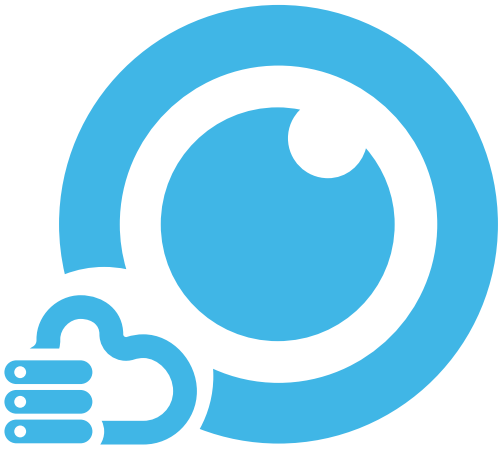
Tiger Surveillance

Surveillance Bridge

Administration Guide

Version: 2.0

Revision: April 2023



Title: Surveillance Bridge Administration Guide

Software version: 2.0

Date: April 2023

Contents

I. Introduction to Surveillance Bridge

Congratulations on your purchase of Tiger Technology's Surveillance Bridge. Surveillance Bridge leverages your VMS (Video Management System) with flexible disaster recovery capabilities and/or seamless extension of the recording storage and archive's capacity to an external storage tier. By enabling a cloud target, a network share, or any local volume to seamlessly integrate into your VMS storage infrastructure, Surveillance Bridge allows for increased maximum recording and archive retention limits and further ensures your VMS against data loss.

How It Works

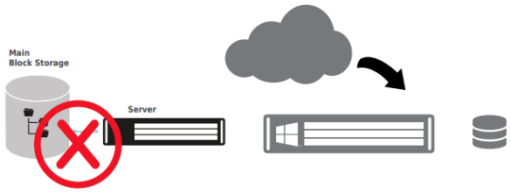
As soon as you install Surveillance Bridge on the recording server(s), you are ready to enable a cloud target, network share or another local volume as an extension and/or disaster recovery storage of a selected recording storage/archive. For the purpose, you should simply provide the credentials for access to the selected extension/disaster recovery storage. As long as Surveillance Bridge is not paused it immediately begins processing data.

You can enable just extension, just disaster recovery or both on a recording storage/archive. When both are enabled for one and the same recording storage/archive, the same cloud storage provider, network share or local volume is used. You can enable immediate tier extension/disaster recovery on a cloud target for a given recording storage and immediate tier extension/disaster recovery on a network share for the same recording server's archive storage, for example. The two mechanisms are not interchangeable - enabling disaster recovery does not free space on your recording storage/archive and data moved to the extension cannot be used for disaster recovery as it does not include system information about your recording storage/archive or recording server.

Note: Although it is technically possible from Surveillance Bridge configuration perspective, it is not advisable to enable extension on both recording storage and archive. Normally it would be one or the other. This is due to the bigger volume of traffic getting generated.

Disaster Recovery

When you enable disaster recovery, Surveillance Bridge copies all data and metadata from the recording storage/archive to the specified cloud, network share or local volume, starting with the newest files. The time for complete backup depends on the network characteristics and the connection speed to the disaster recovery storage target. You can keep track of the data backup progress in the Surveillance Bridge interface.



Surveillance Bridge disaster recovery is meant to provide a safety net in case of an unforeseen failure of a recording storage/archive or the recording server itself. Thus, it keeps backed up data on the disaster recovery storage for as long as you have specified in the configuration. When a recording storage/archive reaches its retention limit, the VMS starts deleting data and Surveillance Bridge then automatically deletes the counterpart from the disaster recovery storage, freeing space for new data.

In case of a failure of a recording server or its recording storage/archive, you can immediately begin recovering all backed up data and make it usable through the VMS again.

Extension

When you extend a recording storage/archive, you simply increase its capacity with the free space on the cloud target, network share, or local volume you have added as an extension.

You can expand the capacity of a recording server's storage with an immediate tier extension, from which data is retrieved as soon as the connection speed allows, or an archive tier extension, from which data is not retrieved immediately, but must first be rehydrated to an intermediate tier. Surveillance Bridge supports many cloud providers and tiers, updated list can be found on the website or per request.

Space on the recording storage/archive is freed by moving recordings to the enabled extension. To determine when to move recordings from the recording storage/archive to the immediate tier extension, Surveillance Bridge utilizes either the "By size" or the "By age" criteria you configure. With the "By age" method, data is moved to the immediate tier extension when it has not been accessed for a specified time interval. With the "By size" criteria, Surveillance Bridge begins moving data when the used space on the recording storage/archive reaches a specified threshold, starting with the least recently accessed files. To determine when a recording should be moved from the immediate tier extension to the archive tier extension, if enabled, Surveillance Bridge utilizes the "By age" criteria i.e. moves files, which have not been accessed for a specified time period.

Once a file is moved to the immediate tier extension, Surveillance Bridge replaces it with a stub file. Stub files look and act exactly like the actual files they replace, but have almost no size and consume almost no capacity on your local storage/archive. Stub files pointing to actual files on the immediate tier extension allow immediate and seamless retrieval when playing back and reviewing timeline video. Surveillance Bridge also allows you to manually move data between the local recording storage/archive and the standard and archive tier extensions.

As with disaster recovery, recordings are kept on the immediate/archive tier extension for as long as the retention limit of the extended recording storage/archive requires. Once the retention limit for a specific recording is reached, both the stub file and its counterpart on the extension are automatically deleted.

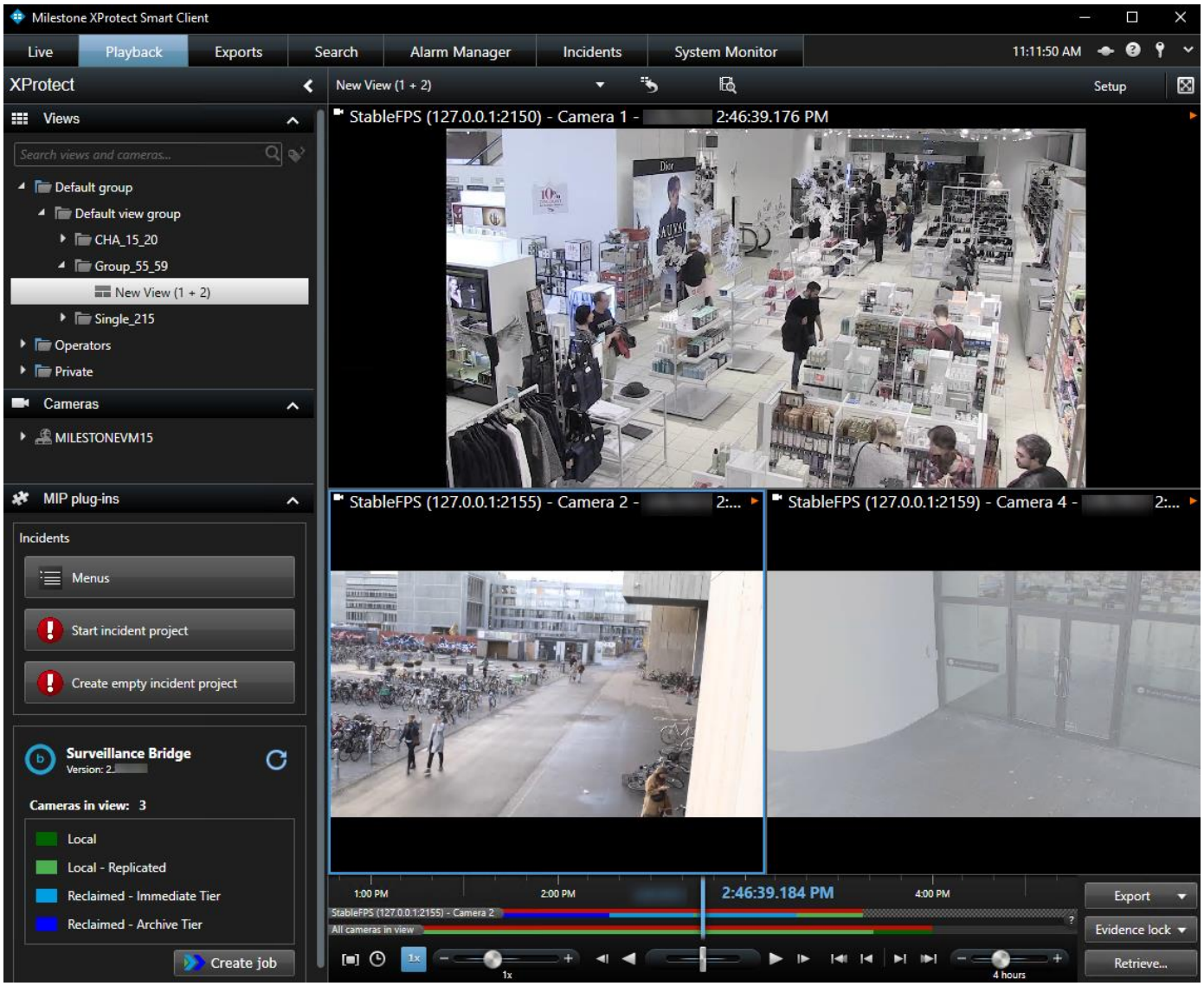
Standard Surveillance Bridge

Surveillance Bridge works with a big list of Video Management Systems. Complete list can be found on the webpage or received upon request as the list keeps growing.

Surveillance Bridge Plug-in

For a few specific video management systems, we have a further integration of Surveillance Bridge into their VMSes in the form of a plug-in. For this current release of Surveillance Bridge, the four systems we have a tight integration with are: XProtect by Milestone, MOBOTIX HUB by Mobotix, Siveillance by Siemens and Velocity Vision by Identiv. We will show some screenshots from our Milestone XProtect integration but we have something very similar with the other three VMSes.

To facilitate the work of Smart/Video Client users, the administrator of your surveillance system can enable or disable the integration of Surveillance Bridge. When enabled, each Smart/Video Client computer running the Surveillance Bridge plug-in sees an additional timeline visually displaying the original recording storage/archive, the immediate tier extension, or the archive tier extension as enabled by Surveillance Bridge.



Additionally, when the VMS Client integration is enabled, users can restore recordings from the immediate or archive tier extension to the recording storage/archive automatically (when reviewing the recording, for example) or manually, for a selected timeframe.

Surveillance Bridge Licensing

In order to benefit from Surveillance Bridge, you need to activate it on each recording server. For activation Surveillance Bridge makes use of a software as a service (SaaS). For more information, refer to “Activate Surveillance Bridge”.

The license holds information about its type, expiration date and time, serial key, supported features, etc. When provided for evaluation purposes, a license may be valid only for a specific amount of time.

You can keep track of the activation status of a recording server, following these steps.

System Requirements

General Requirements

To install Surveillance Bridge on a recording server, it must meet the following minimum requirements:

- PC with 64-bit (x64) processor.

Note: Surveillance 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. As a rule of thumb, Surveillance Bridge will consume approximately 10% of the system resources.

- 64-bit Microsoft Windows® 7/Server 2008 R2/Windows® 8/Server 2012/Server 2012 R2/Windows® 10/Server 2016/Server 2019.

Note: Surveillance Bridge requires the presence of the .Net 4.8 software and will install it if needed as part of its installation. That would require server reboot.

- 4 GB of physical RAM at least.

- 30 MB of available hard-disk space for Surveillance Bridge installation.

Note: Surveillance 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 Surveillance Bridge manages 1 000 000 files, the size of the database is approximately 100MB. Unless there's enough free space for the database, Surveillance Bridge is unable to operate.

- The following TCP ports must not be blocked by the firewall on the recording server or the computer managing the inbound and outbound traffic on your network:
  - ✓ **80** – outbound rule only (for communication with object storage target over http connection)
  - ✓ **443** – outbound rule only (for SaaS activation and/or communication with object storage target over https)
  - ✓ **445** – outbound rule only (for communication with SMB network share target)
  - ✓ **8536** – inbound rule only (for Bridge RPC communication)
  - ✓ **8537** – inbound rule only (for the Bridge REST Service)

To benefit from the Surveillance Bridge Plug-in to your VMS, you must install it on the Management Client and install the Standard Surveillance Bridge on each recording server whose storage you want to extend or back up.

Additionally, to allow the VMS Smart/Video Client integration, you need to install the Smart/Video Client module of Surveillance Bridge on each computer you want to integrate.

Digital Certificate Requirements

Surveillance Bridge uses a digital certificate issued by GlobalSign certification authority. For the digital certificate to be verified upon installing the respective component, GlobalSign's currently used root certificate must be installed in the Trusted Root Certification Authorities of the Certificate Manager on the computer. Additionally, the root certificate's "Code Signing" purpose must not be disabled.

On computers operating in less restrictive environments, this is done automatically during installation of Surveillance Bridge and/or its plug-ins. If the computer, on which you want to install Surveillance Bridge or any of its plug-ins, operates in a more restrictive domain environment, you must manually download the currently used root certificate from GlobalSign and install it yourself, before installing the respective component. In addition, you must ensure that the "Code Signing" purpose of the root certificate is enabled.

Storage Requirements

Recording Storage/Archive Requirements

Currently, Surveillance Bridge supports only recording storage/archive, which is mounted on the recording server as a local NTFS volume with Read & Write permissions and on which the System account is granted Full Control.

Extension/Disaster Recovery Storage Requirements

Currently, Surveillance Bridge supports the following storage types for extension and/or disaster recovery:

- Public cloud storage:
  - Amazon S3 object
  - Microsoft Azure blob
  - Google Cloud
  - IBM Cloud object
  - Huawei Cloud
  - Backblaze B2 cloud
  - Hitachi Content Platform (HCP)
  - LYVE Cloud
  - ORockCloud
  - RSTOR Space cloud
  - S3-compatible object storage
  - Wasabi Hot Cloud
- On-premises storage:
  - Hitachi HCP
  - IBM COS
  - OpenStack Swift
  - Seagate CORTX
  - S3-compatible object storage (using protocol signature version 2)
  - another volume, mounted on the recording server as a local volume with Read & Write permissions
  - SMB/CIFS network share

Extension/Disaster Recovery Storage Prerequisites

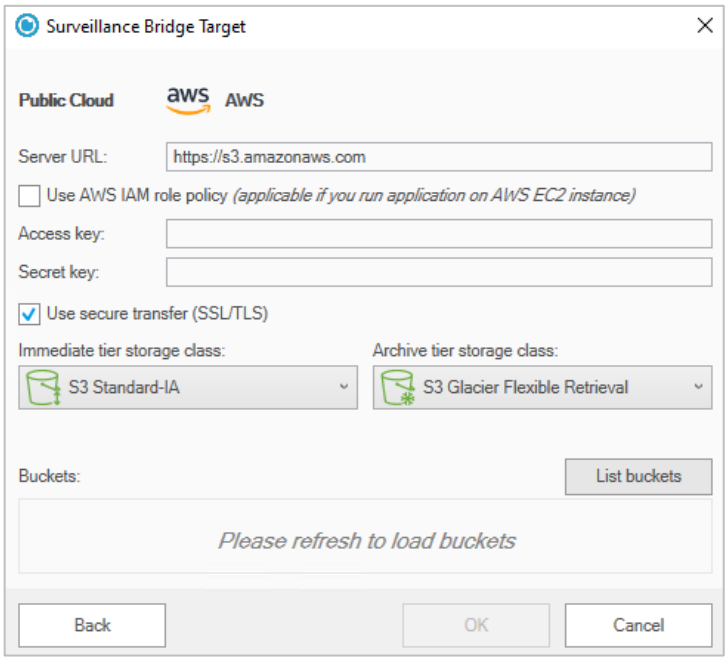
When setting up a cloud target, you have both public cloud and on-premises storage options detailed below.

Amazon S3 Object Storage

When adding Amazon S3 object immediate tier extension/disaster recovery storage, you will be requested to provide the following details:

- the URL of the public Amazon S3 storage server
- the access key and secret key of an IAM user, which to be used by Surveillance Bridge for access to the respective bucket
- a separate empty bucket for each recording storage/archive you want to extend and/or back up on Amazon S3 object storage
- your selection for immediate and archive tier storage classes

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.



Tip: Surveillance 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 recording storage/archive. You can ensure that Surveillance 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”:

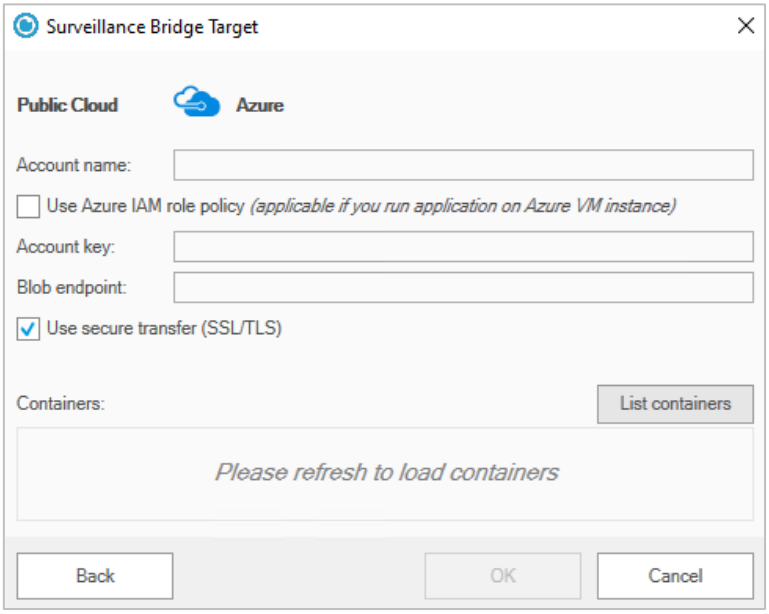
```
{
"Version": "2012-10-17",
"Id": "S3AllActionsOnTigerBucket",
"Statement": [
{
"Sid": "AllowAllActionOnS3ToTigerUsers",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::your_aws_subscription:user/bridge_user"
},
"Action": [
"s3:GetAccelerateConfiguration",
"s3:GetBucketLocation",
"s3:GetBucketVersioning",
"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

Microsoft Azure Blob Storage

When adding Microsoft Azure blob as an extension/disaster recovery storage, you will be requested to provide the following details:

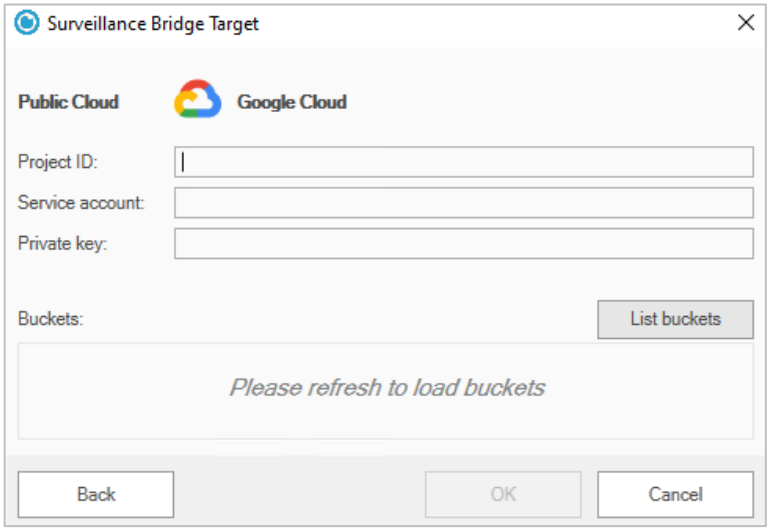
- the Azure Blob endpoint
- account name and key with at least write access to the respective container on the Azure Blob storage
- a separate empty container for each recording storage/archive you want to extend and/or back up on Microsoft Azure blob storage



Google Cloud Storage

When adding Google Cloud storage as an extension/disaster recovery storage, you will be requested to provide the following details:

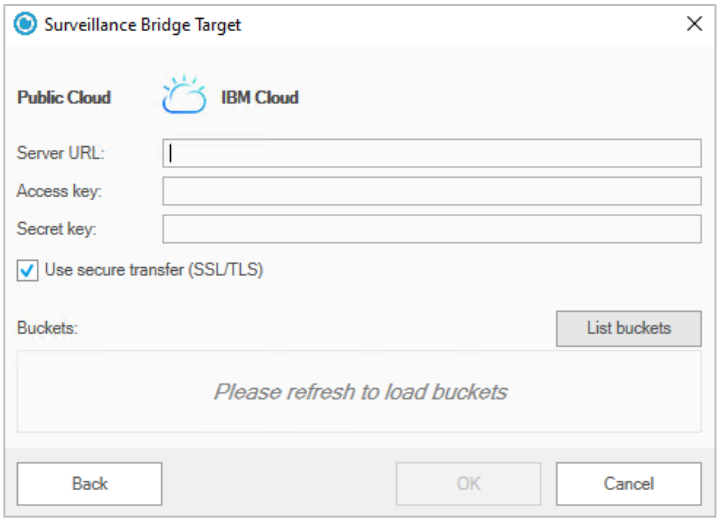
- the project ID,
- the service account email and private JSON key of a service account user, which is owner of the respective bucket
- a separate empty bucket for each recording storage/archive you want to extend and/or back up on the Google Cloud storage



IBM Cloud Storage

When adding IBM Cloud object storage as an extension/disaster recovery storage, you will be requested to provide the following details:

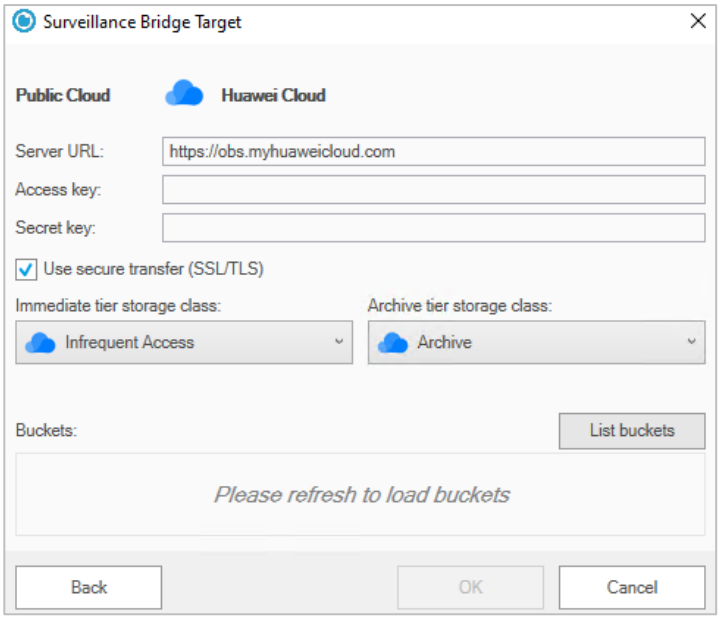
- the URL of the public IBM Cloud object storage server
- the access key ID and secret access key with at least write access to the respective bucket
- a separate empty bucket for each recording storage/archive you want to extend and/or back up on the IBM cloud object storage



Huawei Cloud Storage

When adding Huawei Cloud object storage as an extension/disaster recovery storage, you will be requested to provide the following details:

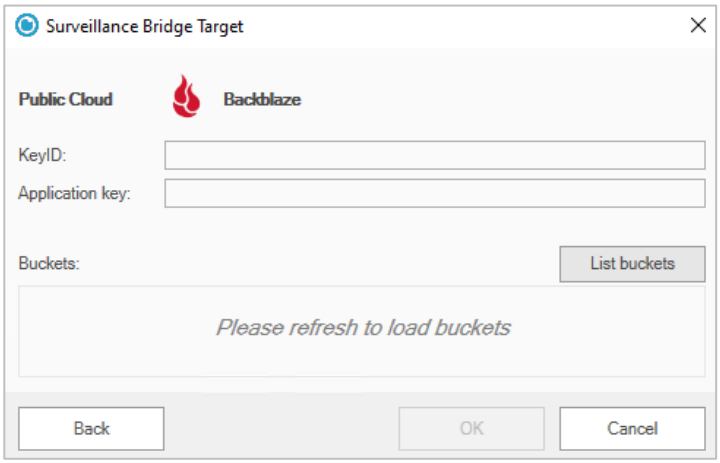
- the URL of the public Huawei Cloud object storage server
- the access key ID and secret access key with at least write access to the respective bucket
- a separate empty bucket for each recording storage/archive you want to extend and/or back up on the Huawei cloud object storage
- your selection for immediate and archive tier storage classes



Backblaze B2 Cloud Storage

When adding Backblaze B2 cloud storage as an extension/disaster recovery storage, you will be requested to provide the following details:

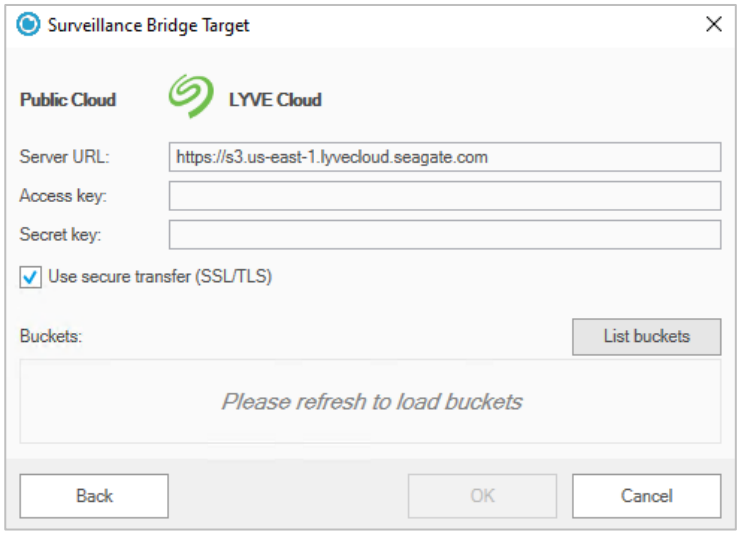
- the application key and keyID, which has at least write access to each respective bucket
- a separate empty bucket for each recording storage/archive you want to extend or back up on the Backblaze B2 cloud storage



LYVE Cloud

When adding LYVE Cloud object storage as an extension/disaster recovery storage, you will be requested to provide the following details:

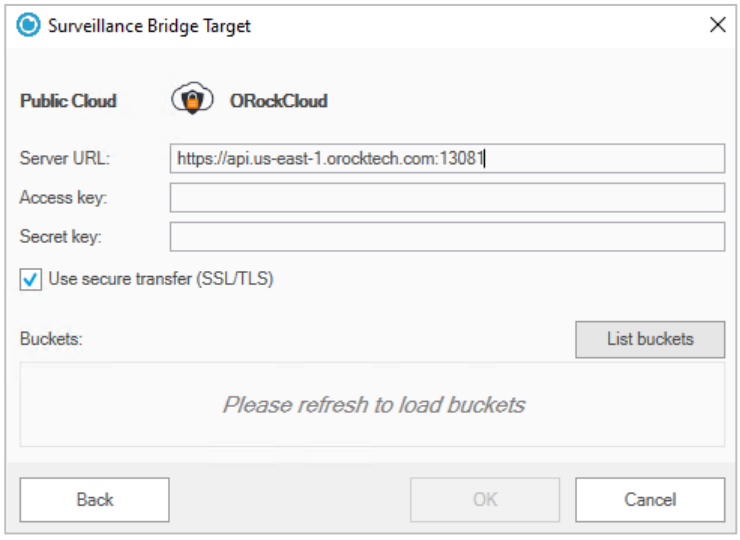
- the URL of the LYVE Cloud server
- the access key ID and secret access key, which provide at least write access to the respective bucket
- a separate empty bucket for each recording storage/archive you want to extend and/or back up on the LYVE Cloud storage



ORockCloud

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

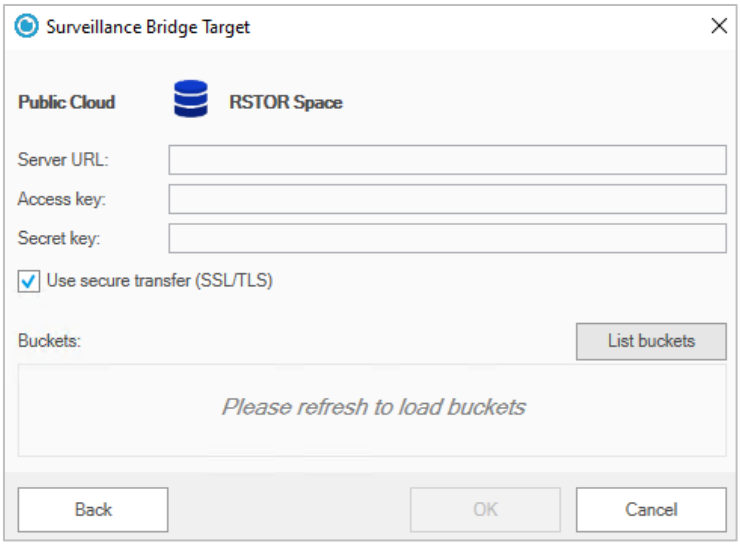
- the URL of the ORock Cloud server
- the access key ID and secret access key of the account, which will be used by Tiger Bridge for access to the ORock Cloud storage
- a separate empty bucket for each recording storage/archive you want to extend and/or back up on the ORock Cloud storage



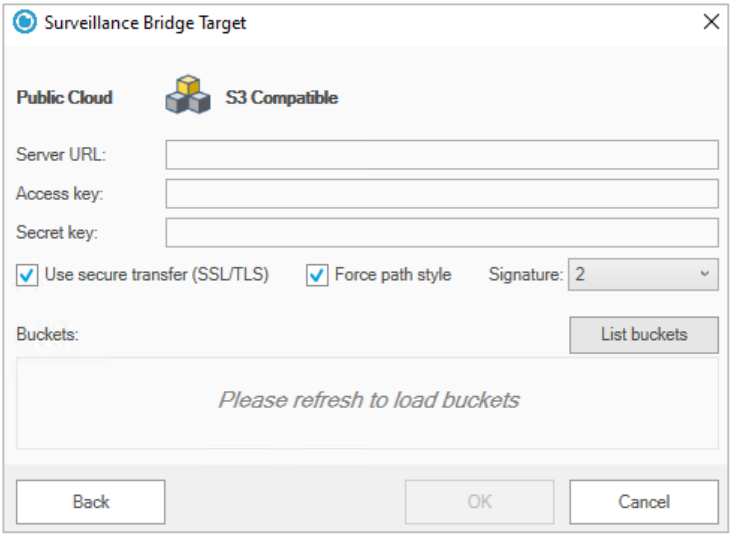
RSTOR Space

To use Tiger Bridge with RSTOR Space storage, you must provide the following information:

- 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.
- a separate empty bucket for each recording storage/archive you want to extend and/or back up on the ORock Cloud storage



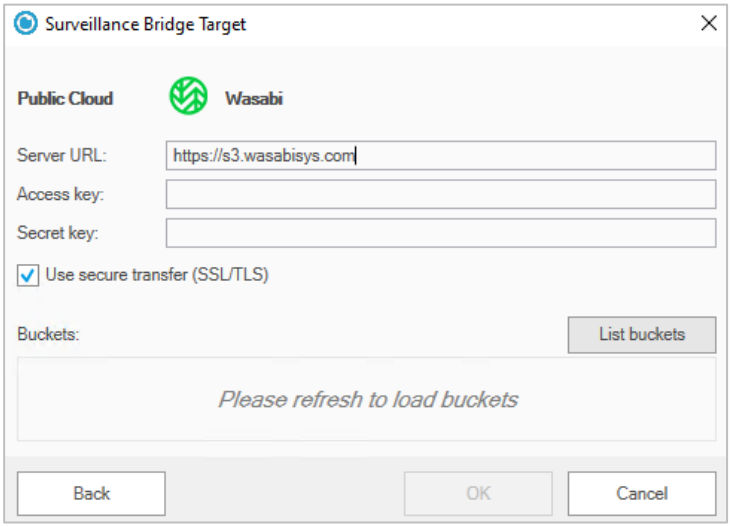
S3-compatible Object Storage



When adding public cloud S3-compatible object storage as an extension/disaster recovery storage, you will be requested to provide the following details:

- the URL or IP address of the S3-compatible object storage server
- the access key ID and secret access key, which provide at least write access to the respective bucket on S3-compatible object storage
- a separate empty bucket for each recording /archive storage you want to extend and/or back up on the S3-compatible object storage

Wasabi Cloud Object Storage



When adding Wasabi cloud object storage as an extension/disaster recovery storage, you will be requested to provide the following details:

- URL of the Wasabi cloud object storage
- a separate empty bucket for each recording storage/archive you want to extend and/or back up on the Wasabi cloud storage

  Important: Region specific target URL may be required.

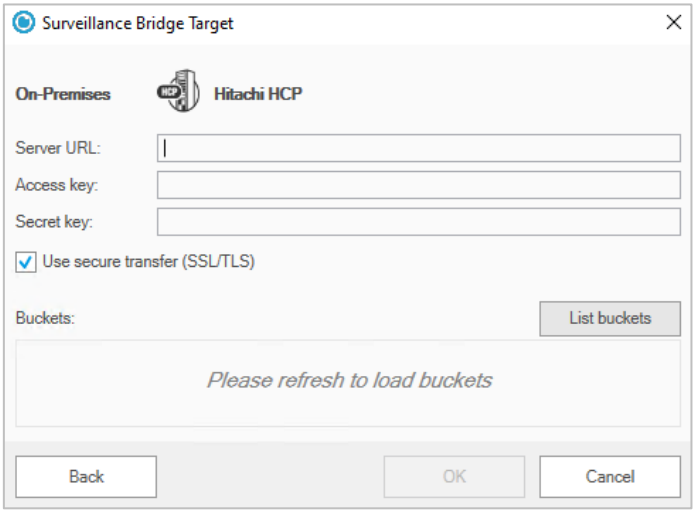
- the access and secret keys, which provide at least write access to the respective bucket

The specific access and secret keys for the different cloud providers can be found on the respective cloud portal when logged in with administrative privileges.

Hitachi Content Platform (HCP)

When adding Hitachi HCP as an extension/disaster recovery storage, you will be requested to provide the following details:

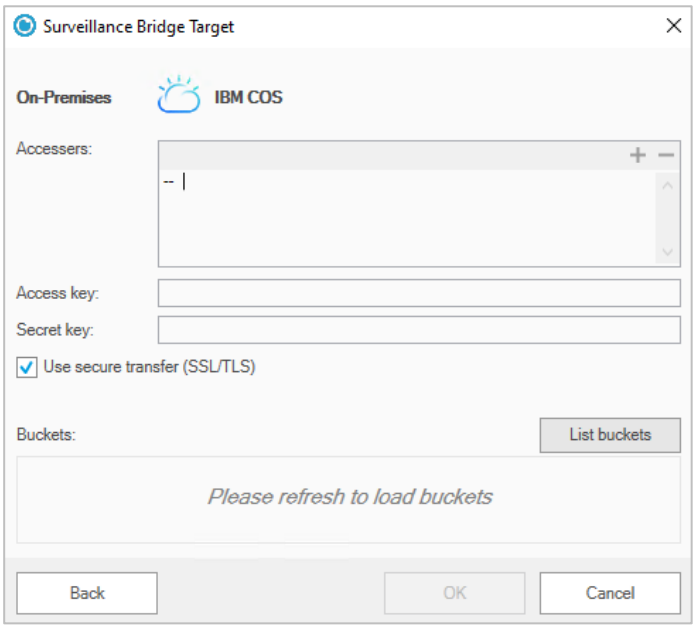
- the URL of the Hitachi HCP server
- the access key ID and secret access key, which provide at least write access to the respective bucket
- a separate empty bucket for each recording storage/archive you want to extend and/or back up on the Hitachi HCP storage



IBM COS

When adding IBM COS on-premises storage as an extension/disaster recovery storage, you will be requested to provide the following details:

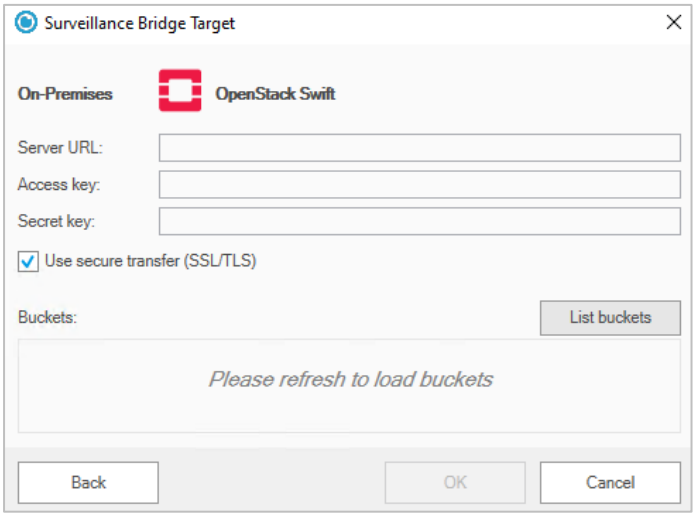
- the IP address of the IBM COS server on your network as well as any other alternative IP addresses through which it can be accessed
- the access key ID and secret access key, which provide at least write access to the respective bucket
- a separate empty bucket for each recording storage/archive you want to extend and/or back up on the IBM COS



OpenStack Swift

When adding OpenStack Swift storage as an extension/disaster recovery storage, you will be requested to provide the following details:

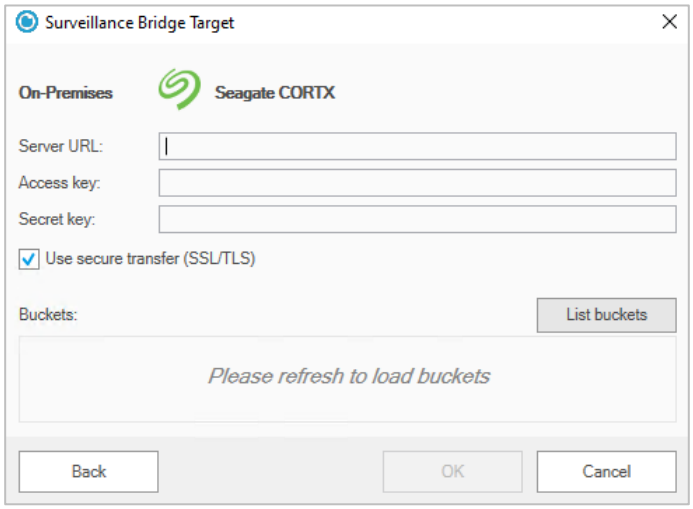
- the URL of the OpenStack Swift server
- the access key ID and secret access key, which provide at least write access to the respective bucket on OpenStack Swift storage
- a separate empty bucket for each recording /archive storage you want to extend and/or back up on the OpenStack Swift storage



Seagate CORTX

When adding Seagate CORTX on-premises object storage as an extension/disaster recovery storage, you will be requested to provide the following details:

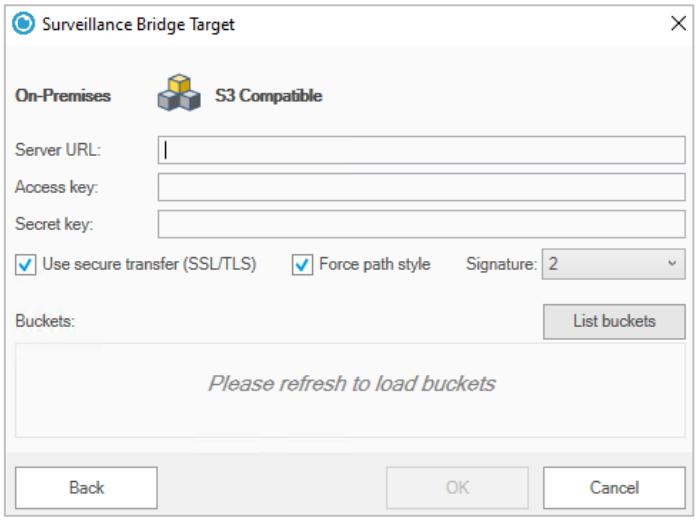
- the IP address of the Seagate CORTX server
- the access key ID and secret access key, which provide at least write access to the respective bucket
- a separate empty bucket for each recording storage/archive you want to extend and/or back up on the Seagate CORTX storage



S3-compatible Object Storage

When adding on-premises S3-compatible object storage as an extension/disaster recovery storage, you will be requested to provide the following details:

- the URL or IP address of the S3-compatible object storage server
- the access key ID and secret access key, which provide at least write access to the respective bucket on S3-compatible object storage
- a separate empty bucket for each recording /archive storage you want to extend and/or back up on the S3-compatible object storage

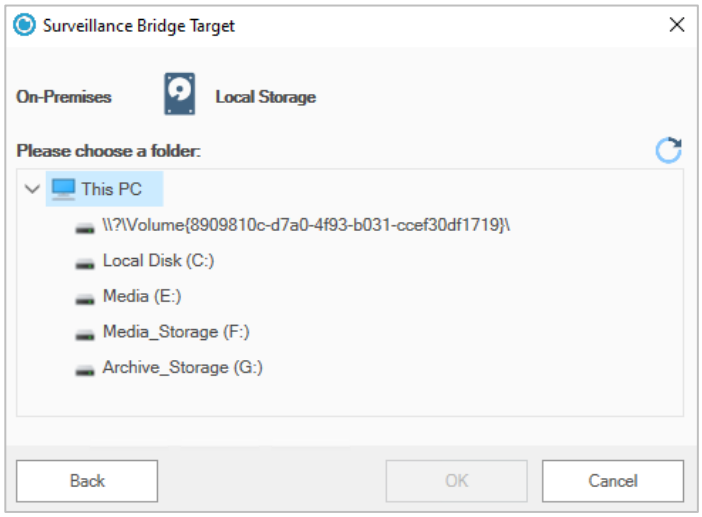


Local Storage

When adding a locally mounted NTFS volume as an extension/disaster recovery storage, you will have to:

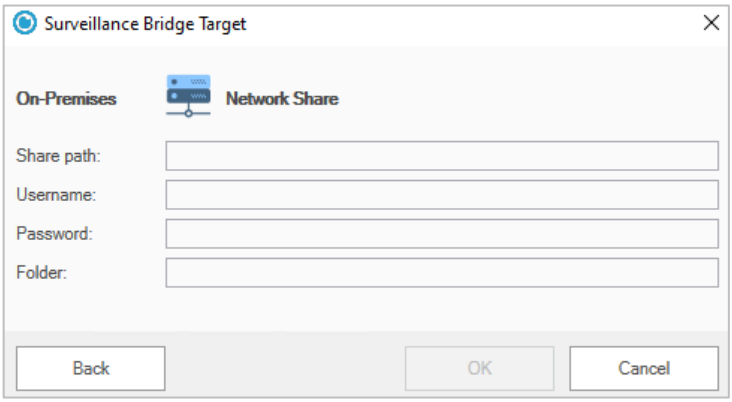
- make sure that the volume is mounted as a local volume with Read & Write permissions on the recording server
- create an empty folder on the volume for each recording /archive storage you want to extend and/or back up

Important: If you want to use the root of the volume as an extension/disaster recovery storage, it must not contain any other data.



Network Share

When adding a SMB/CIFS or NFS network share as an extension/disaster recovery storage, you will be requested to provide the following details:



- an already created empty folder on the network share for each recording /archive storage you want to extend and/or back up
- the full path to the network share
- 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.

Note: 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

---

- NFS share - each recording server whose data you intend to extend or back up must be allowed to access the NFS share and NFS locking must be disabled on it.
- provide the name of the empty folder on the share, designated for the respective recording storage or archive

---

Note: If you want to use the root of the network share as an extension/disaster recovery storage, 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 a 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.

II. Surveillance Bridge Installation and Activation

Install the Standard Surveillance Bridge

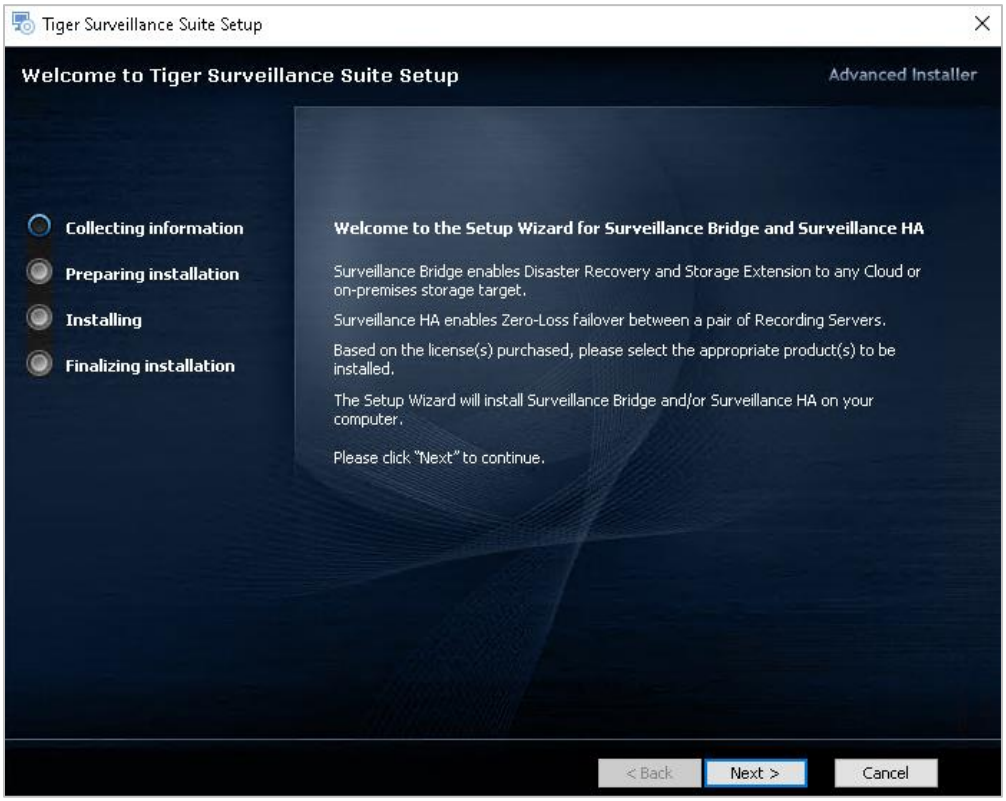
To install Surveillance Bridge on a recording server:

1. Double-click the Surveillance Bridge installation file.

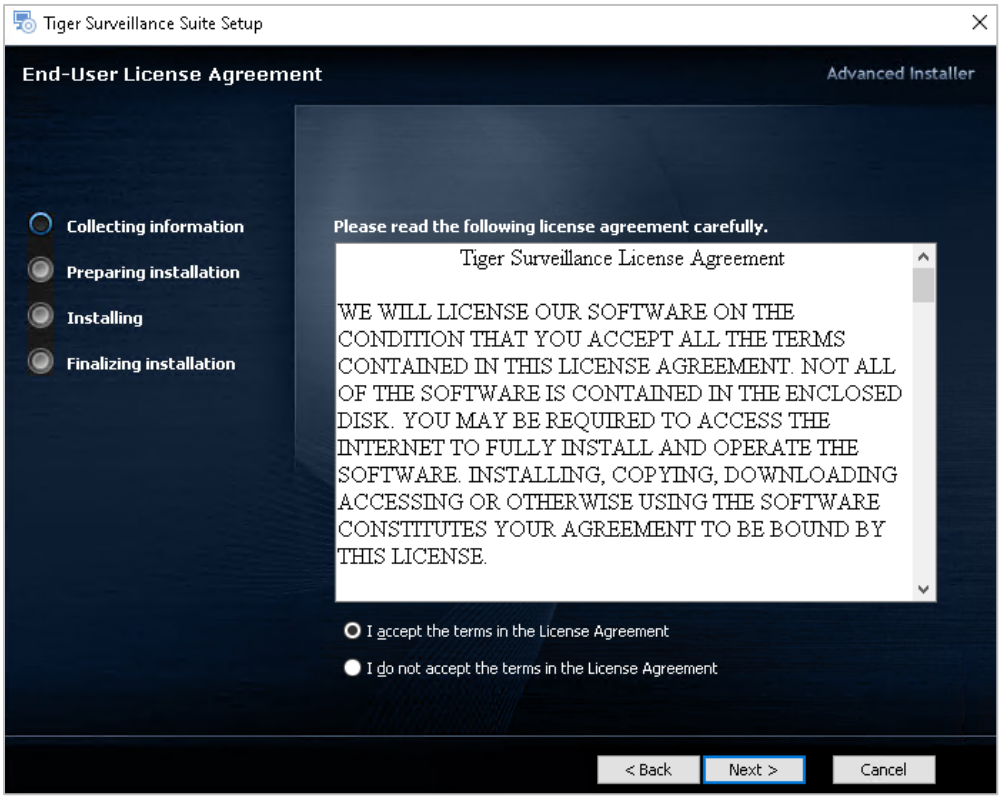
Note: If the setup wizard detects that prerequisites needed to run Surveillance Bridge are not installed on the computer, click next to install them.

---

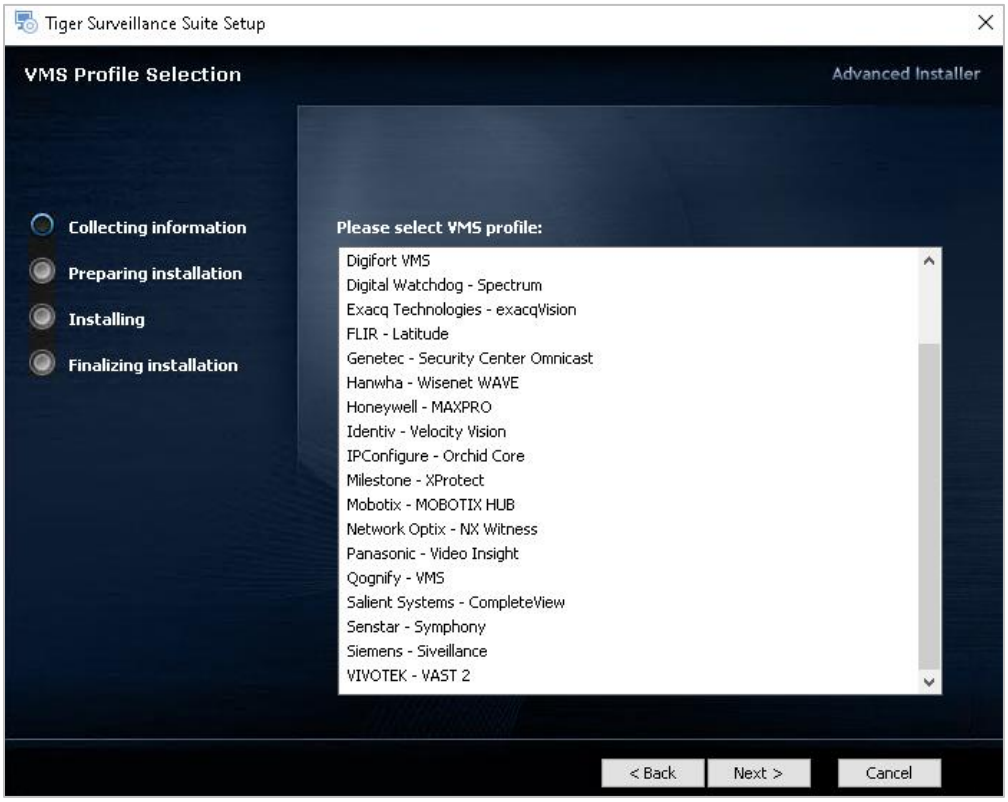
2. In the Surveillance Bridge installation wizard, click **Next**.



3. Accept the terms of the software license agreement and click **Next**. You will not be allowed to continue without accepting

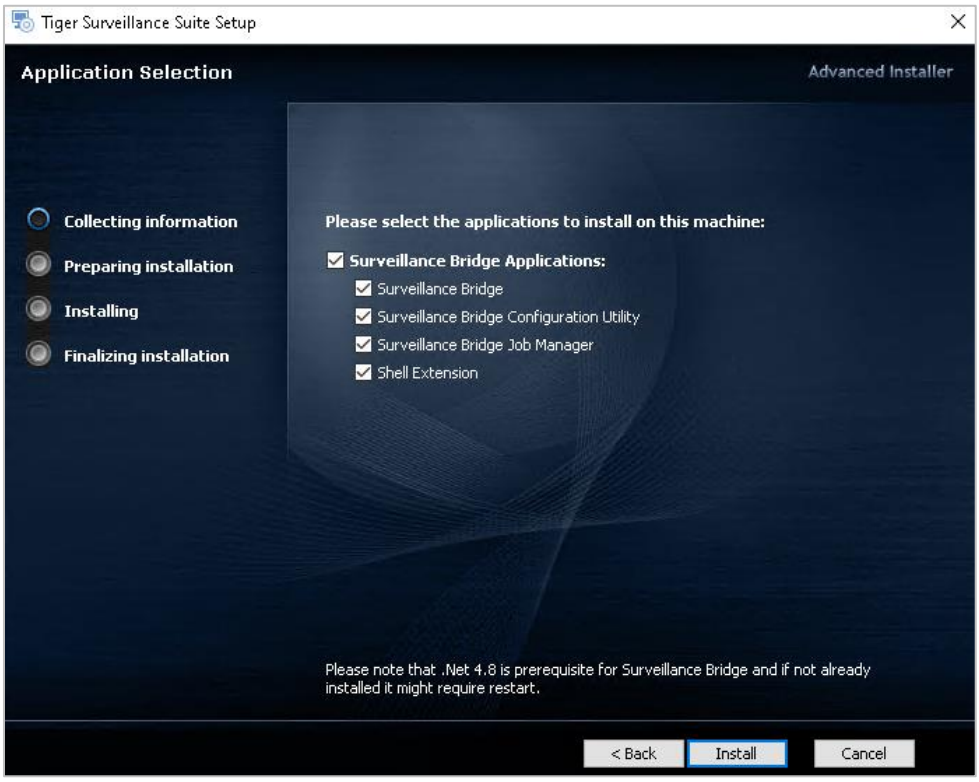


4. Select your VMS from the list.



5. Select the applications you would like to install and click the **Install** button. If unsure, leave all the options enabled.

    - **Surveillance Bridge** carries the main functionality of the product
    - **Surveillance Bridge Configuration Utility** allows you to fine tune your setup
    - **Surveillance Bridge Job Manager** has the job management features built in
    - **Shell Extension** allows you to perform manual data operations and collect statistics right in your Windows Explorer.



Note: This screen will be different for you if your VMS is XProtect by Milestone, MOBOTIX HUB by Mobotix, Siveillance by Siemens and Velocity Vision by Identiv. Check the next section for more details.

6. When the installation is complete, click **Finish**.

Install the Surveillance Bridge Plug-in

To fully benefit from Surveillance Bridge on your supported VMS, you can install the following components:

- Management Client module – is a plug-in which adds our Surveillance Bridge menu in the Management Client's graphical user interface. This module should only be installed on machines with the VMS' Management Client installed;
- Recording Server module – the Surveillance Bridge engine;

- Shell Extension – which allows for an integration with Windows Explorer and respectively manual Surveillance Bridge operations;
- Smart/Video Client module – our module which has to be installed on machines with the Smart/Video Client to enable the additional Surveillance Bridge features within the client. It is installed in disaster recovery or extension use cases. It is not needed for server cluster scenarios;
- Event Server module – just a service with no graphical user interface that sends Surveillance Bridge related information to the VMS' event server so that all events and alarms are in one place – the User-defined Events. There is a specific section in the Surveillance Bridge interface which allows for configuring which events should get logged. If this Event Server module is not installed, that section in the configuration will not be functional.

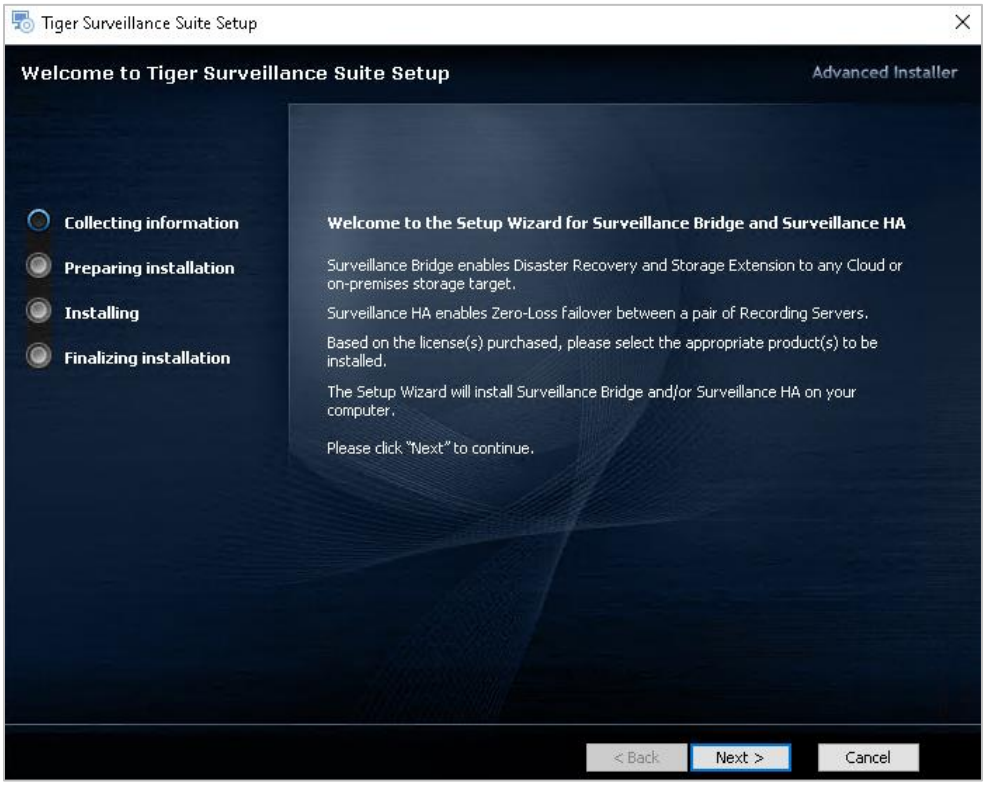
To install the Surveillance Bridge Plug-in on the VMS' Management Client or Smart/Video Client:

1. Double-click the Surveillance Bridge installation file.

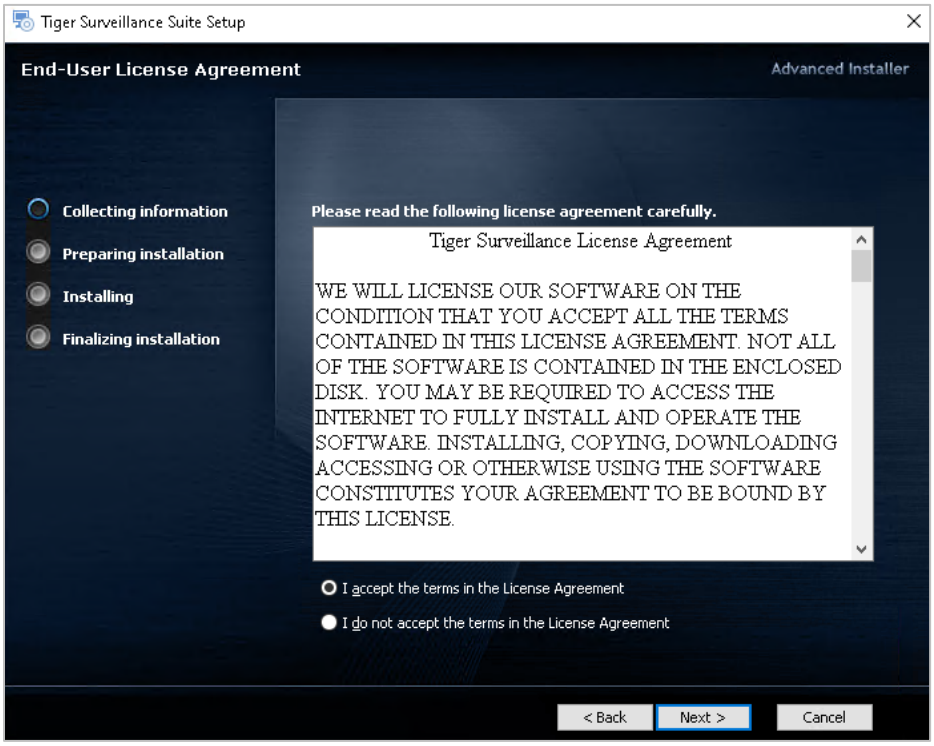
Note: If the setup wizard detects that prerequisites needed to run the Surveillance Bridge Plug-in for the Smart/Video Client are not installed on the computer, click next to install them.

---

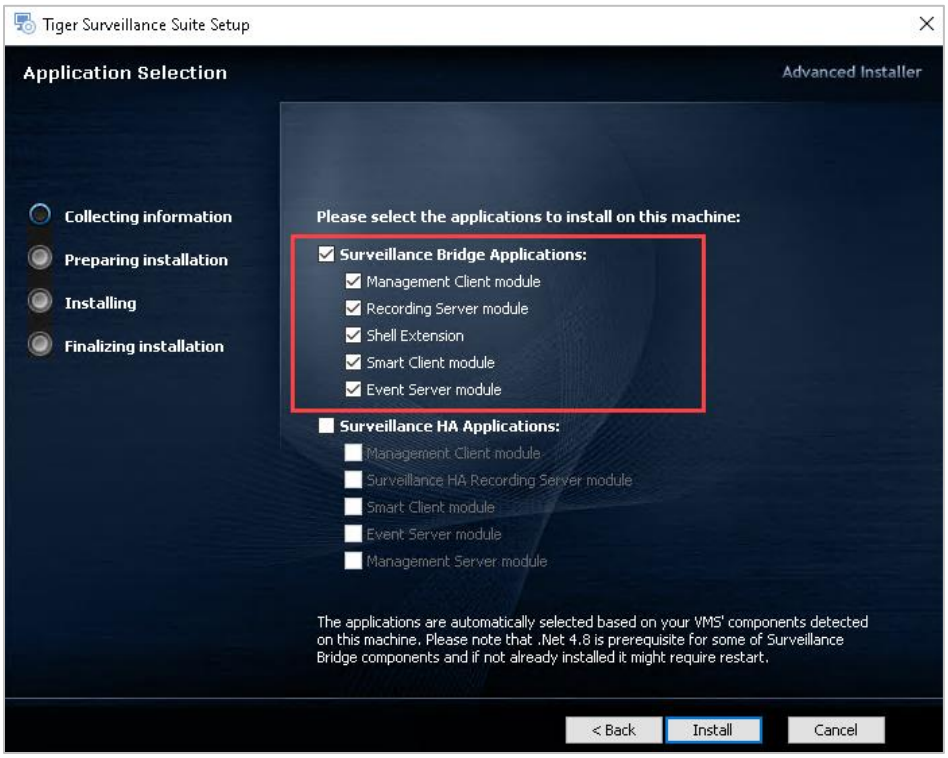
2. In the Surveillance Bridge installation wizard, click **Next**.



3. Accept the terms of the software license agreement and click **Next**. You will not be allowed to continue without accepting



4. Make sure the "**Management Client module**" or "**Smart/Video Client module**" check box (depending on the server you are running the setup on) and the check boxes of all other components that will be running on the same computer are selected in the Surveillance Bridge Applications section, then click **Install**.



Note: If the VMS' Management Client computer does not run Smart/Video Client and is not set up as a recording server, clear the check boxes of the corresponding components and install them separately.

Note: Surveillance HA is a separate product you may or may not want to setup. Its installation, setup and features are described in another document.

5. When the installation is complete, click **Finish**.

Uninstall Surveillance Bridge

You can uninstall Surveillance Bridge and any of its plug-ins at any time.

When you uninstall Surveillance Bridge from a recording server, even if the extension/disaster recovery is not disabled, no further data will be backed up/moved and you will not be able to access already moved data from the extension or recover data from the disaster recovery storage through your VMS.

