Tiger Technology

Storage Bridge Quick Start Guide

Thank you for your choosing Storage Bridge. This document provides step-by-step instructions for configuring and using Storage Bridge. Please refer to the Storage Bridge Administration Guide (https://www.tiger-technology.com/software/storage-bridge-milestone/docs/) for additional information.

Got questions? Feel free to contact our Technical Support at support@tiger-technology.com

Licenses

Download the **Storage Bridge** executable and manuals from the Tiger Technology licensing server

a. Visit: https://license.tiger-technology.com/ and enter your credentials
b. Once you have logged in, you will be prompted to register.
c. If you logged in using a **Client Account**, click on "**Home**" to you see the list of product licenses available. Click on the product license you wish to use.
d. To download the manuals, click on "**Documentation**" (bottom left)
e. To download the executable, click on "**Current Version**" (bottom left)

System Requirements

Plan for a min 3-4 days of local storage retention. This will be used for caching most recent camera data, as well as to act as buffer should you ever run into a problem with the internet upload speed. This buffer will dictate the amount of time you have to identify and solve potential internet connectivity issues. In addition, and while stub files are zero byte in size, they do require an entry in the file system. When looking at long retention periods, keep in mind that every 1 million files will consume 100MB of local disk space.

Storage Bridge will consume ~20% of the CPU during the initial indexing of the file system (each time the drivers are started), then drops to ~5% during normal operations. Memory footprint is typically not an issue.

1) Recording Servers should have:
   a) Internet upload speed at least 25% more than total camera ingests to disk
   b) Access to https://saas.tiger-technology.com
   c) Access to the cloud bucket endpoint
   d) Ports 443 outbound
   e) Ports 8536 and 8537 inbound/outbound with the Management Client
   f) Contact Tiger for additional instructions if using a proxy server

2) Cloud requirements
   a) One cloud bucket/container has been created for each of your recording locations.
   b) Recording Servers should have FULL Read/Write AND Delete capabilities on the objects in the cloud.

Tiger Technology

Preparation

1) Connect and configure your Recording storage and Archive (optional) according to Milestone's guidelines.

   NOTE: Storage Bridge operates directly on your Recording storage (the cloud becomes your archive). When using DR, this gives you the best possible recovery. If you require that your Milestone Recording Server be configured with an Archive, you can use Storage Bridge for either the Recording storage or the Archive, or for both of them.

2) **IMPORTANT:** Under "**Storage and Recording Settings**" in the Management Client, set the "**Retention time**" according to how much **TOTAL** camera data you want to keep on your volume(s). This setting is global and determines when data will be deleted locally and in the cloud:
   a. The retention time should cover local **AND** cloud data
   b. The size should cover local **AND** cloud data (don't worry if your volume is much smaller as it will extend into the cloud)

   EXAMPLE: If you set a 90-day retention time, regardless of where the data actually is, XProtect will delete it. As XProtect deletes the local files, Storage Bridge will then delete the associated data in the cloud tiers (note that there may be a delay with some cloud providers). You choose how much data stays on the local drive vs. nearline (hot) cloud storage vs. archive (cold or frozen) cloud storage using Storage Bridge.

   c. If you need to decommission an Archive volume without losing data, you will need to proceed in two steps:
      i. First make sure the retention time on the Recording storage is at least as long as the current Archive volume
      ii. Until a full Archive period has been met, some of the archive data will continue to come from the current Archive.
      iii. Once passed a full archive period, the Archive volume can be decommissioned as all latest "archive" data is now coming from the cloud.

Setup the Cloud Bucket(s)

1) To quickly estimate your required internet speed, you can use the "**1/5 rule of thumb**":
   a. If you know the average bitrate of all your cameras:
      i. Multiply total recording bitrate x 1.5 (allows for readback and fluctuations)

EXAMPLE: 173 Mbps x 1.5 = ~250 Mbps

b. If you know the current storage requirements for a given retention period:
    i. Multiply #GB / #days x .15

EXAMPLE: 350 GB per day = 350 x.15 = ~50Mbps
100TB per month = 100 x1024 x.15 ÷ 30 = ~500 Mbps

2) Log into your Cloud account and create separate buckets/containers to be associated with each recording server and volumes.

NOTE: If you have a recording server with only a Recording volume (no Archive volume) the same bucket/container is used for storing a single copy of all data and is used for both Disaster Recovery (DR) and Extension. DR contains all camera data, plus XML and index files needed to recreate the XProtect database. Extension only requires a subset, that is, the camera data. If you have more than one volume configured on your recording server, each volume will require its own bucket.

3) Have your Cloud account details ready for the install (Access Key, Secret Key, etc.)

Install the Storage Bridge plug-ins and Activate your License

1) Make sure your recording server is fully configured and able to record prior to installing Storage Bridge.

NOTE: Your recording server can be recording live camera data while installing Storage Bridge (it won't affect operations)

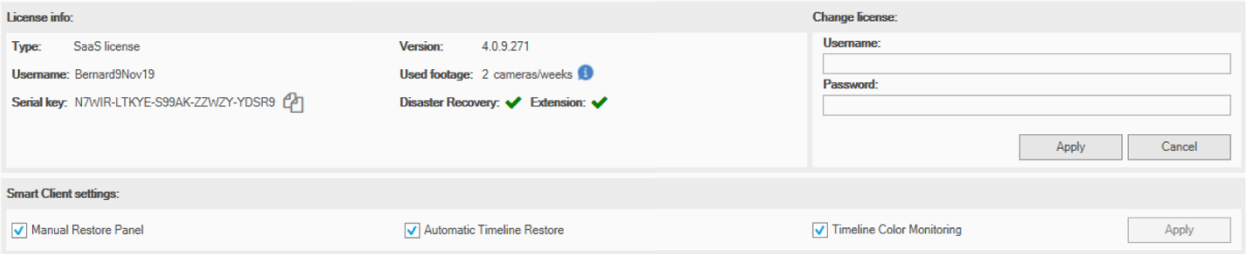
2) Close the XProtect Management Client app

3) Install **Storage Bridge** (follow on-screen instructions)
    a. The installer contains three software components
        - Management Client (for configuration – must be installed)
        - Recording Server (all the cool technology – must be installed)
        - Smart Client (for data visualization and movement – optional)

    b. It is possible to install these components on **ONE** or **SEPARATE** machines
        - Just select/deselect the appropriate option(s)

4) Activate your license by opening the **XProtect Management Client**
    a. Click on the Storage Bridge "**Administration**" tab

b. Select the recording server to activate
c. Enter your Username and Password, and click “Apply” to activate
    - NOTE: If you were provided a **Client Account** in addition to **Product Licenses**, you must use the later credentials for activating your license. In this case, the Product License will typically be identical to your login, but will have the **_SBX** suffix added to it and the password will be empty (you add your own).
d. Once activated, your screen should look like this:



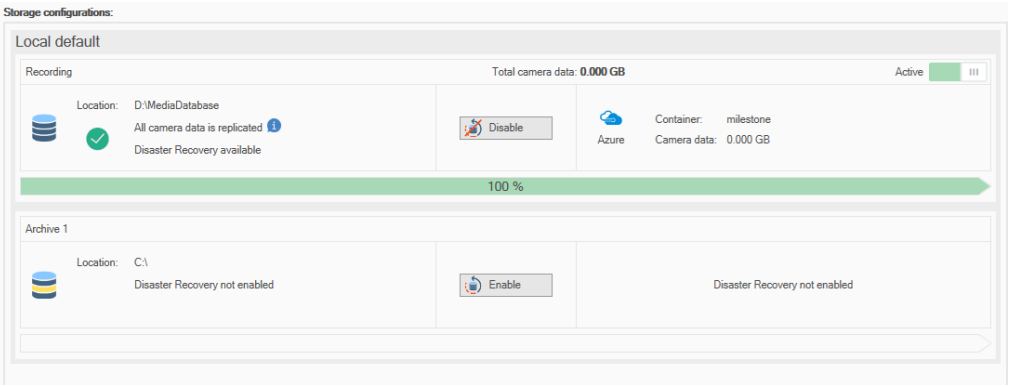
e. If you have any issue activating, please Troubleshooting section below
f. You can choose which options will be available to operators using the XProtect Smart Client (see details below)

Configure the Disaster Recovery

Activating the Disaster Recovery (DR) functionality using Storage Bridge is easy. This functionality can be activated on your Recording storage(s), your Archive(s), or both.

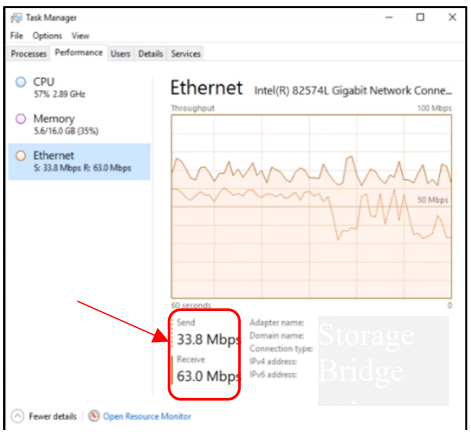
1) Select the Storage Bridge “**Disaster Recovery**” tab
    a. For each volume where you desire DR, click “Enable”
    b. Configure your cloud target
        i. Make sure to select a **DIFFERENT** bucket/container for **EACH** volume
        ii. If **Storage Extension** has already been configured, you will NOT be prompted for cloud details as your data will NOT be replicated twice. The same dataset is used.
    c. To start the replication process, switch the “Inactive” to “Active” (top right)
    d. Within a few minutes (depending how many cameras and files are managed), Storage Bridge will start replicating and display the % of local data that has been replicated to the cloud.

