

Tiger BRIDGE

Veeam Backup with Tiger Bridge: A Quick Start Guide

Get Started with Veeam Backup and Tiger Bridge . 2

Upgrading from Tiger Bridge for Backblaze 14

Veeam Backup with Tiger Bridge: A Quick Start Guide

This document also provides new customers with quick instructions how to configure Tiger Bridge for Veeam backup. Please, refer to the Tiger Bridge Administration Guide for detailed description of the configuration steps. You can find the latest version of the guide here:

<https://www.tiger-technology.com/software/tiger-bridge/docs>

As Tiger Bridge for Backblaze is discontinued this document also describes to upgrade it to the fully functional version of Tiger Bridge and preserve your existing Veeam backup workflow.

Get Started with Veeam Backup and Tiger Bridge

Tiger Bridge's Veeam integration is extremely powerful and easy to use. It will efficiently and cost-effectively improve your backup strategy by maintaining a replica of your backups in the cloud and help increase your retention period by freeing up local space.

A good 3-2-1 backup strategy involves keeping your primary data with two backup copies. Veeam takes care of your primary backup, while Tiger Bridge replicates your Veeam backup to the cloud:



With cloud providers offering a durability of eleven nines (99.999999999%) you can increase your retention period by reclaiming space on your older backups to free up local space.

The instructions below will help you install and configure Tiger Bridge for use on your Veeam server.

Prerequisites:

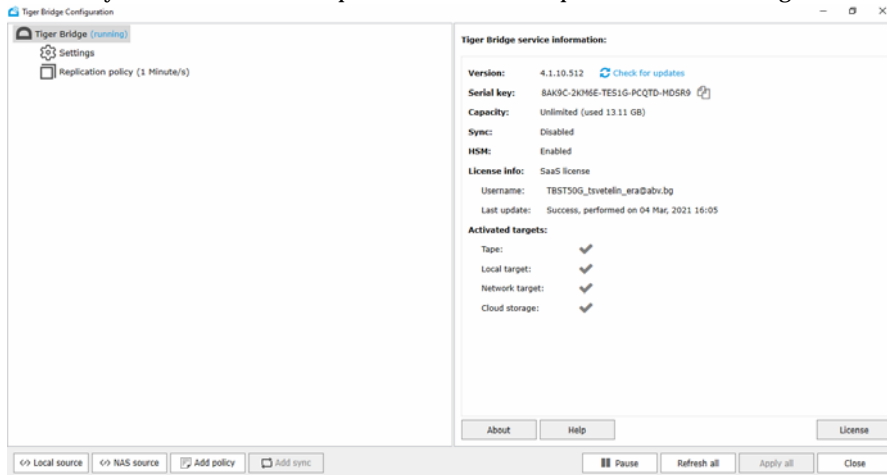
- Veeam server (installed and configured)
- Backup repository on NTFS or ReFS file system

Note: NAS can be used as a source with limitations (no partial upload or download). See "Using NAS as a Source" on page 6

- Cloud account (good Internet speed) for cloud object storage repositories
- (optional) Active Directory

Setup instructions:

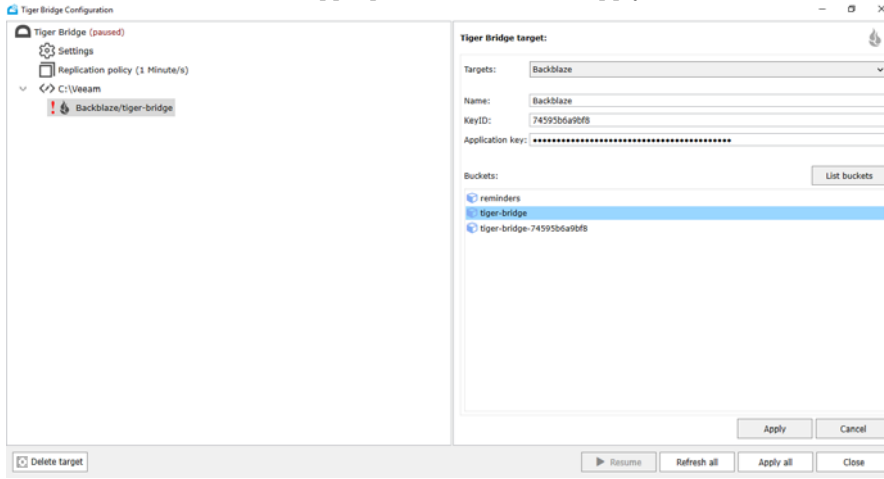
- Have your target credentials handy (e.g. cloud object storage ID and secret key).
- Have a freshcloud bucket ready to store your backup files.
- Run the Tiger Bridge installer on your Veeam server.
- From the desktop, launch the Tiger Bridge Configuration interface
- Activate Tiger Bridge: click Tiger Bridge in the left pane, then click License in the right pane and then enter your SaaS credentials.
- Delete any undesired source or policies until the left pane looks something like this:



