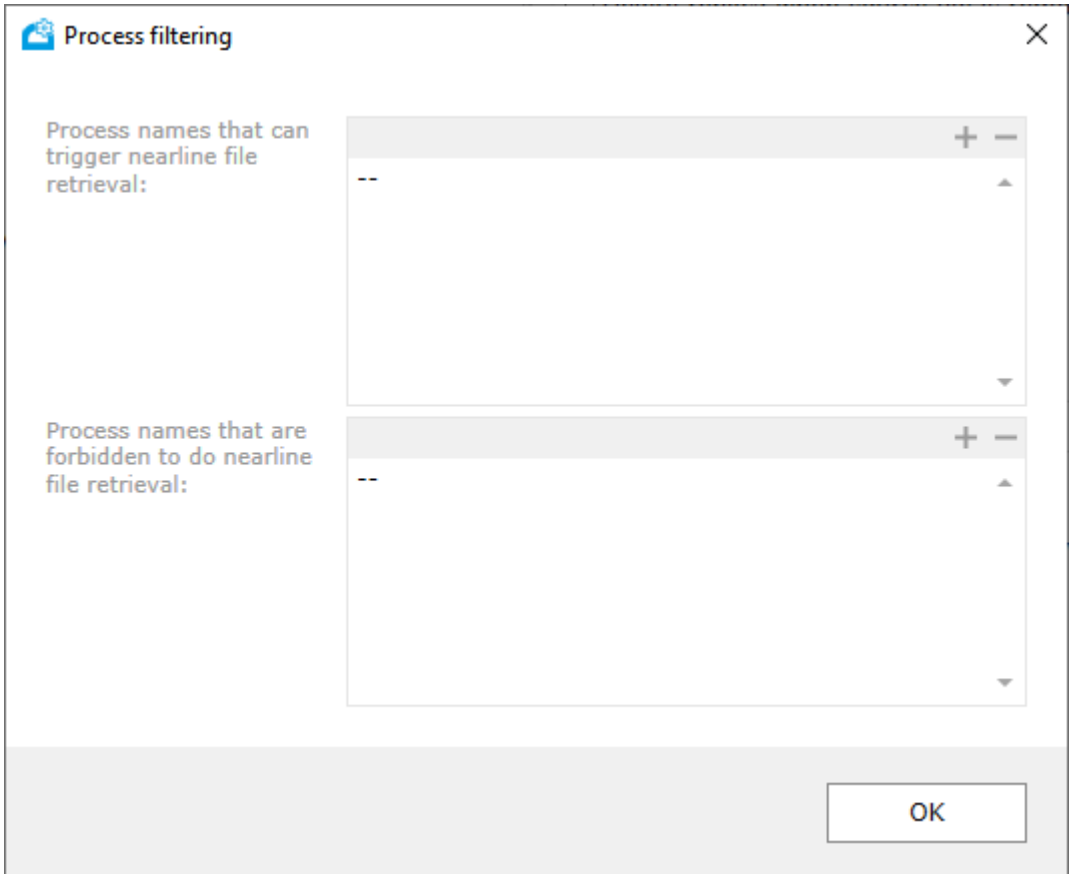
- Enter the name of a process in either the list of processes allowed to trigger the retrieving of nearline files or in the list of processes forbidden to trigger the retrieving of nearline files and click OK.
  Tip: Click the + button on top of each list to place the cursor at the end of each respective list.
- Delete a process from either list and then click OK.
  Tip: Click the - button on top of each list to remove the last process of the respective list.

3. In the 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.
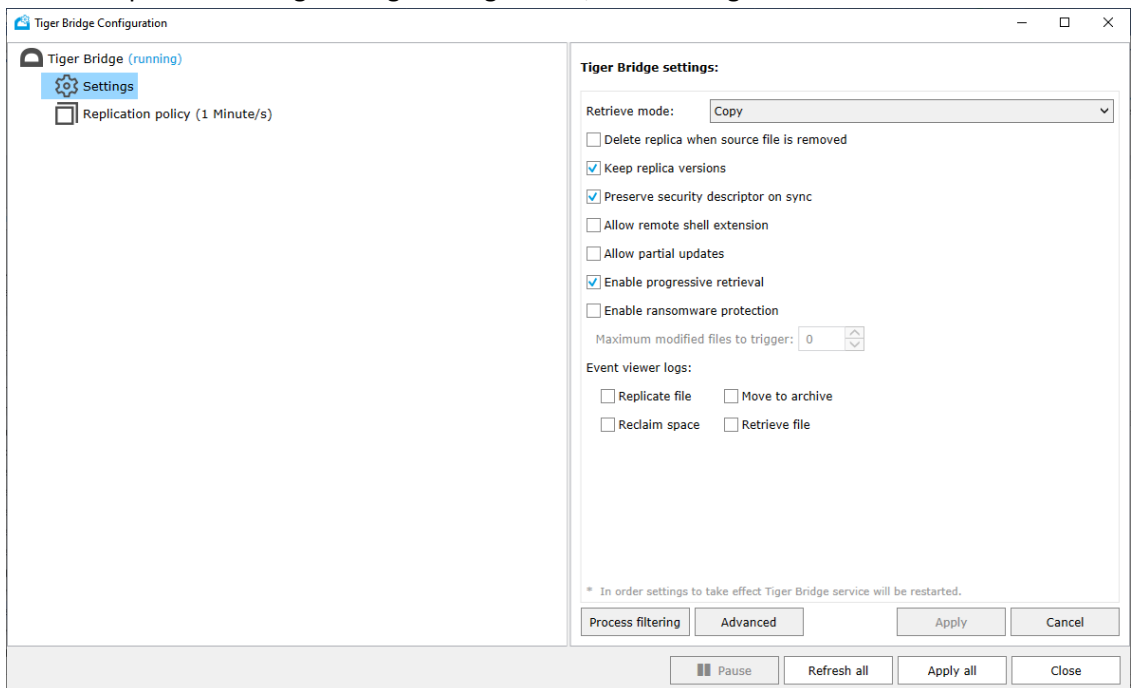
2. In the right pane, click Advanced.

3. In the Advanced Settings dialog, do one of the following:
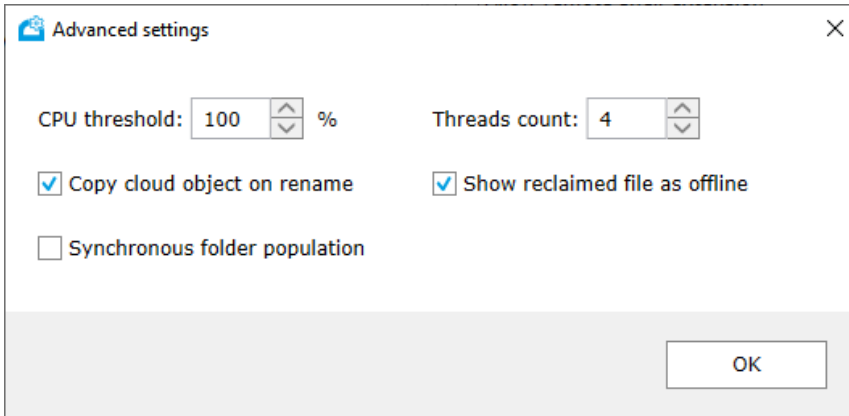
- Select the "Show reclaimed file as offline check box, to show the offline file attribute of stub files on all sources, then click OK.
- Clear the "Show reclaimed file as offline check box, to hide the offline file attribute of stub files on all sources, then click OK.

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 application this is the beginning of the file) and consecutively retrieves the rest, unless you close the file before reading it to its end. You can disable the progressive retrieval of data and configure Tiger Bridge to retrieve only the portion of the file, which is currently being read by the application as long as the respective application supports reading only portions of a file.

Important: For progressive file retrieval to work, reading of partially retrieved files must not be disabled.

To enable/disable progressive file retrieval:

1. In the left pane of the Tiger Bridge Configuration, click Settings.
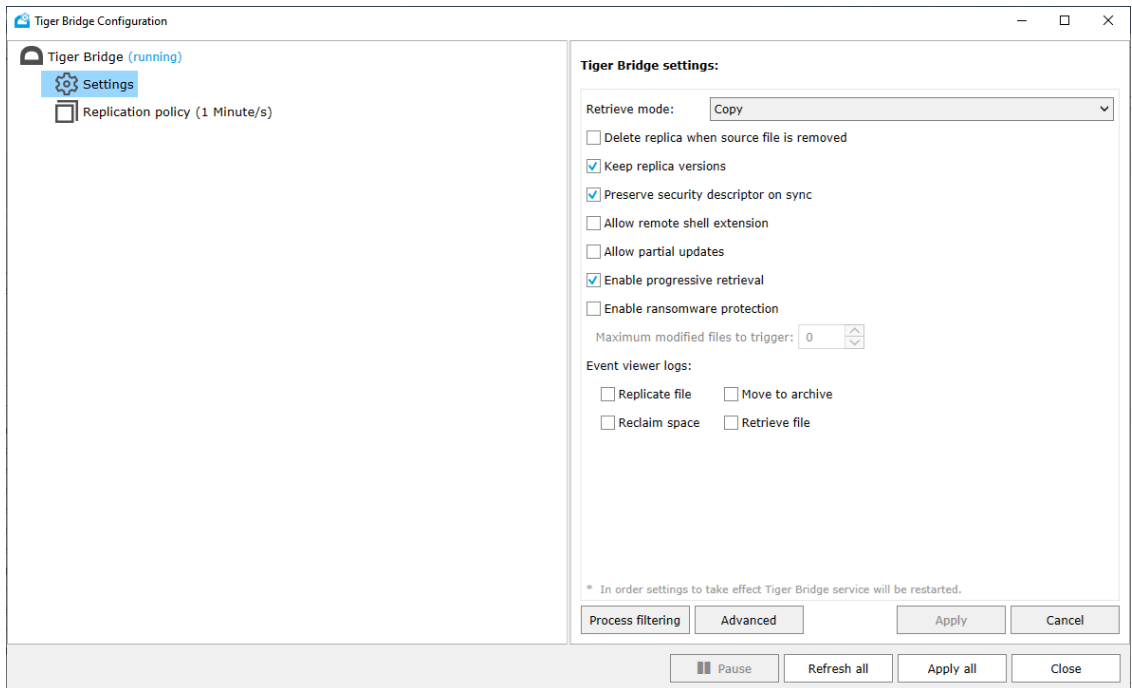
2. In the right pane, do one of the following:
- Select the "Enable progressive retrieval" check box, to let Tiger Bridge retrieve the whole file.
- Clear the "Enable progressive retrieval" check box, to let Tiger Bridge retrieve just the portion of the file, which is currently being read.
3. In the 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 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 and restart the Tiger Bridge service, by executing the following:
   ```
   net stop tiersvc
   net start tiersvc
   ```
   Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt and select "Run as administrator".

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 the purpose you must configure the following string values in the Tiger Bridge registry:

- active_restore_rehydrate_always_update_tier - specifies whether Tiger Bridge should check the tier of the target, on which a file is located. By default, this setting is disabled. Enabling it is indispensable, when you want to enable automatic rehydration on targets, like FujiFilm object archive, which do not notify Tiger Bridge when they move a file to their archive.

- active_restore_rehydrate - specifies whether Tiger Bridge should automatically rehydrate and then retrieve an offline file on the source.

