Tiger Technology

Ransomware Protection with Tiger Bridge

Step-by-step Guide for Using the Tiger Bridge Methods of Protection from Crypto Virus Attacks

Version: 1.0
June 2022

Table of Contents

Send Us Your Feedback

About Tiger Technology

Introduction

A crypto virus is a type of ransomware that is designed to encrypt as many files as possible on a compromised device and demand ransom in exchange for a decryption code. In recent years crypto virus attacks have become increasingly more common, more sophisticated, and more costly, and ransomware groups have grown much more organized. So much so that they are predicted to hit a new victim every few seconds in the coming years.

Preparing your organization to counter crypto virus attacks is a fundamental part of business continuity planning for any organization from SMBs to large governmental entities. This can be achieved in a few ways. Historically, many organizations have been using traditional backup solutions to ensure they have at least one good copy of their data in the event of an attack. However, such backup solutions require additional and often complex infrastructure, more storage, higher maintenance and come at a higher cost. Backups should also be protected from the crypto virus.

Why Tiger Bridge?

Tiger Bridge is a software-only data management solution that offers cloud-enabled Continuous Data Protection and helps you maintain business continuity in the event of a crypto virus attack. Data is stored in a non-proprietary format, which means third-party solutions are not required to access it, and it can easily be recovered from the cloud at any time.

Tiger Bridge protects your data without the extra overhead and complexities of traditional backup solutions. It also offers a number of additional benefits such as file server extension, archive and disaster recovery mechanisms, cloud migration capabilities and multi-site sync. Check out our YouTube channel to learn more.

Tiger Bridge offers three methods of protecting your data from ransomware:

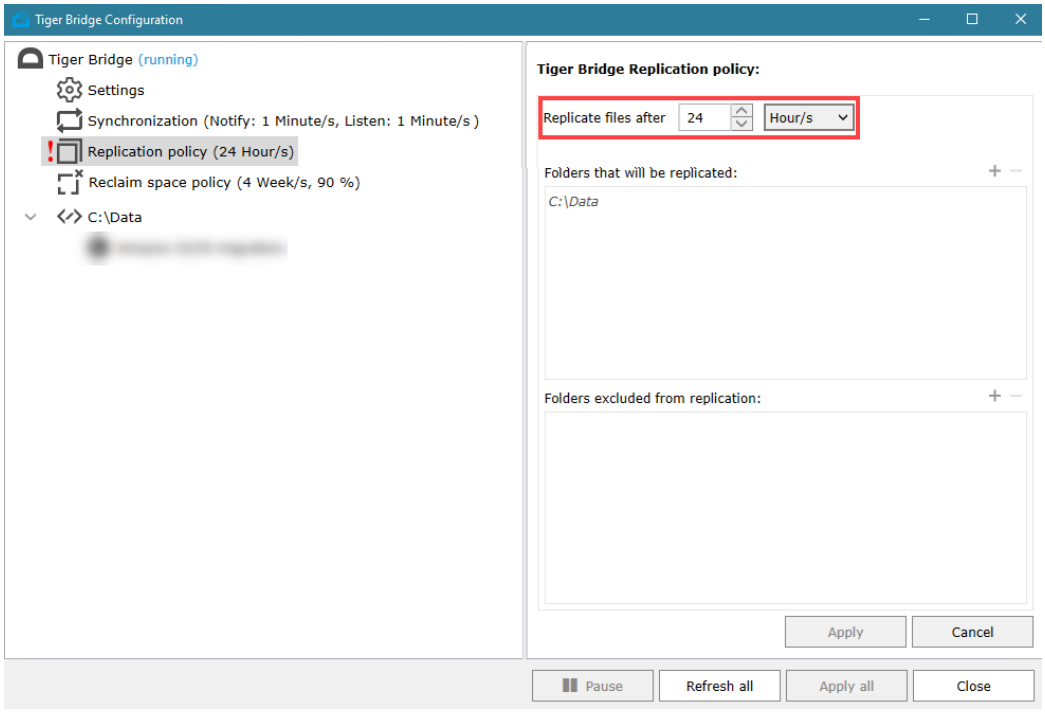
1. Longer Replication Policy
2. Fuse Defense
3. Versioning

Tiger Technology

This method does not allow any infected data to ever reach the cloud, but it requires manual detection as it does not differentiate between good and infected data.

Longer Replication Policy

To set it up, change the replication policy and give it a desired, for example 24-hour, wait period.