- Click Local Source and choose your Veeam repository.
- Click Add Target and choose your target, then enter your cloud credential as required.

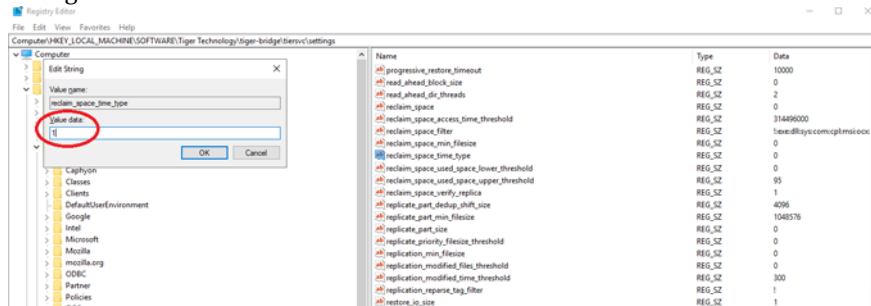
Veeam Backup with Tiger Bridge: A Quick Start Guide

- Click List Buckets, select the appropriate one and click Apply.



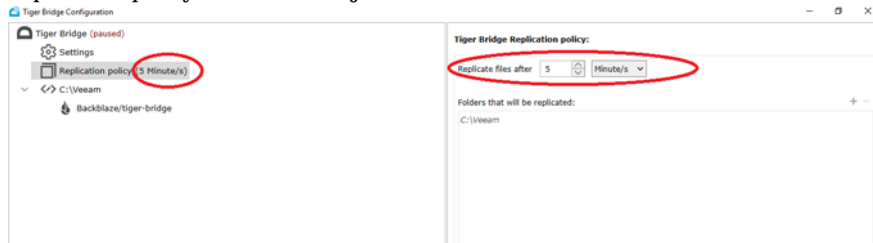
The following Tiger Bridge settings guarantee best Veeam backup workflow:

- Settings in the registry of the computer:
 - Start the Registry Editor (in Start menu type “regedit”)
 - Navigate to:
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tiger Technology\tiger-bridge\tiersvc\settings
 - In the right pane, right-click the reclaim_space_time_type string value and select Modify.
 - Change the value to 1 and click OK.

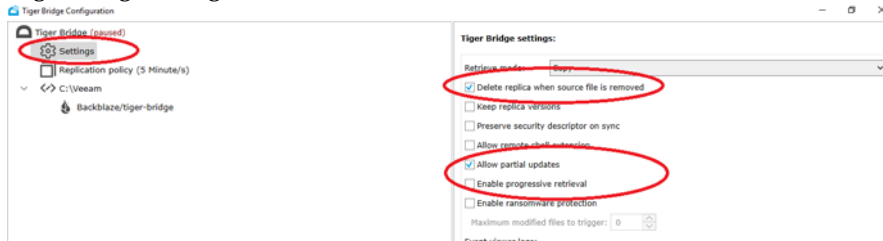


- settings in the Tiger Bridge Configuration:

- replication policy (feel free to adjust):



- Tiger Bridge settings:



Note: When prompted, confirm that you want to restart the Tiger Bridge service in order to apply all new settings.