Additionally, you can configure the processes that can trigger 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 and restart the Tiger Bridge service, by executing the following:

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

To specify the processes allowed to trigger automatic rehydration of offline files:

1. Start the Registry Editor.
   Tip: To start Registry Editor, on the Start menu click Run and in the dialog type regedit.
2. Navigate to:
   HKEY_LOCAL_MACHINE\SOFTWARE\Tiger Technology\tiger-bridge\tiersvc\settings
3. Right-click the active_restore_rehydrate_process_filter string value and select Modify.
4. Do one of the following:
- To allow any process to trigger the automatic rehydration of files, change the value to ! and click OK.
- To prevent any process from triggering the automatic rehydration of files, leave the value empty and click OK.
- To specify which processes can trigger the automatic rehydration of files, enter their names, starting and ending the list with a colon and separating each name with a colon, then click OK.
   Tip: For example, to specify that only Microsoft Paint and AutoCAD can trigger the automatic rehydration of files, enter the following:
   `:mspaint.exe:acad.exe:`
- To specify the processes which cannot trigger automatic rehydration of files, enter their names, starting the list with an exclamation mark followed by a colon, separating each process name with a colon and ending the list with a colon, then click OK.
   Tip: For example, to specify that any process except Microsoft Paint and AutoCAD can trigger the automatic rehydration of files, enter the following:
   `!:mspaint.exe:acad.exe:`
5. Run Command Prompt as an administrator and restart the Tiger Bridge service, by executing the following:
   ```
   net stop tiersvc
   net start tiersvc
   ```

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

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 on 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 the active_restore_partial string value and select Modify.
4. Do one of the following:
- To set Tiger Bridge to allow reading a nearline file, only when it has been fully retrieved, change the value to 0 and click OK.
- To set Tiger Bridge to allow reading a nearline file, when just a part of it has been retrieved only, change the value to 1 and click OK.
5. Run Command Prompt as an administrator and restart the Tiger Bridge service, by executing the following:
   ```
   net stop tiersvc
   net start tiersvc
   ```
   Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt and select "Run as administrator".

Set File Retrieve Timeout

When a user or application opens a nearline file on the source, Tiger Bridge attempts to retrieve it from the target before a specified timeout elapses. If no data begins retrieving before the timeout elapses, Tiger Bridge displays an error. If data begins retrieving, the timeout is reset, until data retrieval is halted, or the file is fully retrieved on the source. By

default, the timeout is set to 60 seconds. You can change the value of the timeout, thus adjusting it to the response time of your target and the connection to it.

Note: When the target cannot be reached or there is another problem, the timeout is not taken into consideration and Tiger Bridge displays an error.

To set the fixed timeout value for successfully retrieving a file:

1. Start the Registry Editor.
    Tip: To start Registry Editor, on the Start menu click Run and in the dialog type regedit.
2. Navigate to:
    HKEY_LOCAL_MACHINE\SOFTWARE\Tiger Technology\tiger-bridge\tiersvc\settings
3. Right-click the active_restore_timeout value and select Modify.
4. Enter the fixed timeout value in seconds and click OK.
    For example, to set the fixed timeout value to 2 minutes, enter 120 and click OK.
5. Run Command Prompt as an administrator and restart the Tiger Bridge service, by executing the following:
    ```
    net stop tiersvc
    net start tiersvc
    ```
    Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt and select "Run as administrator".

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

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

To change the space reclaiming policy file timestamp parameter:

1. Start the Registry Editor.
   Tip: To start Registry Editor, on the Start menu click Run and in the dialog type regedit.
2. Navigate to:
   HKEY_LOCAL_MACHINE\SOFTWARE\Tiger Technology\tiger-bridge\tiersvc\settings
3. Right-click the reclaim_space_time_type value and select Modify.
4. Do one of the following:
- To use the file access time as parameter, change the value to 0 and click OK.
- To use the file modification time as parameter, change the value to 1 and click OK.
5. Run Command Prompt as an administrator and restart the Tiger Bridge service, by executing the following:
   ```
   net stop tiersvc
   net start tiersvc
   ```
   Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt and select "Run as administrator".

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 and restart the Tiger Bridge service, by executing the following:
```
net stop tiersvc
net start tiersvc
```
Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt and select "Run as administrator".

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 to retrieve 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 not an 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 source and 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. Start Command Prompt as administrator.

   Tip: In the Start menu, type cmd, right-click Command Prompt and then 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 configure 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. Start Command Prompt as administrator.

   Tip: In the Start menu, type cmd, right-click Command Prompt and then 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. Start Command Prompt as administrator.
   Tip: In the Start menu, type cmd, right-click Command Prompt and then 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 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 Active Sync

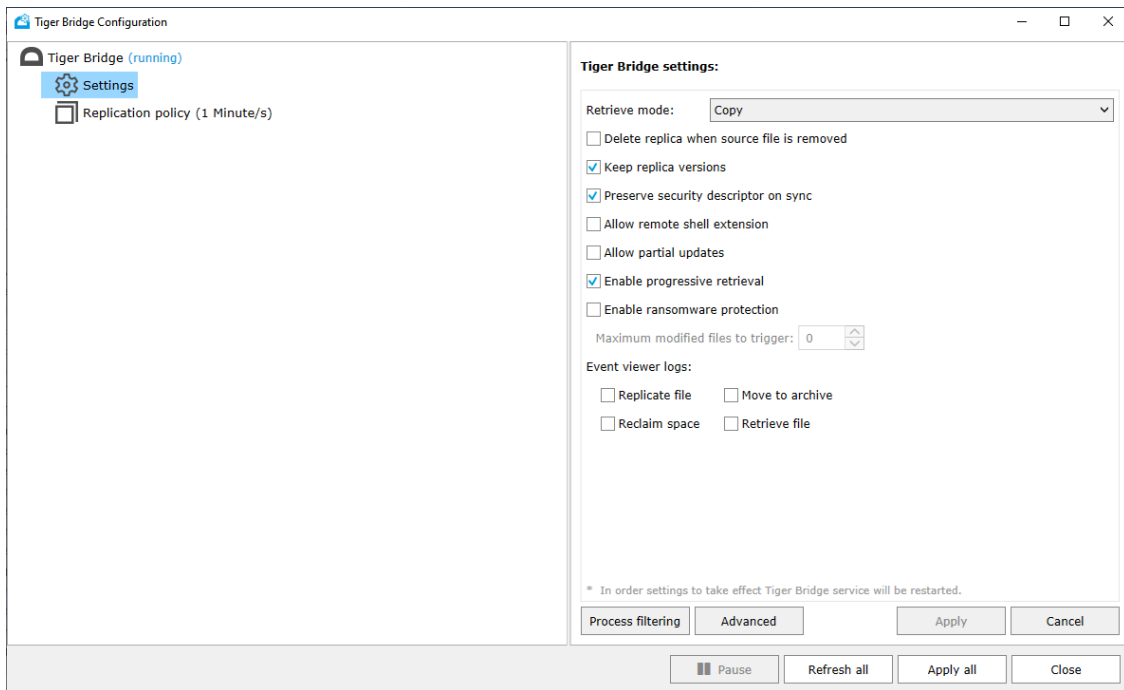### Preserve the Security Descriptor of Retrieved Files

You can configure Tiger Bridge to keep a file's security descriptor when it is being retrieved on other sources through Active 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.

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 on this source from other sources, change the value to 1 and click OK.
    - to retrieve files on this source without preserving their security descriptor, change the value to 0 and click OK.
8. Run Command Prompt as an administrator and restart the Tiger Bridge service, by executing the following:
    ```
    net stop tiersvc
    net start tiersvc
    ```
    Tip: To run Command Prompt as an administrator, click Start, type cmd, right-click Command Prompt and select "Run as administrator".

5

Manually Manage Data

Perform Manual Data Lifecycle Operations

Manage Files That Have Failed to Replicate

Manually Synchronize Sources Through a Common Target

Recover Data from The Target

Revert File Modifications on the Source

Undelete Data from the Source

Manage Files and Folders Versions

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

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 which 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 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.
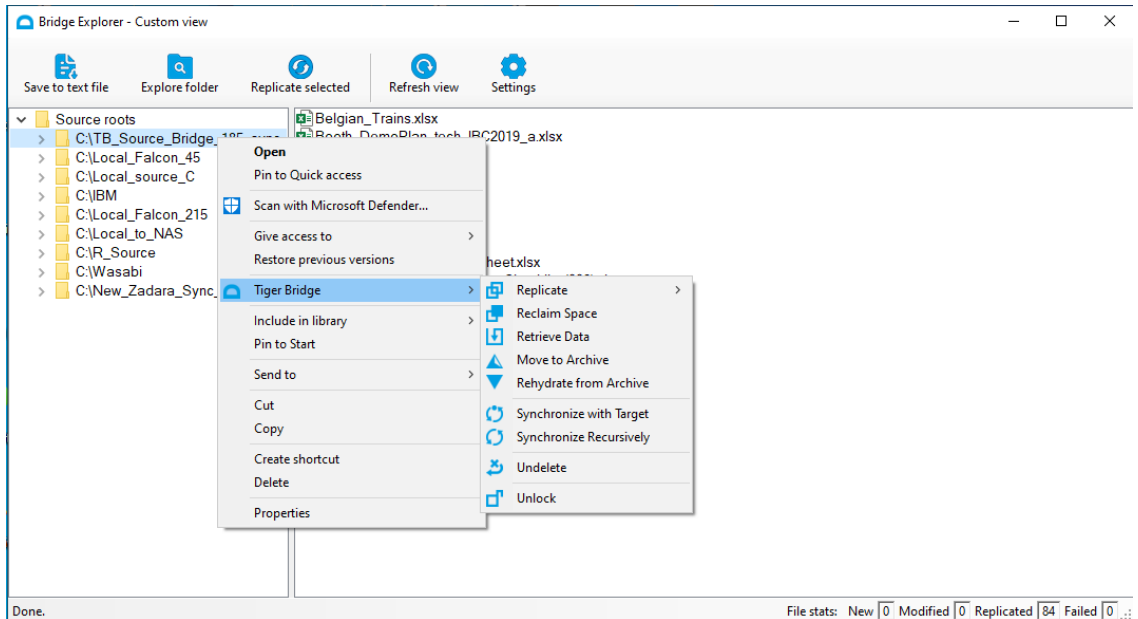
Manage Files That Have Failed to Replicate

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, following these steps:

1. Start Command Prompt as administrator.
    Tip: In the Start menu, type cmd, right-click Command Prompt and then select "Run as administrator".
2. Execute 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.
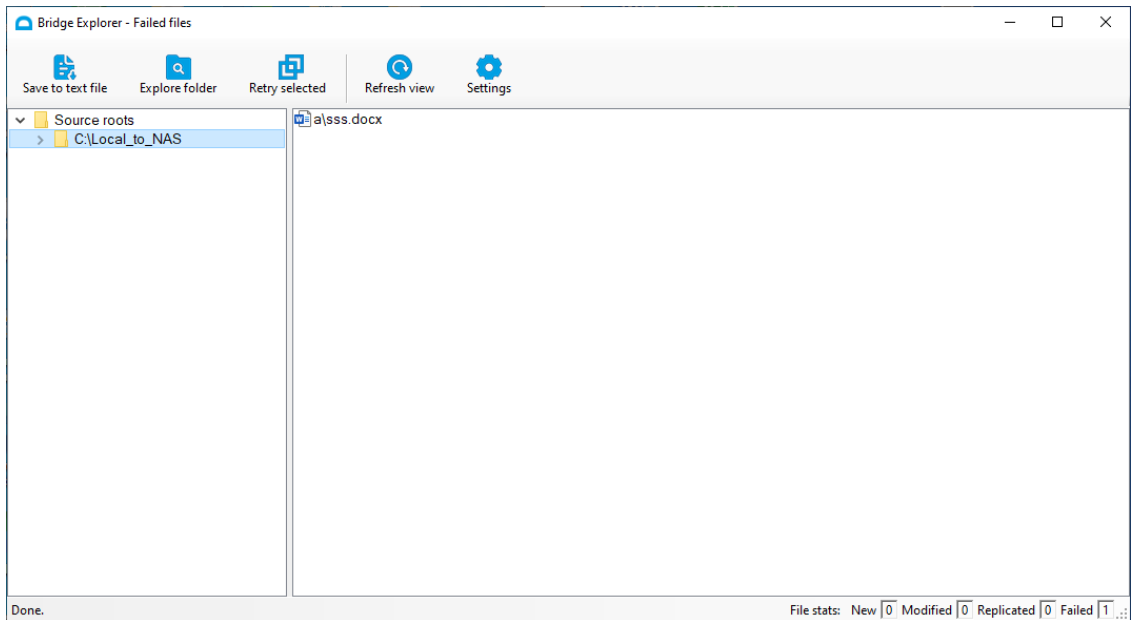
4. Repeat the above step for each source, listed in the left pane.