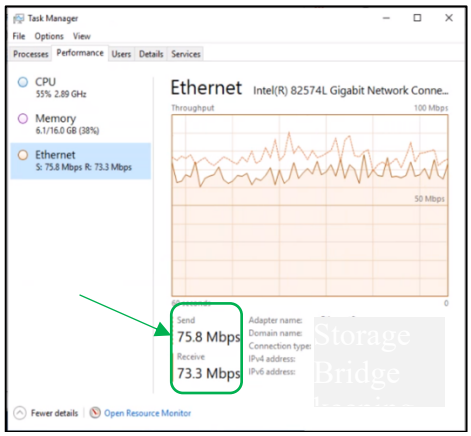
NOTE: After all existing files have been replicated, this number will typically be just shy of 100%, unless you stop the camera streams or the recording server in order for the most current data to reach your cloud target.



Verify that your internet is keeping up

Open Task Manager on the Recording Server to see how fast Storage Bridge can upload to the cloud. Click on the "Performance" tab, and then select "Ethernet". Unless other processes are running in the background, the "Receive" will show the incoming camera data while the "Send" shows the rate at which Storage Bridge is uploading to the cloud. On average, the Send should no less than the Receive:





The screen grab on the left shows a problematic situation where **Send** bandwidth is less than **Receive**. This means Storage Bridge is currently not able to keep up with the incoming data flow. Storage Bridge is barely keeping up on the right and 25% headroom would be desirable (showing about 12%). The % of uploaded camera data should continue to increase and eventually stabilize around 99%.

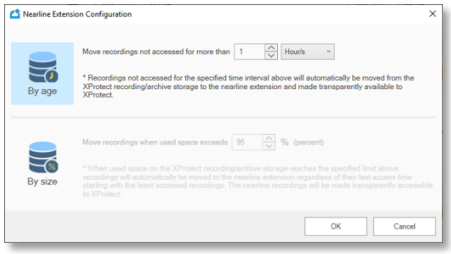
Configure the Storage Extension

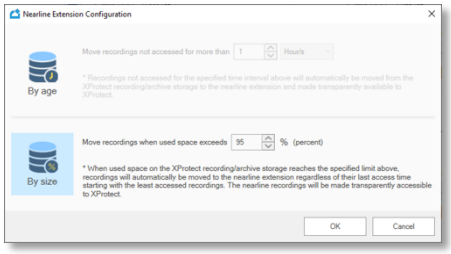
Use the Extension option to make your local volume appear bigger and infinitely scalable. This functionality can be activated on your Recording storage(s), your Archive(s), or both. It can be activated with or without Disaster Recovery. When activated with Disaster Recovery, Extension uses a subset of the data already replicated on the DR target.

Configuration steps:

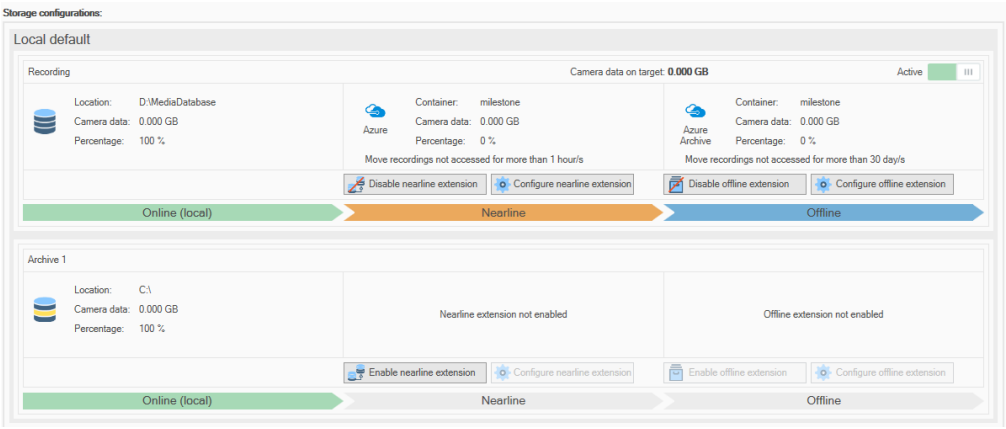
1) Select the Storage Bridge "**Extension**" tab
    a. For each volume where Extension is desired, click "Enable nearline extension"
    b. Configure your cloud target
        i. If **DR** has already been configured for this volume, you will NOT be prompted for cloud details as your data does NOT get replicated twice. The same bucket will be used.
    c. Make sure to select a **DIFFERENT** bucket for **EACH** volume.

2) Click on "Configure nearline extension"
    a. Choose "**By Age**" to keep camera data locally for a specific amount of time or choose "**By Size**" to keep it until your local drive reaches a specified capacity threshold. When either condition is met, content is removed and replaced by zero-byte stub files. Data is safely kept in the cloud until the retention time set on your storage volume is met. Make sure to maintain enough "free" space on your recording drive to ensure Milestone has enough room to continue recording during an internet outage.





    b. To start the replication process, switch from "Inactive" to "Active" (top right)
    c. Within a minute, Storage Bridge will display the % of local data that has been replicated to the cloud.



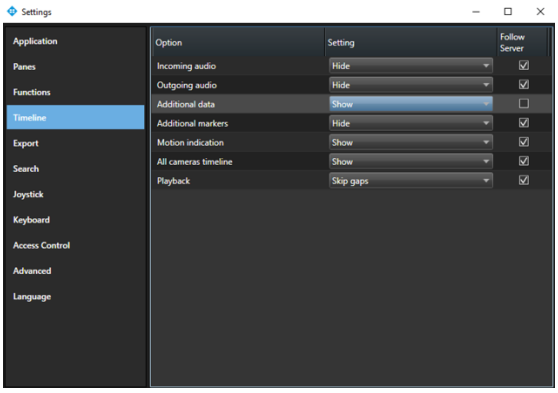
d. If your cloud provider supports an archive tier, Storage Bridge allows you to leverage it. Note that in this case, any archived video will need to be manually recalled BEFORE it can be viewed on the timeline.

Using the XProtect Smart Client plug-in

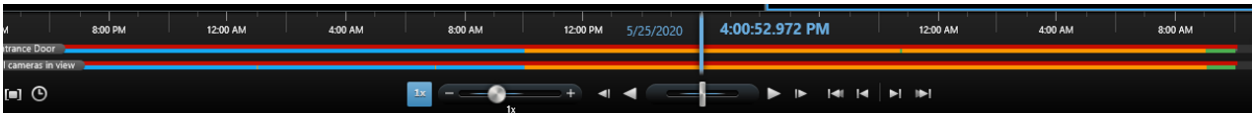
There are a few options available to the XProtect Smart Client. They are all enabled by default but can be disabled through the Management Client (see Installation and Activation steps above).

Timeline Color Monitoring – Visual indication of where the data is currently stored:

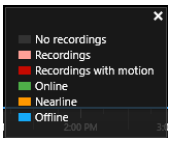
1) Go to Settings, select Timeline, and set “Additional data” to “Show” (vs. “Hide”)



2) When activated, Storage Bridge will display additional colors on the timeline:



Clicking on the XProtect bottom right "?" brings up the timeline legend:



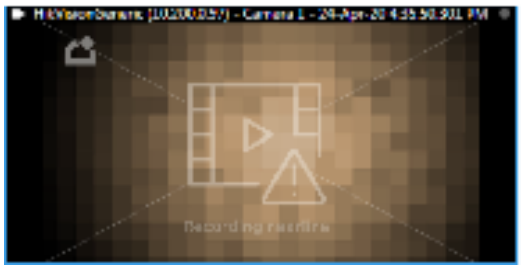
Storage Bridge displays the following storage locations:

- **Online** (Green): Camera data is on the local drive AND replicated to the cloud
- **Nearline** (Orange): Camera data is in the cloud and seamlessly accessible
- **Offline** (Blue): Camera data is in the cloud, but in an archived tier (if applicable)

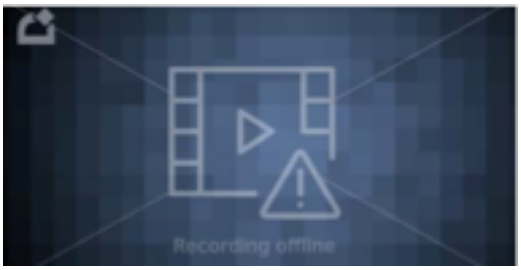
Automatic Timeline Restore:

1) **Online** (Green) camera data is **ALWAYS** available for playback.

2) **Nearline** (Orange) camera data will be automatically retrieved when selected or played on the timeline, unless **Automatic Timeline Restore** is disabled. In this case, camera data will NOT automatically be restored from the cloud (potentially saving cloud egress fees) and Storage Bridge will display a "Recording Nearline" frame:



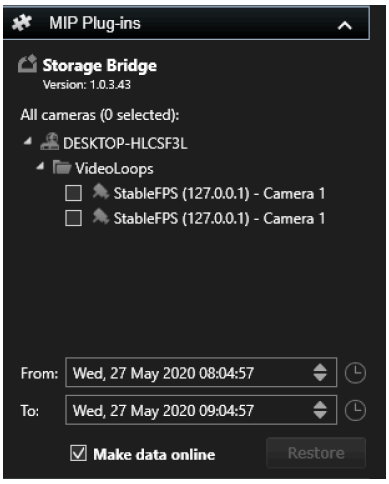
3) **Archived** (Blue) sections must be manually retrieved through the Restore Panel or through the Management Panel (see below). By definition, camera data in a cloud archive tier will typically take hours to restore (thus the significantly lower cost). Storage Bridge has the unique ability to display a "Recording Offline" frame:



Manual Restore Panel:

Storage Bridge will display an “Recording Offline” notice when playing or selecting areas of the timeline that are Archived (frozen) until the archived video has been restored to the nearline (hot) cloud tier.

1) When the **Manual Restore Panel** is activated, XProtect Smart Client operators can restore data for specific **Cameras**.
    a. The speed at which data is retrieved depends on the cloud provider and the options chosen when configuring the cloud target above.

