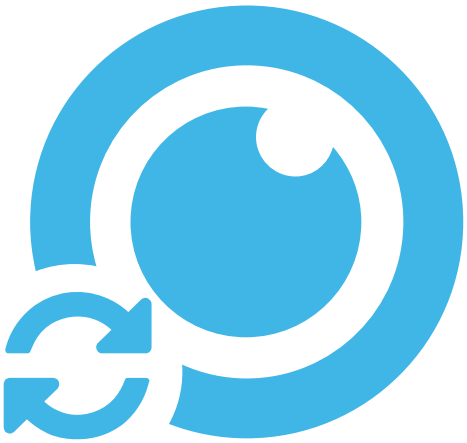
Tiger Surveillance

Surveillance HA

Administration Guide

Version: 2.0

Revision: April 2023



Title: Surveillance HA Administration Guide

Software version: 2.0

Date: April 2023

Table of Contents

Surveillance HA 1

I. Introduction to Surveillance HA 4

Surveillance HA Licensing 4

System Requirements 4

General Requirements 4

II. Surveillance HA Installation and Activation 5

Install Surveillance HA 5

Activate Surveillance HA 8

Upgrade Surveillance HA 9

Uninstall Surveillance HA 10

III. Manage High Availability 11

Server Cloning 12

How it Works 12

Prerequisites for a Server Cloning Configuration 12

Configure Server Cloning 13

Manage the Server Cloning 17

Monitor the Server Cloning 26

Camera Pairing 27

Camera Pairing Prerequisites 27

Configure Camera Pairing 27

Configure Camera Pairing Settings on the Server 31

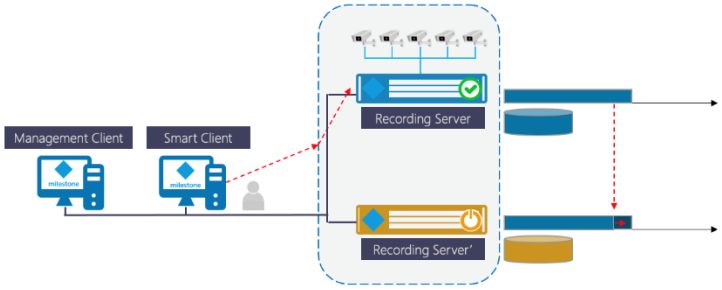
Revisions Record 36

About This Guide 37

I. Introduction to Surveillance HA

Congratulations on your purchase of the Surveillance HA product. It enhances your VMS (Video Management System) with additional high availability methods.

Surveillance Bridge HA provides you with a way to ensure against data loss and downtime. We have two different options for High Availability available – Server Cloning and Camera Pairing. In case of a failover condition (power failure, system crash, etc.) we have different methods for switching the camera feed from one recording server to another transparently.



For the current release of Surveillance HA, the four systems we support are: XProtect by Milestone, MOBOTIX HUB by Mobotix, Siveillance by Siemens and Velocity Vision by Identiv.

Surveillance HA Licensing

In order to benefit from Surveillance HA, you need to activate it on each recording server and for the specific intended purpose of it. For activation Surveillance HA makes use of a software as a service (SaaS). For more information, refer to "Activate Surveillance HA".

The license holds information about the type of the high availability that was purchased. 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 HA on a recording server, it must meet the following minimum requirements:

- PC with 64-bit (x64) processor.
- 64-bit Microsoft Windows® 7/Server 2008 R2/Windows® 8/Server 2012/Server 2012 R2/Windows® 10/Server 2016/Server 2019.
- 4 GB of physical RAM at least.
- 30 MB of available hard-disk space for Surveillance HA installation.

• 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:

- ✓ **443** – outbound rule only (for SaaS activation)
- ✓ **9701** – inbound rule only (for the HA Arbiter)
- ✓ **9702** – inbound rule only (for the HA REST Service)
- ✓ **9706** – inbound rule only (for the HA RPC communication)
- ✓ **9710/9707** – inbound rule only (for intermediate communication between Surveillance HA and Surveillance HA software modules)

To benefit from our tight integration with the VMS' Clients, make sure to install the respective Surveillance Bridge module.

Digital Certificate Requirements

Surveillance HA 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 HA and/or its modules. If the computer, on which you want to install Surveillance HA or any of its modules, 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.

II. Surveillance HA Installation and Activation

Install Surveillance HA

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

- Management Client module – is a module which adds our Surveillance HA menu in the Management Client's graphical user interface. This module should only be installed on machines with the Management Client installed. Should be installed on at least one to allow for licensing and policy configuration;
- Recording Server module – the HA engine. It must be installed on all recording servers as it manages the clustering and backfilling services;
- Smart Client module – our module which is installed on machines with the Smart Client to enable the additional Surveillance HA features within the client. It is required for Camera Pairing configurations and optional for Server Cloning ones. Used for switching cameras between the servers;

- Event Server – just a service with no graphical user interface that sends Surveillance HA 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 HA interface that allows for configuring which events should get logged. This is an optional module but if this Event Server module is not installed, that section in the configuration will not be functional;
- Management Server module – optional module which is not installed by default but might be required in specific configurations where arbitrations operations are needed as identified by the support team.