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 Active 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.
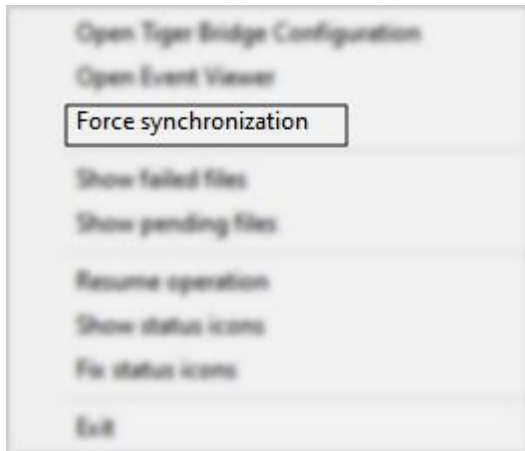
Recover Data from The Target

In contrast to retrieving reclaimed data that is available on the source only in the form of stub files, manually synchronizing the contents of 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 disaster, if you use 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 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.
- 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 the 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 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 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 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 and having copies on the target.
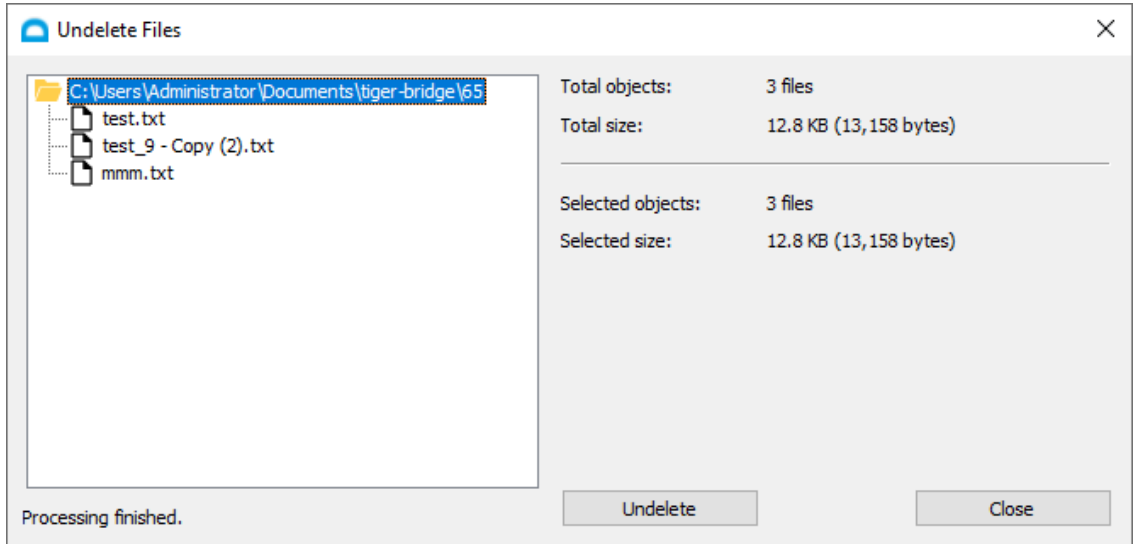
4. Browse to and select a file in the list, then click Undelete.
   Note: To undelete all files in a folder or a sub-folder, select it in the left pane and click Undelete.
   The undeleted files appear on your source as nearline or offline files, which you can retrieve manually or on demand.
   Important: 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, following the steps in Configure Versioning, 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.)

To help you manage versions more efficiently, Tiger Bridge allows you to analyze the contents of a whole folder on your source using a selected point in time as a starting point. The analysis gives you information not only about the total number of files with versions in the folder and the overall size of all versions on the target, but also about the number and size of versions replicated before the selected date and time, and the number and size of file versions, replicated on the target after the selected date and time. With this information in mind, Tiger Bridge then allows you to:

- Delete any selected or all older versions of a file from the target, discarding them as obsolete and thus freeing space on the target. In case the deleted version of a file is the one to which the file on the source is actually linked (i.e. the one that would normally be retrieved, if you attempt to open it), Tiger Bridge automatically links the file to the newest version on the target.
- Delete any selected or all newer versions of a file from the target, discarding them as obsolete and thus freeing space on the target. Newer versions of a file can be considered obsolete, if, for example, they are encrypted versions, replicated on the target after your source has suffered a ransomware attack. In case the deleted version of a file is the one to which the file on the source is actually linked (i.e. the one that would normally be retrieved if you attempt to open it), Tiger Bridge automatically links the file to the last version on the target, which has been submitted before the selected date and time. In case the deleted version of the file is the only version of the

file, it is deleted from both the source and the target, but you can undelete it from the source, as long as a copy is still available in a snapshot on the target.

- Restore the version of one or all files in the folder to the last submitted version before the selected date and time. When performing this operation, you can also select to automatically retrieve on the source 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 on the NAS source.

To restore a specific version of a file:

1. In Windows Explorer, right-click the file and select Properties.
2. In the Properties dialog, select the Versions tab.
   Tiger Bridge lists all available versions of the file in descending order, starting with the newest one. The icon of each version designates the tier on the target it is stored on,

and the version currently stored on the source is displayed with a check mark.
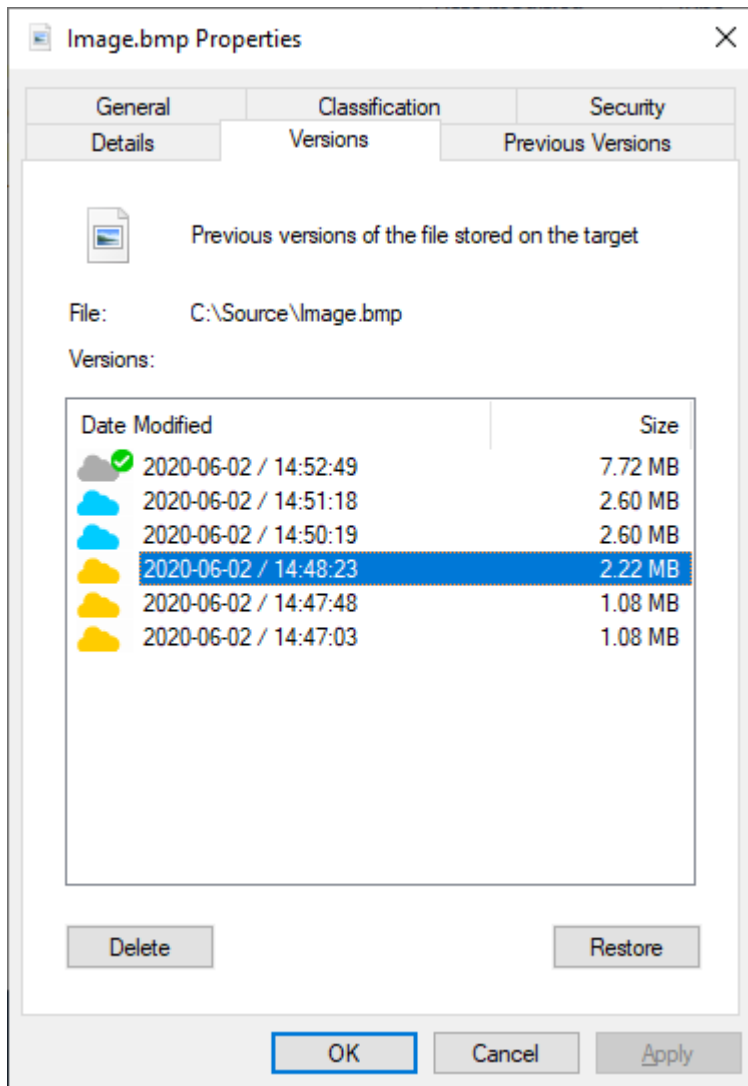
3. Select a file version in the list and click Restore.

To delete a specific version of a file:

1. In Windows Explorer, right-click the file and select Properties.
2. In the Properties dialog, select the Versions tab.

Tiger Bridge lists all available versions of the file in descending order, starting with the newest one. The icon of each version designates the tier on the target it is stored on, and the version currently stored on the source is displayed with a check mark.
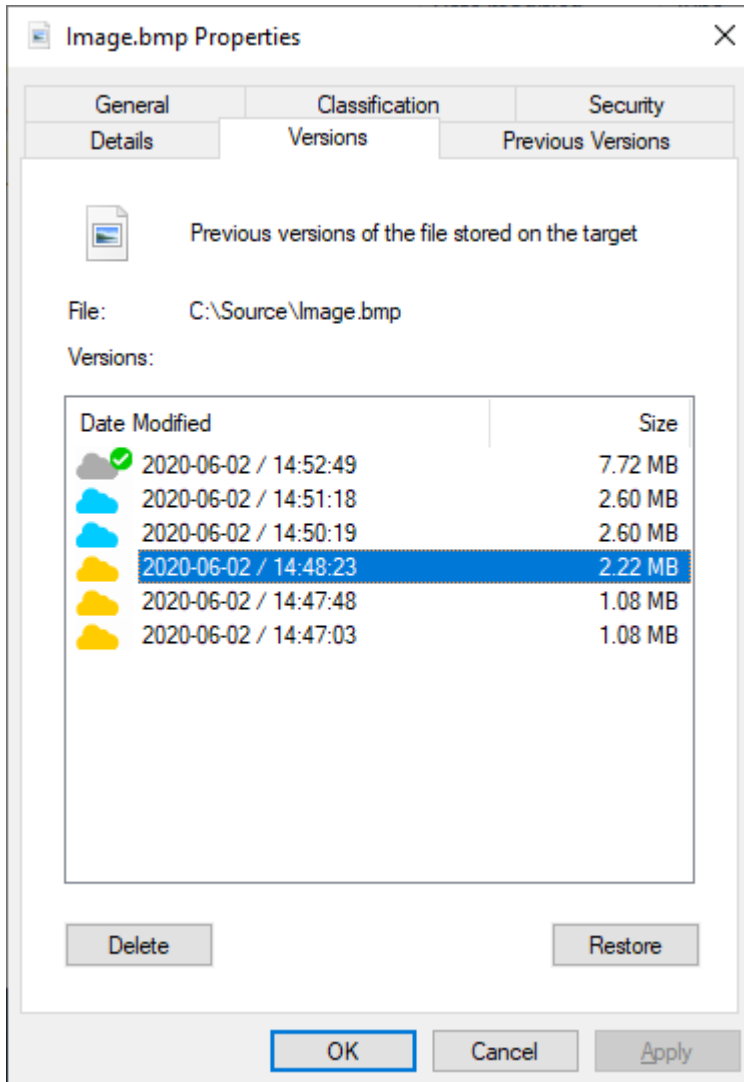
3. Select a file version in the list and click Delete to delete it from the target.
   Note: If you delete the version, which is currently stored on your source i.e., the one with a check mark in its icon, the file on the source is automatically linked to the

newest version of the file on the target. You cannot delete a version of a file, if it is the only version on the target.