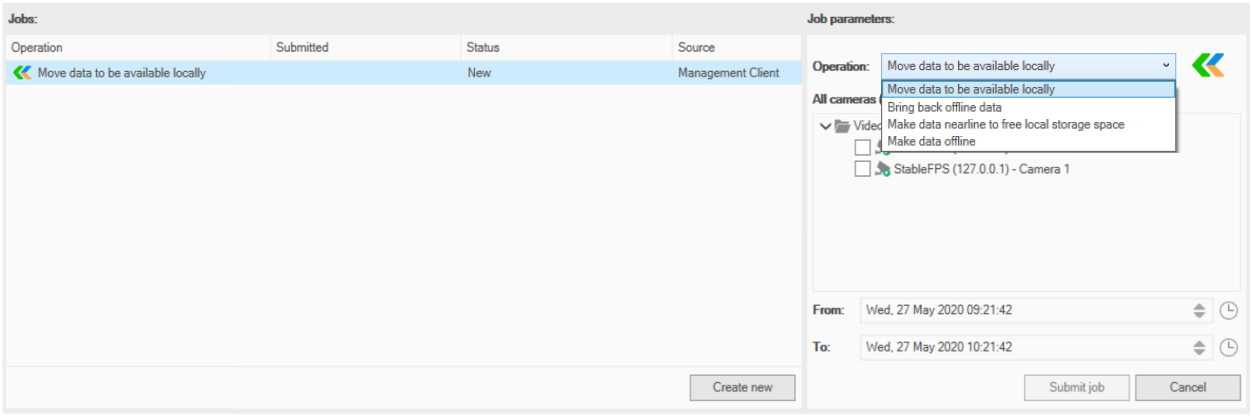


TIP: Use the **Time Selection Mode** or **Set Start/End Time** buttons to automatically set the date and time interval to be restored:

Creating Restore Jobs using the XProtect Management Client

When the Storage Bridge Automatic Timeline Restore option is disabled, restore jobs can be created from within the **XProtect Management Client** plug-in.

1) Open Management Client and go to the Administration tab:

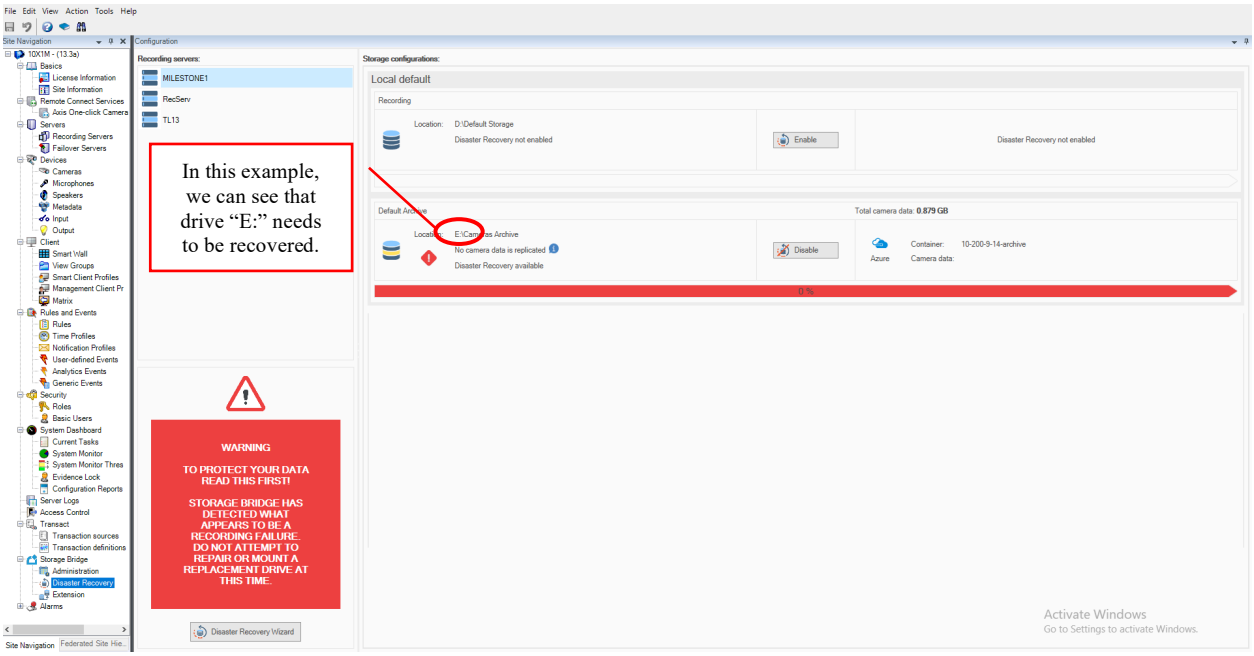


2) Click on "**Create new**"
3) In the dropdown, select the type of job you want to perform
4) Use **From**: and **To**: to set the date and time interval to be restored
5) Click "Submit job"
6) Storage Bridge initiates the restore operation. Note that it may take some time for the operation to complete. A status bar will show the progress.

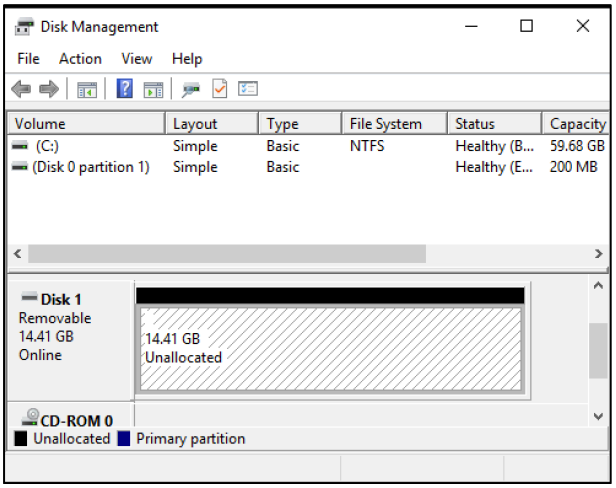
Recovering a Failed Storage After a Disaster

When the **Disaster Recovery** option is enabled, Storage Bridge can recover from a Recording storage or Archive failure. As soon as XProtect detects the failure, Storage Bridge will display a warning message. It is critical to follow the step-by-step instructions of the Wizard.

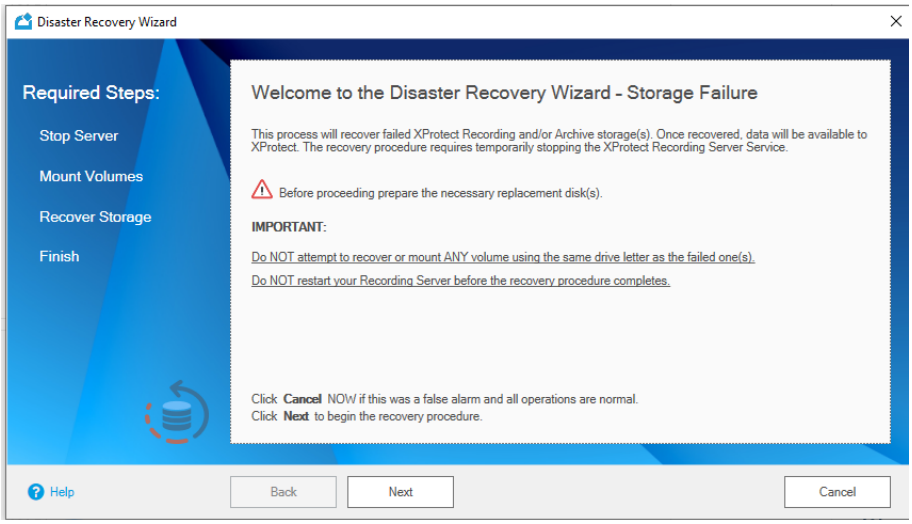
1) Identify the failed drive letter:



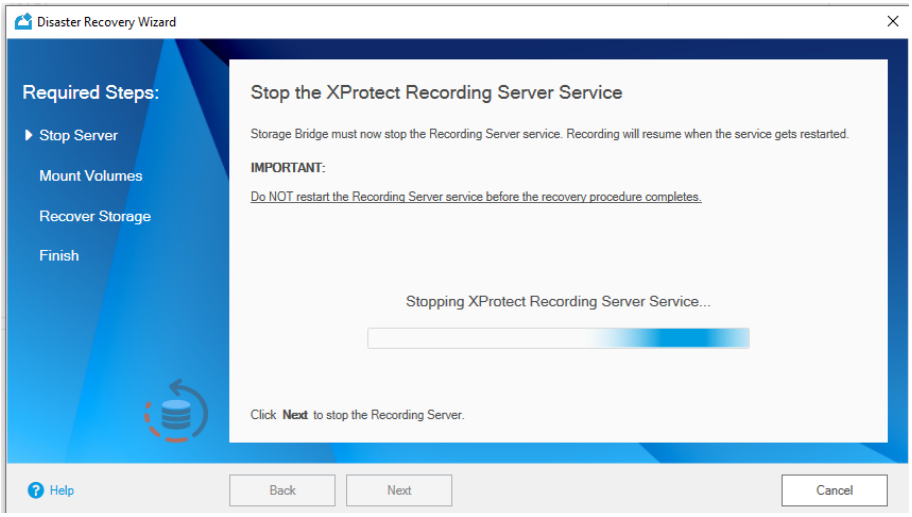
2) Connect a replacement drive to the Recording server, but do **NOT** mount it. To be safe, the replacement drive should **NOT** be formatted (or you should **FIRST STOP** the Recording server **PRIOR** to connecting a formatted drive.