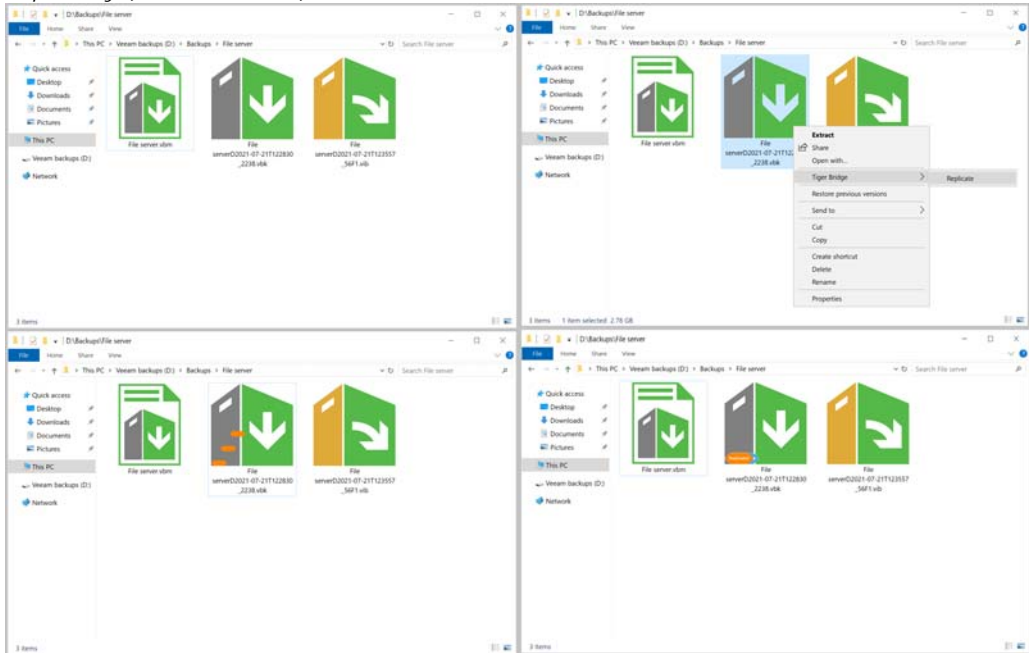
In the Tiger Bridge Configuration click Resume:

- Replication will begin 1-5 min after Veeam has completed its backup job
- Partial upload is enabled for Forever Forward Incremental and Reverse Incremental methods
- Progressive retrieval is best for Guest OS File selective restore.
- Backup files will be deleted in the cloud if deleted locally;
- No version history of your backup files will be kept in the cloud;

Note: If you have lots of backup files and would like to prioritize the upload of your .vbk files, then keep Tiger Bridge in "Paused" mode and go to your Veeam repository. Right-click on the file you want Tiger Bridge to upload then select Tiger Bridge -> Replicate. In Large Icon view, you will see three orange bars indicating that the file is being uploaded. When the upload is complete, the file will display a <Replicated> overlay on it. Click on "Resume" when you want Tiger Bridge to

Veeam Backup with Tiger Bridge: A Quick Start Guide

automatically start detecting and managing uploads of all the files in the selected Backup Repository (and sub-folders).



Important: The *FIRST* time you upload your "full" backup file (.vbk), make sure it is fully uploaded *BEFORE* Veeam attempts to modify it - which depends on your backup chain and backup method. If the file is modified while it is still being uploaded, Tiger Bridge will abort and start the upload over to ensure file integrity. Once the entire file has been fully uploaded to the cloud, Tiger Bridge will be able to identify differences and manage partial uploads. When in doubt, you can consider pausing Veeam backups or increasing the number of recovery points until your .vbk file is fully uploaded and displays the orange <Replicated> overlay in the Large Icon view.

Finally, it is always recommended to keep a local copy of all your backup files. However, if the lack of local space prevents you from extending your retention period, you should consider adding a Reclaim Space policy (requires a license with Continuous Data Protection) so that files older than, say 90 days, are automatically reclaimed. In this case, Tiger Bridge will automatically turn the older files into stub-files to free up local space. Stub-files take no space on your local drive but keep a connection to the cloud so Veeam can still access your older backups on demand.