On the other hand, if you configure extension/disaster recovery in the Management Client module and then uninstall it, Surveillance Bridge will continue to back up/move data from the recording storage/archive to its extension/disaster recovery storage, but you will not be able to change the configuration, to manually move or back up data and to recover data in case of a failure of the recording server or its storage, until you install the Management Client module again.

Uninstalling the Surveillance Bridge module from the Smart/Video Client will simply hide the additional timeline data displaying the exact location of recordings and users will not be able to retrieve data from the immediate/archive tier extension.

To uninstall Surveillance Bridge:

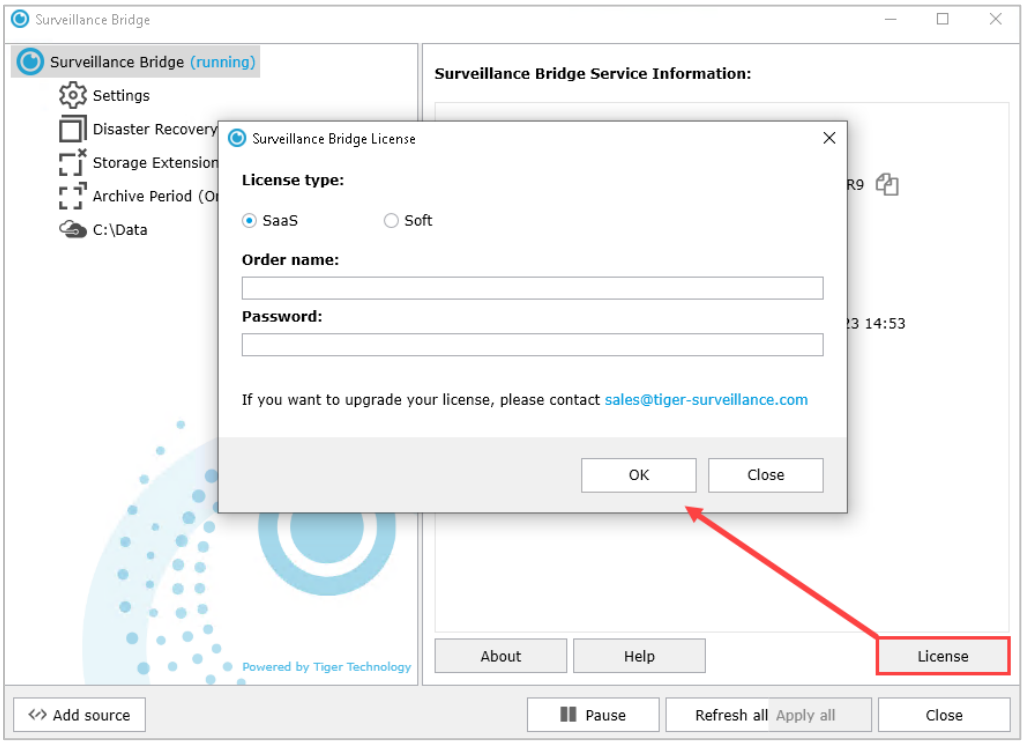
1. In Control Panel, go to Programs and Features / Apps and features depending on the operating system.
2. Click or right-click on the respective Surveillance Bridge component and select Uninstall.
3. When prompted to confirm that you want to remove Surveillance Bridge from the computer, click Yes.

Activate Surveillance Bridge

You can activate Surveillance Bridge using a software as a service (SaaS) license. You need to activate the product on each recording server, whose recording storage/archive you want to extend or back up, or which you want to add in a high-availability cluster. To enable more features once you have activated the product, simply repeat the activation procedure again.

To activate the Standard Surveillance Bridge:

1. Open the Surveillance Bridge tool and click the License button at the bottom right corner of the screen:



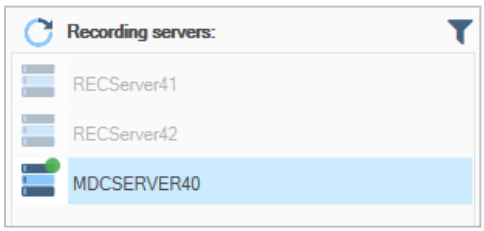
2. Enter your SaaS license. If you do not have your license handy or feel uncertain about the procedure, please reach out to us.

Note: If you are using Surveillance Bridge with XProtect by Milestone, MOBOTIX HUB by Mobotix, Siveillance by Siemens and Velocity Vision by Identiv, then you can license the product directly in your VMS interface – check the next instructions to understand how.

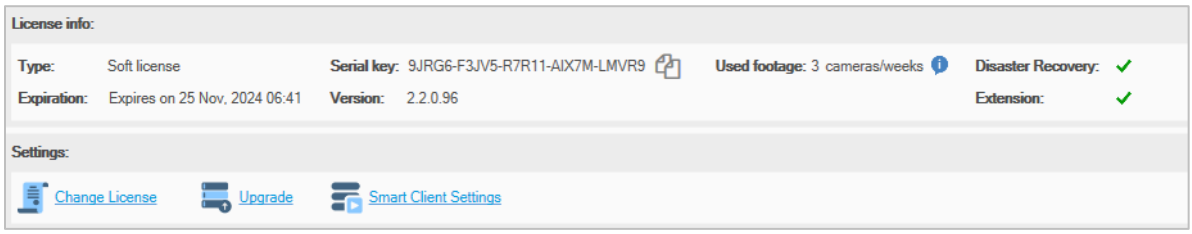
To view the activation status of the Surveillance Bridge Plug-in:

1. In the Navigation pane of the Management Client, click **Administration** under Surveillance Bridge.

2. In the right pane under Recording Servers, click the recording server, whose activation status you want to view.



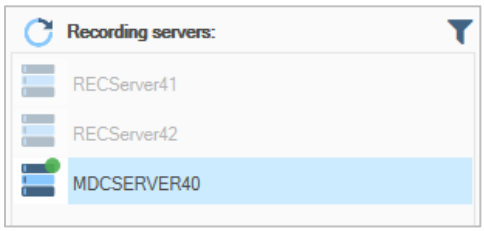
3. The License info pane displays the type of license, your serial key, the version of the product, the number of cameras per week and the activated features.



To activate the Surveillance Bridge Plug-in on a recording server:

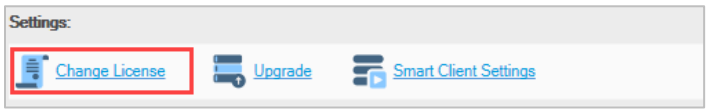
1. In the Navigation pane of the Management Client, click **Administration** under Surveillance Bridge.

2. In the right pane under Recording Servers, click the recording server, which you want to activate.

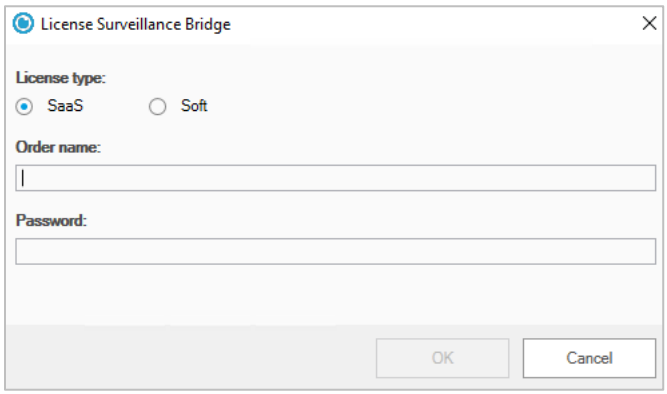


If a recording server is displayed in the list with a grayed-out icon, it is either offline or does not have Surveillance Bridge installed.

3. Click the **Change License** button in the middle of the screen.



4. Under Change license, enter the order name and password for your subscription and then click **OK**.



III. Manage Disaster Recovery

To ensure against data loss, you can configure Surveillance Bridge to automatically copy all data and metadata from a recording storage/archive to a disaster recovery target. For this purpose, you need to enable a cloud target, network share, or local volume as your disaster recovery storage, following the steps in Enable Disaster Recovery.

The time for full backup depends on the network characteristics and connection speed to the disaster recovery storage. You can keep track of the progress of data backup following the steps in **Error! Reference source not found.**.

Surveillance Bridge disaster recovery is meant to provide a safety net in case of an unforeseen failure of a recording server's recording storage/archive or the recording server itself. In case of a failure, you can immediately begin recovering all backed up data by following the steps in Recover Backed Up Data.

What you need to take into consideration when configuring disaster recovery, is the time for resolution in case of a disaster. Normally, you would like that to happen almost immediately, if possible.

If you are not using XProtect by Milestone, MOBOTIX HUB by Mobotix, Siveillance by Siemens and Velocity Vision by Identiv, you can take advantage of the Standard Surveillance Bridge Disaster Recovery functionality potentially by combining it with the high availability functionalities of the Surveillance HA product.

If you are using one of these systems, keep in mind that if you have set up VMS Failover, it protects your recording servers but does not protect the storage underneath.

In case of a storage failure, you will be able to collect and use new camera data from the failover recording server. However, this will not allow you to use the data that was residing on the lost storage. To overcome this problem, the disaster recovery functionality of Surveillance Bridge can very well be used together with the Milestone Failover to achieve protection on both recording server and data level.

In case of a disaster, the Milestone Failover allows you to continue capturing new data on another recording server almost immediately, and with the help of Surveillance Bridge you can also get your previous camera data back, if and when it is needed.

Disaster Recovery for the Standard Surveillance Bridge

With the help of the Surveillance Bridge Configuration Utility, you can prepare your recording servers for a disaster recovery situation.

Note: If you are working with XProtect by Milestone, MOBOTIX HUB by Mobotix, Siveillance by Siemens and Velocity Vision by Identiv, please move to the next section of this document, called The Surveillance Bridge Plug-in Disaster Recovery.

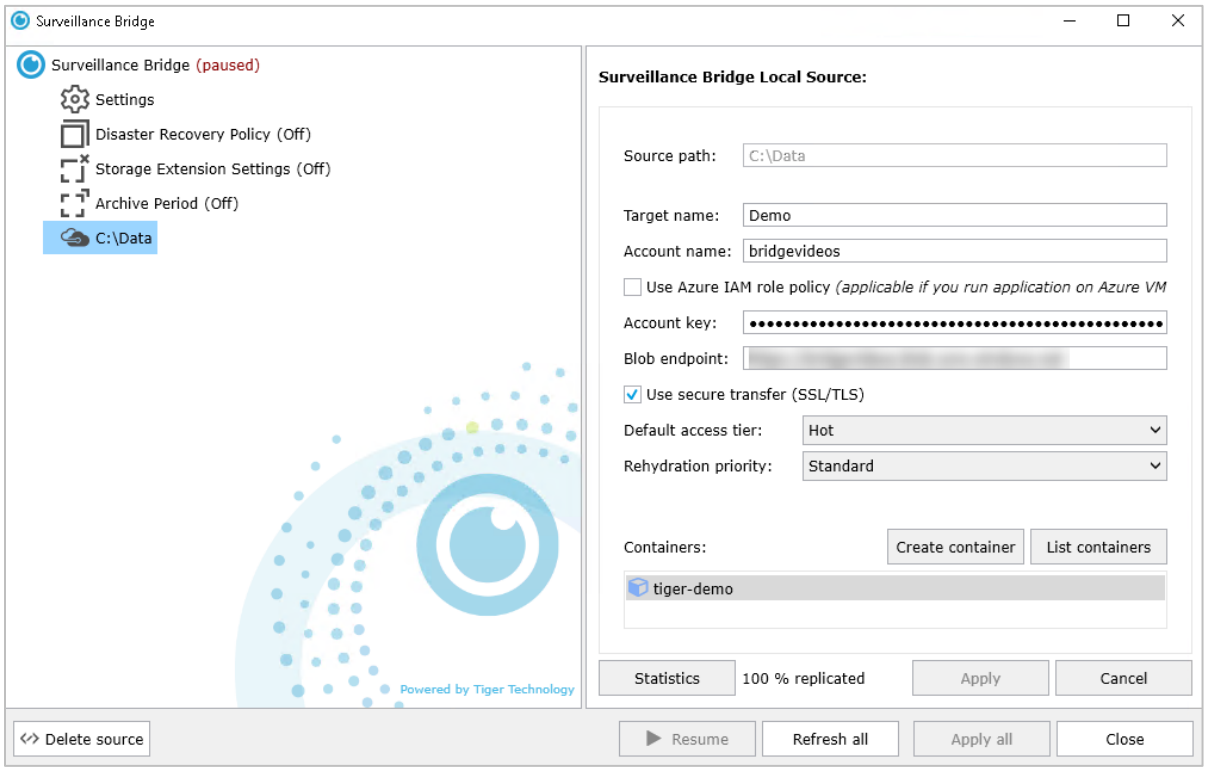
Enable Disaster Recovery

Before you can take advantage of the Disaster Recovery and Extension functionalities of the product, you need to configure your source folder and target cloud or on-premises storage.

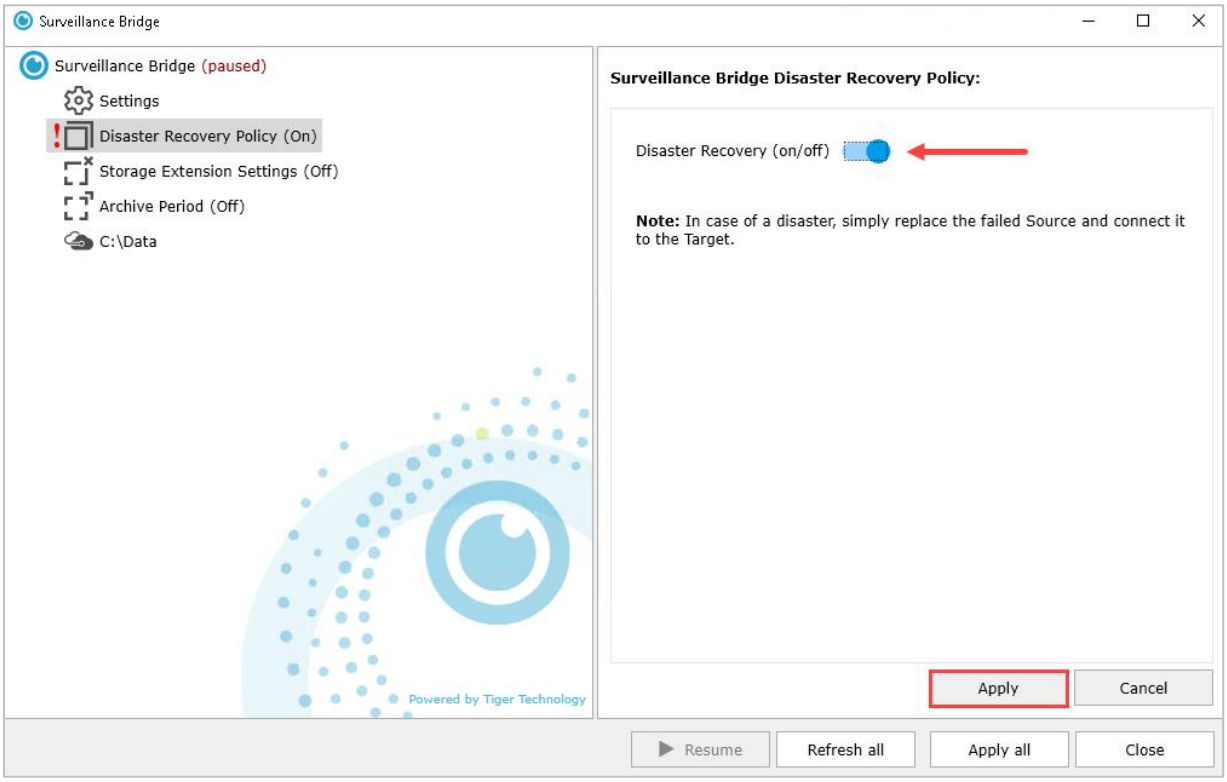
1. Start the Surveillance Bridge product by double-clicking its Desktop icon or finding it in the Start menu.
2. Click the **Add source** button at the bottom left corner of the window to start configuring your environment.

3. **Browse** to the desired folder. That would be the location of your VMS recording files.
4. Select the desired cloud or on-premises storage and click **OK**.
5. Set up the target with all its required details and click **Apply** to save your configuration.
6. You will be asked to choose an action to be performed on any existing data in the target and you can:
    - Take no action – nothing will be imported from the target
    - Disaster Recovery light – only metadata will be imported initially, the rest will only be downloaded on demand
    - Disaster Recovery full – both metadata and content will be restored

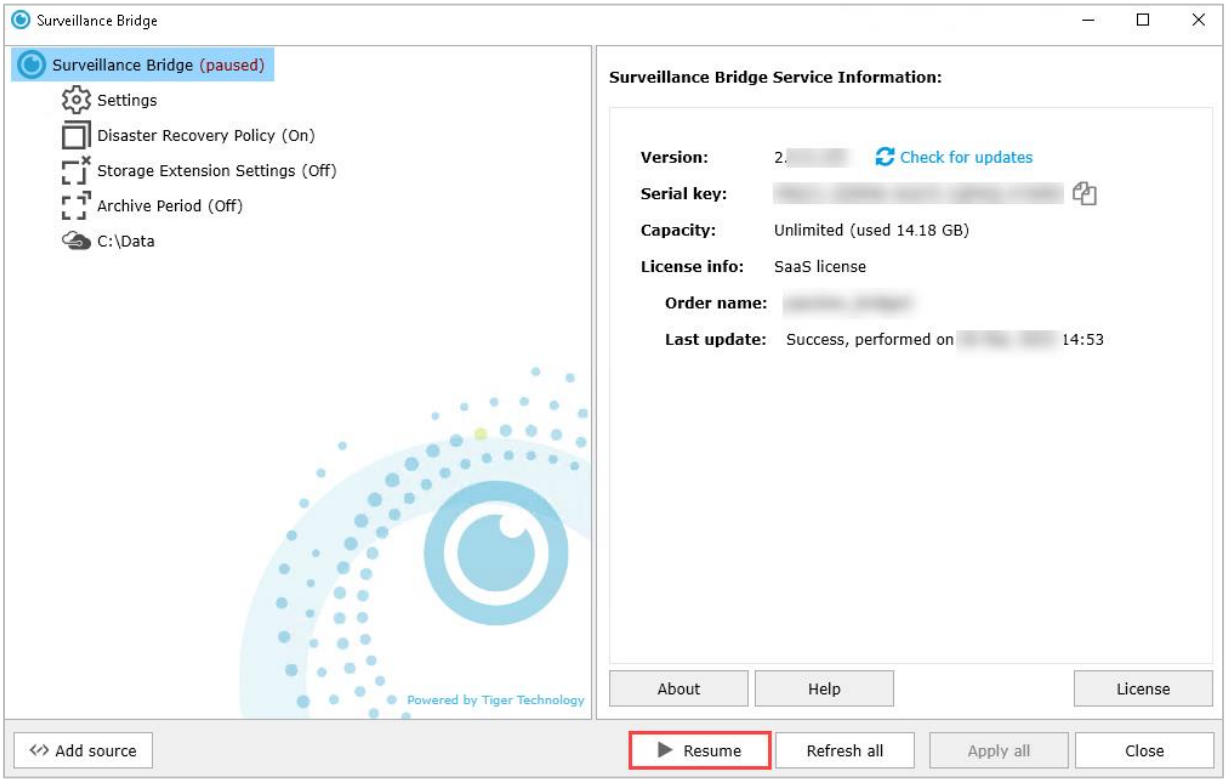
Your already set up target should look similar to this:



7. Go to the Disaster Recovery Policy section and toggle the on/off switch, then click **Apply**.

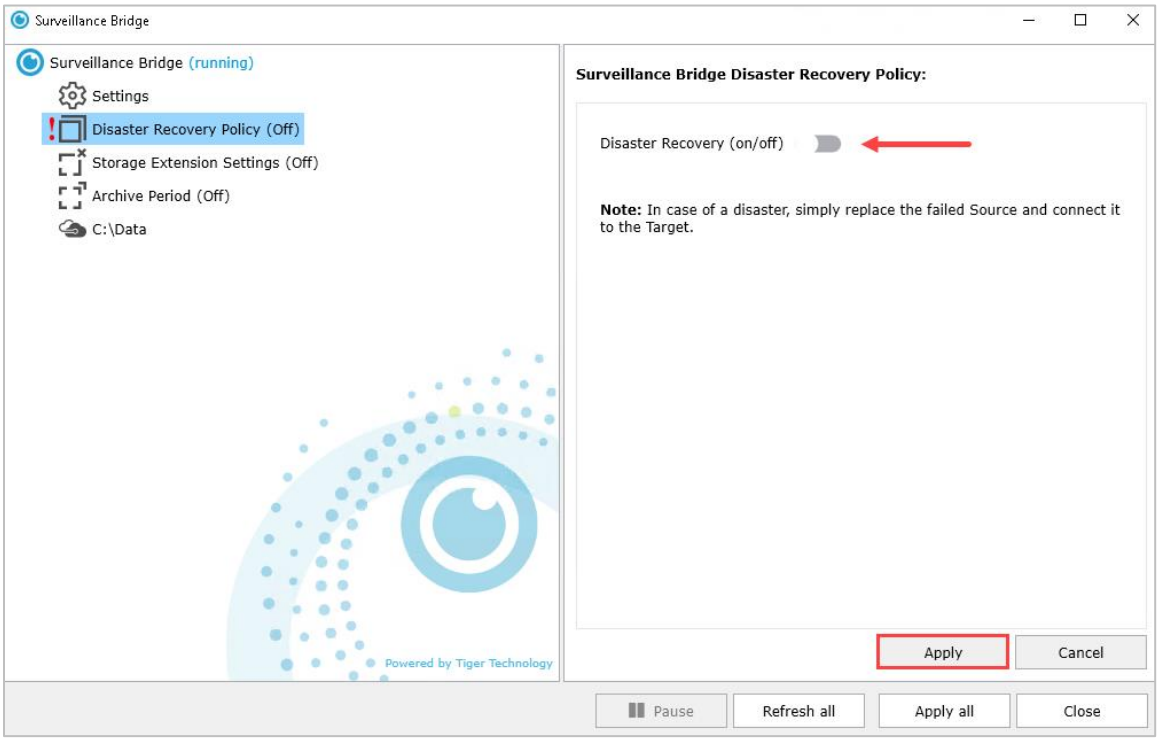


8. Up until that point Surveillance Bridge was in a paused state waiting for your configuration changes. You can now start its work by clicking the **Resume** button. You can further Pause and Resume the work of Surveillance Bridge as needed.



Disable Disaster Recovery

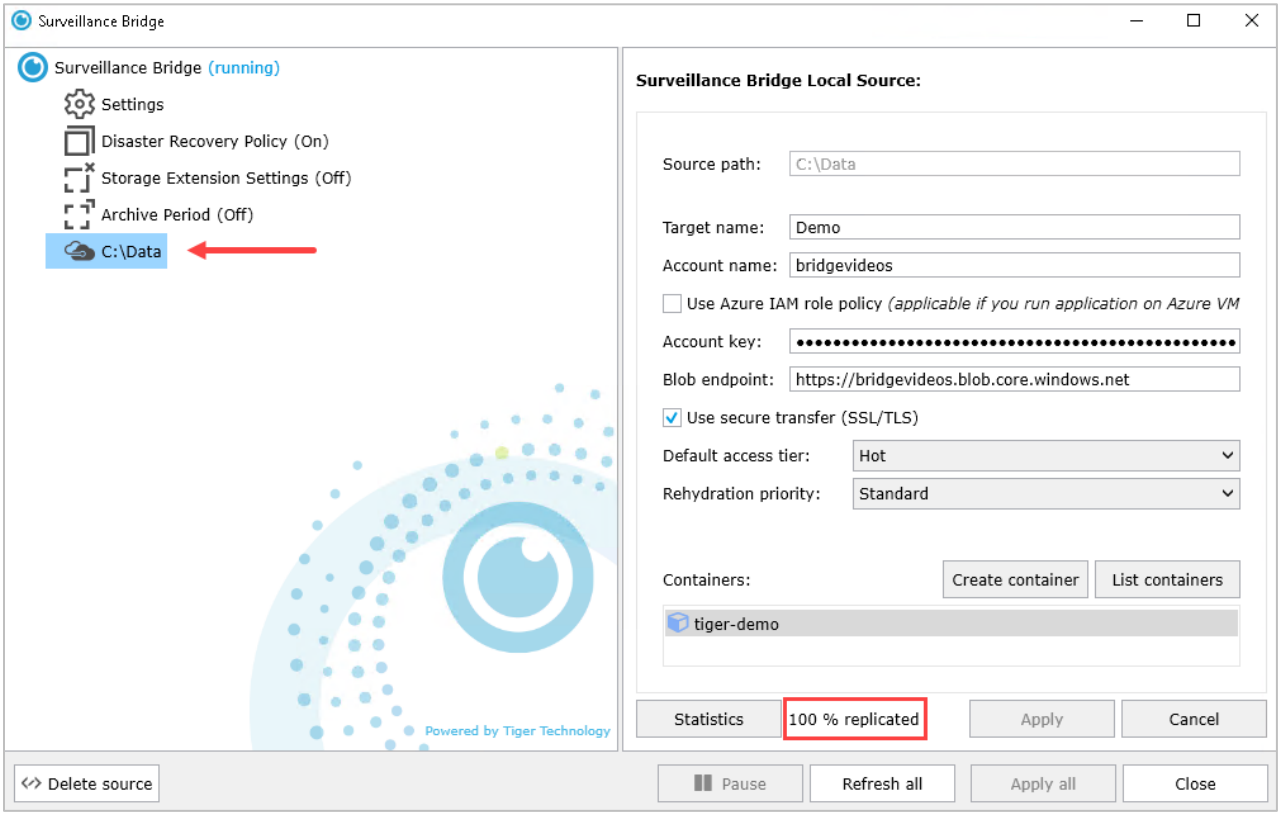
To disable the Disaster Recovery Policy, simply go back to the respective menu, toggle the on/off switch again and click the Apply button.



Monitor Data Backup Progress

To get information on how much of your data has already been replicated and is now protected by your target storage, click on your source and check the percentage in the bottom right corner of the window.

The percentage will initially be 0 and you can monitor its progress until it reaches 100.



For even more detailed information, you can use the Statistics button, which will show you data on how many files have been unprocessed for any reason, excluded, modified, pending, replicated or failed, together with information on how much space the files occupy on the local source.

Recovering Data

In an event of a failure, you would need to set up Surveillance Bridge on a new recording server or configure a new source drive/folder on the same server, then configure it exactly the same as you originally did (follow the steps in the Enable Disaster Recovery section), meaning you need to point it to the same target storage, just make sure to select Disaster Recovery light or Disaster Recovery full, when presented with that option.

This way, you will get back all the lost recordings data information from the cloud or on-premises copy location.

Your data is stored in non-proprietary form in any cloud or on-premises storage, which means that in the event of a failure, you can quickly access it even directly from that target storage until you get ready with your new Surveillance Bridge configuration.

Disaster Recovery for the Surveillance Bridge Plug-in

If you are working with XProtect by Milestone, MOBOTIX HUB by Mobotix, Siveillance by Siemens and Velocity Vision by Identiv, you do not need to use the Surveillance Bridge Configuration Utility. Everything can be configured much simpler in your VMS' graphical user interface directly and you get some additional benefits.

Enable Disaster Recovery

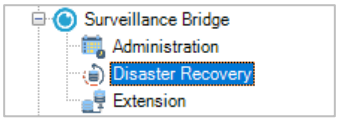
To enable disaster recovery, you should simply provide the credentials for access to the cloud storage, network share or local volume, which will be used for backing data up. If an immediate/archive tier extension is already enabled for the selected recording storage or archive, the same cloud storage, network share or local volume is also used for disaster recovery and there is no need to provide the credentials for access to the disaster recovery storage.

> **Note:** Surveillance Bridge does not allow you to use the same bucket/container (on cloud storage) or folder (on network share or local volume) as a disaster recovery location of more than one recording storage/archive.

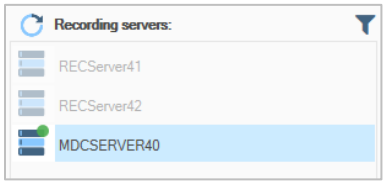
To change the type of disaster recovery storage or the credentials for access to it, you need to first disable disaster recovery, following the steps in Disable Disaster Recovery and then configure it again. Keep in mind that if you want to change the type of disaster recovery storage or the credentials for access to it, and an immediate/archive tier extension is also enabled, you must first disable the extension(s), following the steps in "Disable an Immediate tier extension".

To enable disaster recovery:

1. In the Navigation pane of the VMS Management Client, click **Disaster Recovery** under Surveillance Bridge.

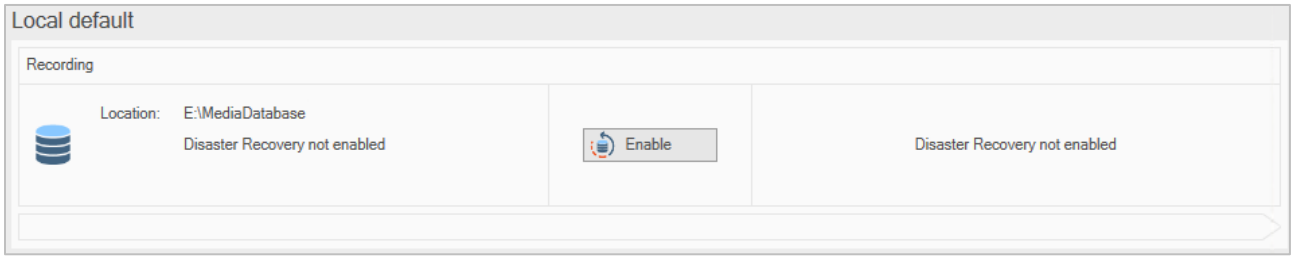


2. In the right pane under Recording Servers, click the recording server, whose recording storage or archive you want to back up.



> **Note:** If a recording server is displayed in the list with a greyed out icon, it is either offline or does not have Surveillance Bridge installed.

The Surveillance Bridge plug-in lists all recording storage/archives configured for the selected recording server.

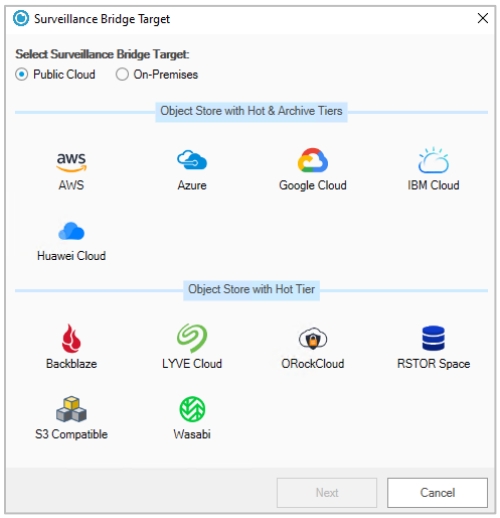


3. Next to the recording storage or the archive pane, click **Enable**.

Note: If immediate/archive tier extension is already enabled for the selected recording storage/archive, the same storage will be used for disaster recovery.

---

4. In the Storage Target dialog, select whether you are adding a Public Cloud or an On-premises storage as disaster recovery storage and then select the type of the disaster recovery storage.



5. Click **Next** and provide the requested configuration details for the selected disaster recovery storage as outlined in "Extension/Disaster Recovery Storage Prerequisites", then click OK.

Important: Never provide the credentials of your root user.

Note: If the account you have specified for access to the disaster recovery storage cannot list all buckets/containers, you must enter the name of the bucket/container manually.

Important: By default, all automatic Surveillance Bridge operations are initially paused. To let Surveillance Bridge begin automatically back up data, follow the instructions in "Start/Pause Automatic Operations".

Disable Disaster Recovery

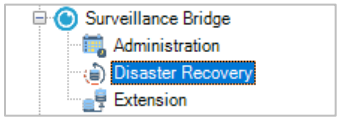
When you disable a recording storage/archive's disaster recovery storage, Surveillance Bridge stops copying data to it both automatically and manually and all already copied data cannot be recovered in case of a recording storage/archive failure. Additionally, once you disable disaster recovery, data on it is no longer automatically deleted once the retention limit set for the respective recording storage/archive is reached.

Important: If the recording storage/archive whose disaster recovery you disable also has an immediate/archive tier extension enabled, Surveillance Bridge stops backing up data, but the immediate tier extension mechanism continues operation. You are also still able to manually move data to and from the extension, following the steps in "Manually Manage Data".

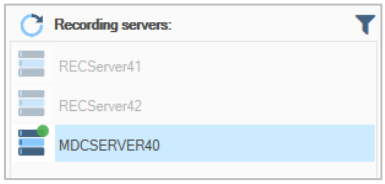
If you want to disable disaster recovery in order to change the credentials for access to the disaster recovery storage, make sure the new credentials provide access to already backed up data. Otherwise, it may remain unavailable for recovery in your VMS. If you want to disable disaster recovery in order to change the type of disaster recovery storage, it is advisable to first migrate all data from your current disaster recovery storage.

To disable Disaster Recovery:

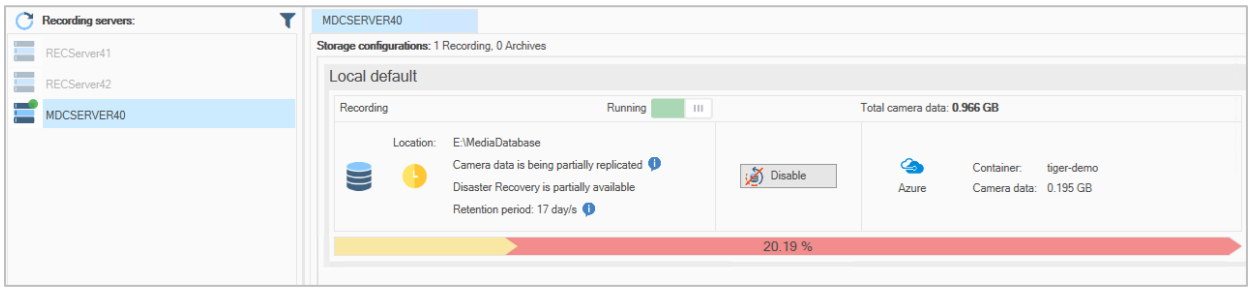
1. In the Navigation pane of the Management Client, click **Disaster Recovery** under Surveillance Bridge.