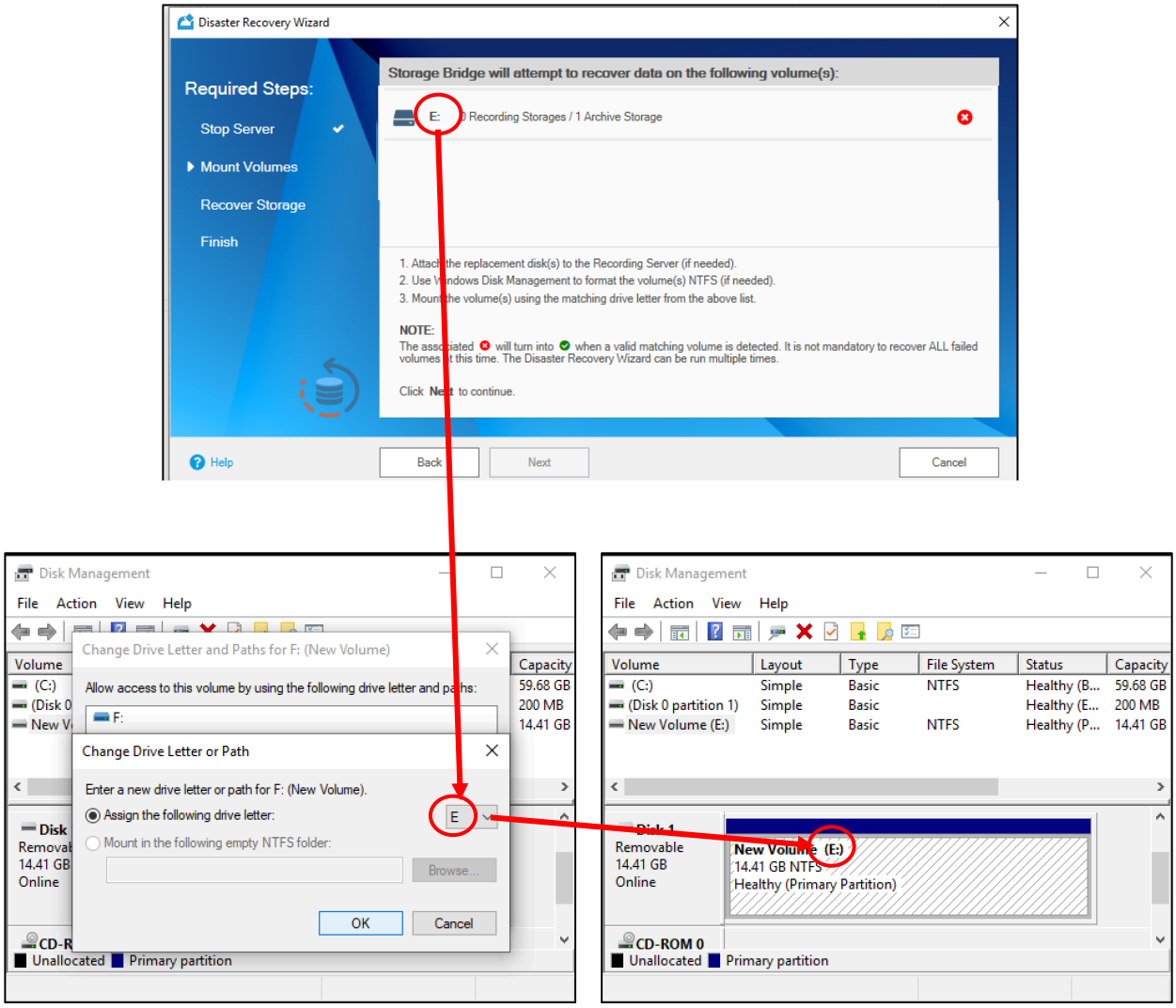
3) Click on “Disaster Recovery Wizard” to begin the recovery process.



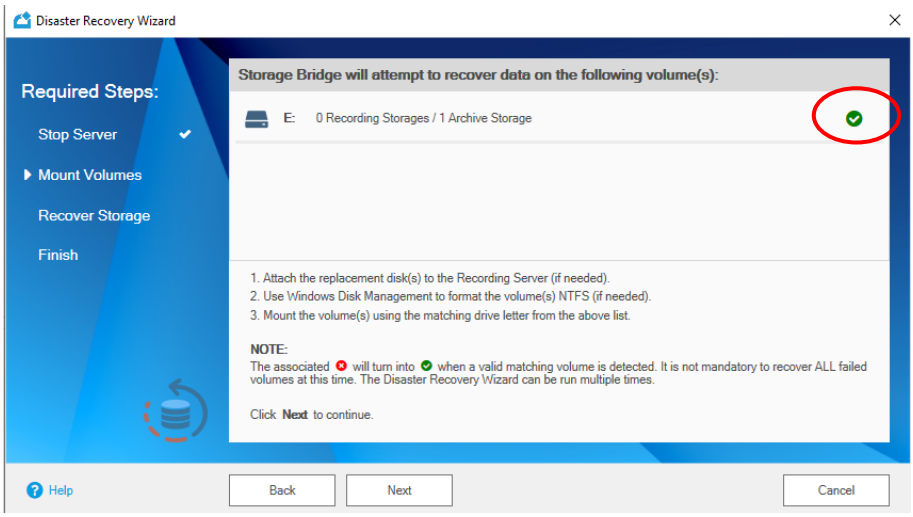
4) The Wizard will first stop the Recording server (if it isn’t already):



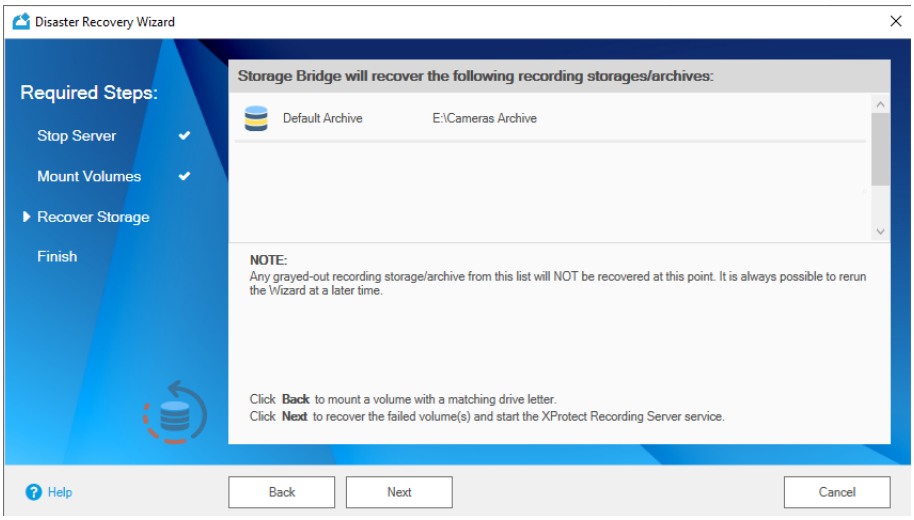
5) It is now time to format and assign the original drive letter to the replacement drive (in this example, the failed drive letter was E:).



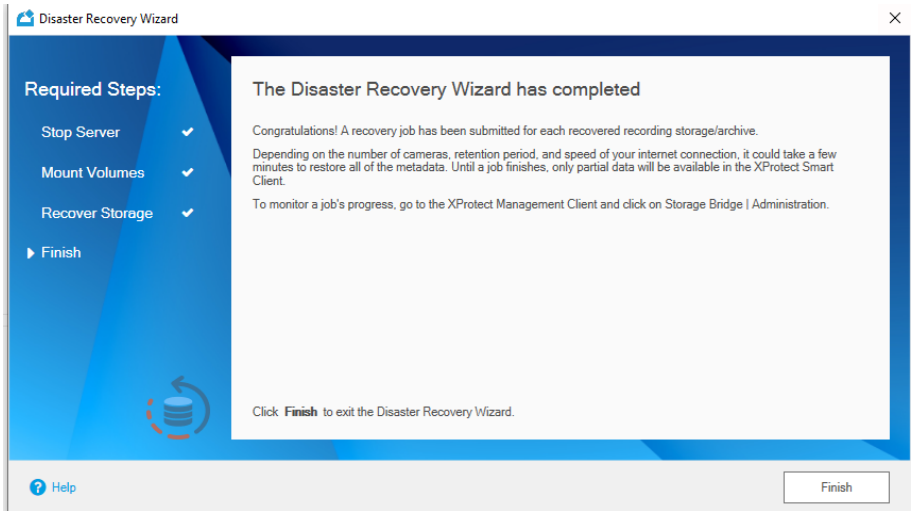
6) When the replacement volume is detected with the proper drive letter, Storage Bridge displays a green checkmark:



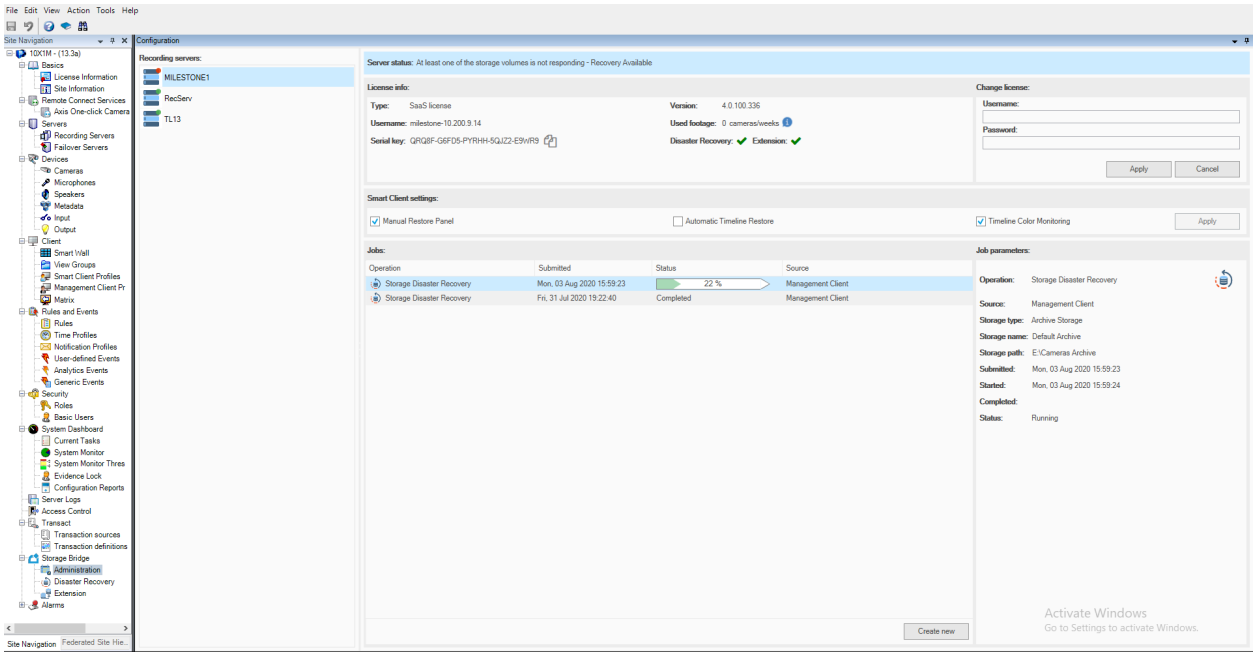
7) Storage Bridge will then ask for confirmation:



8) Congratulations! The Wizard has now completed.