Using NAS as a Source

If your backup repository is accessed over an SMB/NFS share, Tiger Bridge will NOT be able to perform partial upload/download. In this case, it is best to use the Veeam's Forward Incremental method. A new .vbk file will only be created and uploaded once for each backup chain. When using a Forever Forward or Reverse Incremental method, Veeam modifies the .vbk each time it does an incremental backups, which will force Tiger Bridge to re-upload the entire .vbk.

Ways to Secure for Your Backups

The above settings will ensure immediate replication of your backup files when Veeam creates them. You can further secure and protect your backup files by preventing accidental or malicious modification and deletion from taking place when your backups are in the cloud.

Note: *The best defense against ransomware is achieved when using Veeam's Forward Incremental backup method (weekly full/synthetic .vbk with daily .vib/.vbr increments) along with Tiger Bridge's versioning control. While this approach does not take advantage of partial uploads, it offers the best protection.*

Enable Object Immutability

Object Immutability offers a simple, yet efficient protection against malware and accidental file deletion. Activating an immutability policy on a bucket prevents objects from being modified or deleted for a given period of time.

This functionality is not available with every provider (be aware that some may refer to it as Immutability, Object-Locking, or Compliance). Also, in some instances, providers offer object immutability, but do not offer users the ability to activate the functionality at the bucket level.

If your cloud provider offers the ability to automatically delete objects in the cloud when the retention period has expired, then you should make sure the period is slightly longer than your Veeam backup chain.

Compliance Settings

[LOCK COMPLIANCE](#)

Compliance Mode (on/off) ☒

Delete After Retention ☒

Retention Time (30 days):

Number of months:

Time Scale:

[SAVE](#)

If the cloud provider does not offer an auto-delete after retention, it is important that the bucket be configured so objects are no longer immutable, when the backup chain runs out. As such, when Veeam deletes the local backup file, Tiger Bridge will be able to delete it from the cloud as well. If the object is still immutable when the local file is deleted, Tiger Bridge will fail to delete the object in the cloud, and multiple backup files will start accumulating in the cloud (without you knowing until you look inside the bucket).

Important: *Because files can no longer be modified after they have been uploaded, this functionality can only be used with Veeam's Forward Incremental backup method. It is NOT possible to benefit from partial upload, as objects in the cloud can no longer be partially modified.*

Enable Ransomware Protection

Note: *Tiger Bridge ransomware protection is available with the Continuous Data Protection (CDP) subscription plan.*

The simplest and easiest protection you can add to your setup is to Enable ransomware protection in the Settings page and set the Maximum modified files to trigger to:

- "2" when using Forward Incremental method
- "3" when using Forever Forward Incremental or Reverse Incremental method

This will allow Veeam to modify its .vbm file as well as its .vbk and/or .vib/.vbr files, if Tiger Bridge finds that more than one (or two) files were modified (as opposed to created or copied) since the last replication period. If using this method, change your Replication policy to exceed the time it takes Veeam to complete its backup cycle (ex: 2 hrs). This will bring Tiger Bridge to immediately PAUSE replication and prevent any files from being replicated until further action is taken.

Enable Versioning

Note: *Tiger Bridge support for versioning is available with the Continuous Data Protection (CDP) subscription plan.*

The best line of defense is always achieved by enabling versioning in Tiger Bridge and on your cloud bucket. You will need to:

- Enable "Keep replica versions" in the Settings.
- Set a lifecycle policy on your cloud bucket to manage versions

Important: *Because modified files automatically create a full version of the file, this functionality should only be used with Veeam's Forward Incremental backup method. While it can technically be used with partial uploads, your storage consumption will grow substantially, if you use a backup method that relies on partial uploads. In addition, if your cloud provider does not offer a lifecycle management policy to manage old versions, your cloud storage consumption will continue to increase. You can always use Tiger Bridge to manually manage versions, but that isn't a recommended option due to the associated attention it may require.*

Restricting Replication and Deletion

When using a cloud provider that does not offer immutability and/or if you would like to take advantage of partial upload, there is no perfect way to totally safeguard yourself from malware and/or accidental deletions.