To analyze the contents of a folder:

1. In Windows Explorer, right-click the folder and select Properties.
2. In the Properties dialog, select the Versions tab.
3. Select the desired date and time in the Timestamp boxes and then click Analyze Content.
   Note: Depending on the number of files in the folder and their size the analysis may take time. Keep track of the progress bar below, to make sure Tiger Bridge has

gathered the complete information.
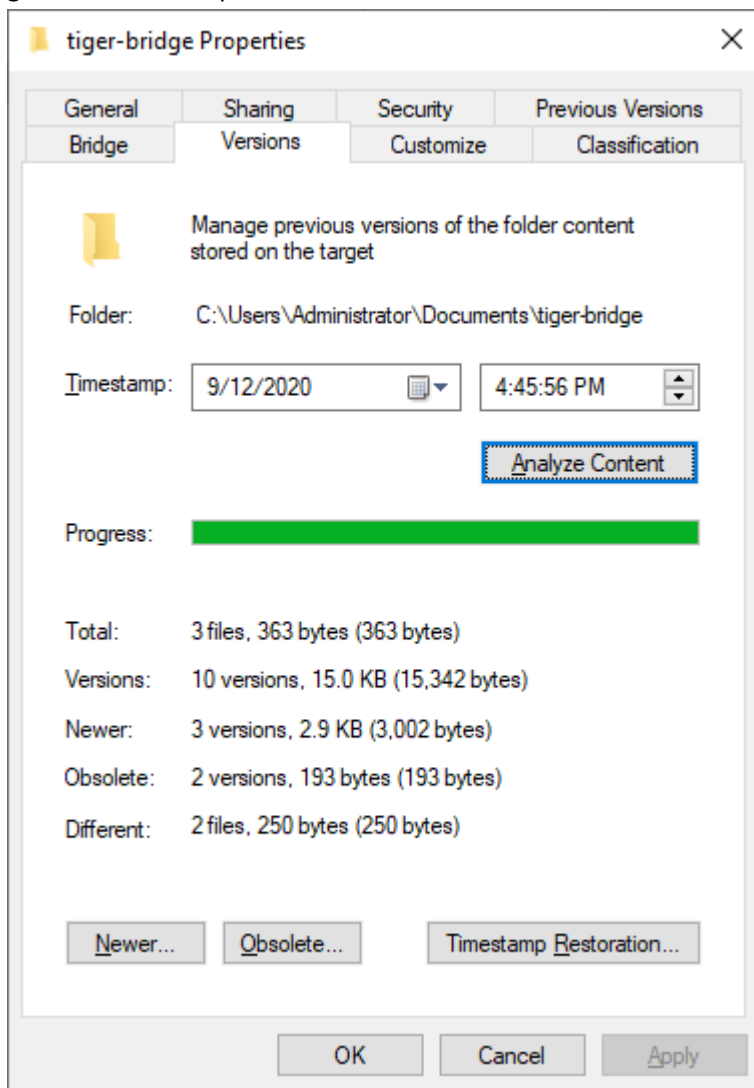
4. Tiger Bridge gives you the following information:

- 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.
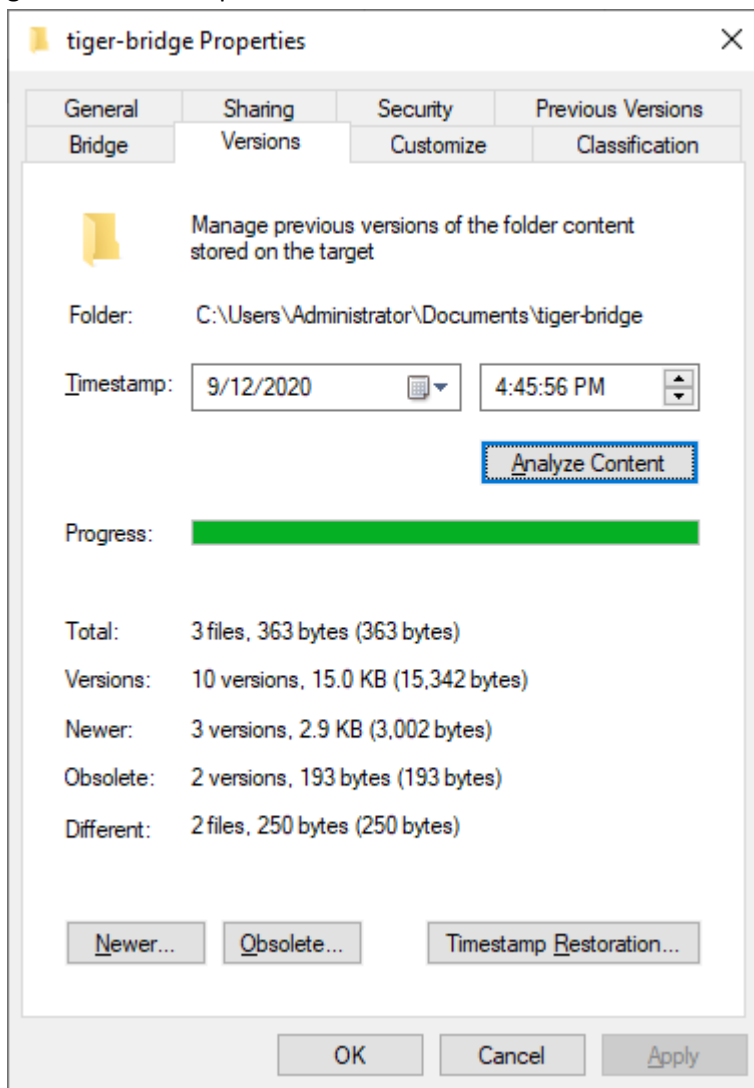
4. Click "Timestamp Restoration…".

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.
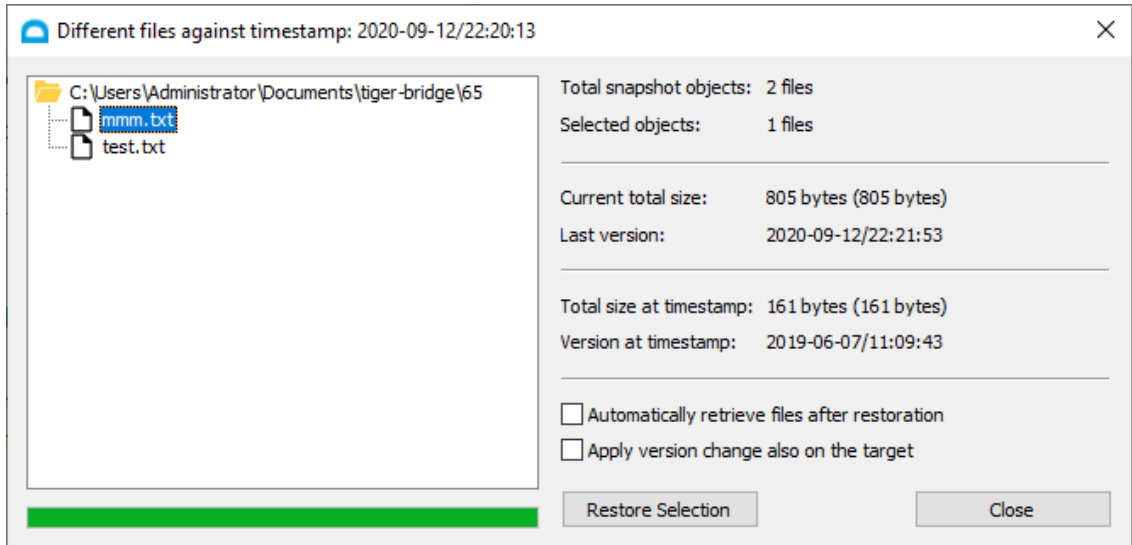
5. Do one of the following:
- In the left pane of the dialog, select a folder, to restore all its files to their version, replicated before the selected timestamp.
- Browse to and select a file, to restore its version to the one, replicated before the selected timestamp.
6. Select whether to automatically retrieve on the source each file, whose current version differs from the one, which will be restored.
7. Select whether the version, which will be restored on the source should be added as a newest version on the target.
8. Click Restore Selection.

To delete obsolete versions of files in a folder:

1. In Windows Explorer, right-click the folder and select Properties.
2. In the Properties dialog, select the Versions tab.
3. Select the desired date and time in the Timestamp boxes and then click Analyze Content.
   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.
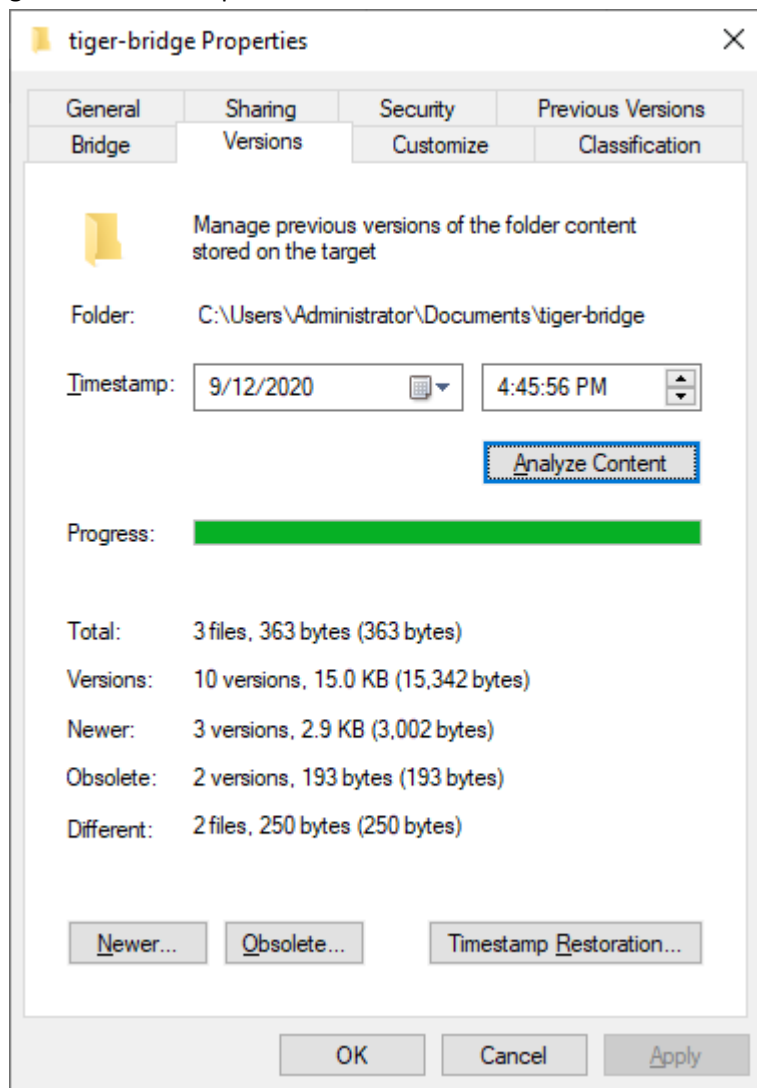
4. Click Obsolete.
5. Tiger Bridge displays a dialog, listing all versions of a file, which have been replicated before the selected time and date, giving you information about the size of each

version as well as about the total size of all versions.

Obsolete versions against timestamp: 2020-09-12/16:45:59		✕
📁 C:\Users\Administrator\Documents\tiger-bridge\65	Total objects:	1 files
⊟ 📄 test.txt	Total versions:	3 versions
2020-09-12/16:45:56	Total size:	132 bytes (132 bytes)
2020-09-12/16:42:20		
2020-09-12/16:42:20	Selected objects:	1 files
	Selected versions:	3 versions
	Selected size:	132 bytes (132 bytes)
	Delete Selection	Close

6. Do one of the following:

    • Select a whole folder, to delete all versions of all its files, which have been replicated before the selected date and time.

    • Select a file, to delete all its versions, which have been replicated before the selected date and time.

    • Select a file version, to delete just this version of the file.

    Important: If you are deleting the version of a file, to which the current file on the source is pointing, the file will automatically be linked to the newest version on the source. If the file does not have a newer version, Tiger Bridge deletes as obsolete only the versions before the one to which the file on the source currently points.