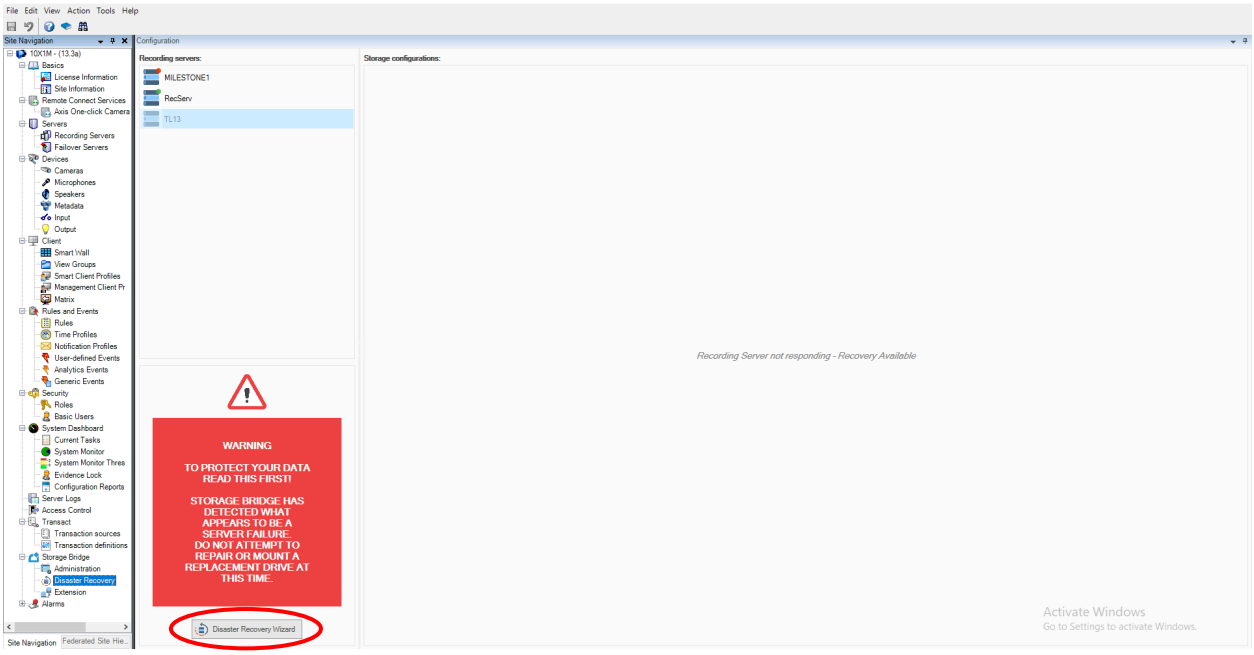
9) You can monitor the recovery progress on the Administration tab. It should only take a few minutes to restore the database. Note that video content will only be restored on demand (by accessing the timeline or by creating a restore job).



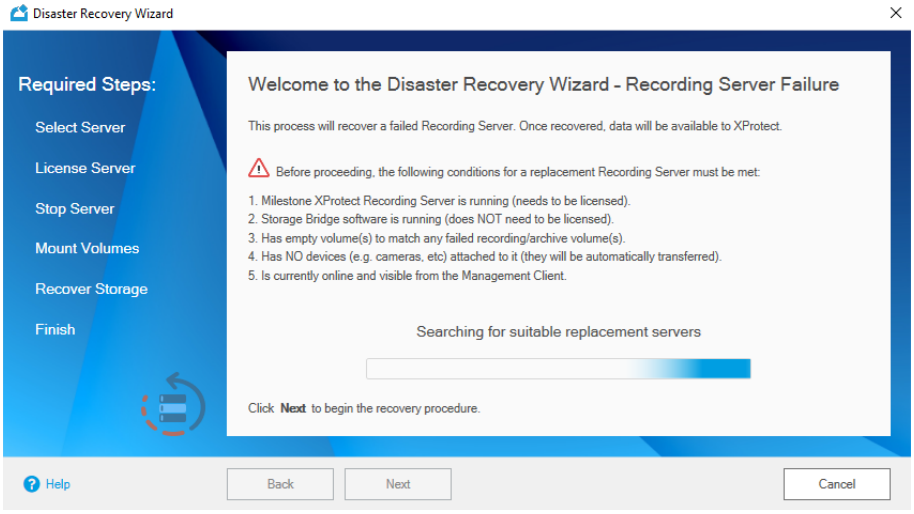
Recovering a Failed Recording Server After a Disaster

When the **Disaster Recovery** option is enabled, Storage Bridge can recover from a Recording server failure. As soon as XProtect detects the failure, Storage Bridge will display a warning message. It is critical to follow the step-by-step instructions of the Wizard.

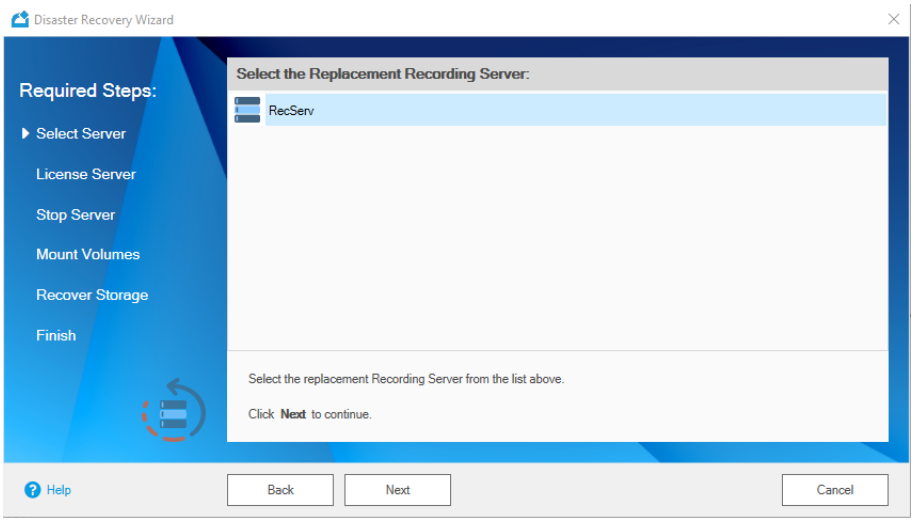
1) Click on “Disaster Recovery Wizard” to engage the recovery procedure.



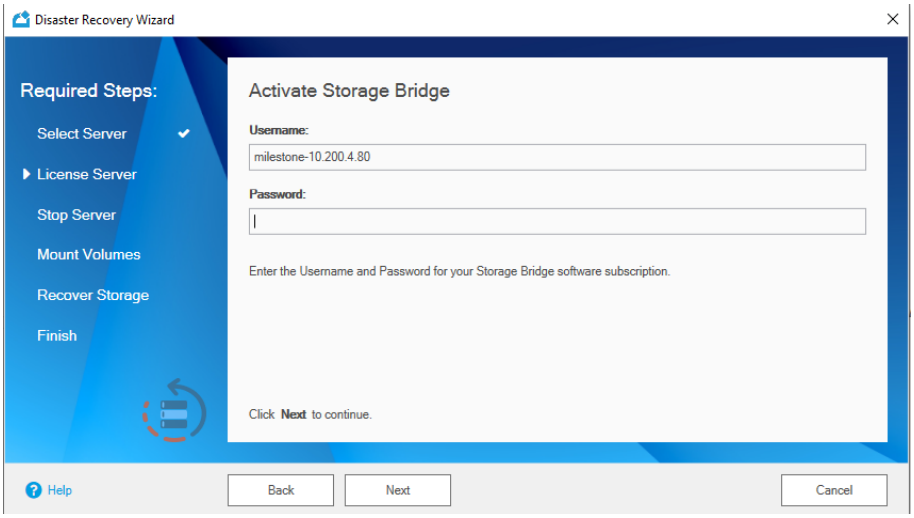
2) First make sure the replacement Recording server is ready and available:



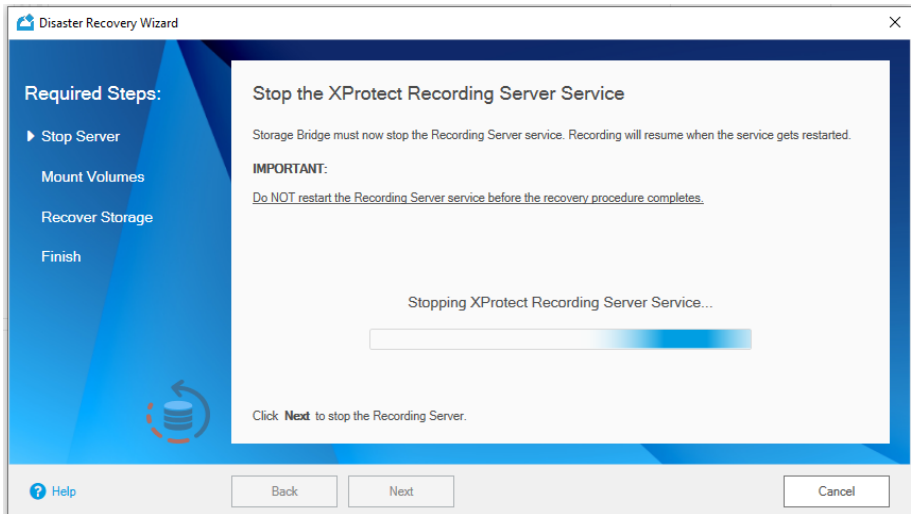
3) Storage Bridge automatically lists the available replacement servers. Select one.