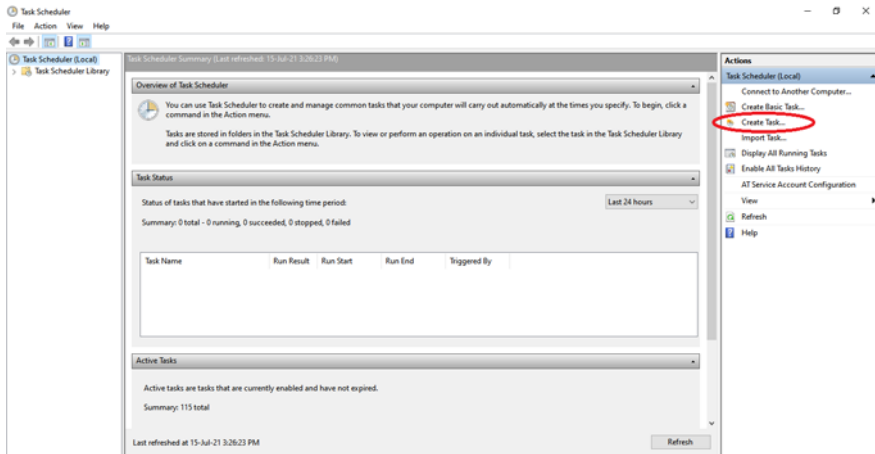
You can still mitigate the risks associated with malware attacks by ensuring replications and deletions only occur after a Veeam's operation completes. To achieve this, three simple tasks can be created in Task Manager that will monitor Veeam's events before acting on files that are stored in your backup repository. One task will enable Tiger Bridge to delete old backups, another task will enable it to replicate new or modified files, and the last task will ensure Tiger Bridge stays in pause mode until the next backup takes place.

| # | Veeam Agent Event | Action to be taken in the cloud | Event ID | Program/script | Add arguments |
|---|--------------------------------|-------------------------------------|----------|----------------|-------------------------|
| 1 | New backup job was started | Delete pending restore points | 110 | tiercli.exe | op pause s |
| 2 | Restore point has been created | Suspend file system operations | 10010 | tiercli.exe | op pause sdf |
| - | Restore point has been removed | Hold deletion until next cycle | 10050 | | |
| 3 | Job finished with success | Replicate created or modified files | 190 | tiercli.exe | op replicate repository |

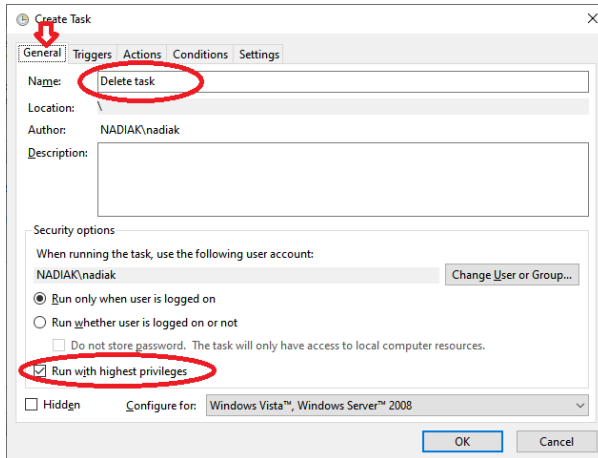
If you are not familiar with Windows' Task Scheduler, here are the steps to create Task #1 (for deletion):

Veeam Backup with Tiger Bridge: A Quick Start Guide

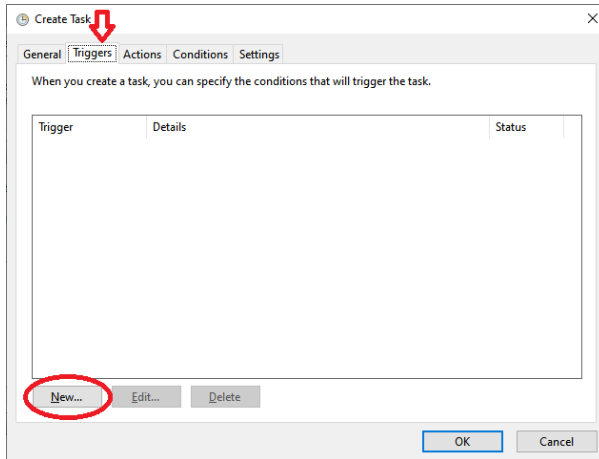
1.