7. Click Delete Selection.

To delete newer versions of files in a folder:

1. In Windows Explorer, right-click the folder and select Properties.
2. In the Properties dialog, select the Versions tab.
3. Select the desired date and time in the Timestamp boxes and then click Analyze Content.
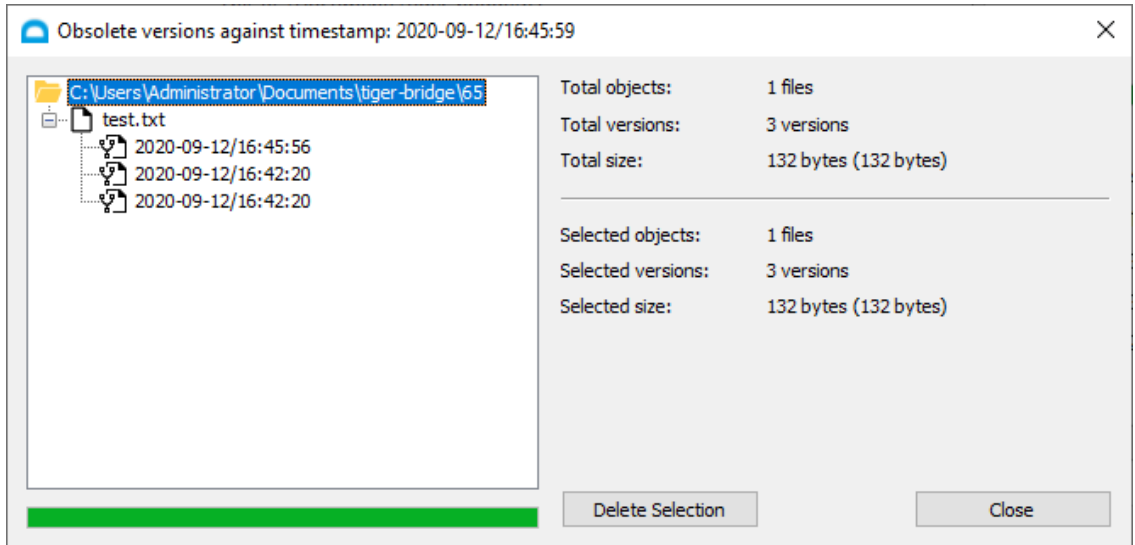
    Note: Depending on the number of files in the folder and their size the analysis may take time. Keep track of the progress bar below, to make sure Tiger Bridge has gathered the

complete information.
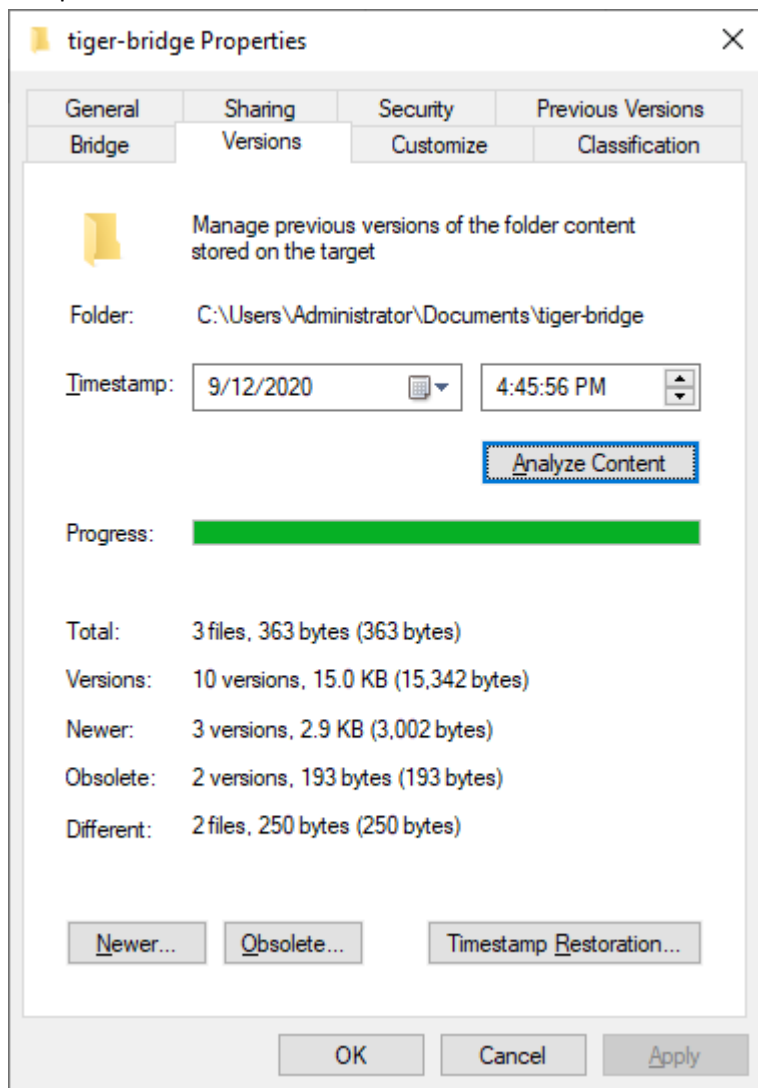
4. Click Newer.

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

as well as about the total size of all versions.
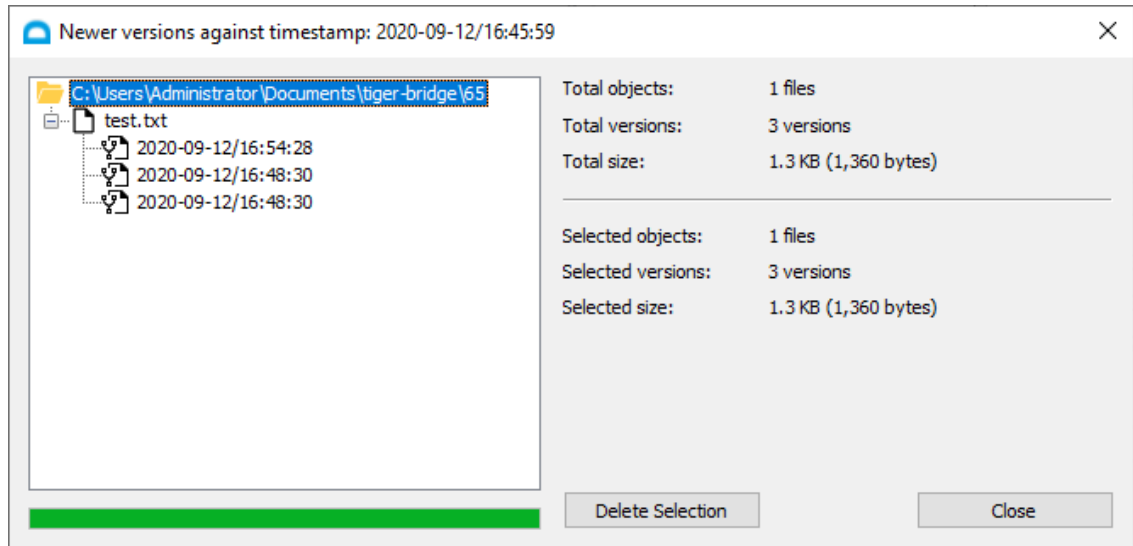
5. Do one of the following:
   - Select a whole folder, to delete all versions of all its files, which have been replicated after the selected date and time.
   - Select a file, to delete all its versions, which have been replicated after the selected date and time.
   - Select a file version, to delete just this version of the file.
6. Click Delete Selection.

6

Monitor Tiger Bridge

Tiger Bridge Configuration and Tray Icon

Monitor Data in the Tiger Bridge Explorer

Tiger Bridge Shell Extension and Windows Explorer

Event Viewer

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

Tiger Bridge Configuration and Tray Icon

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:

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

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:	S8S32-23INE-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 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.

Statistics	0.03 % replicated		Apply	Cancel
	▶ Resume	Refresh all	Apply all	Close
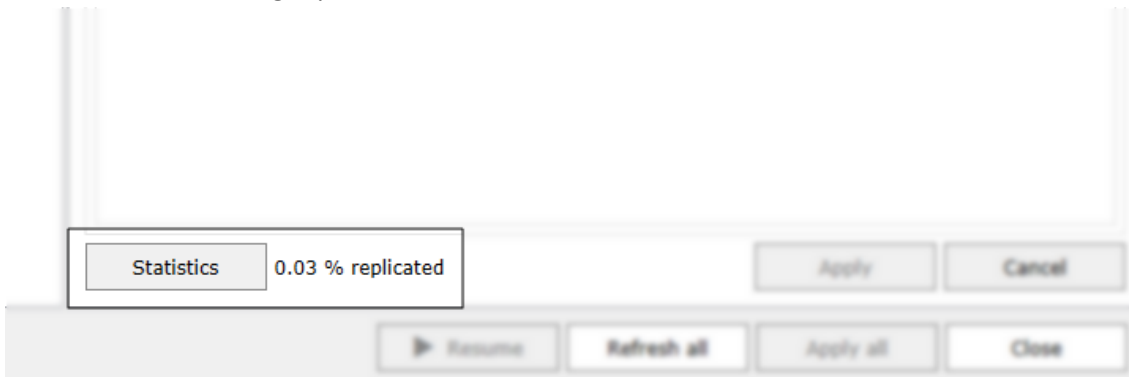
Monitor Tiger Bridge Using the Tray Icon

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 the Tiger Bridge Explorer

The 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 the 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, following the steps in Perform Manual Data Lifecycle Operations.

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

By default, you can use two pre-defined filters:

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

By default, these pre-defined 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 the Tiger Bridge Explorer, 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).
- Target tiers:
  - Unknown – displays the files having copies on a non-object storage target

- o Hot – displays the files having copies on the equivalent of the hot tier of the target
- o Cool – displays the files having copies on the equivalent of the cool tier of the target
- o Archive – displays the files having copies on the equivalent of the archival tier of the target

    Note: When no tier check box is selected, the Tiger Bridge Explorer displays data on all available tiers.

- Flat listing:
  - o 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.
  - o 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 the Tiger Bridge Explorer displays the total numbers about a selected source.

To filter data displayed in the Tiger Bridge Explorer:

1. Right-click the Tiger Bridge tray icon and click either "Show failed files" or "Show pending files".

2. In the Tiger Bridge Explorer, click Settings.
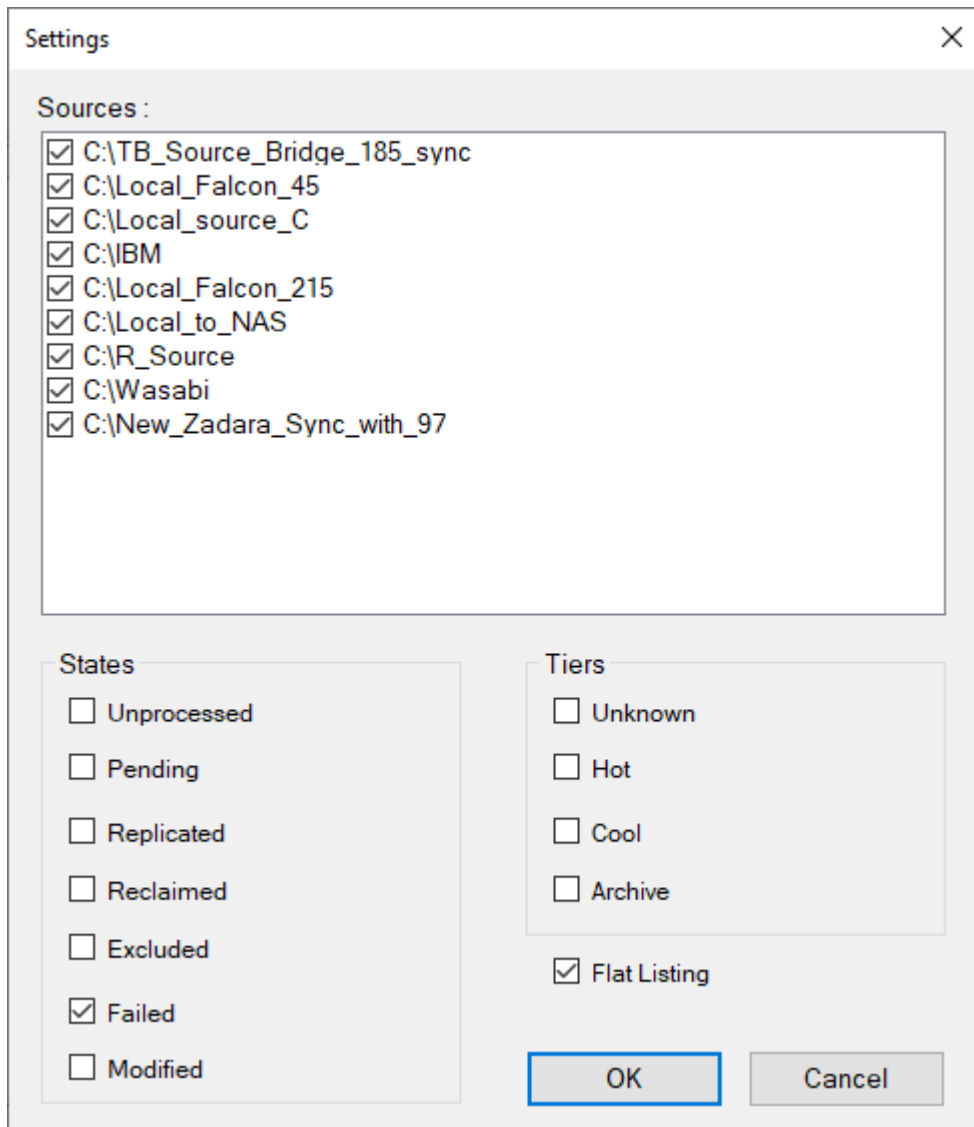
3. Select or clear the desired check boxes and click OK.