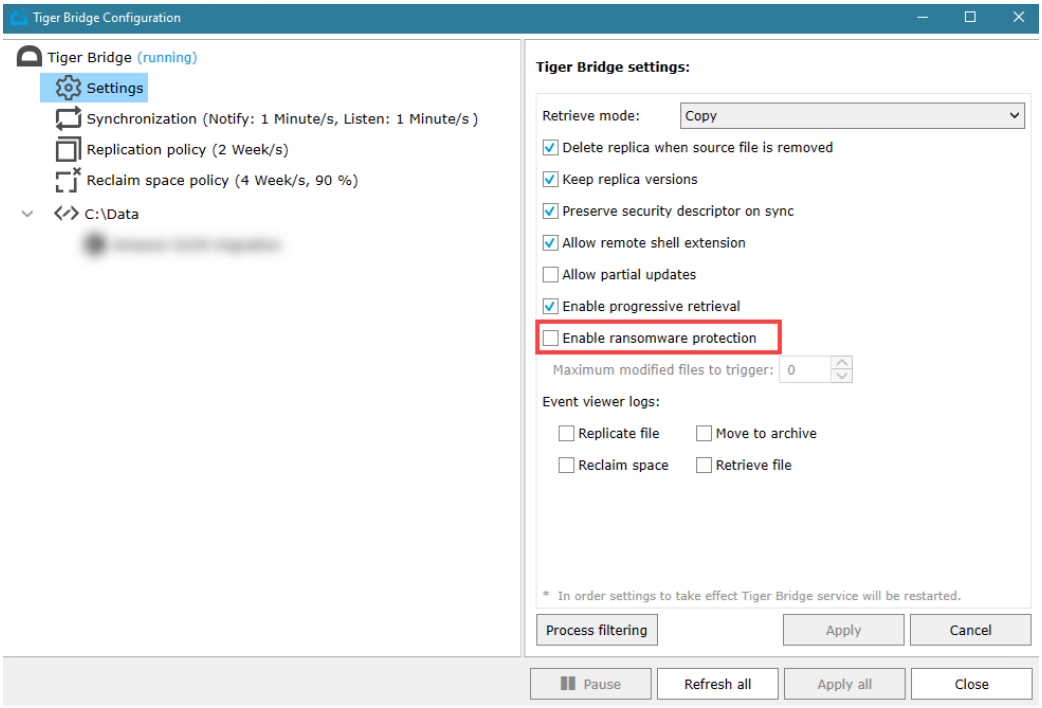


Now you have 24 hours after a crypto virus attack to detect the problem and recover.

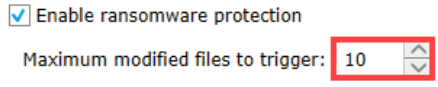
If the files in your source get encrypted, you can go to your cloud portal and download the copies that reside there. As long as you manage to do that within the replication policy time, in our case 24 hours, the files you download will be unencrypted and you will only lose the modifications introduced during this 24-hour wait period.

Fuse Defense

This method offers more advanced defense as it can differentiate between good and bad data. However, you can get “false positives” and files that are not replicated for a longer period of time.
To enable fuse defense, first go to the settings configuration of Tiger Bridge and check the **Enable ransomware protection** box.



Then set a threshold, for example 10.



When the queue of files exceeds this threshold, in our example – 10, the automatic replication of probably encrypted files will be paused, until you decide to start it again. If it begins to kick in too often, you may have to consider setting a higher threshold value.

After applying the setting, if a crypto virus damages a lot of files at once, Tiger Bridge will get paused and you will be able to see the amount of modified and pending files within the directories by checking the properties of the folders in the source directory.

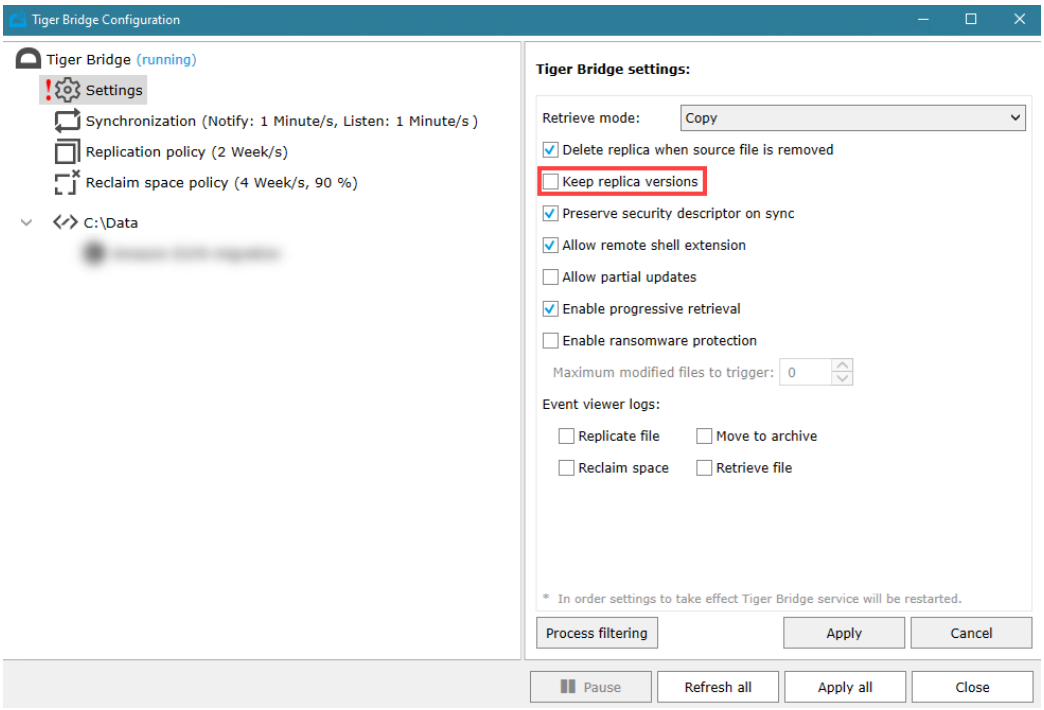
You can download good non-encrypted versions of the files from the cloud portal.