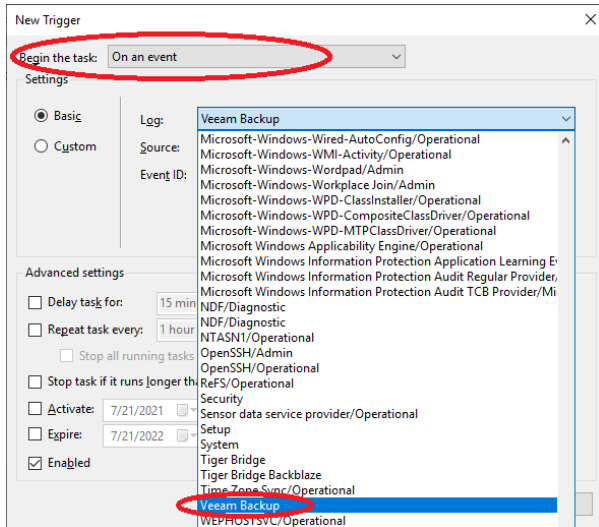
2.



3.



4.



Veeam Backup with Tiger Bridge: A Quick Start Guide

5.

New Trigger

Begin the task: On an event

Settings

☒ Basic

Log: Veeam Backup

Source: Veeam Backup

Event ID: 110

Advanced settings

☐ Delay task for: 15 minutes

☐ Repeat task every: 1 hour for a duration of: 1 day

☐ Stop all running tasks at end of repetition duration

☐ Stop task if it runs longer than: 3 days

☐ Activate: 7/21/2021 2:51:01 PM ☐ Synchronize across time zones

☐ Expire: 7/21/2022 2:51:01 PM ☐ Synchronize across time zones

☒ Enabled

OK Cancel

6.

Create Task

General Triggers Actions Conditions Settings

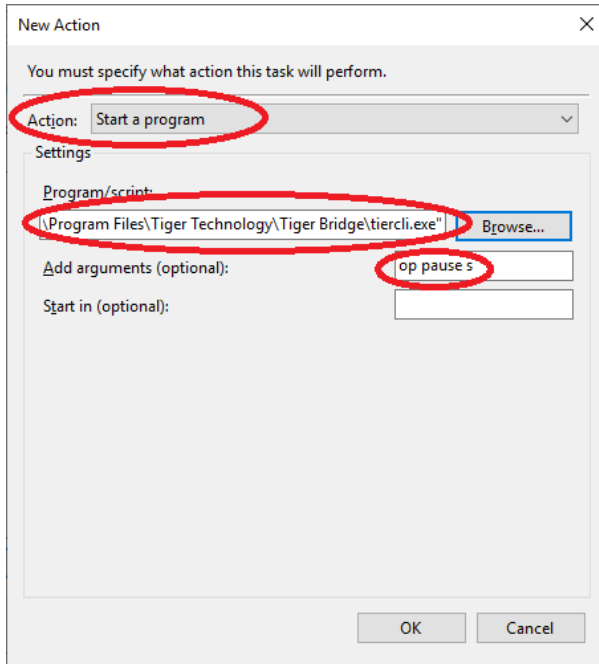
When you create a task, you must specify the action that will occur when your task starts.

