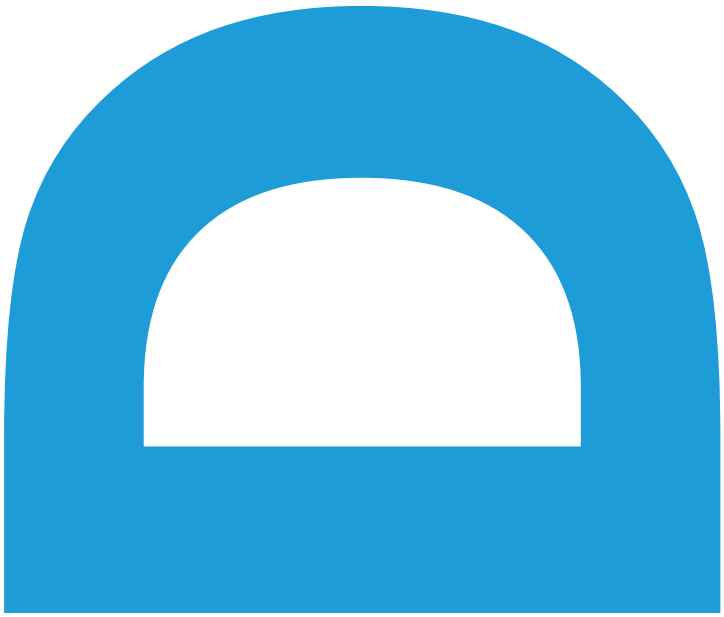
Tiger
Technology



Tiger Bridge 5.1 Release Notes

15 October 2024

Title	Tiger Bridge Release Notes
Software version:	5.1
Date:	15 October 2024

Table of Contents

What's New in Tiger Bridge 5.1?

Persistent Tracked Filesystem Information Database

Tiger Bridge 5.1 introduces a persistent database of tracked filesystem information for each source. The database is stored locally once its size exceeds 200 MB and persists across computer and service restarts. Until the 200 MB threshold is reached the database is stored in the system memory for faster access and regenerated upon each restart of the computer or the Tiger Bridge service.

The locally stored database is continuously updated in real-time as files are added, modified, deleted, replicated, reclaimed, archived or retrieved. This ensures the database always reflects the current state of the source data and eliminates the need for repetitive and time-consuming scans. Should the database be accidentally deleted or become corrupted, Tiger Bridge automatically regenerates it by rescanning its sources.

You can fine-tune the behavior of the tracked filesystem information database by controlling whether to use persistent local database, in-memory database or a combination of both. You can also change the database size threshold that triggers it to be saved locally. For more details, refer to the latest version of the Tiger Bridge manual.

Note: With the changes made to the tracked filesystem information database, downgrade compatibility is ensured after completing the preparation steps outlined in "Downgrading Tiger Bridge from Version 5.1" on page 7.

Compliance Mode

Tiger Bridge 5.1 introduces a compliance policy for workflows requiring strict data integrity and retention. Configurable per source, this policy prevents files from being deleted or renamed on the source after replication for a set retention period. Modifications during this period are allowed only if versioning is enabled in both Tiger Bridge and the target.

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

Checksum Verification of Data Integrity

To support workflows that require checksum verification for data integrity, you can configure Tiger Bridge 5.1 to generate a checksum for each file before it is replicated to the target. The generated checksum is stored on the source in the file's metadata, even if space is reclaimed and the file is replaced by a stub file. This checksum is used for data integrity verification by comparing it with the checksum generated by the same algorithm running on the target. For Azure targets, checksum comparison is performed automatically. For other targets, manual comparison is required - you must compare the checksum generated on the source with the one generated on the target.

Currently, automatic checksum generation is supported for all cloud storage and local storage targets. Refer to the latest version of the Tiger Bridge Administration Guide for details about enabling and managing the checksum verification.

Note: Using checksum together with versioning can result in checksum loss in source data . For more information, see "Checksum Lost When Retrieving a File Version from the Target" on page 7.

Direct Replication to the Archival Tier/Storage Class

In response to customer feedback and to resolve interface inconsistencies on configurations using the option before it was disabled in version 5.0.4, Tiger Bridge 5.1 reintroduces the option to replicate files directly to an archival tier of the target. This change applies to Microsoft Azure, Amazon S3, and Huawei targets. Additionally, on these targets, if Tiger Bridge detects that it should replicate directly to the archive, it does not allow you to add an Archive policy.

Note: This change does not apply to Google Cloud targets. For Google Cloud, direct replication uses the default storage class defined at the target level. Even if the default storage class for the bucket is archival, Tiger Bridge does not prevent the addition of an Archive policy.

In summary, with this new change in version 5.1:

- New sources paired with Microsoft Azure, Amazon S3, or Huawei targets can be configured to replicate data directly to the archival tier of the target but cannot have an Archive policy.
- Sources configured before version 5.0.4 to replicate data directly to the archive will correctly display this setting in the Configuration. Existing Archive policies for these sources will remain active and can be modified. However, if an Archive policy is deleted, it cannot be re-added if the source is set to replicate directly to the archival tier.
- You can modify sources added in version 5.0.4 to replicate data directly to the archival tier/storage class of Microsoft Azure, Amazon S3 or Huawei target, only if they do not have an Archive policy. If an Archive policy is present, it must be deleted (and files manually archived beforehand) to enable direct replication to the archival tier.