2. In the right pane under Recording Servers, click the recording server, whose recording storage or archive's disaster recovery you want to disable.



   The Surveillance Bridge plug-in lists all recording storage/archives configured for the selected recording server.



3. In the recording storage or the archive pane, click **Disable**.

Start/Pause Automatic Operations

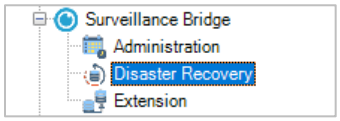
You can pause and start all automatic operations for a specific recording storage/archive at any time. It's important to keep in mind that pausing/starting automatic operations concerns both backing up data and moving data to the extension if extension is enabled for the same recording storage/archive. Additionally, even if automatic operations are started for the disaster recovery mechanism, but then you enable immediate tier extension for the same recording storage/archive, by default the automatic operations will be paused, until you manually start them again.

While automatic operations are paused, Surveillance Bridge stops backing up data to the disaster recovery storage, but already backed up data can be recovered in case of a recording storage/archive failure.

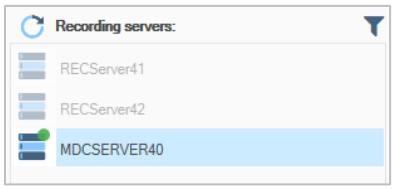
Once you start automatic operations, Surveillance Bridge immediately resumes processing the queue with files scheduled to be backed up.

To start/pause automatic operations for a recording storage/archive:

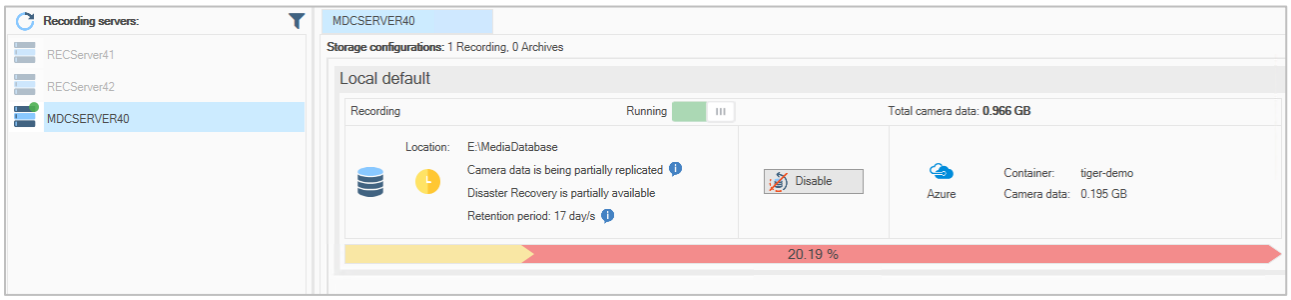
1. In the Navigation pane of the Management Client, click **Disaster Recovery** under Surveillance Bridge.



2. In the right pane under Recording Servers, click the recording server, for whose recording storage or archive you want to start or pause the automatic operations.



The Surveillance Bridge plug-in lists all recording storage/archives configured for the selected recording server.



3. At the top of the recording storage  or the archive  pane, do one of the following:
   - Switch the setting to Running  and when prompted, confirm that you want to start automatic Surveillance Bridge operations.
   - Switch the setting to Paused  and when prompted, confirm that you want to pause automatic Surveillance Bridge operations.

Monitor Data

The Disaster Recovery page of the Surveillance Bridge Plug-in provides you with all information necessary to keep track of the status of a recording server, its recording storage(s)/archive(s), any enabled disaster recovery storage and the data backup progress.

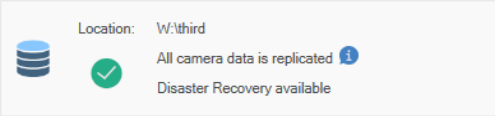
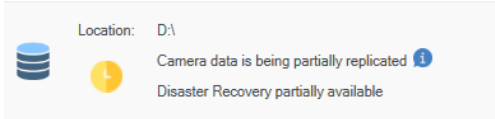
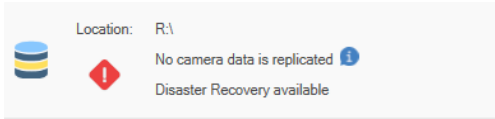
Monitor Recording Servers

To view the status of all recording servers, in the Navigation pane of the Management Client, click Disaster Recovery under Surveillance Bridge and then check the Recording servers pane:

Indicator	Status	Tooltip
Green blinking indicator 	The recording server and its recording storage(s)/archive(s) are operating normally. If a disaster recovery storage is enabled for a recording storage/archive, all data is fully backed up.	Healthy online
Yellow blinking indicator 	The recording server is operating normally, but Surveillance Bridge has detected one or all of the following problems: A disaster recovery storage is inaccessible. Check the panes of the recording storages/archives for this icon to identify it. For more information, refer to Monitor the Recording Storage/Archive. One or more files on a recording storage/archive cannot be backed up. Check the panes of the recording storages/archives for this icon to identify it. For more information, refer to Monitor the Recording Storage/Archive.	Target is offline
Red blinking indicator 	The recording server is operating normally, but Surveillance Bridge has detected one or all of the following problems:	
	A recording storage or archive is not responding and Surveillance Bridge cannot back up any more data from it. To identify it, refer to Monitor the Recording Storage/Archive.	Storage is not responding
	A recording storage or archive has failed. To identify it, refer to Monitor the Recording Storage/Archive.	Storage is offline
	Surveillance Bridge has failed to perform a scheduled operation.	Generic error
Greyed out icon 	One of the following problems has been detected:	
	Surveillance Bridge is either not installed or not responding on the recording server.	Server is offline
	The recording server is offline and may need to be recovered. Refer to "Diagnose a Failed Recording Server" to confirm that you need to run the Disaster Recovery Wizard.	Recording server is offline

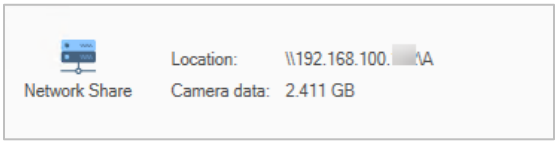
Monitor the Recording Storage/Archive

The Surveillance Bridge plug-in lists all recording storages and archives configured for a selected recording server in the Disaster Recovery page of the Management Client. The recording storage or archive pane, gives you information about its mount path on the recording server as well as the status of the recording storage/archive. Click the info button in the pane, to display a tooltip with additional information.

	The recording storage or archive is available and as long as disaster recovery storage is enabled for it, all its data is fully backed up.
	The recording storage or archive is available and data on it is still being backed up. The data backup progress bar below the pane is displayed in yellow and shows you the percentage of backed up data.
	Surveillance Bridge could not back up one or more files on the recording storage/archive. To confirm this is the problem, check the progress bar below the pane - it should be displayed in pink. For more information, refer to Monitor Data Backup Progress.
	The disaster recovery storage of the selected recording storage/archive is inaccessible. Check for changed credentials for access to it or for connectivity problems.
	The recording storage or archive has been dismounted from the recording server because it has suffered a failure. If disaster recovery has been enabled, Surveillance Bridge displays the Disaster Recovery Wizard button below the recording servers' pane. For more information, refer to Recover Recording Storage/Archive.
	The storage on which the selected recording storage/archive is located has failed. The Disaster Recovery Wizard button is not present, if no disaster recovery storage has been enabled.
	The storage on which the selected recording storage/archive is located is not responding.

Monitor Disaster Recovery Storage

The disaster recovery storage pane gives you information about the storage type, the name of the container in which data is backed up and the size of the total data already backed up.



Note: If the disaster recovery storage is inaccessible for some reason (changed credentials for access to it or connectivity problems), the pane of the recording storage/archive displays this icon . Refer to "Monitor the Recording Storage/Archive" for more details.

Monitor Data Backup Progress

You can view the total size of camera data, which needs to be backed up in the header of a recording storage/archive and keep track of the percentage of already backed up data in the progress bar below.

 all data from the recording storage/archive has been fully backed up

 data from the recording storage/archive is being backed up.

Note: Keep in mind that if cameras are actively recording on the recording storage and data is being constantly sent to the archive, the percentage of backed up data may never reach 100%.

 Surveillance Bridge failed to back up some data from the recording storage/archive. To identify the exact files, check the logs in Windows Event Viewer.

Recover Backed Up Data

The Disaster Recovery Wizard of Surveillance Bridge guides you in recovering a failed recording storage, archive or recording server. The wizard becomes available only when a disaster recovery condition is present. That is why it is important to carefully monitor your recording server(s) and storages, before attempting to recover them. Detailed steps about diagnosing a disaster recovery condition are provided below.

To speed up the disaster recovery and reduce downtime, you can prepare your recording server(s) system and storage, following the disaster recovery prerequisites provided below. It is of great importance to adhere to the disaster recovery precautions, provided before the recovery procedures in order to prevent irrecoverable data and metadata.

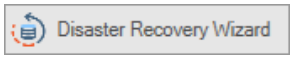
Recover Recording Storage/Archive

Follow these procedures to recover backed up data from a failed recording storage or archive:

- diagnose the failed recording storage/archive
- prepare the storage for recovery of backed up data
- recover data and metadata with the Disaster Recovery Wizard

Diagnose a Failed Recording Storage/Archive

You can diagnose a recording storage/archive failure in the Disaster Recovery page of the Management Client:

- a recording server whose recording storage and/or archive has failed is displayed in the page with a red blinking icon 
- a failed recording storage or archive is displayed in the list with a warning sign 
- the Disaster Recovery Wizard button is available in the recording servers' pane 

Storage Disaster Recovery Precautions and Prerequisites

Once you have ensured that a recording storage and/or an archive has indeed failed, you must take the following precautions in order to ensure that data can be recovered:

- Do not attempt to recover or mount on the recording server any volume with the same drive letter as the failed one(s), on which a recording storage/archive has been stored.
- Once you start the disaster recovery procedure, do not restart the recording server until you complete the procedure in the Disaster Recovery Wizard.

The disaster recovery procedure requires that the Wizard temporarily stops the Recording Server service. As long as a failover recording server is configured, it will take over recording data until the Wizard starts the service again. To speed up the recovery procedure, you can:

- prepare a new disk, on which to recover the failed recording storage/archive

---

Note: The capacity of the disk should be enough to accommodate all backed up data. You can easily calculate the needed capacity by checking the Camera data field in the Disaster recovery storage pane of the failed recording storage/archive (see Monitor Disaster Recovery Storage).

- attach the new disk to the recording server and create an NTFS volume on it, but DO NOT assign a drive letter.

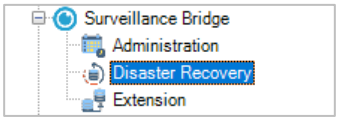
Note: If you need to recover data from recording storages/archives stored on more than one volume on your recording server, attach as many new NTFS volumes to the server as needed or repeat the recovery procedure for each volume that has failed later on.

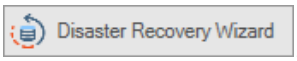
Recover a Recording Storage/Archive Using the Wizard

Important: During the recovery procedure, the Wizard stops the Recording Server service on the computer and when finished automatically starts it again. As long as there is a failover recording server configured, it will take over recording data from the attached devices until the recovery procedure finishes.

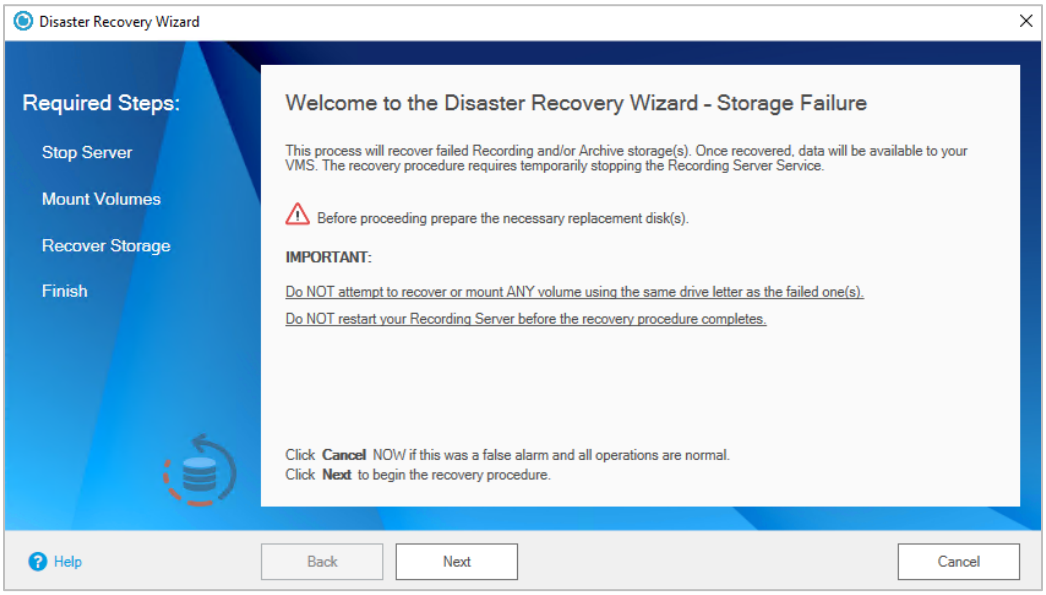
To recover failed recording storage(s)/archive(s) using the Wizard:

1. In the Navigation pane of the Management Client, click **Disaster Recovery** under Surveillance Bridge.

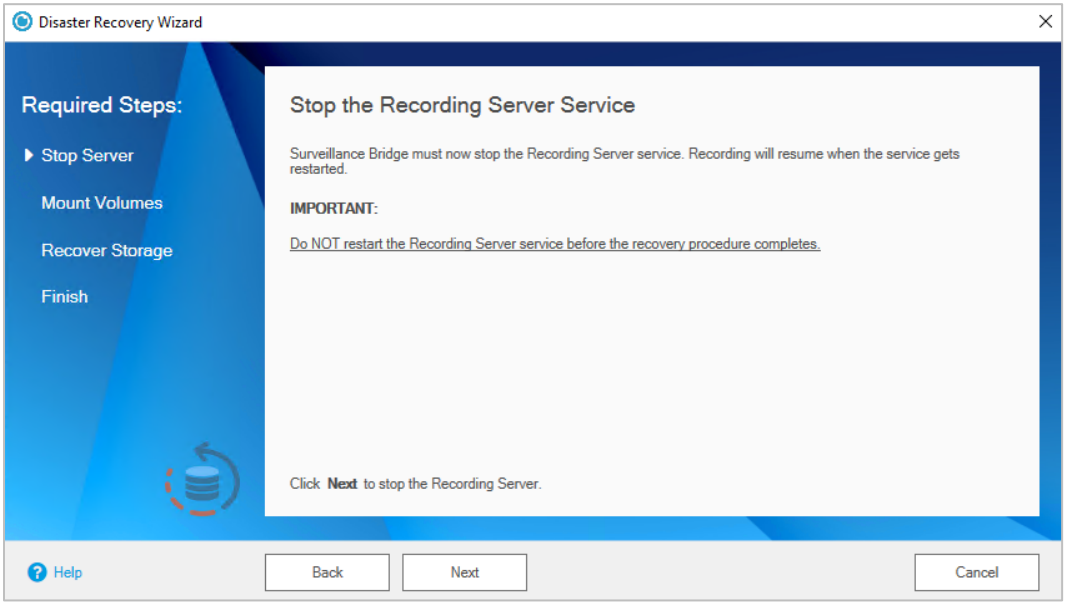


2. In the right pane under Recording Servers, click the recording server, whose recording storage/archive you want to recover. It is displayed with a red blinking icon and a big red warning message underneath.
3. Below the list of recording servers, click the **Disaster Recovery Wizard** button 

.
4. In the Disaster Recovery Wizard, click **Next**.

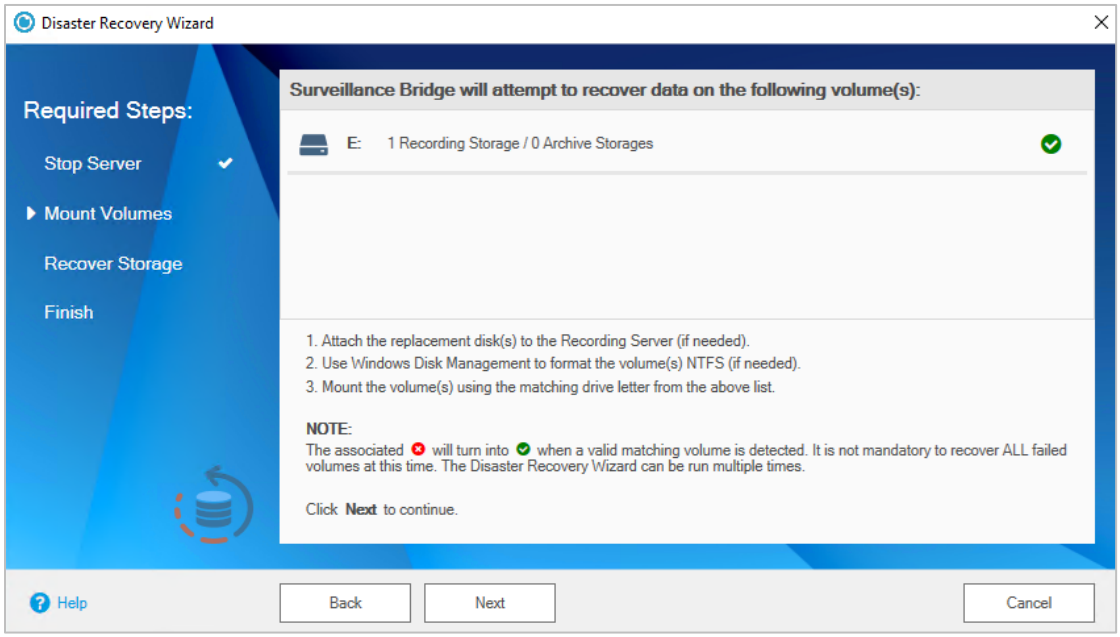


5. To let the Disaster Recovery Wizard stop the Recording Server service on the recording server, click **Next**.



Important: You must not restart the recording server until the data recover procedure finishes.

The Wizard displays a list of all volumes, on which it has detected a failed recording storage and/or archive for which there is a data backup available.



6. In Windows, do one of the following:

   - (if the NTFS volumes are already formatted) assign the same drive letters as the ones of the volumes listed in the Wizard.
   - insert one or more disks, format them to NTFS and assign the same drive letters as the ones of the volumes listed in the Wizard.

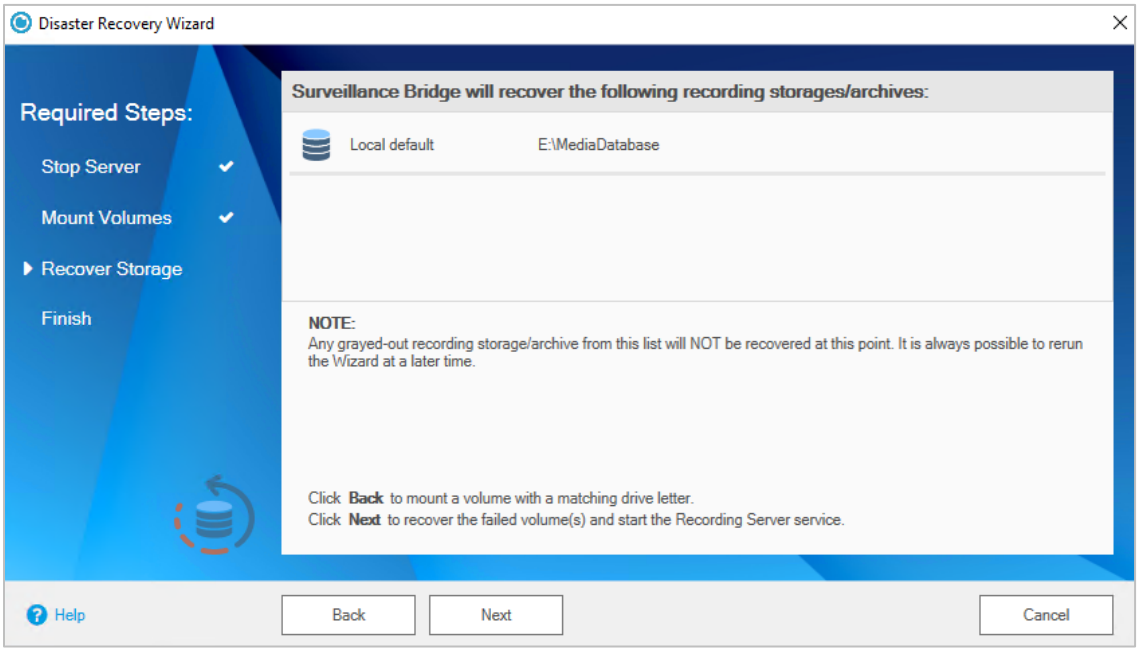
   The Wizard automatically detects each newly added volume with matching drive letter and updates its status in the list with this icon , designating that it can recover data on it.

Note: There must be at least one volume with matching drive letter in the list in order to continue. You can run the wizard later on for each volume, which you are not ready to recover now.

---

7. Click **Next** to continue.

   The wizard displays a list of recording storage(s)/archive(s), which it can recover. If a recording storage/archive is greyed out, the wizard cannot recover its data as it cannot detect a volume with matching drive letter mounted on the recording server.



Note: You can click Back in the wizard and repeat the previous step in order to recover data from a recording storage/archive, which is greyed out in the list.

8. Click **Next** to confirm that you want to recover data from the listed recording storage(s)/archive(s).

   The Disaster Recovery Wizard creates a stub file for each recovered file on the respective recording storage/archive. You can create a manual job for retrieving the actual data from the Disaster Recovery storage, following the steps in "Manually Manage Data" or you can retrieve the recordings on demand by previewing them in the VMS Smart/Video Client (for more information, refer to "Work with the Surveillance Bridge Plug-in").

9. In the Disaster Recovery Wizard, click **Finish** to let it start the Recording Server service.