| Action | Details |
|--------|---------|
|--------|---------|

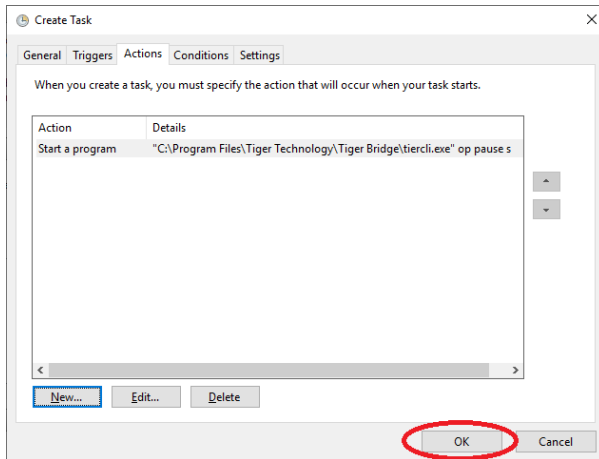
New... Edit... Delete

OK Cancel

7.



8.



Note: Tiger Bridge's Ransomware protection feature will NOT work with this approach as ALL files in the backup repository will be manually scheduled to be replicated (thereby bypassing the automatic protection).

Veeam Backup with Tiger Bridge: A Quick Start Guide

Important: *There is still vulnerability using this approach as any file deleted locally will still be deleted in the cloud, when the next backup job starts. Also, if an attack takes place, you will only be safe if you can act on it before the next backup job runs.*

If you suspect an attack or file deletion took place you should immediately take one of the following actions to prevent any further replication from taking place and give you time to seek assistance and plan for recovery:

- Disconnect Tiger Bridge server from the Internet
- Shutdown the Tiger Bridge server
- Stop the tiersvc.exe driver
- Delete your Source/Target connection in the Tiger Bridge Configuration application

Please, email support@tiger-technology.com with any questions about making the most out of your Tiger Bridge Veeam deployment.

Upgrading from Tiger Bridge for Backblaze

Editions Compatibility

Tiger Bridge for Backblaze is a tailored edition of the fully functional Tiger Bridge. Apart from the differing interfaces, you can expect no change of workflow or incompatible functionalities, depending on the subscription plan you have chosen.

One of the functionalities lacking in Tiger Bridge for Backblaze is the ability to re-activate your SaaS license locally in case you have changed the password of your account on the licensing server. In case you need to change your password before upgrading to the fully functional version of Tiger Bridge, follow the steps below.

To apply new SaaS license password locally:

1. Run Command Prompt as an administrator and execute the following:

```
tiercli license saas deconfigure
```

Tip: *To start Command prompt, on the Start menu click Run and in the dialog type cmd, then right-click Command Prompt and select "Run as administrator".*

2. Apply the new password, by executing the following:

```
tiercli license saas [account] [new password]
```

where:

[account] is the name of your account on the licensing server

[new password] is the new password for your account

3. In the Tiger Bridge Configuration, click Tiger Bridge in the left pane and check the activation status in the right pane.

Upgrade Procedure

Follow the steps below, to ensure that your existing Tiger Bridge for Backblaze configuration and settings are preserved after migrating to the fully functional version of Tiger Bridge.

To upgrade Tiger Bridge for Backblaze to Tiger Bridge:

1. Register for a selected Tiger Bridge subscription plans here:
<https://www.tiger-technology.com/getbridge/>
You will receive an email with a link to complete your registration. Once your registration is complete, you will be able to access the licensing server and proceed with the upgrade procedure outlined below.
2. Log in to the Tiger Technology licensing server at:
<https://license.tiger-technology.com/>
3. Download the latest Tiger Bridge installation from the Current Version menu on the left.
4. Download the latest version of the Tiger Bridge Administration Guide, available at:
<https://www.tiger-technology.com/software/tiger-bridge/docs/>
5. Uninstall Tiger Bridge for Backblaze and the Tiger Bridge Configuration, following the steps in the Administration Guide.
6. Install the latest version of Tiger Bridge and any additional components, following the instructions in the Administration Guide.
7. Open the Tiger Bridge Configuration and activate the SaaS license for the selected subscription plan, following the steps in the Administration Guide.
8. Check if all previously configured sources and targets are preserved.

Note: *Contact the Tiger Technology support team if you notice any discrepancy.*