Grouped Storage Classes for Direct Replication

When pairing a source with a Microsoft Azure, Amazon S3, or Huawei target you can select the storage class/tier to which to replicate data directly. With Tiger Bridge 5.1, the available options in the drop-down box of the source configuration are grouped by categories. This helps you easily distinguish between instantly available and archival storage classes/tiers. Additionally, for Microsoft Azure and Huawei targets, you have the option to use the storage class/tier defined at the target level. This facilitates bulk changes to the storage class of already replicated data and also allows you to adopt a newly added tier/storage class before Tiger Bridge adds support for it in its interface.

Multi-Site Sync Not Paused on Manual Synchronization with Target

In Tiger Bridge 5.1, the automatic synchronization with other sources through a common target in a multi-site sync setup continues uninterrupted even if you manually synchronize the source on one computer

with the target. This enhancement ensures that notifications about updated content from other computers are not delayed while Tiger Bridge rescans the source and target for inconsistencies.

File System Auditing Logs

To ensure better tracking and management of file activities, Tiger Bridge 5.1 logs all file rename and file delete operations of replicated files in both the source and the target. You can find the logs in C:\ProgramData\Tiger Technology\Logs. By default, Tiger Bridge starts logging to a new file once the size of the current log file reaches 5 MB and deletes the oldest log file when the number of log files reaches 10. You can change these auditing logs settings, by following the steps in this article: https://kb.tiger-technology.com/file-system-auditing-logs-manage-output-path-and-maximum-size

Troubleshooting Data Replication Through the Command-line Interface

The command-line interface of Tiger Bridge 5.1 adds new commands that allow you to troubleshoot data replication:

- create a log listing all source files with replicated files whose replicas are not present on the target
- undelete a soft-deleted replica from a cloud storage target
- re-link a replicated source file to its replica on the targe
- revert the replicated status of a source file if its replica is missing from the target

Version 5.1 also adds command that allow you to set the number of threads used for the execution of any Tiger Bridge job on a specific source location as well as commands for viewing the checksum of a file and for performing a checksum verification of the replica on the target, Refer to the latest version of the Tiger Bridge Administration Guide for details about executing the commands.

Fixes in Version 5.1

Faster Synchronization of File Rename and File Delete Operations on the Target

With Tiger Bridge 5.1, the synchronization speed for file rename and file delete operations on the target has been visibly increased, reducing the time required for these actions to be reflected across the system.

Tiger Bridge Explorer Stability

Version 5.1 further improves the stability of the Tiger Bridge Explorer.

Improved Support for Sources on Mount Points

With Tiger Bridge 5.1, you can integrate volumes mounted in mount points on the computer as sources or targets by following the workaround described in the following Tiger Technology knowledge base article: https://kb.tiger-technology.com/use-a-volume-mounted-in-a-mount-point-as-a-source-or-a-target

Upgrading to Tiger Bridge 5.1

Upgrading from Version 4.x and Above

To upgrade Tiger Bridge to this new version, you should simply run the installation of version 5.1 on the computer running Tiger Bridge. All configuration settings will be preserved after the upgrade.

Upgrading from Version 3.x and Below

To avoid having two instances of the Tiger Bridge Configuration after the upgrade, it is advisable to uninstall the previous version from the computer and then perform a clean installation of version 5.1 by following the steps in the Administration Guide. All configuration settings will be preserved after the upgrade.

New Known Issues

Checksum Lost When Retrieving a File Version from the Target

If versioning is enabled both in Tiger Bridge and on the target, when you retrieve a version of the file back on the source it is being retrieved without its checksum.

Downgrading Tiger Bridge from Version 5.1

If you choose to install a previous version of the software after upgrading to version 5.1, you will need to ensure that the service is running after the downgrade. To do this, you will have to clear the Read-Only attribute from all files with the .store extension located in the program's data folder. For detailed instructions on how to clear the Read-Only flag, refer to the following Knowledge Base article:

https://kb.tiger-technology.com/how-to-clear-the-read-only-flag-of-tiger-bridge-program-files

Unresolved Known Issues

Displaying the Tiger Bridge Tray Icon

In some cases, after upgrading to version 5.x, the Tiger Bridge tray icon may not show initially. To resolve the problem, you should either restart the computer after the upgrade or start the tray icon manually by double-clicking tier_tray.exe in the installation folder of Tiger Bridge.

Retrieving Offline Files from Google Cloud

Unlike other cloud targets, offline files stored on a Google Cloud target are retrieved directly on the source when you attempt to open them or to rehydrate them manually.

Using Versioning Software on Azure Append/Page Blob

When using versioning on Microsoft Azure append or page blob as a target, you should keep in mind that the first version of each file is not kept, and the second version overwrites it. From the second version onwards, versioning works as expected on Azure append and page blobs.

A workaround to the problem is to introduce an insignificant change to the file after it has been initially replicated on the Azure append/page blob (such as an added interval at the end of a text document, for example) to trigger versioning for that file from that change onwards.