Recover a Failed Recording Server

Follow these procedures to recover backed up data from a failed recording server:

- diagnose a failed recording server
- prepare the replacement server
- recover the recording server and its recording storage(s)/archives with the Disaster Recovery Wizard

Diagnose a Failed Recording Server

A failed recording server is displayed in the Disaster Recovery page of the Management Client with a greyed out icon  in the list and the Disaster Recovery Wizard button is displayed below the servers' list.

Note: If the Disaster Recovery Wizard button is not present, there is either no backup available for this recording server or Surveillance Bridge is not installed/not responding on the computer.

To ensure that you need to recover the recording server, make sure that:

- the recording server is not turned off
- the recording server's network cable is not disconnected

If none of the above resolves the problem with the inaccessible recording server, proceed with preparing for recovery.

Recording Server Recovery Prerequisites

To speed up the recovery procedure, before starting the Disaster Recovery Wizard you can prepare a replacement recording server, which meets the following requirements:

- has at least one empty NTFS volume mounted with the same drive letter as that of a volume, on which a recording storage/archive of the failed server has been stored

  ---

  Note: Once you recover the recording server, you can recover any remaining recording storage(s)/archive(s) stored on other volumes, following the steps in Recover Recording Storage/Archive

  ---

- Recording Server is installed and is using a valid license
- no devices (like cameras, for example) are attached to the new recording server in the VMS

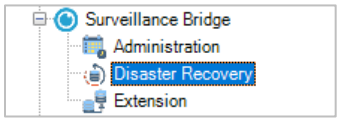
  Note: Once the recovery procedure finishes, all devices previously attached and recording on the failed recording server will automatically be attached to the new one.

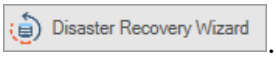
- the computer is turned on and can be accessed through the Management Client
- Surveillance Bridge is installed, but is not activated

Recover a Recording Server Using the Wizard

To recover failed recording server using the Wizard:

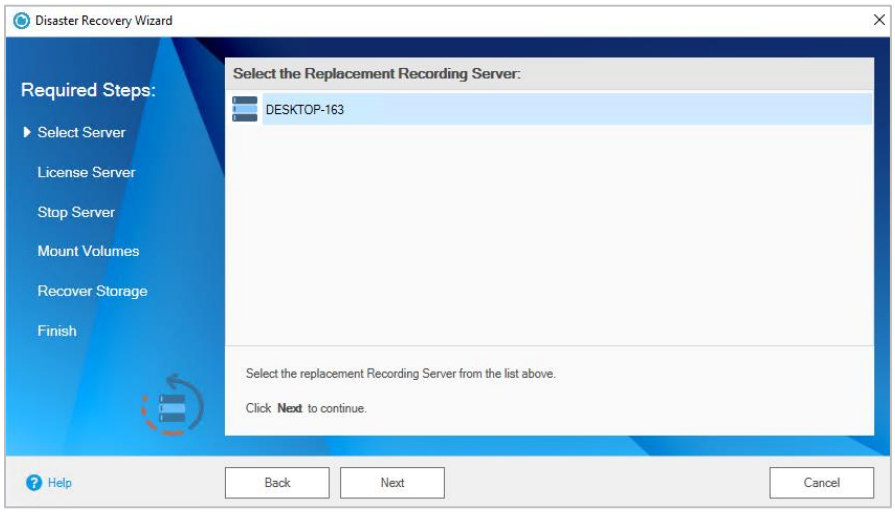
1. In the Navigation pane of the Management Client, click **Disaster Recovery** under Surveillance Bridge.



2. In the right pane under Recording Servers, click the failed recording server. It is displayed with a greyed out icon .
3. Below the list of recording servers, click the **Disaster Recovery Wizard** button 

.
4. In the Disaster Recovery Wizard, click **Next**.

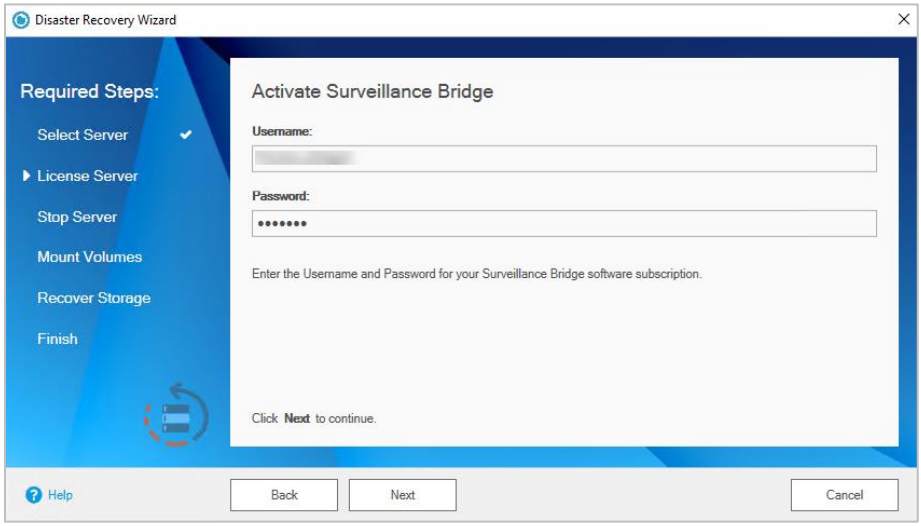
The Disaster Recovery Wizard lists all detected recording servers, which match the requirements for a replacement server.



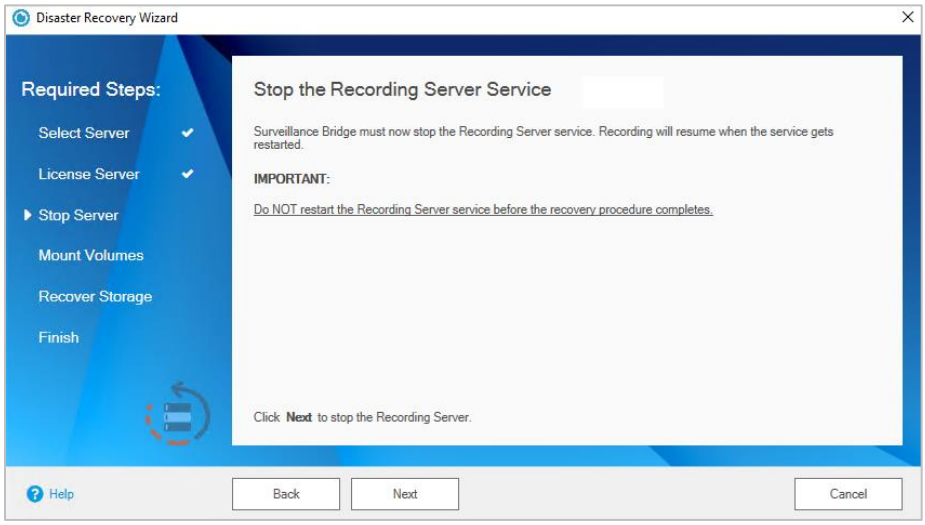
Note: If no suitable recording server is detected, click Back and prepare a computer, which meets the prerequisites outlined in "Prepare the New Recording Server", and then click Next in the Wizard.

5. Select the computer, on which to recover the failed recording server and click **Next**.

6. Enter the username and password of your Surveillance Bridge subscription and click **Next** to activate Surveillance Bridge on the new recording server.

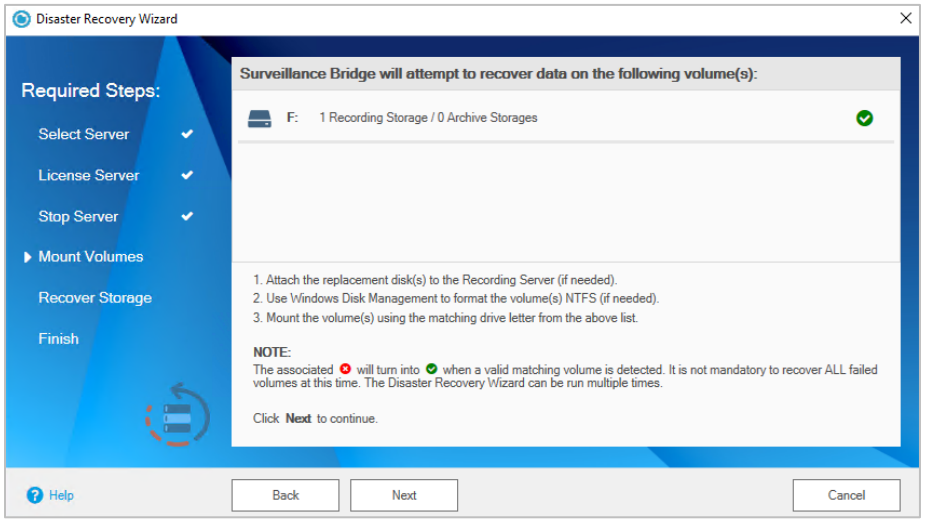


7. To let the Disaster Recovery Wizard stop the Recording Server service on the recording server, click **Next**.



Important: You must not restart the new recording server until the recovery procedure finishes.

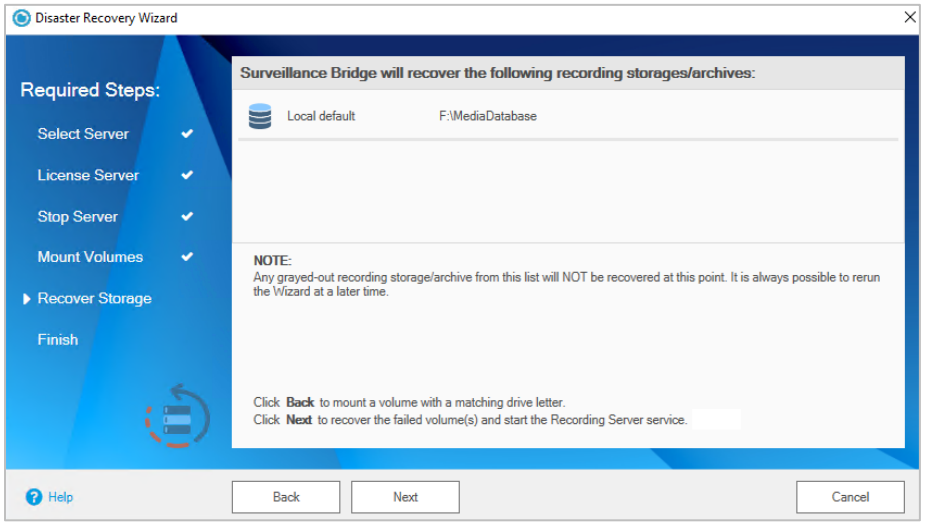
The Wizard displays a list of all volumes on the failed recording server, on which it can recover a recording storage and/or archive.



Note: If a volume is displayed with this icon in the list, the Wizard cannot recover any recording storage/archive from it as it cannot find a volume with matching drive letter on the new recording server. If you attach an empty NTFS volume with matching drive letter at this point, the Wizard will automatically detect it and change its icon to . As long as there is at least one volume with matching drive letter, you can proceed with the recovery procedure and recover any recording storage/archive on other volumes later on, following the steps in Recover Recording Storage/Archive.

8. Click **Next** to confirm that you want to recover data only on volumes, displayed with this icon .

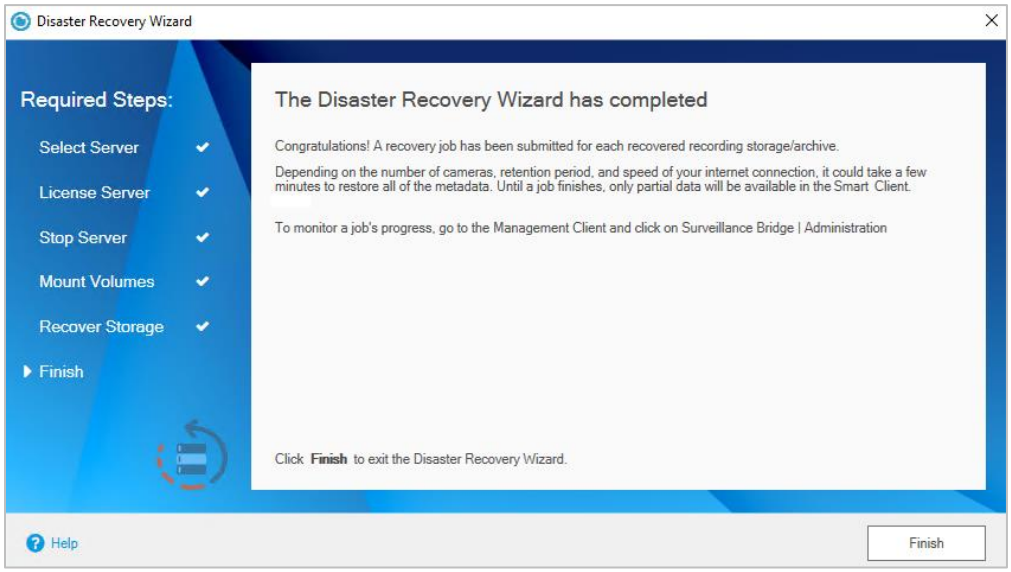
   The Wizard lists all recording storages/archives it can recover. If a recording storage/archive is listed with a greyed out icon, the Wizard cannot recover it on the new recording server.



9. Click **Next** to confirm that you want to recover data from the listed recording storage(s)/archives.

   The Disaster Recovery Wizard creates a stub file for each recovered file on the respective recording storage/archive. You can create a manual job for retrieving the actual data from the Disaster Recovery storage, following the steps in "Manually Manage Data" or you can retrieve the recordings on demand by previewing them in the Smart/Video Client (for more information, refer to "Work with the Smart/Video Client Plug-in").

10. In the Disaster Recovery Wizard, click **Finish** to let it start the Recording Server service on the new recording server.



IV. Manage Extension/Archival

When you extend the recording storage of a recording server, you simply increase its capacity with the free space on the cloud storage, network share or local volume you have added as an extension. You can expand the capacity of a recording server's storage with an immediate tier extension, from which data is transparently retrieved as soon as the connection speed allows, or an archive tier extension, from which data is not retrieved immediately, but must first be rehydrated to an intermediate tier.

Once the retention limit you have specified for the respective recording storage is reached, data contents are automatically deleted from it and from its extension to make way for newly recorded data.

To extend the recording storage or archive of a recording server, you should do the following:

- enable the immediate tier extension
- configure what data should be automatically moved to the extension and made accessible from there
- turn on automatic Surveillance Bridge management of data between the extended recording storage/archive and the extension

To enable an extension, you should simply provide the credentials for access to the cloud storage, network share or local volume, which will be used as an extension. If disaster recovery is already enabled for the selected recording storage or archive, the same cloud storage, network share or local volume is used as an immediate tier extension. Thus, there is no need to provide the credentials for access to the extension, but simply configure the extension and enable automatic Surveillance Bridge operations on it.

Depending on the video management system you are using, the steps will be slightly different. They are outlined below.

The archive tier extension can only be on the same storage as the immediate tier extension and uses the same credentials for access. You cannot enable an archive tier extension of a recording storage/archive, which does not have an immediate tier extension already enabled. Also, you cannot enable an archive tier extension of a recording storage, which has an archive, as moving groomed data to the archive would require unnecessary retrieval of data from the archive tier extension.

Important: Surveillance Bridge does not allow you to use the same bucket/container (on cloud storage) or folder (on network share or local volume) as an extension of more than one recording storage/archive.

To change the type of immediate tier extension or the credentials for access to it, you need to first disable the current extension and then enable it again. Keep in mind that if you want to change the type of immediate tier extension or the credentials for access to it of a recording storage/archive, which also has Surveillance Bridge disaster recovery enabled, you must first disable disaster recovery too, following the steps outlined in the specific Disable Disaster Recovery section of this document.

When you are enabling your configuration, you will be asked for some configuration. To configure an immediate tier extension means to specify the criteria based on which Surveillance Bridge automatically moves data from the recording storage/archive to the extension. On both immediate and archive tier extensions you

can instruct Surveillance Bridge to move recorded data to the extension using the “By age” criteria. On the immediate tier extension, you can also utilize the “By size” criteria.

 **By age**

Surveillance Bridge moves to the immediate or archive tier extension recordings that have not be accessed on your recording storage/archive for a specified time interval. Once the “By age” interval is reached for a specific recording, Surveillance Bridge copies it to the respective extension and then replaces it on the recording storage/archive with a stub file, pointing to the copy on the extension and allowing it to be transparently retrieved upon request from the immediate tier or rehydrated from the archive tier storage.

 **By size**

Surveillance Bridge moves recorded data to the immediate tier or archive tier extension, when the used space on the extended recording storage/archive reaches a specified threshold. Once the threshold is reached, Surveillance Bridge begins copying data to the extension, starting with the least recently accessed files. Once a recording is copied to the extension, Surveillance Bridge replaces it on the recording storage/archive with a stub file. The stub file points to the copy on the extension, allowing it to be transparently retrieved upon request from the immediate tier extension or rehydrated from the archive tier extension.

By default, immediate tier extensions use the “By size” method with a used space threshold of 95%. By default, files are moved from the immediate to the archive tier, when they have not been accessed for 1 day. You can change the configuration of the immediate and archive tier extensions at any time and the changes are being applied immediately.

The extension policies in Surveillance Bridge are being configured with the purpose of reducing the usage of expensive local storage in favor of using cheaper cloud storage. Usually, we use more cloud storage than local to save some expenses. The open-ended question, which usually remains unanswered, is – How much local storage exactly do you still need when also using extension to the cloud? Here, we will help you do the math.

For the sake of our calculations, let us assume that you have a local storage with capacity **X**, where **X** could be any number of gigabytes or terabytes (for example, 2 TB).

If that drive is what you have configured for Surveillance Bridge to use as a source as this is the location where you keep your camera data, then this storage is used from Surveillance Bridge for two important purposes:

- as a **cache** - to keep some (latest) camera data locally before it gets deleted locally and stored only in the extension in the cloud
- as a **buffer –** in case you lose your connection to the cloud for whatever reason, until that connection is restored

The way the local storage space is divided for these two purposes is dictated by the Extension configuration settings and could be “By age” or “By size”.

“**By age**” means that camera data, not accessed for more than a certain number of hours, days, or weeks, will be moved to the cloud. If you already have a working environment, you probably know that your local storage is enough for keeping, let us say, 10 days of camera data. This means that if you configure the policy “By age” and set a value of, let us say 5 days, then your local storage will be divided approximately equally – 5 days to cache

data locally and 5 more days as a buffer in case something goes wrong with the connection to the cloud. This will give you 5 days to fix your connection before you run out of storage and potentially lose camera data.

As another example, if your local storage is enough for keeping, let us say 7 days, and you want to have bigger cache, like 5 days, and lower buffer, like 2 days – then your local storage will keep 5 days of camera data again but the reaction time in case of a failure would be just 2 days. 5 days of camera data will always be present and the other space will only be used in case of a problem. As in the previous example, if a problem happens and you lose your connection to the cloud for more than 2 days, your buffer, then you will start losing camera data.

"**By size**" can be quite helpful when you want to keep a percentage of the local storage, enough for keeping a certain amount of data, free during normal operation. This helps you make sure you have the required buffer in case of a problem. The setting could be set very aggressively to something like 95%. Setting it like this would mean that during normal operation 95% of the storage (if there is enough data to fill that) will always be full and used for cache and only 5% will be used as a buffer in case of a problem. This could be dangerous, depending on your workflow and how much recording time these 5% of the local storage could store.

Depending on your workflow and needs, you can make the cache and buffer sizes bigger or smaller with either one of the settings – "By age" or "By size".

If you are preparing a new infrastructure, on the other hand, chances are that you don't know how big of a local drive you will need to buy or, respectively, if you have already bought a drive, you may not know how much space your cameras need for 5 days of cache or how much camera data you will be able to store in 5% of the local storage.