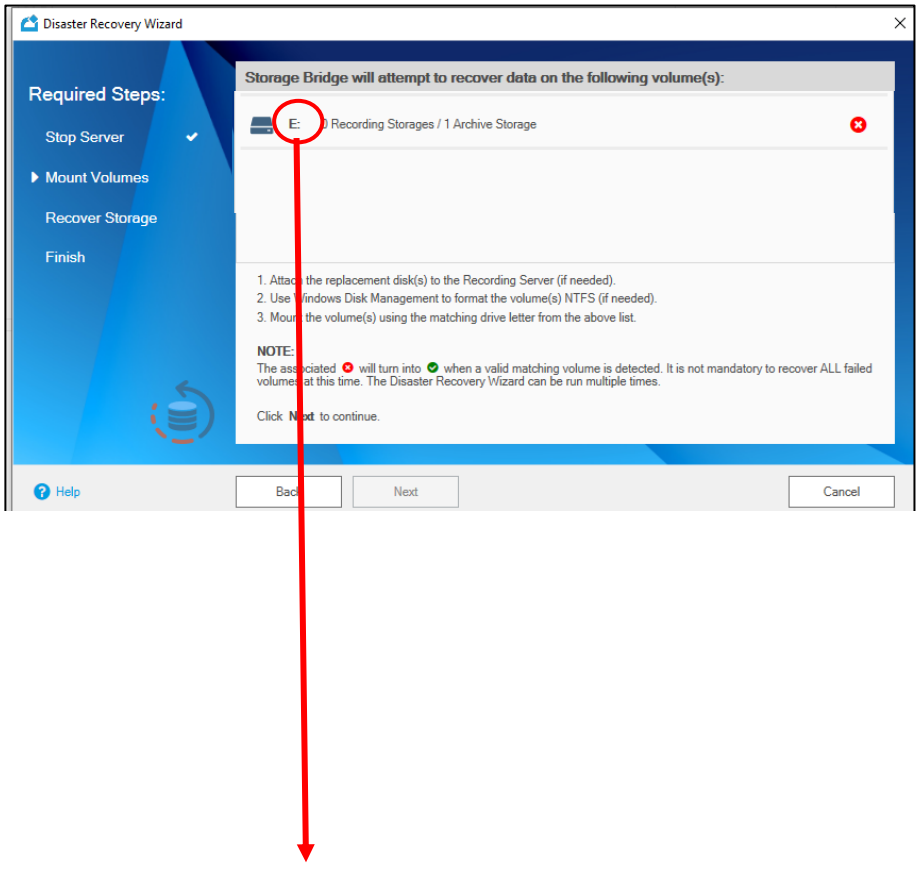
4) Active the Storage Bridge license on the replacement server (your credentials are listed above):

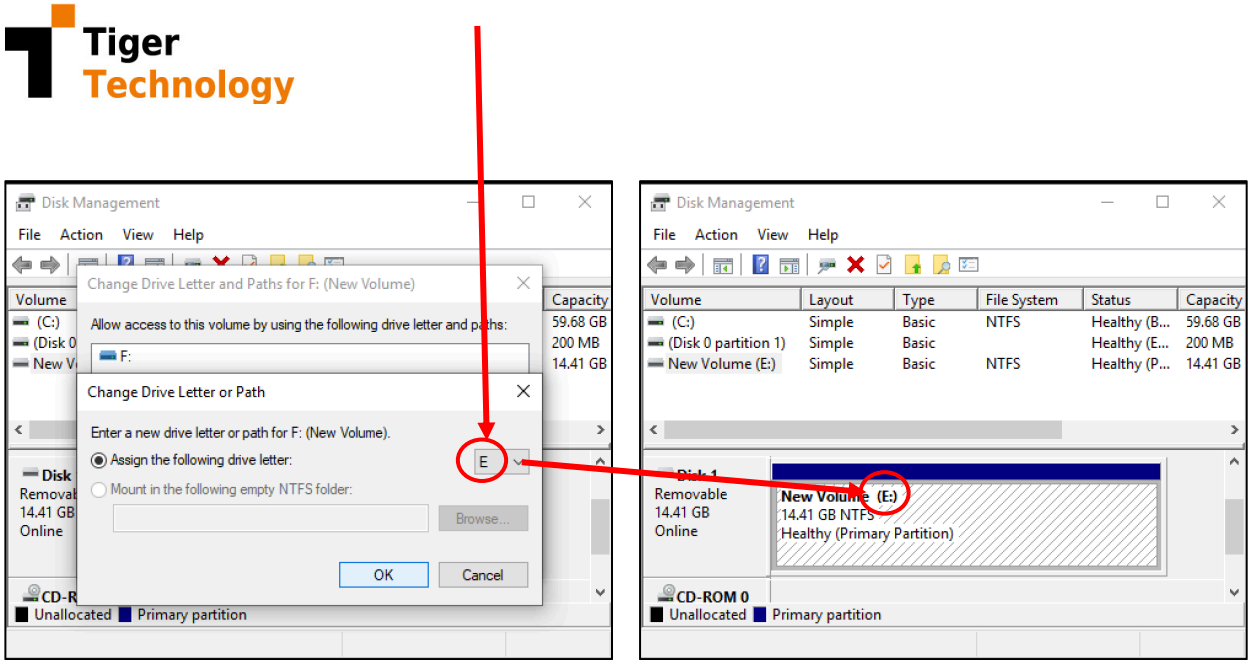

Disaster Recovery Wizard
Required Steps:
Select Server
License Server
Stop Server
Mount Volumes
Recover Storage
Finish
Activate Storage Bridge
Username:
milestone-10.200.4.80
Password:
Enter the Username and Password for your Storage Bridge software subscription.
Click Next to continue.
Help
Back
Next
Cancel

5) The Wizard will now stop the replacement Recording server

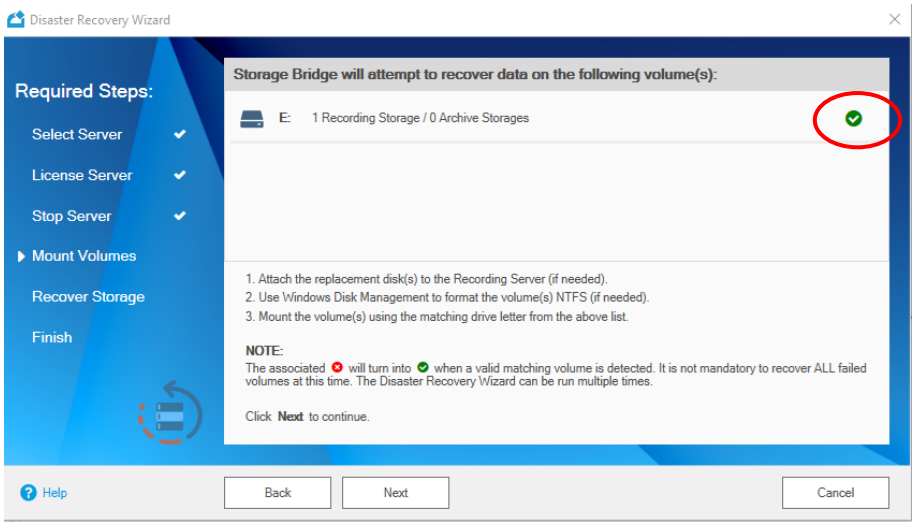


6) It is now necessary to format assign the same drive letter to the replacement drive (in this example, the original drive letter was E:).

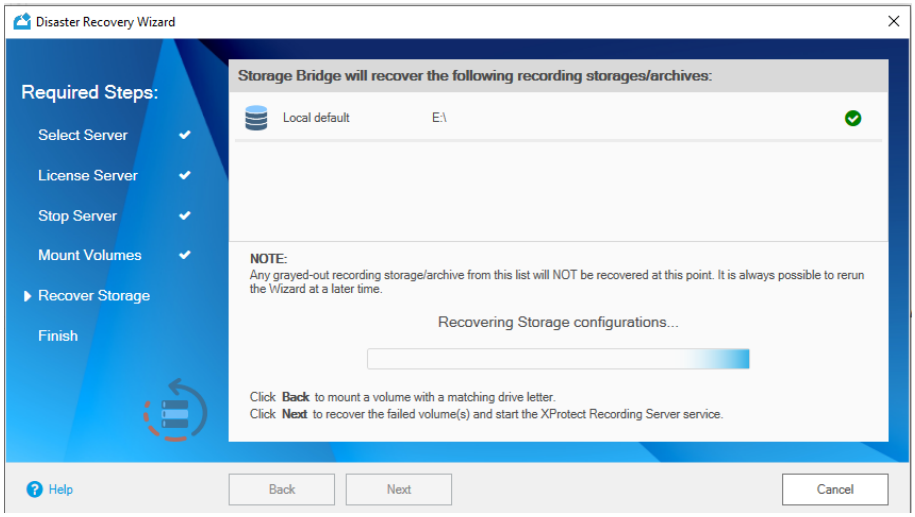




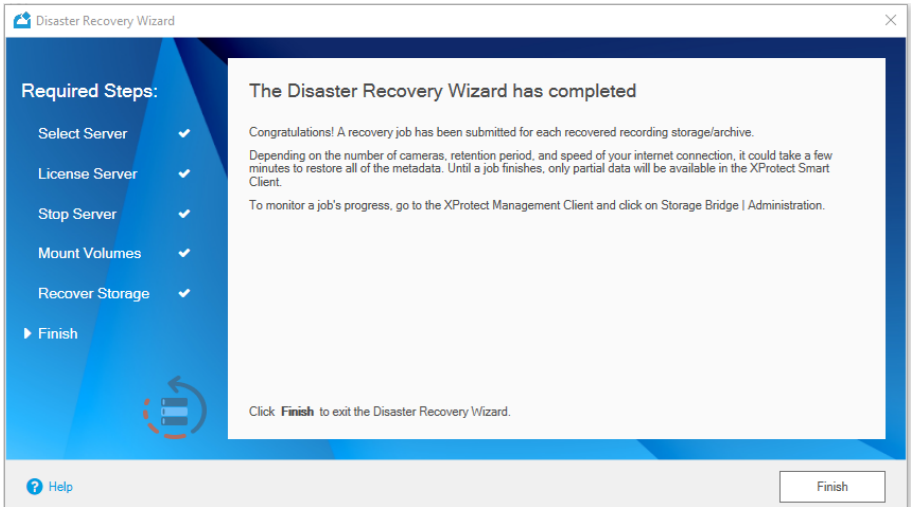
7) When the replacement volume is detected with the proper drive letter, Storage Bridge displays a green checkmark:



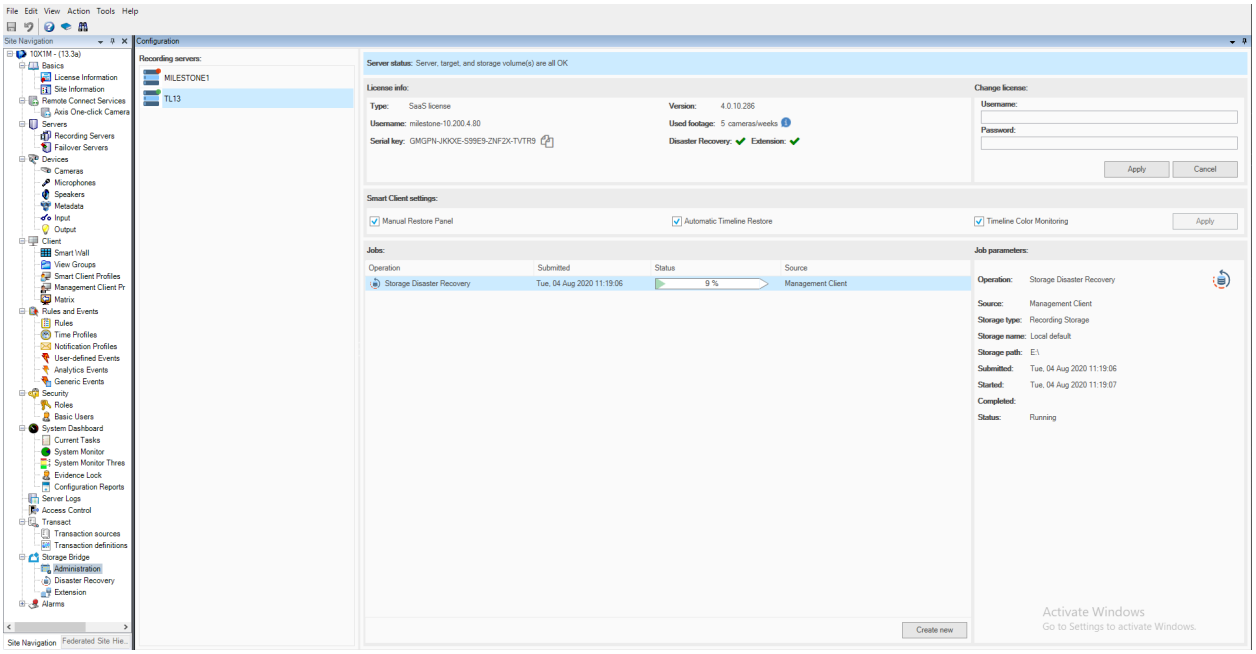
8) Storage Bridge will then ask for confirmation:



9) Congratulations! The Wizard has now completed.



10) You can monitor the recovery progress on the Administration tab. It should only take a few minutes to restore the database. Note that video content will only be restored on demand (by accessing the timeline or by creating a restore job).



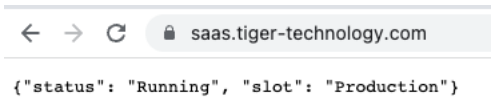
Tiger Technology

Configuring Firewalls and Proxy Servers

Storage Bridge must communicate with the cloud target as well as with the Tiger Technology licensing server for activating your license and for keeping them activated.

1) Make sure that the following requirements are met:

    a. Can reach the Azure service running at https://saas.tiger-technology.com.
        i. When typing the URL, you should in your browser, you should obtain the following response:



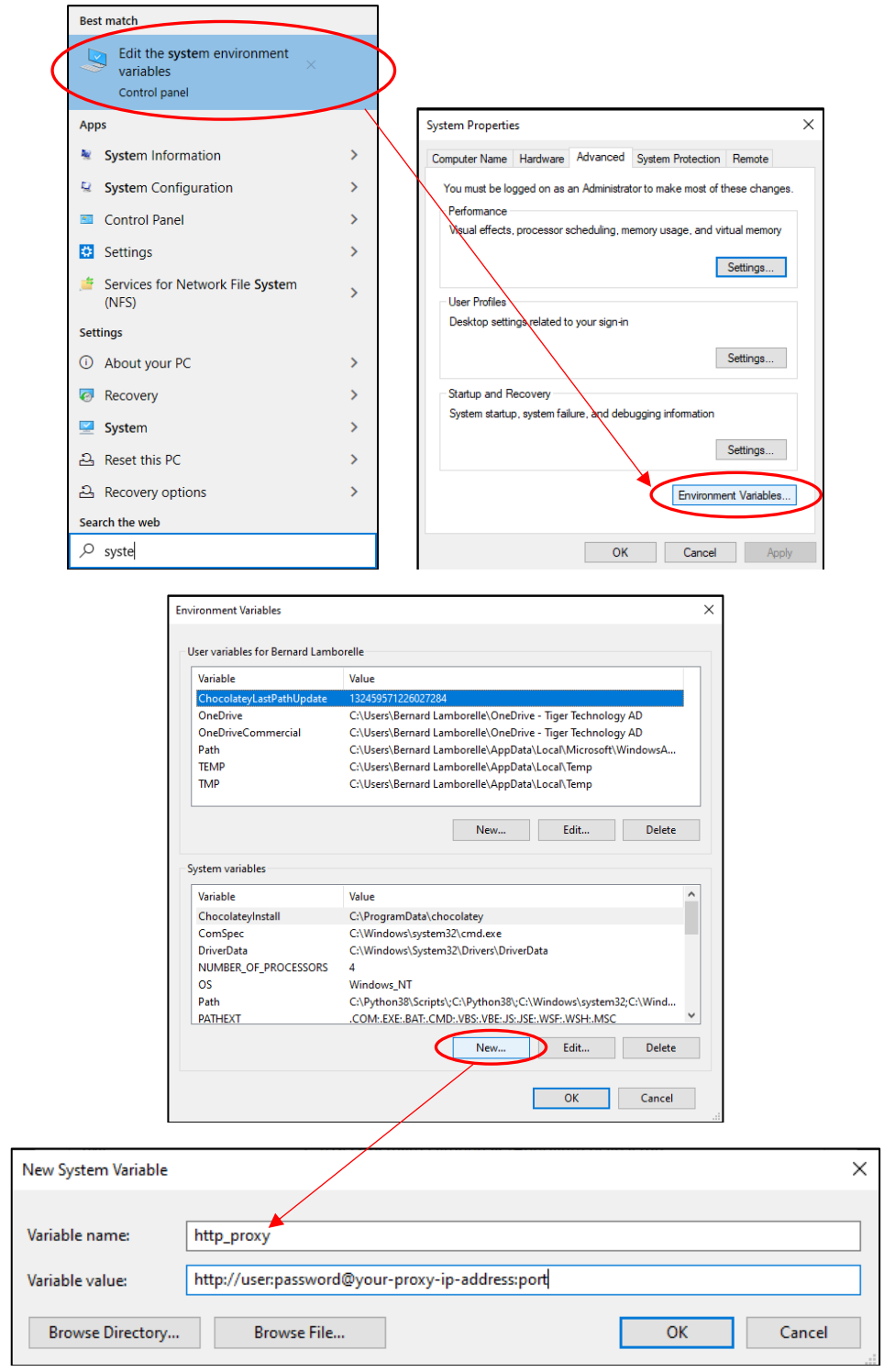
        ii. If you get an error, you will need to whitelist the domain name

    b. Check your firewall. The following ports must be open:
        - (for object storage target over http connection) **80** - outbound rule only
        - (for SaaS activation and/or communication with object storage target over https) **443** - outbound rule only
        - (for a network target) **445** - outbound rule only
        - (for remote connection) **8536** - inbound and outbound rules
        - (for remote connection) **8537** - inbound and outbound rules
            i. You can test this connection AFTER you have installed the Storage Bridge plugin by entering the following URL in a web browser on the Management Server: https://xxx.xxx.xxx.xxx:8537/version (where xxx.xxx.xxx.xxx is the IP address of the Recording Server you are testing)

2) If you are using a proxy server, Bridge uses different mechanisms for accessing the cloud and for communicating with the licensing server.
    a. To configure proxy for the cloud target:
        i. Open a Command prompt in elevated mode and type:

```
C:\Windows\system32\tiercli config global proxy <proxyserver:port> [username] [password]
```

    b. To configure proxy for the licensing server:
        i. Set your System Environment Variables:



Variable name	**Variable value** (try the following formats)
`http_proxy`	`proxyserver:port` ***or***

	http://user:password@your-proxy-ip-address:port/
https_proxy	proxyserver:port ***or*** https://user:password@your-proxy-ip-address:port/

IMPORTANT: It is required to reboot your computer after changing system variables.

ii. If you are still experiencing issues activating the Bridge software, please use the SaaS-Check utility to troubleshoot your issue, as described below.

Saas-Check Utility

Tiger Technology has developed a troubleshooting application that can help identify the source of the problem.

NOTE: Troubleshooting firewalls and proxy issues will likely require the assistance of your System Administrator.

If you are experiencing issues activating your Bridge software, download the saas-check.exe utility (https://tinyurl.com/8fjjaby4).