To save a list of the filtered results:

1. Right-click the Tiger Bridge tray icon and click either "Show failed files" or "Show pending files".

2. In the Tiger Bridge Explorer, click Settings and apply the desired filters.

3. In the left pane of the Tiger Bridge Explorer, navigate to the desired source or any of its sub-folders to display the filtered results in the right pane.

4. Click "Save to text file" and choose where to save the list.

To open the browsed path in Windows Explorer:

1. Right-click the Tiger Bridge tray icon and click either "Show failed files" or "Show pending files".
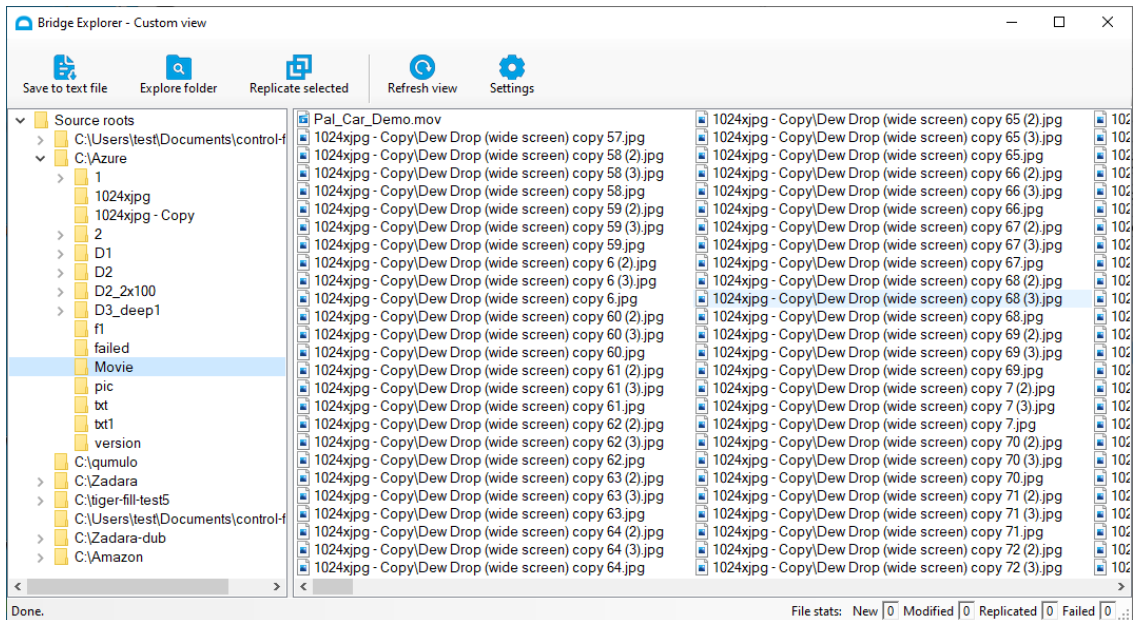
2. In the Tiger Bridge Explorer, click Settings and apply the desired filters.

3. In the left pane of the Tiger Bridge Explorer, navigate to the desired source or any of its sub-folders to display the filtered results in the right pane.
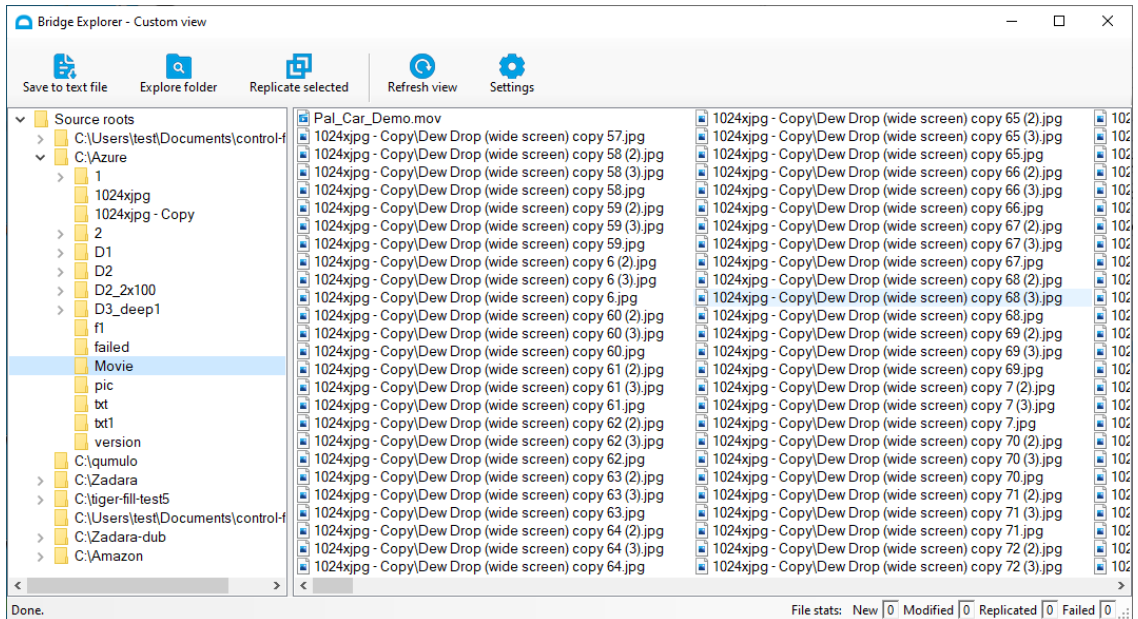

4. Click "Explore folder" to open the browsed path in Windows Explorer.

Tiger Bridge Shell Extension and Windows Explorer

Monitor Data Status

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, following the steps in Manage Shell Extension Icon Overlays.

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).
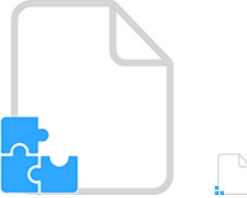
To select the icon overlays statuses that you will use:

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
No overlay	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.		
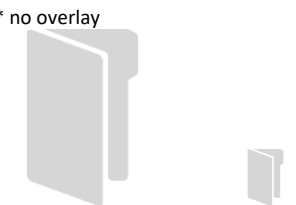
File icon	With replication policy	Without replication policy	Legacy status
	This file has a copy only on the target and cannot be retrieved immediately for one of the following reasons: • This is an offline file (its copy is on the archival tier of the target) and to retrieve it on the source you must first rehydrate it. • This is a nearline file (its copy is on the hot/cool tier of the target), but at the moment the target is inaccessible, and you cannot retrieve it on the source.	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.	
	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 on the source only partially. For more information about partial data retrieval, refer to Progressive File Retrieval.	-	
	Replication of the file has failed.	-	

Folder Icon Overlays

Folder status unlike file status often designates a combination of statuses as it may contain heterogenous files.

Folder 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.		
* no overlay	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.	-	

❄️ (folder icon)	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 on the source.	The folder contains at least one offline file.	
▶️ (folder icon)	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.	-	-
🧩 (folder icon)	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.	-
➕ (folder icon)	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 on the source on demand.		

	N/A	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.
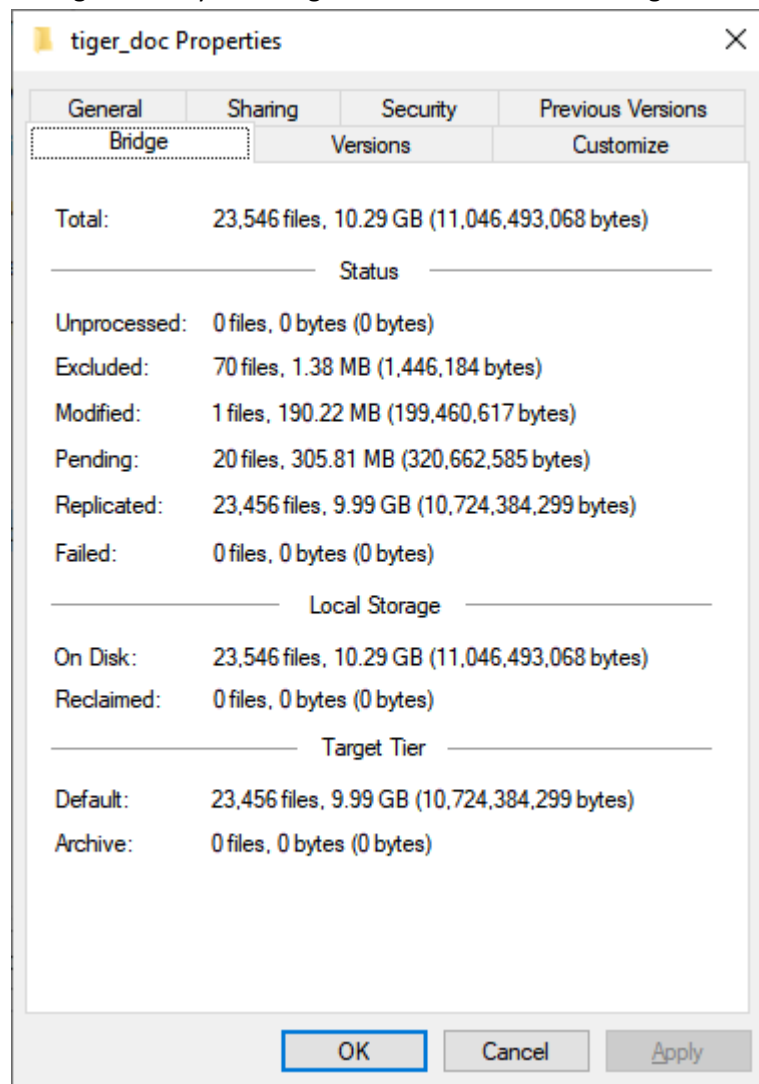
The statistics are divided in the following categories:

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

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, following these steps:

1. In the left pane of the Tiger Bridge Configuration, click Settings and then do one of the following in the right pane:
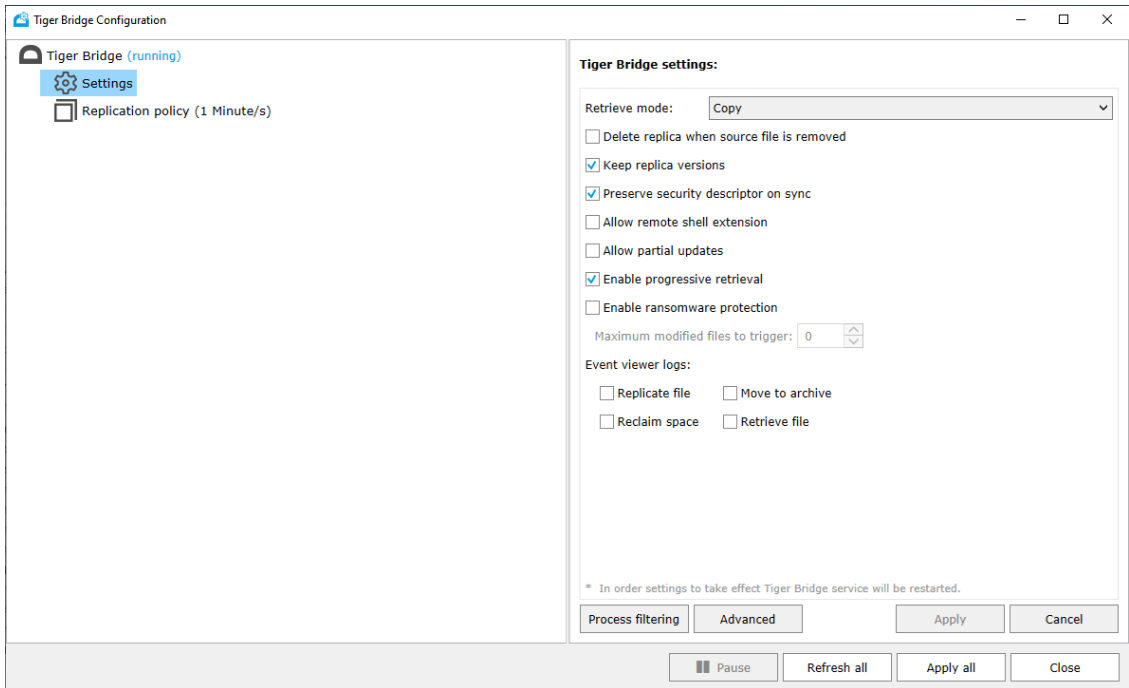
- Select the check box of an operation, to let Tiger Bridge output logs for it in Windows Event Viewer.
- Clear the check box of an operation, to prevent Tiger Bridge from outputting logs for it in Windows Event Viewer.