You can do these calculations with the help of the average bandwidth for your cameras. If you have 80 cameras with 3 Mbit per second average bandwidth, then you can calculate 240 Mbit times the number of seconds you need for cache and buffer together and you will get the needed total storage capacity.

To continue our example, if we divide 240 Mbit by 8, we would get the same value in Mbytes. That would be 30.

If you configure your policy "By age", we would recommend a value of 3 days so you can have at least one working day for reaction in case of problem, even if that problem happens on a Friday evening.

1 day measured in seconds is 24 hours * 60 minutes per hour * 60 seconds per minute = 86 400.

If we multiply that number, 86 400, by the average bandwidth of our 80 cameras, which is 30, we would get approximately 2.5 TB per day.

With that number, we can multiple the 3 days we would like to have for a buffer. That would give us 7.5 TB of storage needed just for the buffer.

Then we can multiply the same number, 2.5 TB, by the number of days we would like to have for a cache. That depends very much from one workflow to another but let us say, for this example, that we would like to keep just 1 day worth of data for a cache. That gives us 2.5 TB for that.

Then the total number, needed for local storage in this example, would be 7.5 + 2.5 = 10 TB. If we buy a 10 TB big local drive (or two of them if you would like a local redundancy), then that would be ideal, not too big, not too small, for our imaginary environment.

Important: Be careful with these settings. Although Surveillance Bridge allows you to operate with a very small local drive (like a single 200GB drive for 80 cameras), to take the most out of the solution make sure to keep in mind the local storage's purpose – to serve as a cache and a buffer.

Think about how much time you may need in the worst-case scenario to recover from a problem – that would help you calculate **the size of the buffer**.

Then think about how long you need to keep data locally to review it easily on the timeline without being charged for that by the cloud provider – for just a couple of hours or maybe days or weeks. The answer to this question will help you calculate **the size of the cache**. Once the data is on the cloud, you can still retrieve it and use it on the timeline. However, that will come with additional charges. With proper configuration, these charges would be minimal.

The sum of the above two will give you the size of the local storage you need.

Additionally, when configuring an Amazon S3 or Azure archive tier extension, you can configure the following options:

 **Amazon S3**

- change the archive retrieval option, choosing between Expedited, Standard or Bulk.

 **Azure**

- change the rehydration priority for files on the archive tier extension, choosing between Standard or High.

Extension/Archival with the Standard Surveillance Bridge

With the help of the Surveillance Bridge Configuration Utility, you can configure the extension between your local storage hosting your VMS data and the cloud or on-premises target of your choosing.

Note: If you are working with the Surveillance Bridge Plug-in, please move to the next section of this document, called Extension with The Surveillance Bridge Plug-in.

Enable Extension

Before you can take advantage of the Disaster Recovery and Extension functionalities of the product, you need to configure your source folder and target cloud or on-premises storage. **Move directly to Step 7**, if you have already done that.

---

1. Start the Surveillance Bridge product by double-clicking its Desktop icon or finding it in the Start menu.

2. Click the **Add source** button at the bottom left corner of the window to start configuring your environment.

3. **Browse** to the desired folder. That would be the location of your VMS recording files.

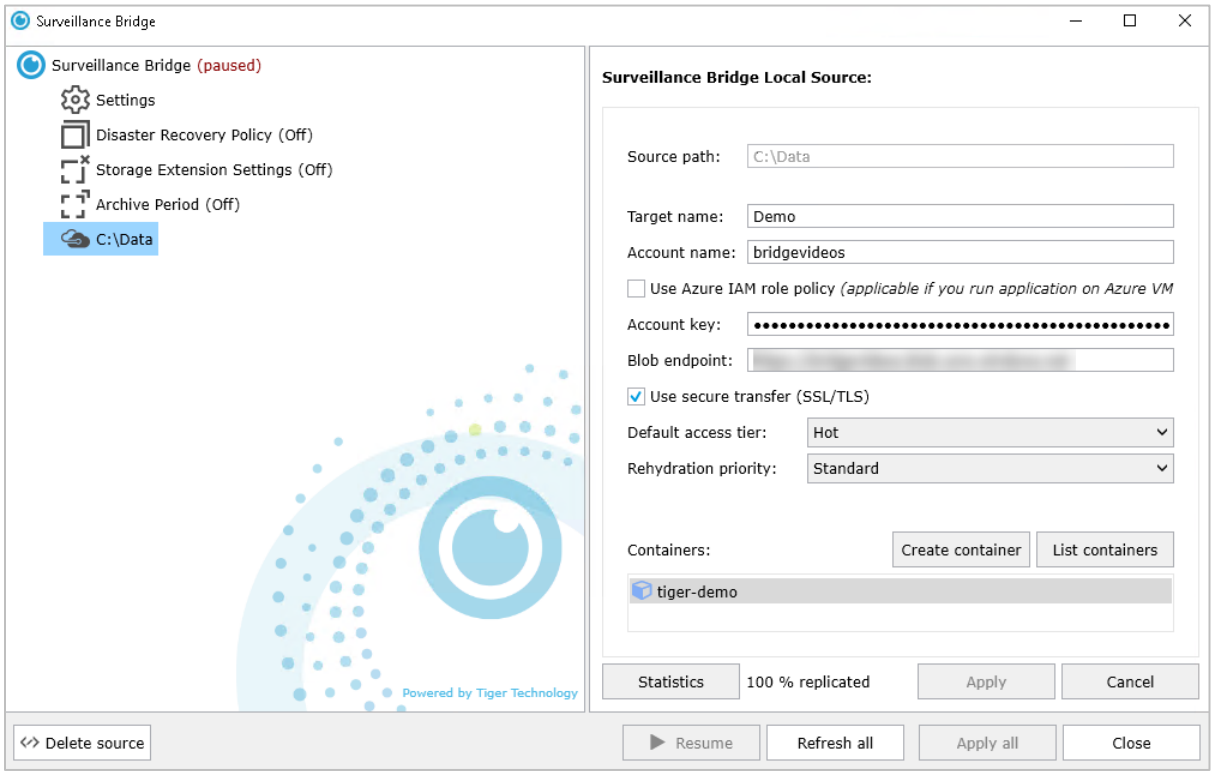
4. Select the desired cloud or on-premises storage and click **OK**.

5. Set up the target with all its required details and click **Apply** to save your configuration.

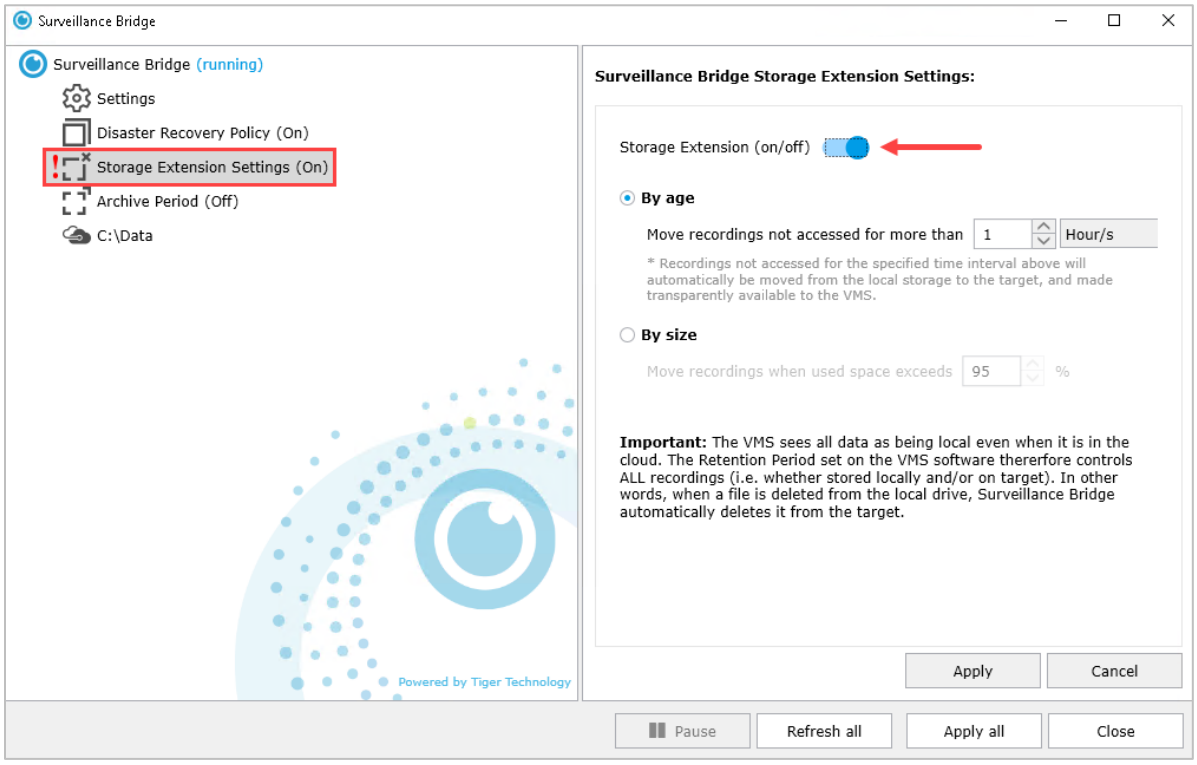
6. You will be asked to choose an action to be performed on any existing data in the target and you can:

    - Take no action – nothing will be imported from the target
    - Disaster Recovery light – only metadata will be imported initially, the rest will only be downloaded on demand
    - Disaster Recovery full – both metadata and content will be restored

    Your already set up target should look similar to this:



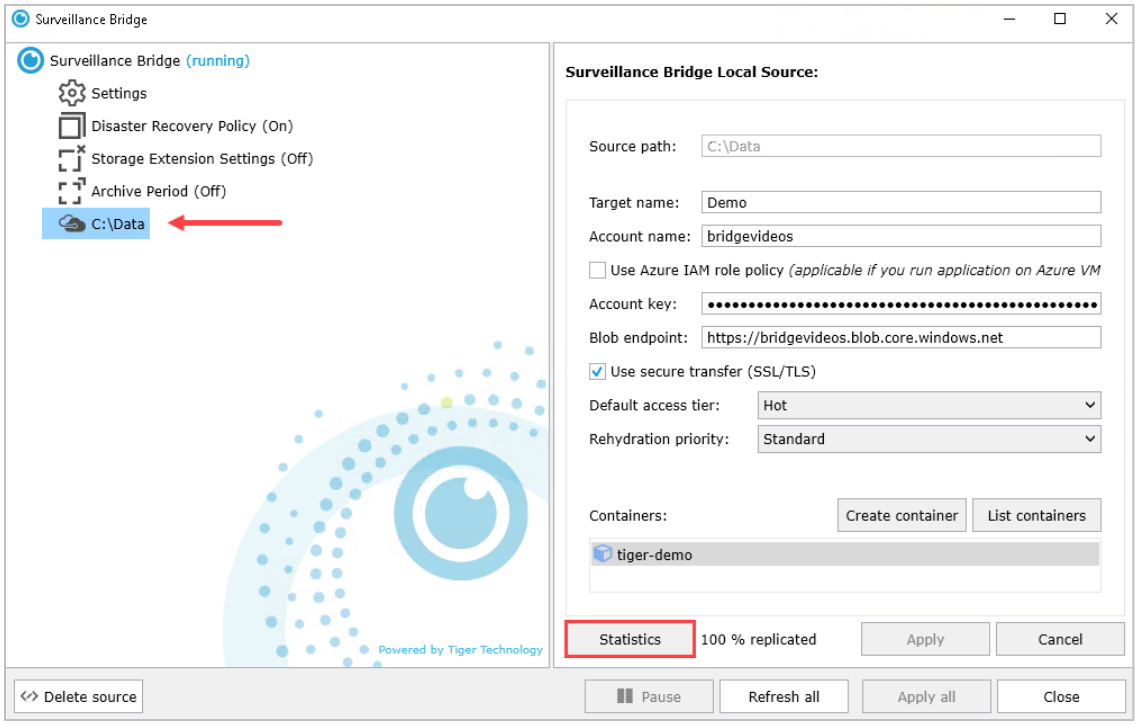
7. Go to the Storage Extension Settings section and toggle the on/off switch.



8. You will be presented with the options to configure your Extension policy By Age or By Size. Make your selection and click **Apply**. If you are feeling unsure which option you need to select and what value to put in the configuration, please check our intro section with the examples and instructions provided there.

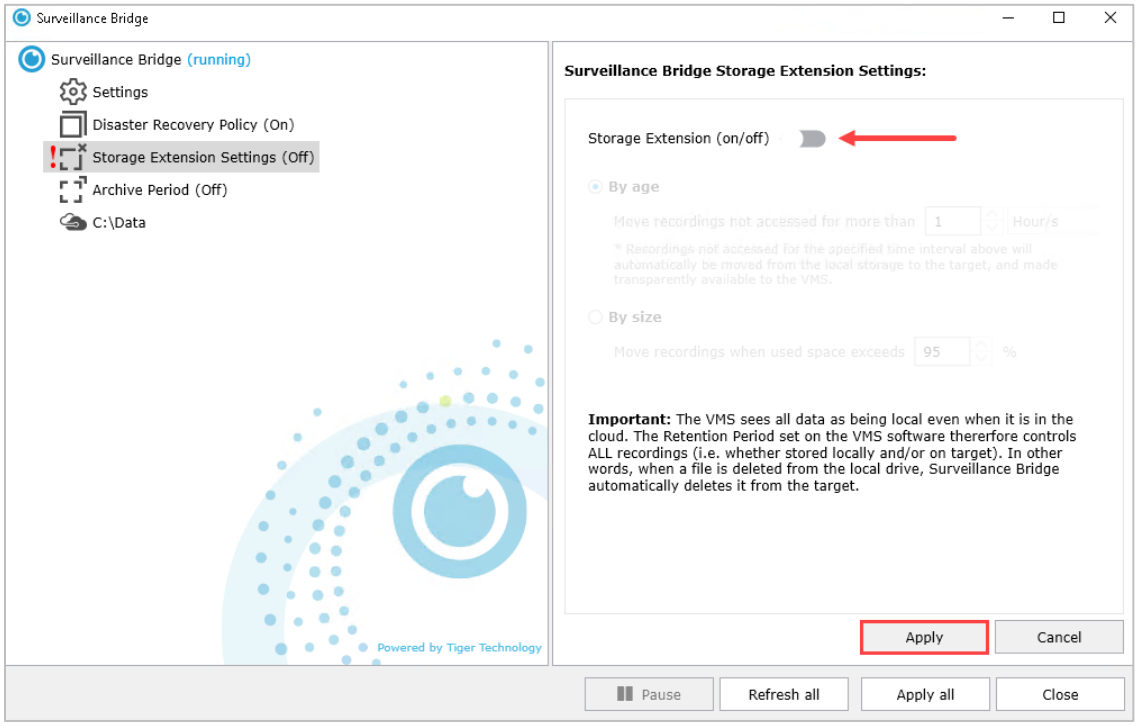
9. Make sure Surveillance Bridge is not left in a paused state. Click to **Resume** its work, if needed.

To get information on how much space you have reclaimed on your local storage, click on your source on the left and use the **Statistics** button.



Disable Extension

To disable the storage extension, simply go back to the respective menu, toggle the on/off switch again and click the **Apply** button.

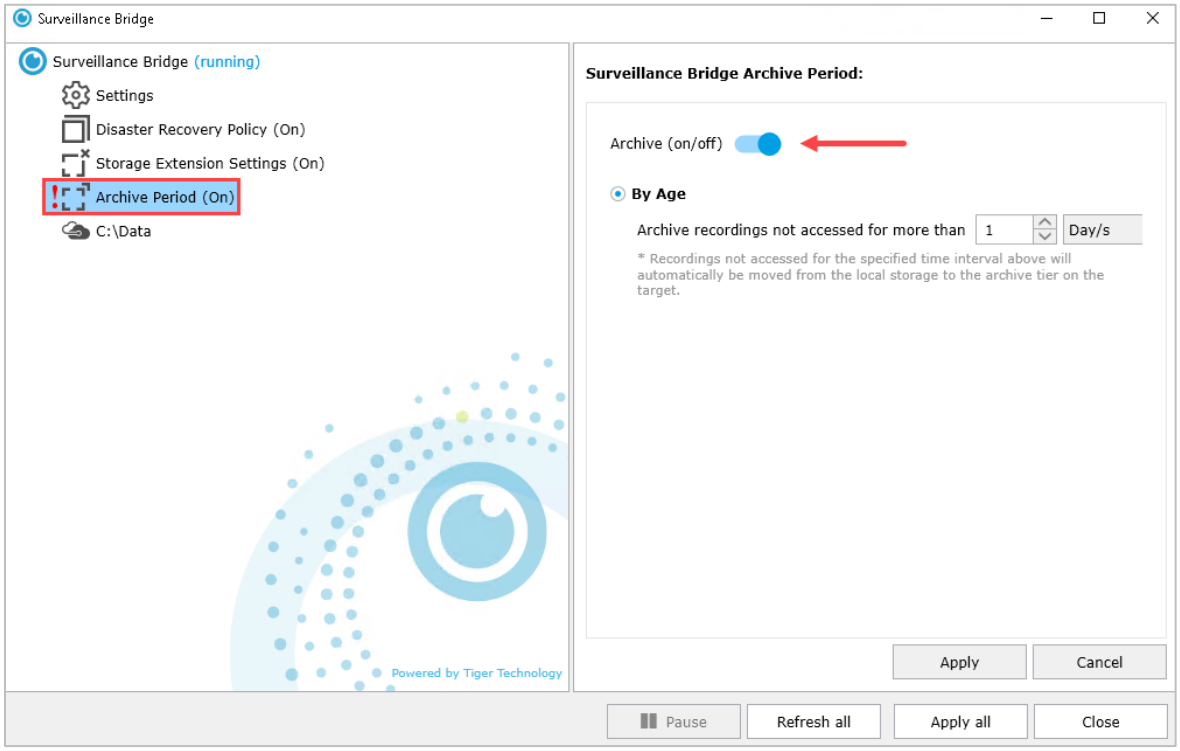


Enable Archival

Archival is a form of Extension which guides Surveillance Bridge to send data, not accessed for a certain pre-configured period of time, to the archival tier of the target storage. You can play with the Immediate tier extension Settings and the Archive Period so that you can find what suites your needs.

It can only be configured with the “By Age” policy. To set it up you will need to:

1. Go to the **Archive Period** menu and toggle the on/off switch.



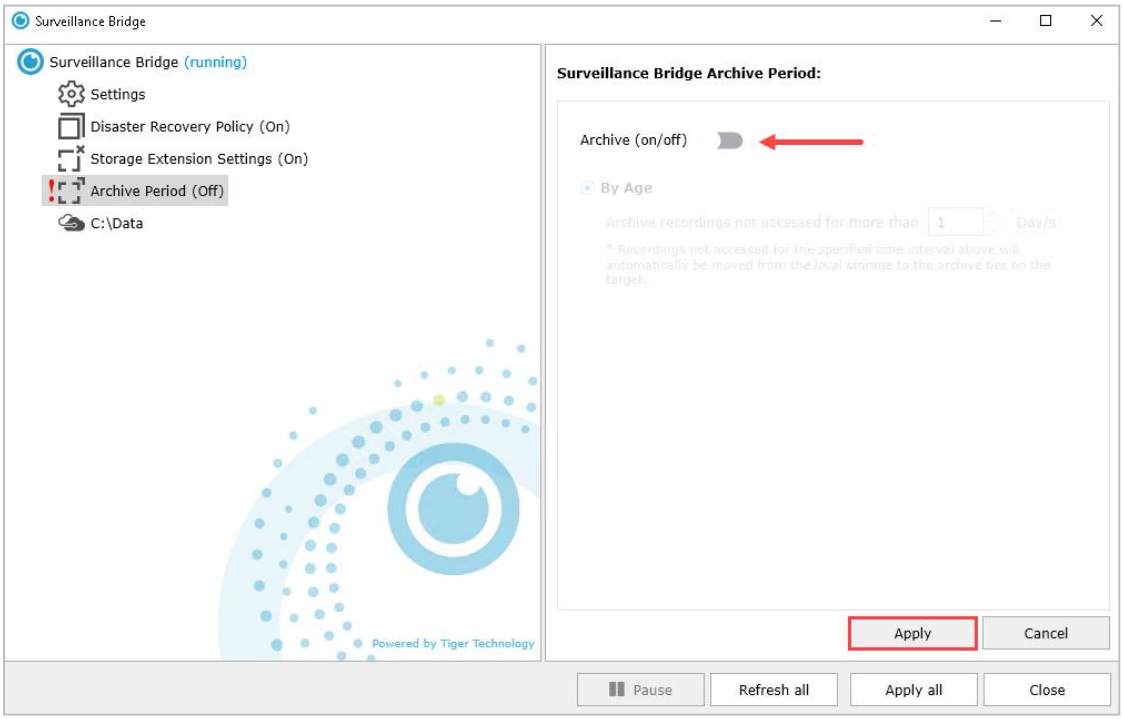
2. Configure the desired waiting period before data gets transferred to the archive tier storage and click **Apply**.

   Be careful with your selection. The bigger the value in the configuration, the more data will go to cheaper archive storage, however, the more expensive the retrieval of that data will become. You need to find the right balance for your workflow. You can come back and edit this setting later.

3. Make sure Surveillance Bridge is not left in a paused state. Click to **Resume** its work, if needed.

Disable Archival

To disable the Archive Period, simply go back to the respective menu, toggle the on/off switch again and click the **Apply** button.



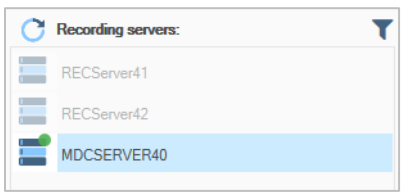
Extension/Archival with The Surveillance Bridge Plug-in

Enable Extension

To enable extension:

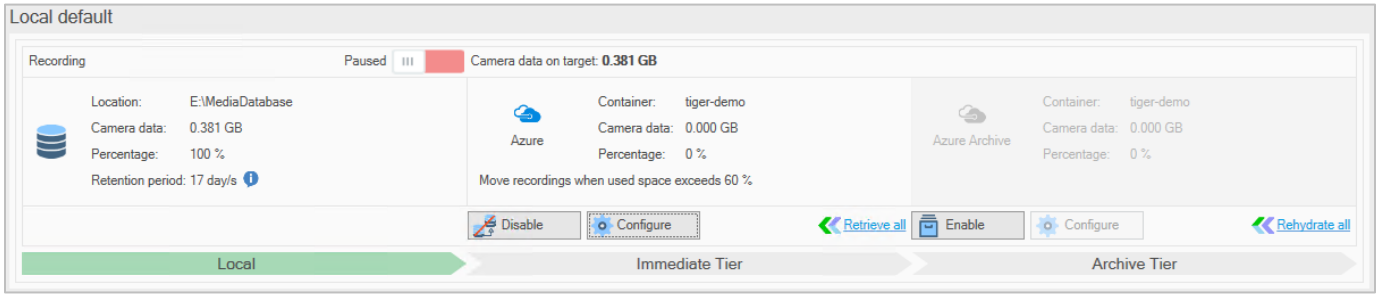
1. In the Navigation pane of the Management Client, click **Extension** under Surveillance Bridge.

2. In the right pane under Recording Servers, click the recording server, whose recording storage or archive you want to extend.



Important: If a recording server is displayed in the list with a greyed out icon, it is either offline or does not have Surveillance Bridge installed.

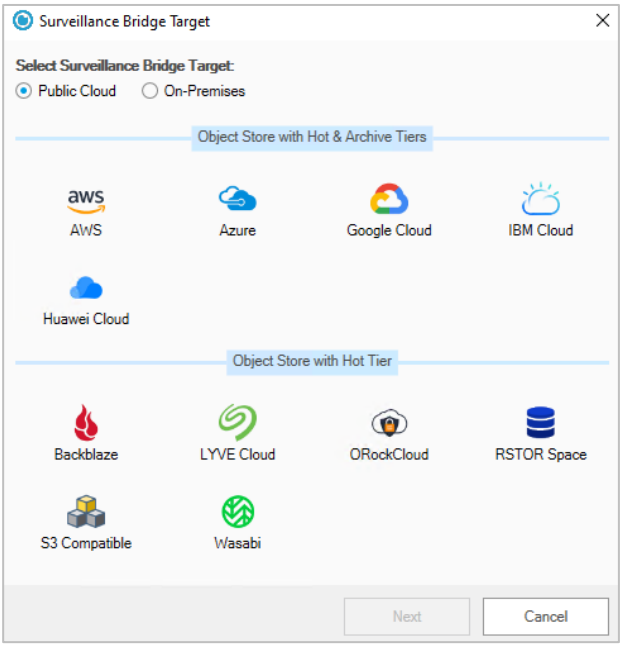
The Surveillance Bridge plug-in lists all recording storages/archives configured for the selected recording server.



3. In the Immediate Tier pane of the recording storage or the Archive Tier you want to extend, click **Enable**.

Note: If disaster recovery is already enabled for the selected recording storage/archive, the same storage will be used as immediate tier extension. To enable the extension, in the dialog which opens, configure either by size or by age criteria for moving data, following the steps in **Error! Reference source not found.**.

4. In the Surveillance Bridge Target dialog, select whether you are adding a Public Cloud or an On-Premises storage as immediate tier extension and then select the type of the immediate tier extension.



5. Click **Next** and provide the requested configuration details for the selected disaster recovery storage as outlined in "Extension/Disaster Recovery Storage Prerequisites", then click OK.

Important: Never provide the credentials of your root user.

Note: If the account you have specified for access to the disaster recovery storage cannot list all buckets/containers, you must enter the name of the bucket/container manually.

Important: By default, all automatic Surveillance Bridge operations are initially paused. To let Surveillance Bridge begin automatically back up data, follow the instructions in "Start/Pause Automatic Operations".

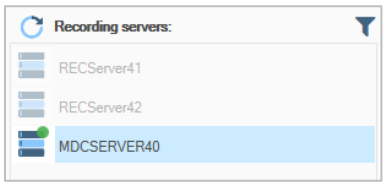
Until you configure the extension, Surveillance Bridge uses the default parameter - data is automatically moved to the immediate tier extension and is made accessible from there, when the used space on your recording storage/archive reaches 95%. You can change this default parameter, following the steps in **Error! Reference source not found.**.

To enable an archive tier extension:

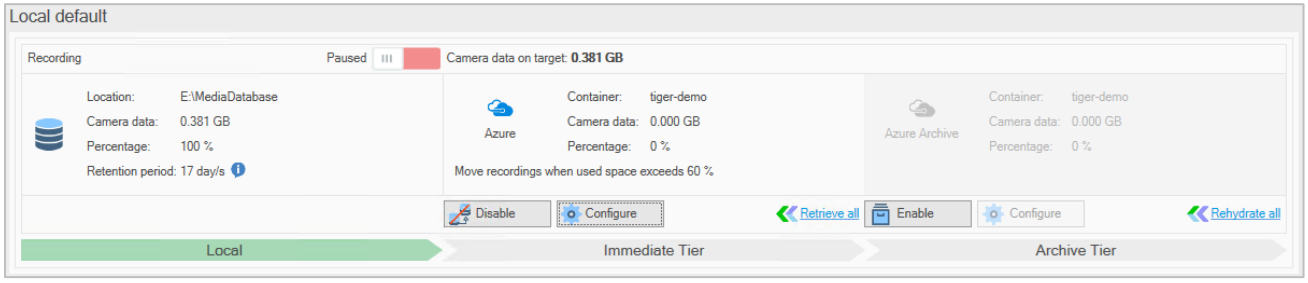
Important: You cannot enable an archive tier extension of a recording storage/archive, which does not have an immediate tier extension enabled. Additionally, you cannot enable an archive tier extension of a recording storage, which has a VMS archive enabled.

1. In the Navigation pane of the VMS Management Client, click **Extension** under Surveillance Bridge.

2. In the right pane under Recording Servers, click the recording server, whose recording storage or archive you want to extend.



The Surveillance Bridge plug-in lists all recording storages/archives configured for the selected recording server.

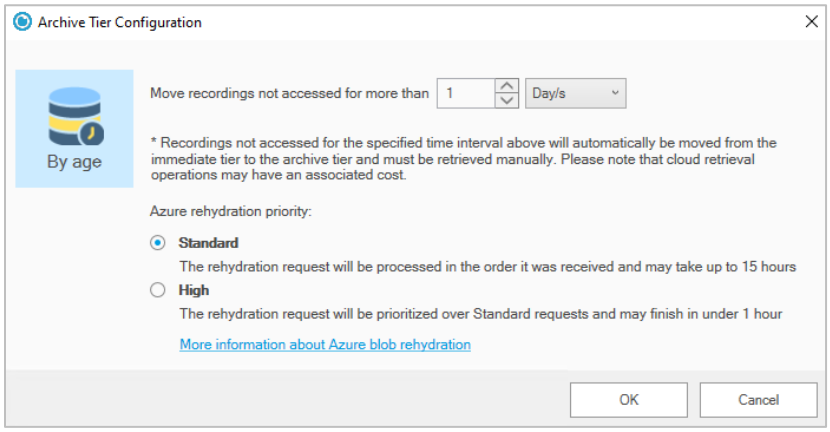


3. In the Archive Tier pane of the recording storage or the archive you want to extend, click **Enable**.

> **Note**: The button is inactive, if no immediate tier on a supported cloud target is enabled or if you attempt to enable an archive tier extension of a recording storage, which has a VMS archive.

4. (Amazon S3 only) Select the archive retrieval option, choosing between Expedited, Standard or Bulk.
5. (Azure only) Select whether files from the archive tier extension should be rehydrated to the Standard or the High tier.

6. In the Archive Tier Configuration dialog, make your selections and click **OK**.



Until you configure the parameters for automatically moving data to the archive tier, Surveillance Bridge uses the default parameter - data is made accessible from there, when it has not been accessed for 1 day on your recording storage/archive. You can change this default parameter, following the steps in **Error! R eference source not found.**.

Important: By default, all automatic Surveillance Bridge operations are initially paused and you can move data to the archive tier extension only manually, following the steps in "Manually Manage Data". To let Surveillance Bridge automatically move data, follow the steps in Start/Pause Automatic Operations.

Disable Extension

When you disable a recording immediate/archive tier extension, Surveillance Bridge stops moving data to it both automatically and manually and all already moved data is accessible only directly from the extension i.e. cannot be retrieved through your VMS. Thus, if you attempt to review footage from the extension using the VMS Client, for example, the operation will fail. Additionally, once you disable the extension, data on it is no longer automatically deleted once the retention limit set for the respective recording storage/archive is reached.

Important: If the recording storage/archive whose extension you disable also has disaster recovery enabled, Surveillance Bridge stops moving data to the extension only automatically, but the disaster recovery mechanism keeps on copying data based on the criteria you have specified and you are still able to move data to and from the extension manually, following the steps in "Manually Manage Data".

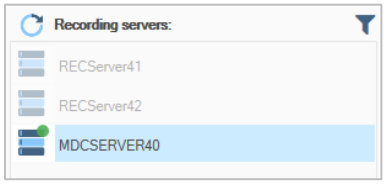
You can select to disable just the archive tier extension and leave the immediate tier extension active. But if you disable the immediate tier extension, the archive tier extension is automatically disabled too.

If you want to disable an immediate tier extension, in order to change the credentials for access to it, make sure the new credentials provide access to data already moved there, otherwise it may remain inaccessible in your VMS. If you want to disable the extension in order to change the type of storage used as an extension, it is advisable to first migrate all data from your current extension to the new one.

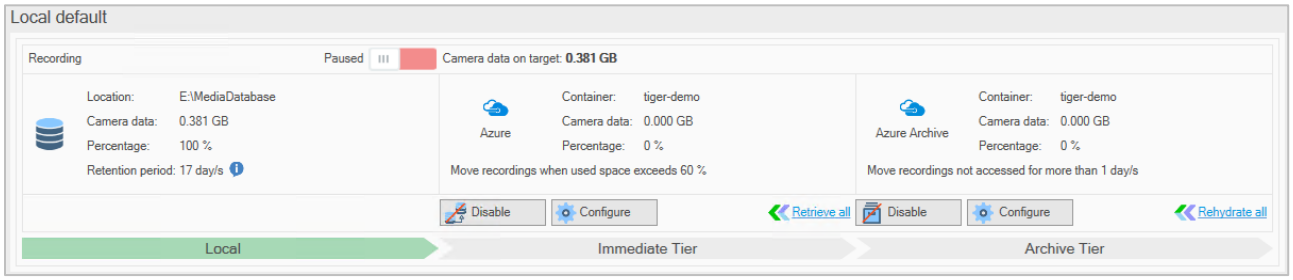
To disable an extension:

1. In the Navigation pane of the Management Client, click **Extension** under Surveillance Bridge.

2. In the right pane under Recording Servers, click the recording server, whose recording storage or archive's extension you want to disable.



The Surveillance Bridge plug-in lists all recording storage/archives configured for the selected recording server.

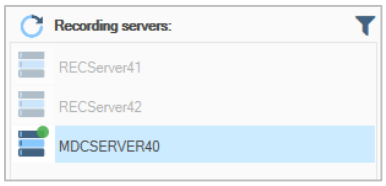


3. In the Immediate or Archive tier extension pane of the recording storage or the archive , click **Disable**.

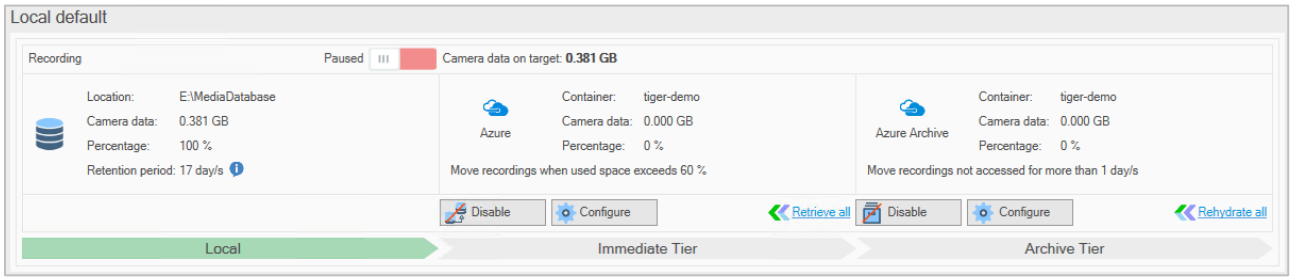
To configure an Immediate Tier extension:

1. In the Navigation pane of the Management Client, click **Extension** under Surveillance Bridge.

2. In the right pane under Recording Servers, click the recording server, whose recording storage or archive you want to extend.



The Surveillance Bridge plug-in lists all recording storage/archives configured for the selected recording server.

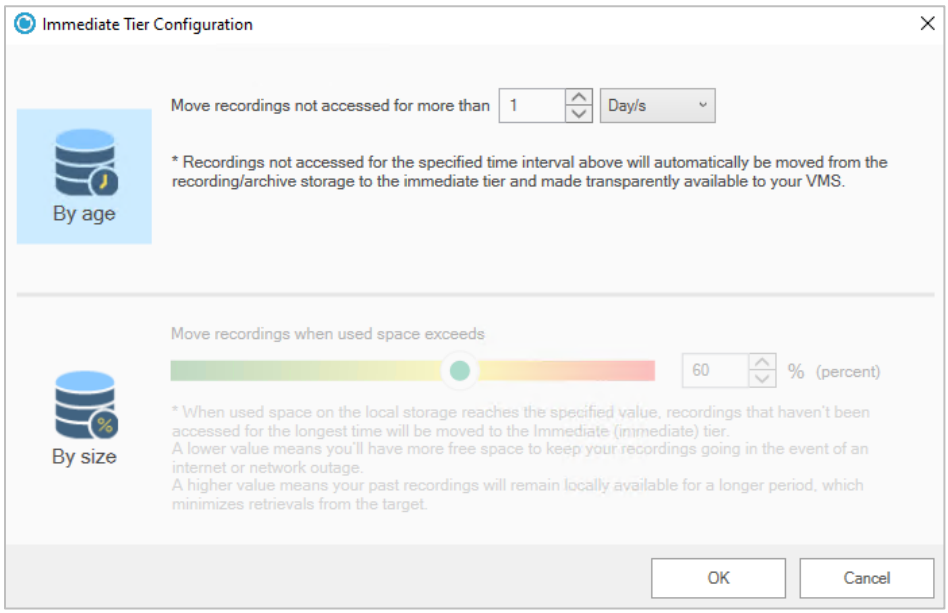


3. In the Immediate Tier pane of the recording storage or the archive, click **Configure**.

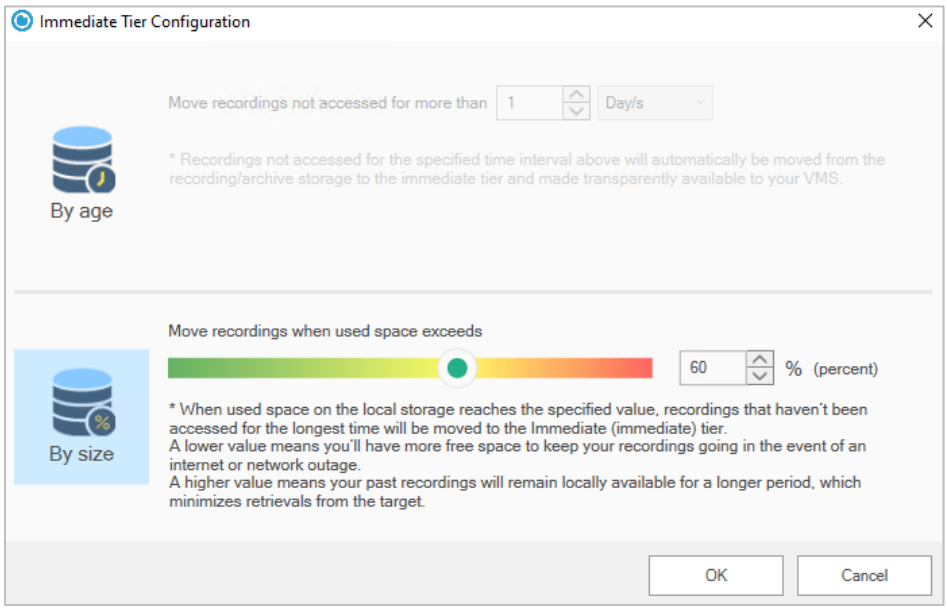
> **Note**: The button is inactive if the Immediate tier extension has not been enabled.

4. In the Immediate Tier Configuration dialog, do one of the following:

- Click "**By age**" and specify for how long a recording on the recording storage/archive should not have been accessed for Surveillance Bridge to move it to the extension.



- Click “**By size**” and specify the percent of used capacity on the recording storage/archive, which when reached triggers Surveillance Bridge to move recordings to the extension.

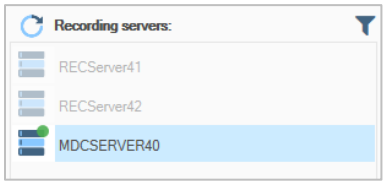


5. In the Immediate Tier Configuration dialog, click **OK**.

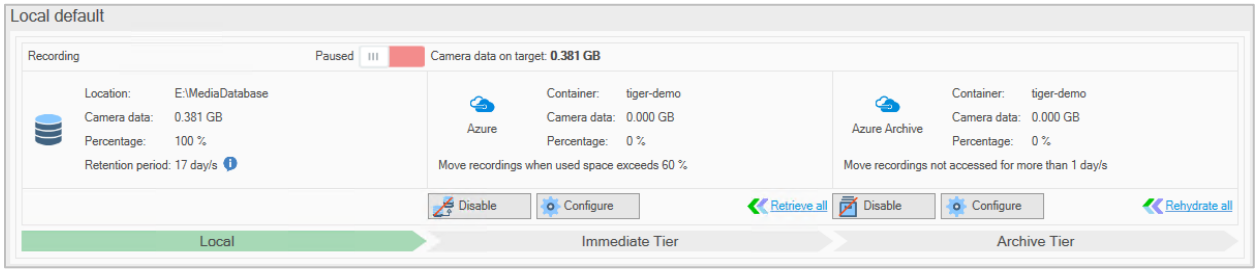
To configure an Archive Tier extension:

1. In the Navigation pane of the Management Client, click **Extension** under Surveillance Bridge.

2. In the right pane under Recording Servers, click the recording server, whose recording storage or archive you want to extend.



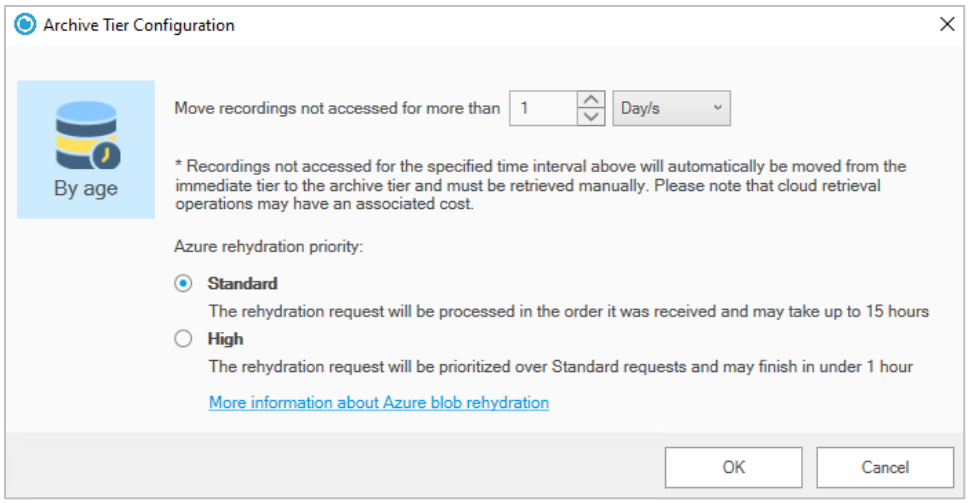
The Surveillance Bridge plug-in lists all recording storage/archives configured for the selected recording server.



3. In the Archive Tier pane of the recording storage or the archive , click **Configure**.

> **Note**: The button is inactive if the Archive Tier extension has not been enabled.

4. In the Archive Tier Configuration dialog, specify for how long a recording on the recording storage/archive should not have been accessed for Surveillance Bridge to move it to the archive tier extension.



5. (optional) Specify additional options for Amazon S3 or Azure archive tier extension:
   - (Amazon S3 archive tier extension only) Change the archive retrieval option, choosing between Expedited, Standard or Bulk.
   - (Azure archive tier extension only) Change whether files from the archive tier extension should be rehydrated using Standard or High priority.

6. In the Archive tier extension Configuration dialog, click **OK**.

Start/Pause Automatic Operations

You can pause and start all automatic Surveillance Bridge operations for a specific recording storage/archive. It's important to keep in mind that pausing/starting automatic operations concerns both moving data to the extension as well as backing up data, if Disaster Recovery is enabled for the same recording storage/archive. Additionally, even if automatic Surveillance Bridge operations are started for the extension, but later on you enable disaster recovery for the same recording storage/archive, by default the automatic operations will be paused, until you manually start them again.

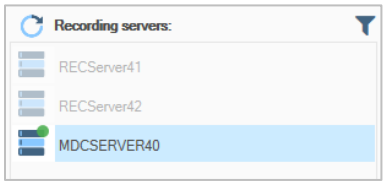
While automatic operations are paused, Surveillance Bridge stops automatically moving any data to the extension, but already moved data remains accessible from the extension, when you want to review it in the VMS Smart/Video Client, for example. While automatic Surveillance Bridge operations are paused for a recording storage/archive, you can also manually move data to the extension, following the steps in "Manually Manage Data".

Once you resume automatic operations, Surveillance Bridge immediately begins parsing data on your recording storage/archive and resumes processing the queue with files scheduled to be moved to the extension.

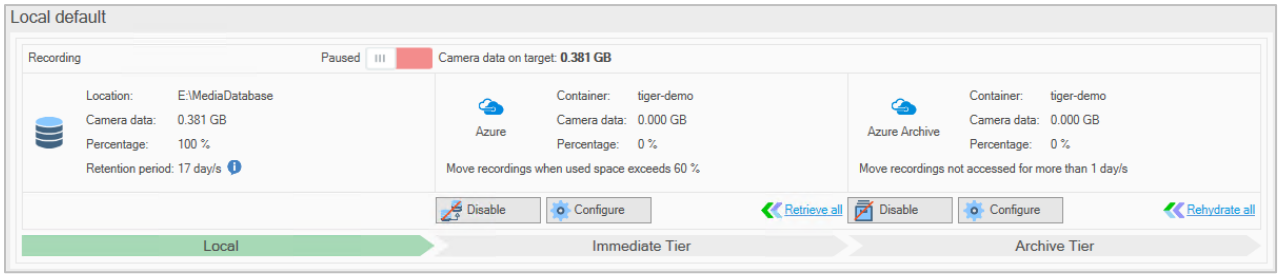
To start/pause automatic operations for a recording storage/archive:

1. In the Navigation pane of the Management Client, click **Extension** under Surveillance Bridge.

2. In the right pane under Recording Servers, click the recording server, whose recording storage or archive you want to extend.



The Surveillance Bridge plug-in lists all recording storage/archives configured for the selected recording server.



3. At the top of the recording storage or the archive pane, do one of the following:

- Switch the setting to **Running** and when prompted, confirm that you want to start automatic Surveillance Bridge operations.
- Switch the setting to **Paused** and when prompted, confirm that you want to pause automatic Surveillance Bridge operations.

Monitor Immediate Tier Extensions

The Extensions page of the Surveillance Bridge Plug-in provides you with all information necessary to keep track of the status of a recording server, its recording storage(s)/archive(s), their extension(s) and the distribution of data between them.

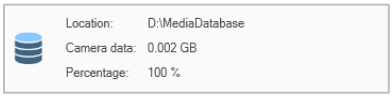
Monitor Recording Servers

To view the status of all recording servers, in the Navigation pane of the Management Client, click **Extension** under Surveillance Bridge and then check the Recording servers pane:

Indicator	Status	Tooltip
Green blinking indicator	The recording server and its recording storage(s)/archive(s) are operating normally. If an extension is enabled for a recording storage/archive, all necessary data is fully copied to the extension.	Healthy online
Yellow blinking indicator	The recording server is operating normally, but either the extension is inaccessible or Surveillance Bridge could not copy one or more files. Check for changed credentials to the extension or connectivity problems or the Windows Event Viewer log for the paths of the files, which could not be copied.	Target is offline
Red blinking indicator	The recording server is operating normally, but Surveillance Bridge has detected one or all of the following problems:	
	A recording storage or archive is not responding and Surveillance Bridge cannot copy its data to the extension.	Storage is not responding
	A recording storage or archive has failed.	Storage is offline
	Surveillance Bridge has failed to perform a scheduled operation.	Generic error
Greyed out icon	One of the following problems has been detected:	
	Surveillance Bridge is either not installed or not responding on the recording server.	Server is offline
	The recording server is offline.	Recording server is offline

Monitor Recording Storage/Archive

The pane of a recording storage or an archive gives you the following information:



Location - the path on the recording server, on which the respective recording storage/archive is mounted

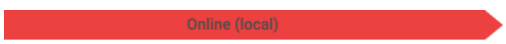
Camera data - the total size of recordings accessible directly from the recording storage/archive

You can view the total size of camera data both on the recording storage/archive and on any of the extensions in the Camera data on target field above each listing.

Percentage - the percentage of recordings accessible directly from the recording storage/archive

Additionally, the color label below a recording storage/archive's pane shows you its status on the recording server:

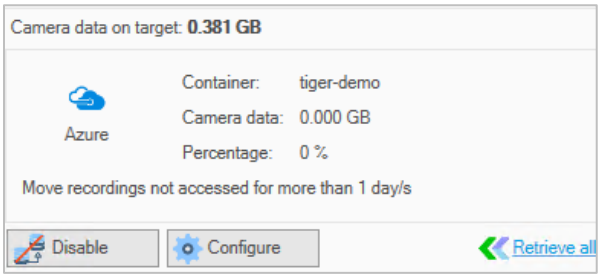
the recording storage/archive is available



the recording storage/archive is not available to the recording server

Monitor the Extensions

The panes of the immediate and the archive tier extensions, displayed next to the pane of the respective recording storage/archive, give you the following information:



Extension storage type - the pane displays the logo of the storage provider, on which the extension is located

Bucket/Container/Folder - displays the name of the bucket/container/folder, to which data from the recording storage/archive is moved

Camera data - the total size of recordings accessible only from the immediate/archive tier extension

---

Tip: You can view the total size of camera data both on the recording storage/archive and on any of the extensions in the Camera data on target field above each listing.

Percentage - the percentage of recordings accessible only from the immediate/archive tier extension

---

Note: Keep in mind that the percentage may never reach 100%, if the cameras recording on the respective recording storage are continuously writing data on it.

Additionally, the color label below the immediate/archive tier extension's pane shows you its status:

- automatic Surveillance Bridge operations are started for immediate tier extension

- automatic Surveillance Bridge operations are started for archive tier extension

- the immediate/archive tier extension is either not enabled or automatic Surveillance Bridge operations for the extension are paused and you can move data to it only manually

V. Surveillance Bridge Plug-in

The Surveillance Bridge plug-in provides you with the following features:

- additional timeline data that displays the origin of the recording you are reviewing - local, the immediate tier extension or the archive tier extension.
- automatic retrieval of recordings from the extension - allows you to retrieve camera in real-time while reviewing it on the timeline.
- manual retrieval of recordings from the extension - allows you to manually retrieve camera data from the extension to the recording storage/archive for a selected time interval.

An administrator of your VMS can enable or disable most of these features for a specific recording server in the Surveillance Bridge Plug-in. For more details, refer to Configure Smart/Video Client Integration.

For more information about using the above options on a Smart/Video Client computer, refer to Work with the Smart/Video Client Plug-in.

Configure Smart/Video Client Integration

In the Surveillance Bridge plug-in for your Management Client, you can enable or disable any of the VMS Client integration features for a specific recording server. Enabling or disabling any of the features is valid for all VMS Client computers reviewing footage from the same recording server.

Enable/Disable Manual Data Retrieval

When you enable manual data retrieval from the extension, you allow users on the VMS Smart/Video Client to retrieve camera recordings within a selected period from the extension to the recording storage/archive. The operation is identical to manual data retrieve operation initiated in the Surveillance Bridge plug-in for the Management Client and appears as a job in the manual operation jobs queue.

Enabling manual data retrieval may be especially useful, when automatic retrieval is disabled, but you still want to allow VMS Client users to be able to work with recordings available only on the extension.

Note: Manual data retrieval operations retrieve all data for the specified time interval and not just the frames currently being played as is with automatic retrieval of recordings.

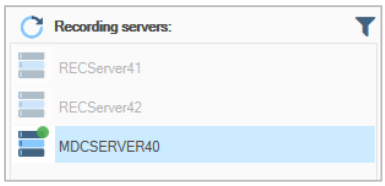
When both automatic and manual data retrieval are disabled, should a user attempt to review a recording stored either on the standard or the archive tier extension, the VMS Smart/Video Client player reports that the recording is standard or archive and does not play it.

By default, the manual retrieval of data is enabled on each recording server.

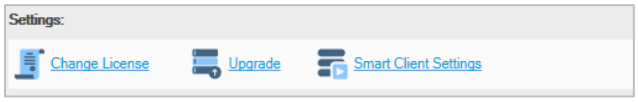
To enable/disable manual data retrieval:

1. In the Navigation pane of the Management Client, click **Administration** under Surveillance Bridge.

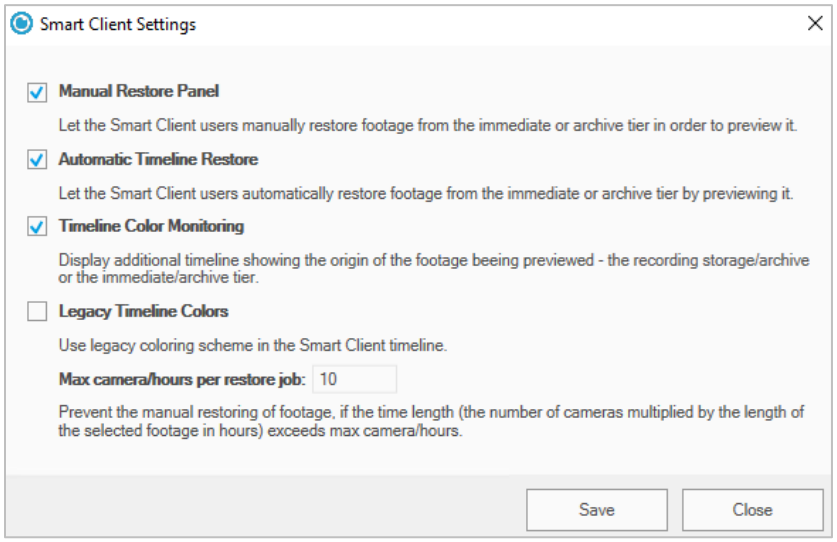
2. In the right pane under Recording Servers, click the recording server, whose integration features you want to manage.



3. In the middle, click **Smart Client Settings**.



4. In the dialog, do one of the following:



- Select the “Manual Restore Panel” check box, to display the manual restore panel in the VMS Smart/Video Client and allow users to manually retrieve data, then click **Apply**.
- Clear the “Manual Restore Panel” check box, to hide the manual restore panel in the VMS Smart/Video Client and prevent users from manually retrieving data from the extension, then click **Apply**.

Enable/Disable Automatic Data Retrieval

When automatic data retrieval is enabled for a recording server, a user reviewing recordings moved to the immediate tier extension automatically triggers the retrieval of the currently reviewed data on the recording storage/the archive. The retrieval of data from the immediate tier extension is typically in real-time as determined by the network and connection characteristics. To retrieve footage from the archive tier extension, you must first manually rehydrated it to the immediate tier extension. Surveillance Bridge is able to partially retrieve data to efficiently play timeline video during reviewing operations.

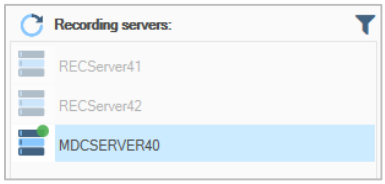
When automatic data retrieval is disabled, should a user attempt to review footage stored either on the standard or the archive tier extension, the VMS Smart/Video Client player will report that the recording is standard or archive and will not play it.

By default, the automatic retrieval of data is enabled on each recording server.

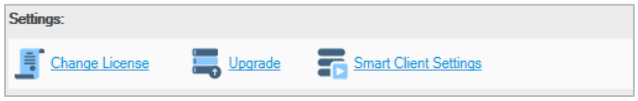
To enable/disable automatic data retrieval:

1. In the Navigation pane of the Management Client, click **Administration** under Surveillance Bridge.

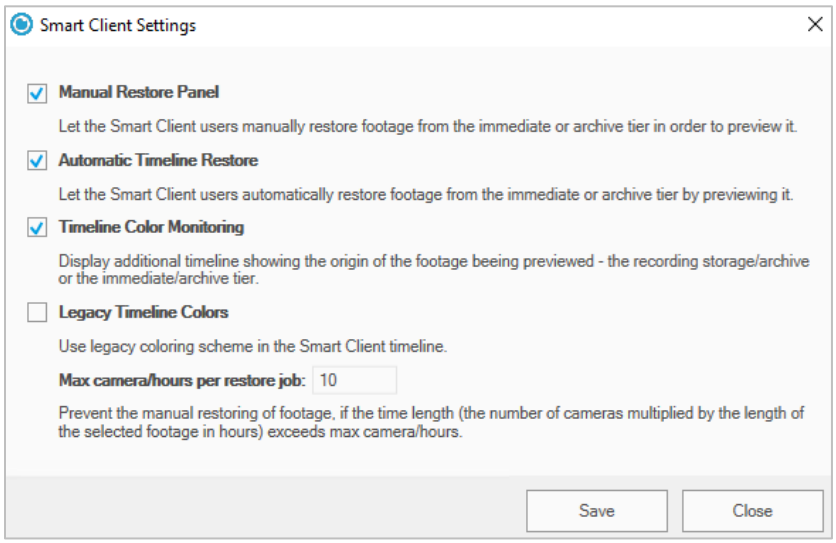
2. In the right pane under Recording Servers, click the recording server, whose Smart/Video Client integration features you want to manage.



3. In the middle, click **Smart Client Settings**.



4. In the dialog, do one of the following:



- Select the “Automatic Timeline Restore” check box, to let Surveillance Bridge retrieve data run time while users review it, and then click Apply.
- Clear the “Automatic Timeline Restore” check box, to prevent users from retrieving data run time when they attempt to review it, and then click Apply.

Enable/Disable the Additional Surveillance Bridge Timeline Data

When the Surveillance Bridge additional timeline data is enabled, it appears right below the default VMS Smart/Video Client timeline on the Playback tab. It changes color depending on the origin of the recording currently being reviewed indicating to users if the data is from the immediate or archive tier extension. When manual retrieval of data from the extension is also allowed, Surveillance Bridge allows users to easily select the section of the recording they want to retrieve locally or to manually rehydrate from the archive tier extension.

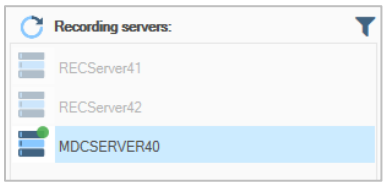
When the additional Surveillance Bridge timeline data is disabled, but automatic retrieval from the extension is enabled, you can still review footage originating from the immediate tier extension.

By default, the additional Surveillance Bridge timeline data is enabled on each recording server.