1. On the Bridge machine (i.e. Recording Server), open a Command prompt in Elevated mode
2. Run saas-check with the following parameters

Usage: **saas-check.exe** <server_host> <cabundle_path> <username> <password> <serial>

Where:
<server_host> is **saas.tiger-technology.com**
<cabundle_path> is **"C:\ProgramData\Tiger Technology\backup\cert\cacert.pem"**
<username> is your activation **Username**
<password> is your activation **Password**
<serial> is the **?????- ?????- ?????- ?????- ?????** serial key found in the Bridge interface

The command above assumes C: is where the utility was copied. Successful output of this tool should look like this:

```
message: "Successfully updated/activated license";
update-url: "https://license.tiger-technology.com";
```

```
220321 14:57:10.424.001;    saas:________:00006C8C; F(01); message: "Successfully updated/activated license"; main()
220321 14:57:10.424.002;    saas:________:00006C8C; F(01); update-url: "https://license.tiger-technology.com"; main()
220321 14:57:10.424.003;    saas:________:00006C8C; F(01); next-fetch: 3600 (seconds); main()
220321 14:57:10.435.001;    saas:________:00006C8C; F(01); ????? - ????? - ????? - ????? -?????; main()
```

If you do not receive a successful activation message, please check if the error falls in one of the following categories:

Failed SSL Connect Error

A “Failed SSL Connect Error” will likely occur due to improper firewall configuration. SaaS-Check.exe will report something like this:

```
curl_easy_perform() failed: SSL connect error;
SaaS HTTP POST request failed Result is 0x82100
```

For a quick test, you can try disabling Windows Defender on Management Server and Recording Server. If you are using advanced firewalls, such as Palo Alto Networks, make sure you are not blocking access to encrypted websites (https://saas.tiger-technology.com). Also make sure you are disabling control of decrypted SSL. These settings can be used to limit or block SSL sessions based on criteria including the use of unsupported cipher suites or protocol versions, or the availability of system resources to process decryption.

Peer Certificate Authentication Error

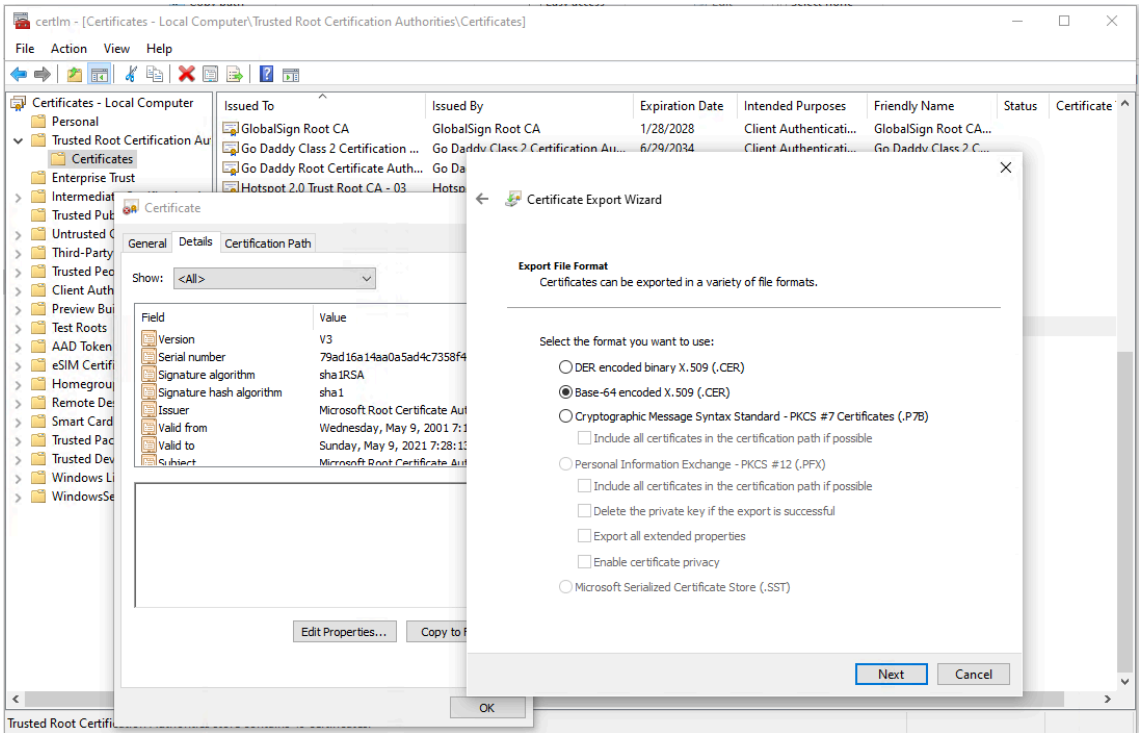
A “Peer Certificate Authentication Error” will likely occur due to missing security certificate. SaaS-Check.exe will report something like this:

```
curl_easy_perform() failed: Peer certificate cannot be authenticated with given CA certificates;
SaaS HTTP POST request failed Result is 0x82100000 (error "Generic" from "SANDS tool (sntool)");
```

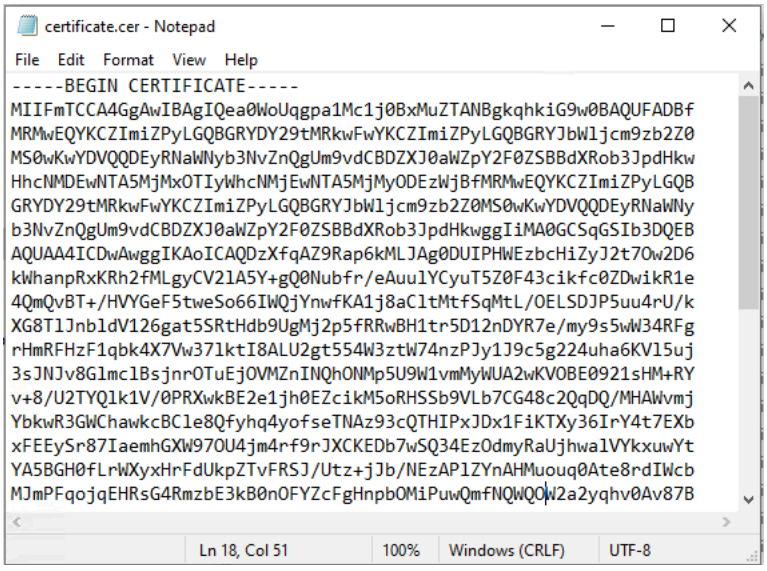
Bridge uses cURL to communicate with its licensing server. However, cURL may not automatically integrate your domain security certificates. If your organization uses domain security certificates, you will need to follow these steps:

3. In Windows, search for “Manage computer certificates” and open

4. Locate your domain security certificate (most likely stored under Trusted Root Certification Authorities/Certificates)
    a. Look for a certificate that contains the name of your organization (typical)
    b. Double click on the certificate
    c. Select the “Details” tab
    d. Click on “Copy to files…”
    e. Select “Base-64 encoded X.509 (.CER)



f. Specify file name to export
g. Locate the exported file
h. Open the exported file with Notepad

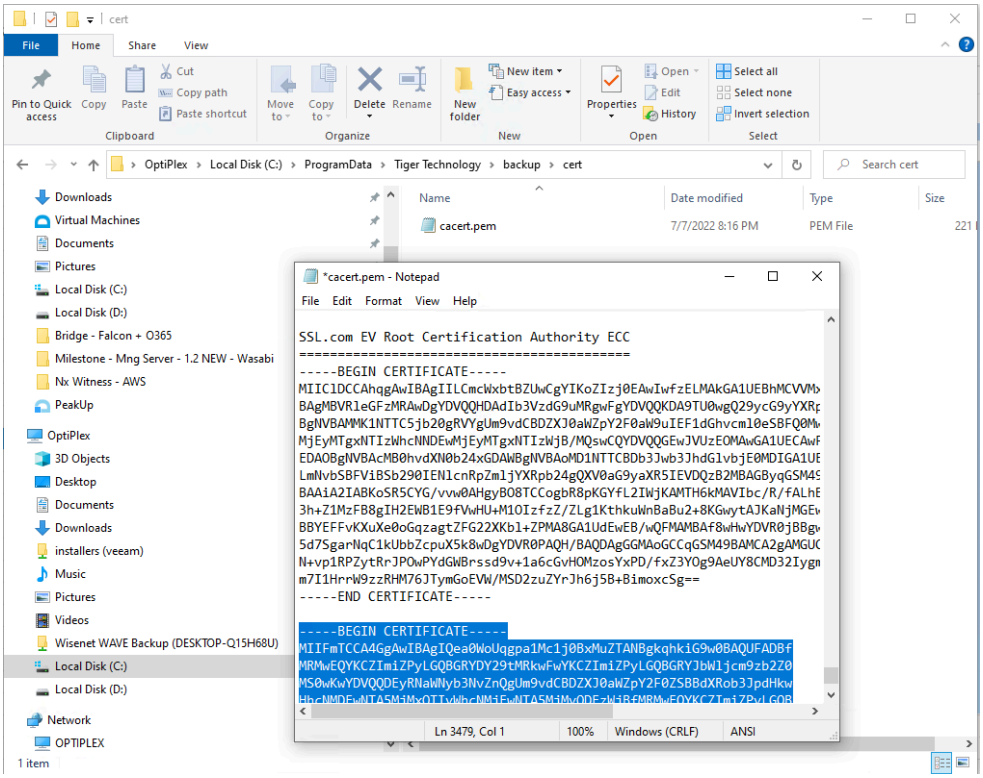


i. Copy the ENTIRE content of the file

5. Locate the security certificate used by Bridge, and open it in Notepad:

`C:\ProgramData\Tiger Technology\backup\cert\cacert.pem`

6. Append the copied certificate to the existing list of certificates by pasting it at the end of the file. Save the file.



7. Try activating the software again. If none of the above works, send us the output you are getting when running the **saas-check.exe** command.