2. 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 operation.

Success - logs information about successfully performed operation.

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

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

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.

Appendix 1: Tiger Bridge Command-line Interface

Activate Tiger Bridge

View Activation Status

    tiercli license info

Activate Tiger Bridge using SaaS License

    tiercli license saas <username> <password>

Example:

    tiercli license saas JohnSmith P@ssword

Deconfigure the SaaS License Credentials

    tiercli license saas deconfigure

Activate Tiger Bridge with a Software Activation Key

    tiercli license soft <activation key>

Example:

    tiercli license soft 5ZRPF-ALZ8D-ZV7WZ-S271N-VNTCW

Activate Tiger Bridge with a Software-protection Dongle

    tiercli license hasp <path to lic file >

Example:

    tiercli license hasp C:\Users\user\Downloads\license.lic

Configure Tiger Bridge

Important: To apply any changes to the Tiger Bridge configuration, reload it by executing the following command:

    tiercli config reload

View Current Configuration

    tiercli config show

Add NAS Source

    tiercli config <control folder path> naas <sharepath> <username> <password>

Example:

tiercli config D:\NasSource naas \\testsrv\share test 1234

Pair Source with Target

Microsoft Azure

> I.   Using Account Key or SAS Token

1. tiercli config <source or control folder path> target azure <account_name> <account_key or SAS token> <blob_endpoint>

2. tiercli config <source or control folder path> container <container name>

   Example:

1. tiercli config F: target azure rwaccount
   OPEkmf7v9ZHZPvNy2HWoxhDZu6QSFwollCxam+ltoPegcAyw9YoJu8suuA/QvDPQ4WdbekaT
   uoDn0wmDwoZ6pg== https://test.blob.core.windows.net/

2. tiercli config F: container bridge

> II.   Using Connection String

1. tiercli config target azure "" "" "" <connection_string>

2. tiercli config <source or control folder path> container <container name>

   Example:

1. tiercli config F: target azure "" "" ""
   DefaultEndpointsProtocol=https;AccountName=TTtests;AccountKey=LDYFUJ3gYaTT3fxnEpiq
   42buUof79pVgpnd2QLujrQ83aFTyeVbz988V4LMF1CbpAlWM7ip2SnizRRrgsmKaWj==;Endpoi
   ntSuffix=core.windows.net

2. tiercli config F: container bridge

AWS S3

1. tiercli config <source or control folder path> target s3 <access_id> <secret_key> <server>

2. tiercli config <source or control folder path> container <bucket name>

   Example:

1. tiercli config F: target s3 AKIAI633LOZJPNTZUIBA
   Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4LfF s3.amazonaws.com

2. tiercli config F: container bridge

Wasabi

1. tiercli config <source or control folder path> target s3compat <access_id> <secret_key>
   <server>

2. tiercli config <source or control folder path> container <bucket name>

   Example:

1. tiercli config F: target s3compat AKIAI633LOZJPNTZUIBA
   Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4LfF s3.eu-central-2.wasabisys.com

2. tiercli config F: container bridge

IBM Cloud Object Storage

1. tiercli config <source or control folder path> target icos <access_id> <secret_key> <accesser ip>

2. tiercli config <source or control folder path> container <bucket name>

   Example:

1. tiercli config F: target icos AKIAI633LOZJPNTZUIBA
   Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4LfF 10.200.4.10

2. tiercli config F: container bridge

Backblaze

1. tiercli config <source or control folder path> target b2 <account_id> <application_key>

2. tiercli config <source or control folder path> container <bucket name>

   Example:

1. tiercli config F: target b2 63cd7057483d 000d6f3065670683d6250863c0746278cbbad71771

2. tiercli config F: container bridge

S3-compatible Object Storage

1. tiercli config <source or control folder path> target s3compat <account_id> <application_key>

2. tiercli config <source or control folder path> container <bucket name>

   Example:

1. tiercli config F: target s3compat 63cd7057483d
   000d6f3065670683d6250863c0746278cbbad71771

2. tiercli config F: container bridge

Blackpearl Object Storage

1. tiercli config <source or control folder path> target blackpearl <access_id> <secret_key>
   <endpoint>

2. tiercli config <source or control folder path> container <bucket name>

   Example:

1. tiercli config F: target blackpearl AKIAI633LOZJPNTZUIBA
   Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4LfF 10.200.6.30

2. tiercli config F: container bridge

Coeus Managed Digital Content Library

1. tiercli config <source or control folder path> target era <username> <password> "<share
   path>;<archive folder>;<address>;<port>;<API Key>"

2. tiercli config <source or control folder path> container <watch folder name>

   Example:

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

2. tiercli config F: container incoming

Network Share

1. tiercli config <source or control folder path> target network <sharepath> <username>
   <password>

2. tiercli config <source or control folder path> container <folder name>

   Example:

1. tiercli config F: target network \\server\share rwaccount rwaccountpassword

2. tiercli config F: container bridge

NTFS or ReFS Volume

1. tiercli config <source or control folder path> target local set

2. tiercli config <source or control folder path> container <full path to folder>

   Example:

1. tiercli config F: target local set

2. tiercli config F: container G:\Projects

Configure Target Settings

Configure Target Server Side Encryption

Disable SSE:

tiercli config <source> sse None

Example:

198

tiercli config D:\test-source sse None

Encryption with Amazon S3 Key (SSE-S3):

tiercli config <source> sse SSE-S3

Example:

tiercli config D:\test-source sse SSE-S3

Encryption with AWS Key Management Service Key (SSE-KMS):

tiercli config <source> sse SSE-KMS [AWS KMS key ARN]

Example:

tiercli config D:\test-source sse SSE-KMS 0987dcba-09fe-87dc-65ba-ab0987654321

Encryption with Customer-provided encryption key (SSE-C):

tiercli config <source> sse SSE-C <encryption key>

Example:

tiercli config D:\test-source sse SSE-C <encryption key>

Configure the Target Hot, Cool and Archive Tiers

Customize Tiers

```
tiercli config <path to source> tiers <hot> <cool> <archive>
```
Example:

```
tiercli config D:\test-source tiers nearline "" coldline
```

Reset to Default Tiers

```
tiercli config D:\test-source tiers "" "" ""
```

Configure a Proxy Server for Access to the Target

Enable Proxy Server Access to the Target

tiercli config global proxy <server:port> <username> <password>

Example:

tiercli config global proxy 10.200.9.16:3128 john.smith@domain.com p@33w0rD

Disable Proxy Server Access to the Target

tiercli config global proxy ""

Configure Data Format on the Cloud

Display Files with Name and Path in the Cloud Browser

tiercli config global cloudfmt path

Display Files with Object IDs in the Cloud Browser

tiercli config global cloudfmt id

Configure Data Replication

Configure Global Replication Policy

tiercli config policy replicate < interval in secons [s], minutes [m], hours [h], days [d], weeks[w]>

Example:

tiercli config policy replicate 12h

Overwrite the Global Replication Policy for a Source

tiercli config <path to source> policy replicate < interval in secons [s], minutes [m], hours [h], days [d], weeks[w]>

Example:

tiercli config D:\test-source policy replicate 12h

Configure Included Locations

tiercli config include <folder path> ... [folder path]

Example:

tiercli config include D:\test-source\new G:\source I:\projects\finished

Clear the List of Included Locations

       tiercli config include ""

Configure Excluded Locations

       tiercli config exclude<folder path> ... [folder path]

Example:

       tiercli config include D:\test-source\temp G:\Drafts H:\

Clear the List of Excluded Locations

       tiercli config exclude ""

Overwrite the Global Replication Policy for a Source

       tiercli config <path to source> policy replicate < interval in secons [s], minutes [m], hours [h], days [d], weeks[w]>

Example:

       tiercli config D:\test-source policy replicate 12h

Configure Different Container for Metadata Replication

       tiercli config <path to source> meta <bucket_name> [access_id] [access_key]

Example:

> tiercli config D:\test-source meta metadata-only AKIAI633LOZJPNTZUIBA
> Y2n1rXwda3T9yB7DEE7hRFtC6sMP83jeecwd4LfF

Configure Space Reclaiming

Configure Global Space Reclaiming Policy

Enable Global Space Reclaiming

> tiercli config policy reclaimspace turn on

Disable Global Space Reclaiming

> tiercli config policy reclaimspace turn off

Configure Space Reclaiming Policy File Access Parameter

> tiercli config policy reclaimspace < interval in secons [s], minutes [m], hours [h], days
> [d], weeks[w]>

Example:

> tiercli config policy replicate 12h

Configure Space Reclaiming Policy Minimum File Size

> tiercli config policy reclaimspace size <size in bytes [b], kilobytes [k], megabytes [m],
> gigabytes [g], terabytes [t]>

Example:

> tiercli config policy reclaimspace size 1m

Configure Space Reclaiming Policy Minimum Used Space Threshold

> tiercli config policy reclaimspace minused <percentage>

Example:

> tiercli config policy reclaimspace minused 50

Configure Space Reclaiming Policy Maximum Used Space Threshold

        tiercli config policy reclaimspace maxused <percentage>

Example:

        tiercli config policy reclaimspace maxused 90

Configure Unreclaimed Portion of a File Type

View List of Configured File Types

        tiercli config policy reclaimspace ondisk show

Add and Configure File Type

        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

Remove File Type

        tiercli config policy reclaimspace ondisk clear <file-extension>

Example:

        tiercli config policy reclaimspace ondisk clear jpg

Remove All File Types

        tiercli config policy reclaimspace ondisk clear *

Overwrite the Global Space Reclaiming for a Source

Enable Space Reclaiming for a Pair

        tiercli config <path to source> policy reclaimspace turn on

Example:

        tiercli config D:\test-source policy reclaimspace turn on

Disable Space Reclaiming for a Pair

tiercli config <path to source> policy reclaimspace turn off

Example:

tiercli config D:\test-source policy reclaimspace turn off

Configure a Pair's Space Reclaiming Policy File Access Parameter

tiercli config <path to source> policy reclaimspace < interval in secons [s], minutes [m], hours [h], days [d], weeks[w]>