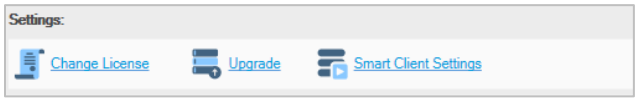
To enable/disable the additional Surveillance Bridge timeline data:

1. In the Navigation pane of the Management Client, click **Administration** under Surveillance Bridge.

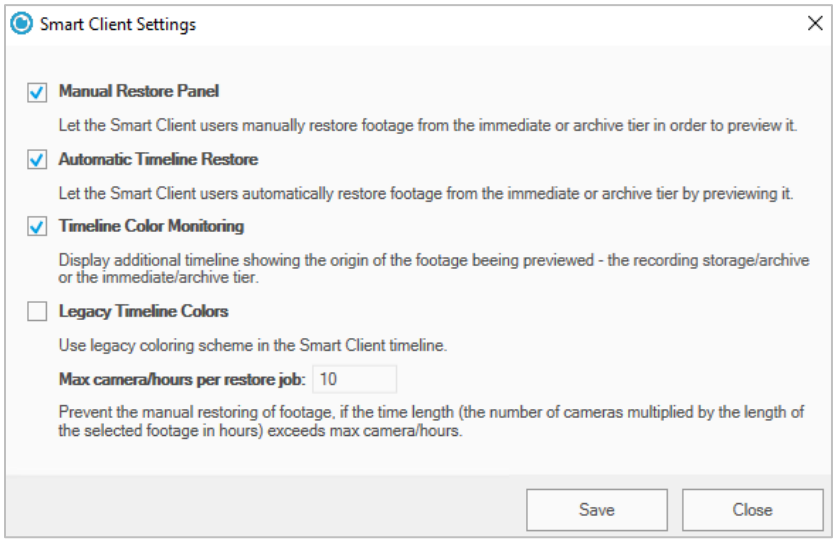
2. In the right pane under Recording Servers, click the recording server, whose Smart/Video Client integration features you want to manage.



3. In the middle, click **Smart Client Settings**.



4. In the dialog, do one of the following:



- Select the “Timeline Color Monitoring” check box, to allow displaying the additional Surveillance Bridge timeline data on each VMS Smart/Video Client reviewing footage from this recording server and then click Apply.
- Clear the “Timeline Color Monitoring” check box, to hide the additional Surveillance Bridge timeline data on each VMS Smart/Video Client reviewing footage from this recording server and then click Apply.

Enable/Disable Legacy Timeline Colors

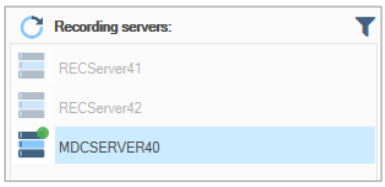
The legacy timeline colors previously used with Surveillance Bridge were green for locally accessible data, orange for data available with Immediate tier extension and light blue for data available only after retrieval from Archive tier extension. You can still use them with this setting. The new colors which currently come with Surveillance Bridge are green for locally accessible data, light blue for data available with Immediate tier extension and dark blue for data available only after retrieval from Archive tier extension.

By default, legacy timeline colors are is disabled.

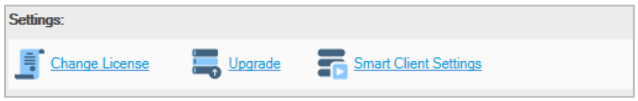
To enable/disable automatic switching to primary server cameras:

1. In the Navigation pane of the Management Client, click **Administration** under Surveillance Bridge.

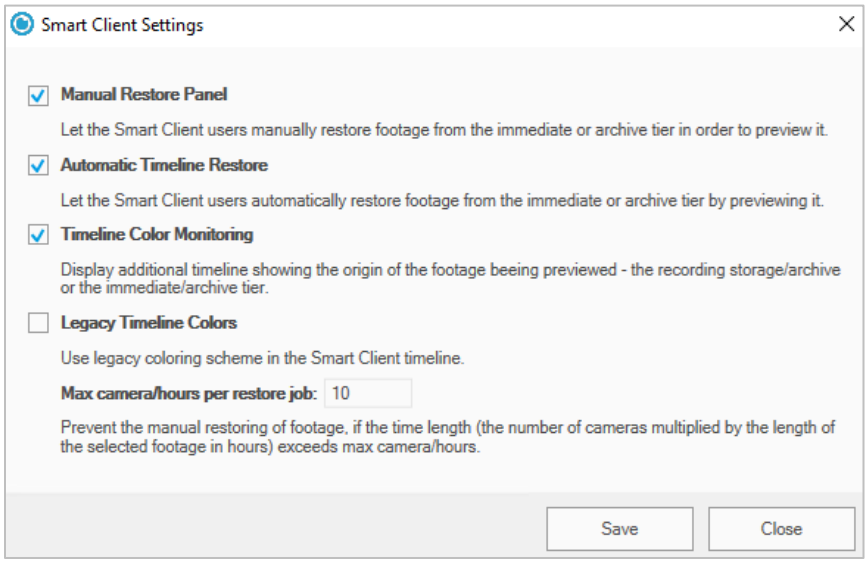
2. In the right pane under Recording Servers, click the recording server, whose Smart/Video Client integration features you want to manage.



3. In the middle, click **Smart Client Settings**.



4. In the dialog, do one of the following:

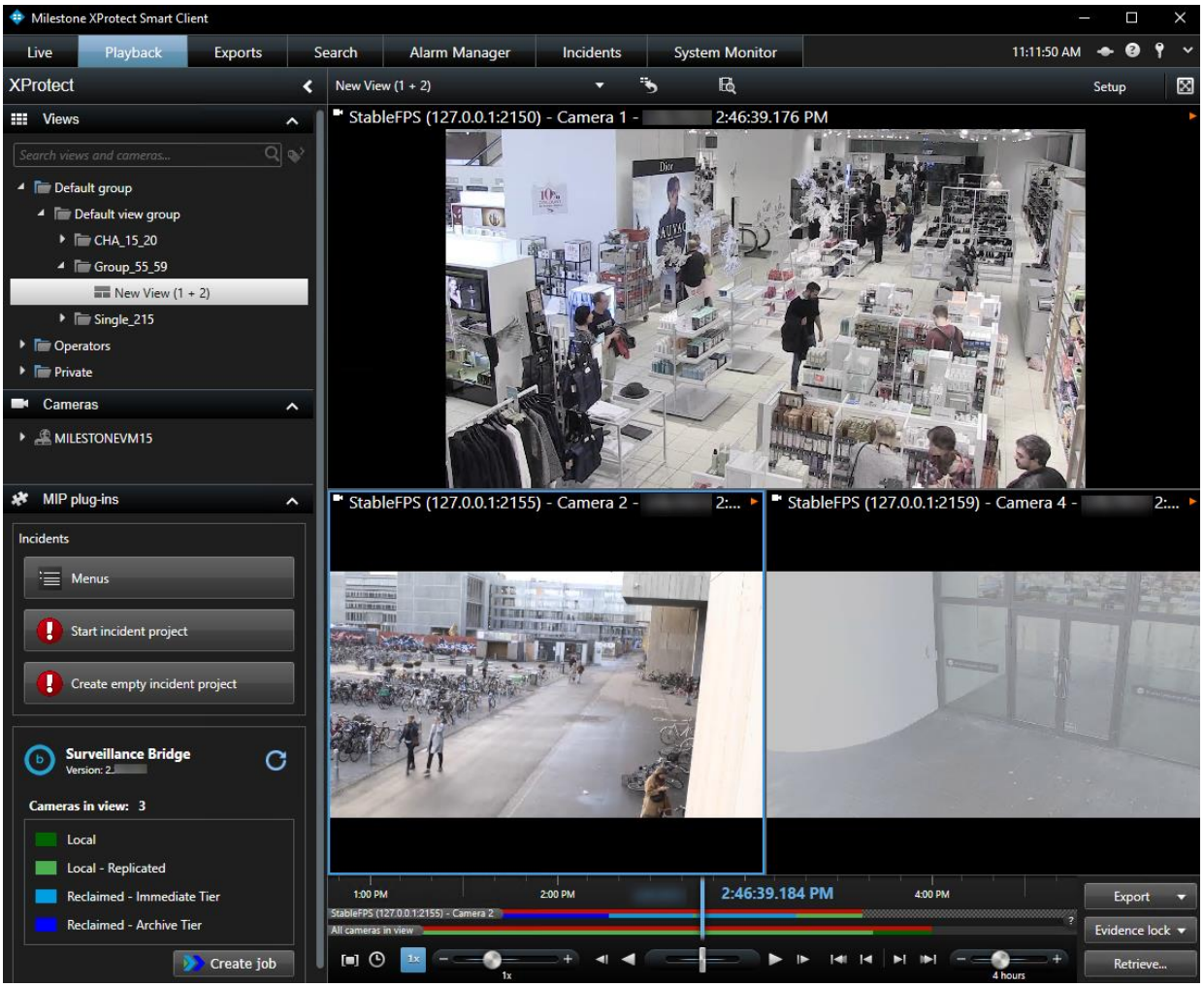


- Select the “Legacy Timeline Colors” check box, to switch to the old green – orange – light blue color scheme, then click Apply.
- Clear the “Legacy Timeline Colors” check box, to use the new green – light blue – dark blue color scheme, then click Apply.

Work with the Smart/Video Client Plug-in

When the Surveillance Bridge plug-in is installed on a VMS Smart/Video Client, it appears in the MIP Plug-ins pane in the Playback tab. It complements your VMS Smart/Video Client workflow with the following additional features:

- additional timeline data, which shows you whether a recording is accessible from the local recording storage/archive, the immediate tier or the archive tier extension.
- real-time retrieval of recordings from the immediate tier extension by reviewing or exporting them in the Smart/Video Client.
- panel for manual retrieval of recordings within a specified time range from the immediate/archive tier extension.



The Surveillance Bridge Timeline

Note: To be able to view the Surveillance Bridge timeline information, configure your Smart/Video Client to display additional timeline data - in Settings, click Timeline and in the Additional data drop-down box, select Show.

When enabled through the Management Client plug-in, the additional Surveillance Bridge timeline appears right below the Smart/Video Client player timeline both for a selected camera in the pane and for all cameras.

It gives you the following information:

the recording is accessible directly from the recording storage or the archive.

the recording is accessible directly from the recording storage or the archive and is already replicated to the target storage.

the recording is accessible only from the immediate tier of the recording storage or the archive. Reviewing the recording depends on the setting for automatic and/or manual retrieval of data from the extension.

the recording is accessible only from the archive tier extension of the recording storage or the archive. Reviewing the recording depends on the setting for automatic and/or manual retrieval of data from the extension.

Important: Whether or not a recording is available locally or only through the extension, your VMS metadata is kept and the Smart/Video Client timeline displays the markers for recordings with or without motion.

Work with Standard or Archive Recordings

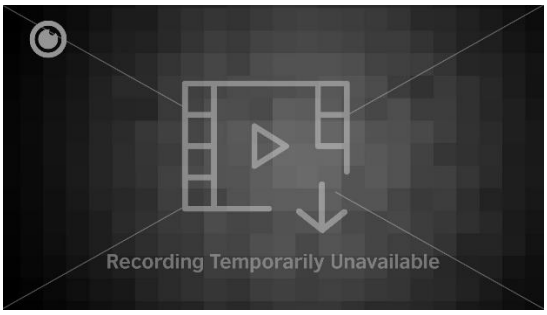
Note: Keep in mind that retrieving data from most cloud targets may be associated with additional costs.

As long as automatic retrieval of recordings is enabled for a recording server, you can play, export or lock its recordings as you would normally do with recordings stored on the recording storage or the archive. With standard recordings (marked in orange in the Surveillance Bridge timeline) the retrieve operation depends on the network and connection speed to the immediate tier extension. In most cases this should be in real-time with minimal delay. With offline recordings (marked in blue on the timeline), data must first be retrieved to the standard storage tier. Once retrieved and in the immediate tier extension, the timeline data can be retrieved to the local storage and will display green on the timeline.

If automatic retrieval of data is disabled for a Recording server, attempting to play or export or lock recordings available from the immediate or archive tier extension will fail and the recordings will be displayed in the Smart/Video Client player with one of the following thumbnails:

A recording on an Immediate Tier extension

A recording on an Archive Tier extension



A recording that is currently unavailable

If manual retrieval from the extension is enabled for the recording server, to play or export such recordings,

Manually Manage Data

Using the Surveillance Bridge Plug-in, you can manually move data between a selected recording storage or archive and its immediate/archive tier extension. This way you can move data, which does not yet meet the criteria you have specified for the extension. You can perform manual operations for data recorded by all cameras on a selected recording server or just for a selected one. You can also limit the number of recordings you perform the desired manual operation on for a selected time interval only.

Additionally, the manual operations are indispensable for Surveillance Bridge's disaster recovery mechanism. When you recover backed up data, it is retrieved from the disaster recovery storage in the form of stub files. To retrieve the actual recordings, you should either review them in the Smart/Video Client (on-demand data retrieval) or by executing a manual data retrieval job, following the steps in "Recover Backed Up Data".

You can perform manual data operations even if automatic Surveillance Bridge operations for the recording storage or archive have been paused. Manually initiated operations take precedence over automatic operations, i.e. until the manual jobs queue is processed, Surveillance Bridge does not perform any automatic operations.

Manually Manage Data

To manually manage data, you must create a separate job for each of the following operations:

 move data to be available locally - retrieve back selected data from the extension and make it accessible directly from the respective recording storage or archive. You can use this operation to actually recover backed up data, in case of disaster.

Important: Keep in mind that the operation requires enough free space on your recording storage/archive to accommodate all data retrieved from the extension.

 bring back archived data - rehydrate recordings from the archive tier extension of a recording storage or archive and make them accessible from the immediate tier extension, which allows their automatic retrieval upon request from a Smart/Video Client computer as soon as the connection speed allows.

Note: If you execute this job for recordings which are not replaced by stub files on the recording storage/the archive i.e. data is still available locally, Surveillance Bridge will move these files to the standard tier of your cloud target, but their status will remain online until they are replaced with stubs, based on the standard policy.

 make data standard to free local storage space - move data to the immediate tier extension and replace it on the recording storage/archive with stub files, which point to the copies on the immediate tier extension, but take no space on your local storage.

 archive data - move data from the immediate tier extension to the archive tier extension.

Important: If you select to perform the above operation for recordings that are still stored on your recording storage or archive, they will first be moved to the immediate tier extension and only after that to the archive tier extension.

Note: If some data for the specified time period does not yet meet the criteria for space reclaiming, it will remain accessible locally and will be reported as offline only after it is replaced by stub files.

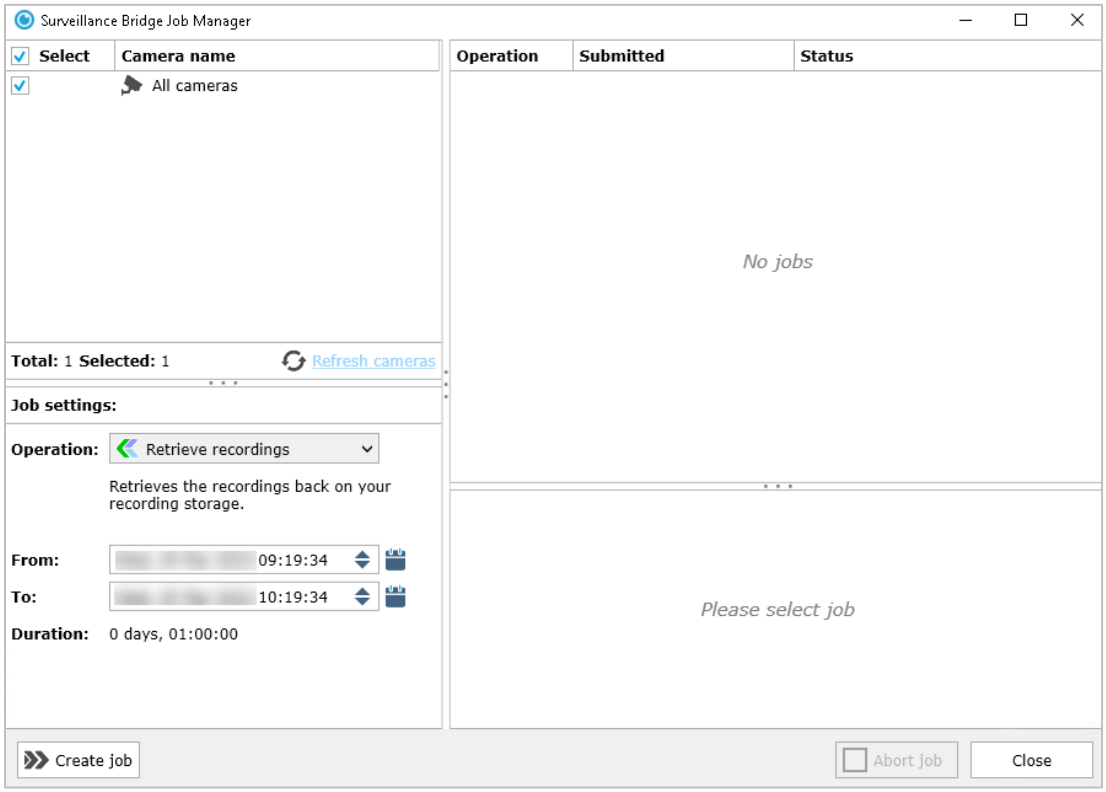
You can create as many manual operation jobs as you wish. Once you create a job, it is automatically added to the end of the jobs queue. Surveillance Bridge processes the queue one job at a time, starting with the first in line. You can monitor the jobs queue, following the steps in the

Monitor Manual Jobs Status section.

Manage Jobs with the Standard Surveillance Bridge

To create a manual data operation job:

1. Start the Surveillance Bridge Job Manager (a desktop icon gets created with the installation).
2. Then do the following:



- Select the cameras you are interested in, potentially all cameras
- In the Operation drop-down box, select the type of operation
- Select the start and end time of the recordings in the respective boxes

> **Note**: Click next to the From or To box, to display the Calendar and more easily navigate to the respective date or enter the respective start/end time.

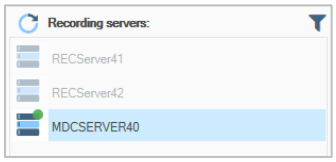
3. Click **Create job**.
4. When prompted, confirm that you want to manually move the specified amount of data between the recording storage/the archive and the immediate or archive tier extension.
5. The job appears on top of the jobs queue pane. You can monitor its status on the right.

Manage Jobs with the Surveillance Bridge Plug-in

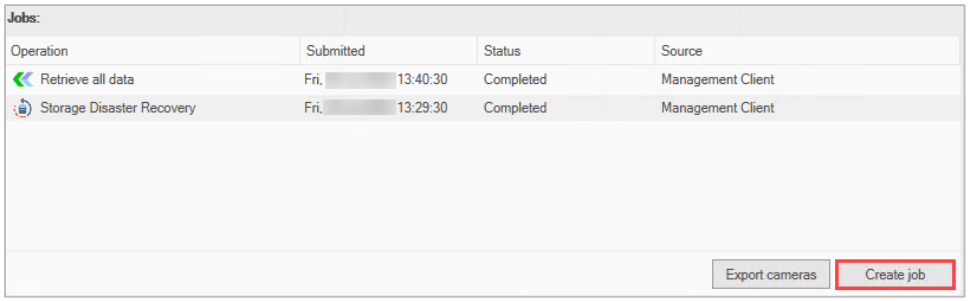
To create a manual data operation job:

1. In the Navigation pane of the Management Client, click **Administration** under Surveillance Bridge.

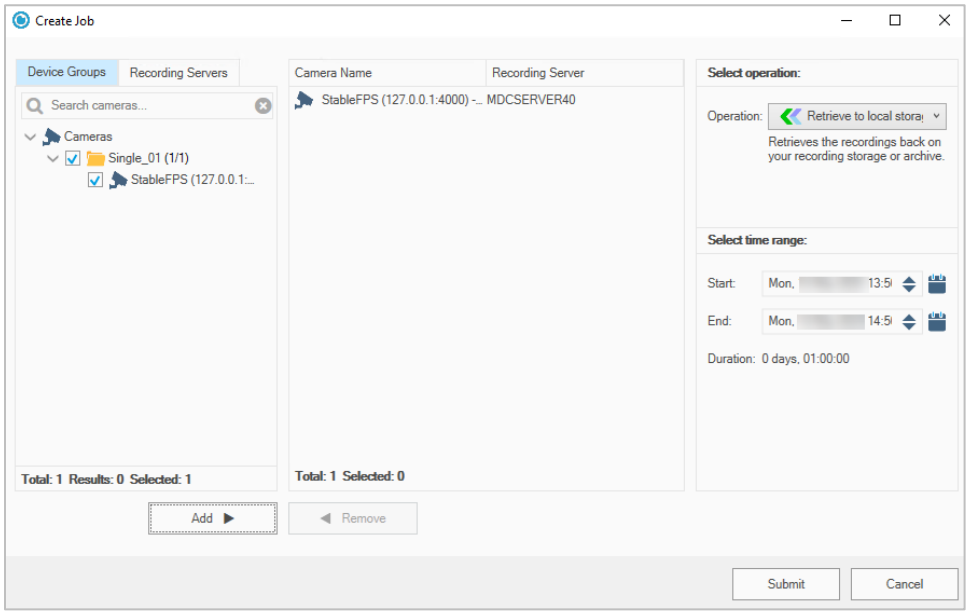
2. In the right pane under Recording Servers, click the recording server, whose recording storage or archive data you want to manually manage.



3. Under the Jobs pane, click **Create job**.



4. In the Job parameters pane, do the following:



- Choose Device Groups or Recording Servers and use the search box if needed to select the camera(s), whose recordings you want to manually manage.
- Click the **Add** button to select the desired camera(s)
- Click the **Remove** button to remove wrongly selected camera(s)
- In the Operation drop-down box, select the type of operation.
- Select the start and end time of the recordings in the respective boxes.

Note: Click next to the From or To box, to display the Calendar and more easily navigate to the respective date or enter the respective start/end time.

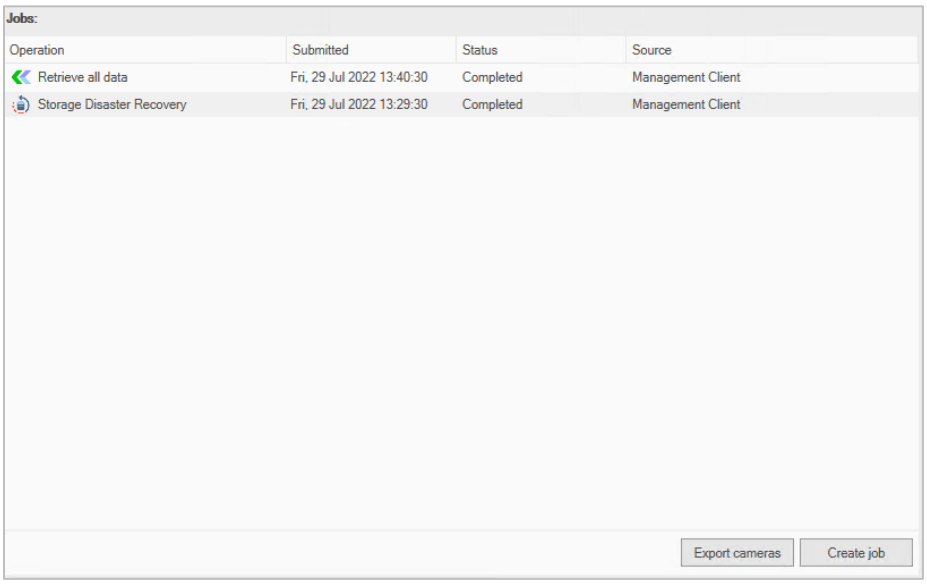
5. Click **Submit job**.
6. When prompted, confirm that you want to manually move the specified amount of data between the recording storage/the archive and the immediate or archive tier extension.

   The job appears on top of the jobs queue pane. You can monitor its status, following the steps in the

Monitor Manual Jobs Status section.

Monitor Manual Jobs Status

The Jobs queue pane displays the list of all jobs, arranged in descending order starting with the most newly added job. If you have allowed users to manually retrieve footage from the immediate/archive tier extension through the Smart/Video Client plug-in, the list also includes jobs initiated there.



The listing of each job gives you the following information:

- type of the manual operation
- date and time the job has been submitted
- status of the job
    - Completed - the job has been successfully completed
    - Pending - Surveillance Bridge is still processing the manual operation job and may display a progress bar
    - Completed (failed) - Surveillance Bridge's attempt to perform the manual operation has failed. The reason for the failed operation may be temporary inaccessibility of the extension, for example. Click Retry next to a failed job to queue it again in the list.
- source - whether the manual operation job has been submitted through the Management Client Plug-in or through the Smart/Video Client Pflug-in.

Note: To clear the jobs queue, you must restart the respective recording server.

Revisions Record

Revisions			
Date	**Description**	**Page(s)**	**Version**
03 Feb. 2020	Initial Draft		
16 Sept. 2020	Recovering a failed recording server and recording storage/archive data using the Surveillance Bridge Disaster Recovery Wizard steps added.	38	1.1
19 Feb. 2021	Added support for OpenStack Swift extension/disaster recovery storage.	12, 15	1.2
19 Feb. 2021	Added support for Seagate CORTX extension/disaster recovery storage.	12, 15	1.2
29 Jul. 2022	New layout, formatting and pictures.	All	
08 Apr. 2023	Revised for the new version and branding of the product.	All	2.0

Tiger Surveillance

About This Guide

The Surveillance Bridge Administration Guide provides details about the set up and usage of the product.

Tiger Surveillance's web site has the latest product information for further information:

https://www.tiger-surveillance.com/

Contact a Tiger Surveillance Support representative if you need assistance:

support@tiger-surveillance.com