Tiger Technology

This method provides versions of all modified files, and it is within your control to select which version you would like to restore. This method may require more cloud storage in order to keep new versions when necessary.

Versioning

To set versioning up, check the **Keep replica versions** box.



It is also very important to make sure that the cloud provider you use as a target has versioning enabled.

For example, in Azure:

1. Navigate to your storage account in the portal.
2. Under Blob service, choose Data protection.
3. In the Versioning section, select Enabled.

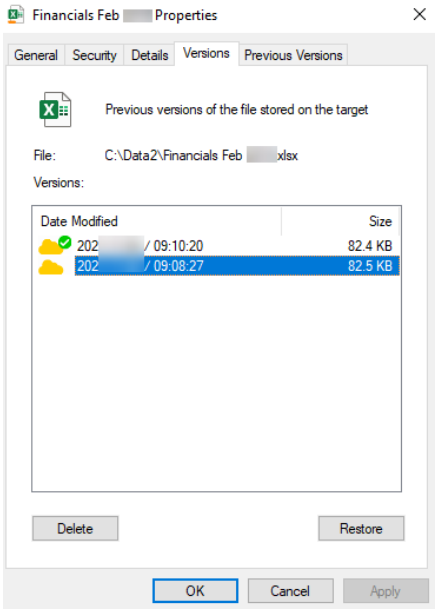
In Amazon:

1. Sign in to the AWS Management Console and open the Amazon S3 console.
2. In the Buckets list, choose the name of the bucket that you want to enable versioning for.
3. Choose Properties.
4. Under Bucket Versioning, choose Edit.
5. Choose Suspend or Enable, and then choose Save changes.

Other cloud provides have similar methods for enabling versions.

Once versioning is enabled, you can see the Versions tab in the properties of each file and folder in the source.

In case you get attacked and want to revert to the previous unencrypted version of some files, you should check the properties of the file and select a version you want to restore.



The good thing about the versioning mechanism is that it can be applied specifically to a certain file or broadly to a whole folder during the recovery process. Since versions will be kept for all files, you get to choose which ones you want to recover – only a certain file, a group of files, a folder, or the whole source. It can also be useful when the crypto virus does not attack all files at once, but it affects one file today, one file tomorrow.

Sometimes we get other types of virus attacks that delete our files, instead of encrypting them. Tiger Bridge helps in such a situation too with the help of the 'undelete' feature. It can recover the last replicated version of a file, even if it has been deleted.

View our How to survive a crypto virus attack by using the cloud video here.

Tiger Technology

Send Us Your Feedback

Did you find the information you were looking for?
Email us your feedback at info@tiger-technology.com.

About Tiger Technology

Founded in 2003 and headquartered in Sofia, Bulgaria and Alpharetta, GA, USA, Tiger Technology specializes in the underlying technology of hybrid cloud workflows. The company develops data management software solutions designed to help customers of any size, scale and industry optimize their on-premises storage and enhance their workflows through cloud services. Tiger Technology solutions are admin-friendly, non-disruptive, transparent, and highly cost-effective.

Tiger Technology brings over 15 years of expertise in developing high-performance storage solutions for the most demanding workflows, which includes cross-platform NAS/SAN file system sharing, storage, user, project, and media management.

Throughout the years and the multitude of changes in IT and the digital landscape, Tiger Technology has chosen the path of growth and continual improvement, but it has never lost sight of what it all starts with - data. The company's current focus is enabling "on-premises-first" hybrid cloud workflows.

Find out more about Tiger Technology here. Catch up on our blog here.

Follow us on social media:

LinkedIn | Twitter | YouTube | Facebook