Example:

tiercli config D:\test-source policy reclaimspace 1h

Configure a Pair's Space Reclaiming Policy Minimum File Size

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

Configure a Pair's Space Reclaiming Policy Minimum Used Space Threshold

tiercli config <path to source> policy reclaimspace minused <percentage>

Example:

tiercli config D:\test-source policy reclaimspace minused 50

Configure a Pair's Space Reclaiming Policy Maximum Used Space Threshold

tiercli config <path to source> policy reclaimspace maxused <percentage>

Example:

tiercli config D:\test-source policy reclaimspace maxused 90

Configure Unreclaimed Portion of a File Type

View List of Configured File Types

tiercli config <path to source> policy reclaimspace ondisk show

Add and Configure File Type

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

Remove File Type

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

Example:

tiercli config D:\test-source policy reclaimspace ondisk clear jpg

Remove All File Types

tiercli config <path to source> policy reclaimspace ondisk clear *

Configure the Processes Allowed or Forbidden to Retrieve Files

Configure the Processes Allowed to Retrieve Files

tiercli config global whiteproc <process> ... <process>

Example:

tiercli config global whiteproc mspaint.exe acad.exe

Configure the Processes Forbidden to Retrieve Files

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

Example:

tiercli config global blackproc explorer.exe nod32.exe

Configure Data Archiving
Enable Data Archiving
tiercli config <path to source> policy archive turn on

Disable Data Archiving
tiercli config <path to source> policy archive turn off

Configure Data Archiving File Access Parameter
tiercli config <path to source> policy archive archive <size in bytes [b], kilobytes [k], megabytes [m], gigabytes [g], terabytes [t]>

Example:

tiercli config D:\test-source policy archive archive size 1g

Configure Data Archiving File Size Parameter
tiercli config <path to source> policy archive archive size <file access time in seconds [s], minutes [m], hours [h], days [d], weeks [w]>

Example:

tiercli config D:\test-source policy archive archive age 12w

Configure Active Sync
Configure Global Active Sync Policy
Configure Global Active Sync Mode
Disable Active Sync
tiercli config sync mode off

Enable Listen Only Active Sync
tiercli config sync mode listen

Enable Notify Only Active Sync
tiercli config sync mode notify

Enable Both Listen and Notify Active Sync

tiercli config sync mode both

Configure The Interval for Checking for Updates

tiercli config sync listen <interval in seconds [s], minutes [m], hours [h], days [d], weeks [w]>

Example:

tiercli config sync listen 30m

Configure The Interval for Sending Notifications

tiercli config sync notify <interval in seconds [s], minutes [m], hours [h], days [d], weeks [w]>

Example:

tiercli config sync notify 1h

Enable Automatic Retrieval of Synchronized Files

tiercli config sync autorestore on

Disable Automatic Retrieval of Synchronized Files

tiercli config sync autorestore off

Overwrite the Active Sync Policy for a Source

Configure a Pair's Active Sync Mode

Disable Active Sync for a Pair

tiercli config <path to source> sync mode off

Enable Listen Only Active Sync for a Pair

tiercli config <path to source> sync mode listen

Enable Notify Only Active Sync for a Pair

tiercli config <path to source> sync mode notify

Enable Both Listen and Notify Active Sync for a Pair

tiercli config <path to source> sync mode both

Configure a Pair's Active Sync Interval for Checking for Updates

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

Configure a Pair's Active Sync Interval for Sending Notifications

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

Enable Automatic Retrieval of Synchronized Files for a Pair

tiercli config <path to source> sync autorestore on

Disable Automatic Retrieval of Synchronized Files for a Pair

tiercli config <path to source> sync autorestore off

Configure File Retrieval Mode

Keep File on the Target When Retrieving it on the Source

tiercli config global resmode copy

Remove File from the Target When Retrieving it on the Source

tiercli config global resmode move

Configure File Deletion Mode

Keep File on the Target When Deleting it on the Source

tiercli config global delmode off

Delete File from the Target When Deleting it from the Source

> tiercli config global delmode on

Perform Manual Operations

Replicate Data Manually

> tiercli op replicate <path to a file or a whole folder>

Example:

> tiercli op replicate d:\source\final-versions

Manually Reclaim Space on a Source

> tiercli op offline <path to a file or a whole folder>

Example:

> tiercli op offline d:\source\final-versions

Retrieve Data from the Target

> tiercli op restore <path to a file or a whole folder>

Example:

> tiercli op restore d:\source\final-versions

Retrieve Data from the Target Preserving the Last Access Time

> tiercli op restore -p <path to a file or a whole folder>

Example:

> tiercli op restore -p d:\source\final-versions

Retrieve Data from the Skipping Files Accessed Earlier Than Specified Time

> 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

Delete Any Data from Both the Source and the Target
tiercli op delete <path to a file or a whole folder>

Example:

tiercli op delete d:\source\final-versions

Delete Any Data from the Source Keeping the Replica on the Target
tiercli op delete -l <path to a file or a whole folder>

Example:

tiercli op delete -l d:\source\final-versions

Delete Reclaimed Files from Both the Source and the Target
tiercli op delete -o <path to a file or a whole folder>

Example:

tiercli op delete -o d:\source\final-versions

Delete Reclaimed Data from the Source Keeping the Replica on the Target
tiercli op delete -o -l <path to a file or a whole folder>

Example:

tiercli op delete -o -l d:\source\final-versions

Retrieve Data from the Target
tiercli op restore <path to a file or a whole folder>

Example:

tiercli op restore d:\source\final-versions

Synchronize Source and Target Contents

Synchronize Contents of Current Folder Only

tiercli op sync <path to folder>

Example:

tiercli op sync d:\source\final-versions

Synchronize Contents of Current Folder Only and Retrieve Data

tiercli op sync -d <path to folder>

Example:

tiercli op sync -d d:\source\final-versions

Synchronize Content of Current Folder and Its Sub-folders

tiercli op sync -r <path to folder>

Example:

tiercli op sync -r d:\source\final-versions

Synchronize Content of Current Folder and Its Sub-folders and Retrieve Data

tiercli op sync -r -d <path to folder>

Example:

tiercli op sync -r -d d:\source\final-versions

Undelete Data

tiercli op sync -u <path to folder>

Example:

tiercli op sync -u d:\source\final-versions

Revert Modification on Source File to the Last Replicated State

tiercli op revert <path to file or folder>

Example:

> tiercli op revert d:\source\final-versions

Move Data Between Target Tiers

Move Data to the Hot Tier

> tiercli op move_hot <path to file or folder>

Example:

> tiercli op sync move_hot d:\source\test.txt

Move Data to the Hot Tier and Preserve The Last Access Time

> tiercli op move_hot -p <path to file or folder>

Example:

> tiercli op sync move_hot -p d:\source\test.txt

Move Data to the Cool Tier

> tiercli op move_cool <path to file or folder>

Example:

> tiercli op sync move_cool d:\source\test.txt

Move Data to the Cool Tier and Preserve The Last Access Time

> tiercli op move_cool -p <path to file or folder>

Example:

> tiercli op sync move_cool -p d:\source\test.txt

Move Data to the Archival Tier

> tiercli op move_archive <path to file or folder>

Example:

        tiercli op sync move_archive d:\source\test.txt

Move Data to the Archival Tier and Preserve The Last Access Time
        tiercli op move_archive -p <path to file or folder>

Example:

        tiercli op sync move_archive -p d:\source\test.txt

Revert Replicated Status if Replica is Missing from Target
        tiercli op verify <path to file or folder>

Example:

        tiercli op verify d:\source\test.txt

Manage Manual Jobs
List Current Jobs

List Pending Jobs ID
        tiercli op list p

List Running Jobs ID
        tiercli op list a

List Completed Jobs ID
        tiercli op list c

List System Jobs ID
        tiercli op list s

View Job Status
        tiercli op status

Abort a Job
        tiercli op abort

Check the Availability of Reclaimed Files on the Target

tiercli op avail <path to file or folder>

Pause Operations

Pause All Operations

tiercli op pause all

Pause Automatic Policies

tiercli op pause s

Pause Retrieving Data from the Target on Demand

tiercli op pause a

Pause Checking for Updates in Active Sync

tiercli op pause l

Pause Notifying for Updates in Active Sync

tiercli op pause n

Pause Replication

tiercli op pause b

Pause Space Reclaiming

tiercli op pause o

Pause Data Retrieval from the Target

tiercli op pause r

Pause Data Deletion

tiercli op pause d

Resume All Paused Operations

tiercli op pause none

Monitor Tiger Bridge

Monitor Data Status

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 on the source.	The specified nearline file on the source has been successfully retrieved from the target. If the nearline file has been retrieved manually through the shell extension or the command-line interface, the process name is "user operation", if the nearline file has been retrieved by attempting to open it on the source, the message displays the name of the process.
File <path to file on source> is moved to <tier type> storage on the target.	A replicated file has successfully been moved from the hot/cool tier of the target to the archival tier, the automatic or manual data archiving mechanism. The stub file icon on the source changes from nearline to offline.
License capacity exceeded.	You have reached the capacity of your license and Tiger Bridge will not replicate any more data until you upgrade your license or delete data on your source.

Warning Logs

Log message	Description
Source <path to source> failed to connect to <target type> target.	The target of the specified source is currently inaccessible. The reason for the problem may be lost connection or changed credentials for access to the target. Tiger Bridge attempts to connect to the target and in case it fails to do so until a specified timeout expires, it displays an error message.
Replication target for source <path to source> is not accessible.	The specified source has been disconnected from its target, because it is currently inaccessible. The reason for the problem may be lost connection or changed credentials for access to the target. Tiger Bridge attempts to re-connect to the target and in case it fails to do so until a specified timeout expires, it displays an error message.
Replication of file <path to file on source> failed.	Tiger Bridge's attempt to replicate the specified file to the target has failed. The reason for the failed operation may be temporary inaccessibility of the target, for example. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.
Replacing file <path to file on source> with a stub file on the source failed.	Tiger Bridge's attempt to automatically reclaim space on the source by replacing the specified file with a nearline file has failed. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.
Moving file <path to file on source> to <tier type> storage on the target failed.	Tiger Bridge's attempt to move the specified replicated/nearline file from the hot/cool tier of the target to the archival tier has failed. The reason for the failed operation may be temporary inaccessibility of the target, for example. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.
Adding file <file name> failed.	Tiger Bridge's attempt to synchronize the contents of two sources through a common target by creating a nearline/offline file in the source of one computer upon receiving notification for replicated file from another computer has failed. The reason for the failed operation may be temporary inaccessibility of the target, for example. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.

Tiger Bridge 5.0.1 Administration Guide

Log message	Description
Removing file <file name> failed.	Tiger Bridge's attempt to synchronize the contents of two sources through a common target by removing a nearline/offline file in the source of one computer upon receiving notification for removed file from another computer has failed. The reason for the failed operation may be temporary inaccessibility of the target, for example. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.
Renaming file <current file name> to <updated file name> failed.	Tiger Bridge's attempt to synchronize the contents of two sources through a common target by renaming a nearline/offline file in the source of one computer upon receiving notification for file rename on another computer has failed. The reason for the failed operation may be temporary inaccessibility of the target, for example. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.
Failed to parse sync notification <notification ID>.	Tiger Bridge's attempt to parse a notification for updated contents on one computer when synchronizing it with the contents of another computer through a common target (active sync) has failed. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.
Failed to process notification <notification ID>.	Tiger Bridge's attempt to process a notification for updated contents on one computer when synchronizing it with the contents of another computer through a common target (active sync) has failed. The message is displayed until the operation succeeds or until Tiger Bridge reaches the maximum number of attempts in which case it displays an error message.

Error Logs

Log message	Description	Suggested action
Source location is missing. Volume with guid <volume GUID> is not mounted.	Tiger Bridge failed to load a source, because the GUID of the volume, on which it is stored, does not match the GUID of any volume accessible to Tiger Bridge.	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). • 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 does not match the source storage requirements any more.	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.

Log message	Description	Suggested action
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 Tiger Bridge Operations.*	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, following the steps in Manage Files and Folders Versions. • If none of the files is encrypted, change the ransomware protection threshold, following the guidelines provided in Enable and Configure Ransomware Protection.
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.