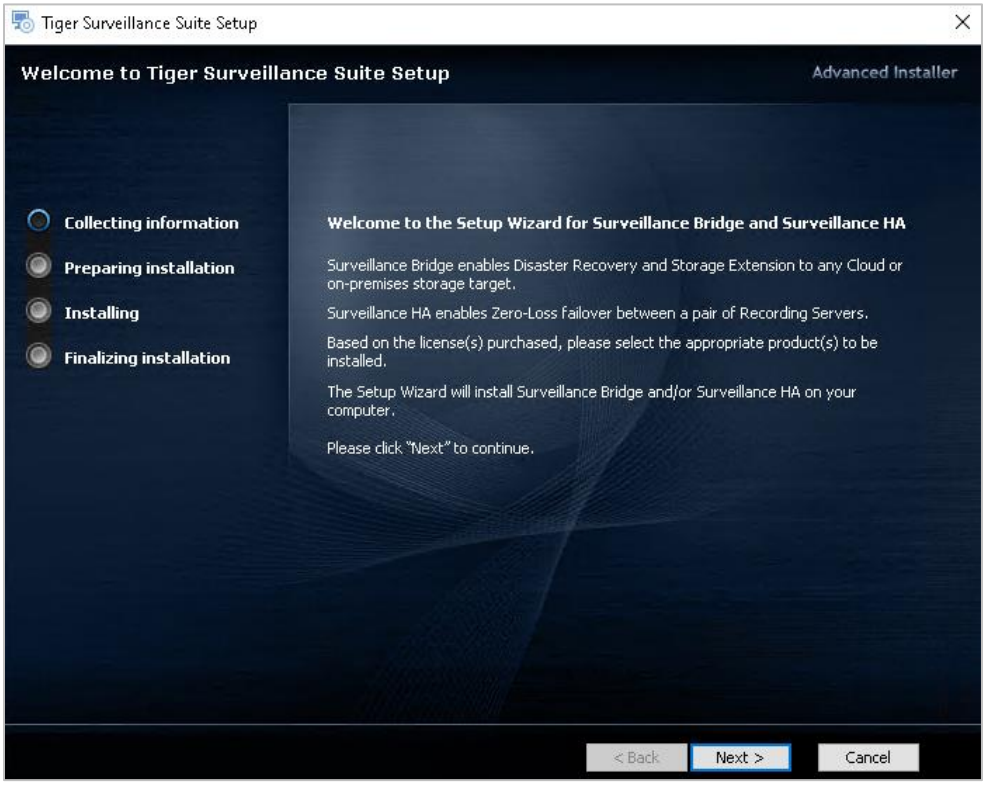
To install Surveillance HA:

1. Double-click the Tiger Surveillance Suite Setup installation file.

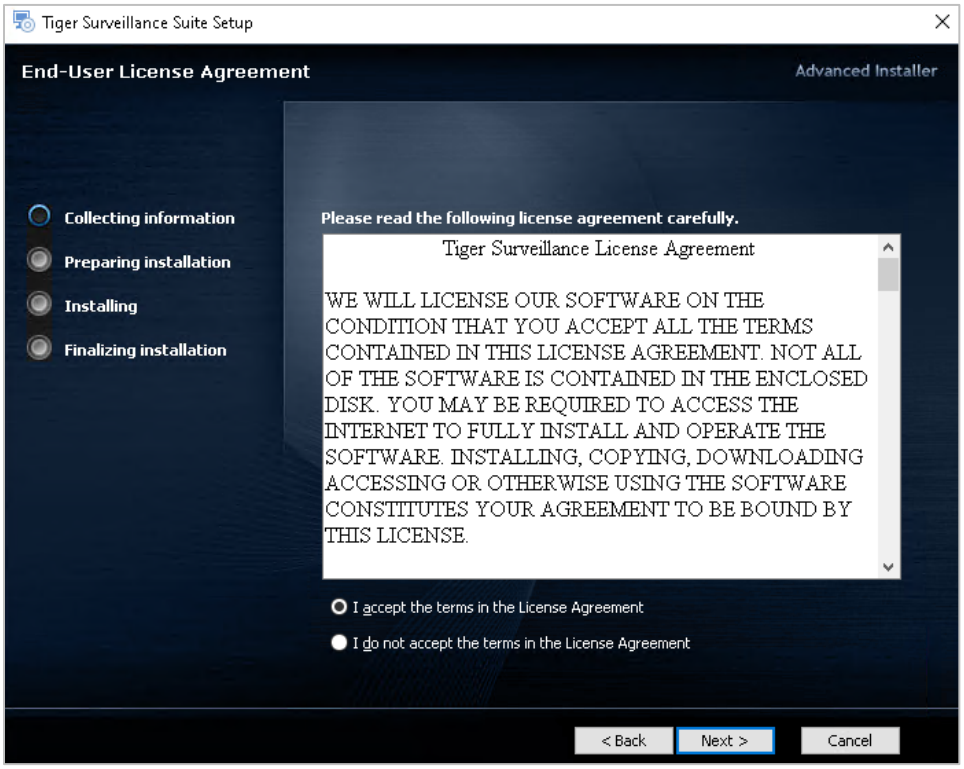
Note: If the setup wizard detects that prerequisites needed to run the Surveillance HA Client module are not installed on the computer, click next to install them.

---

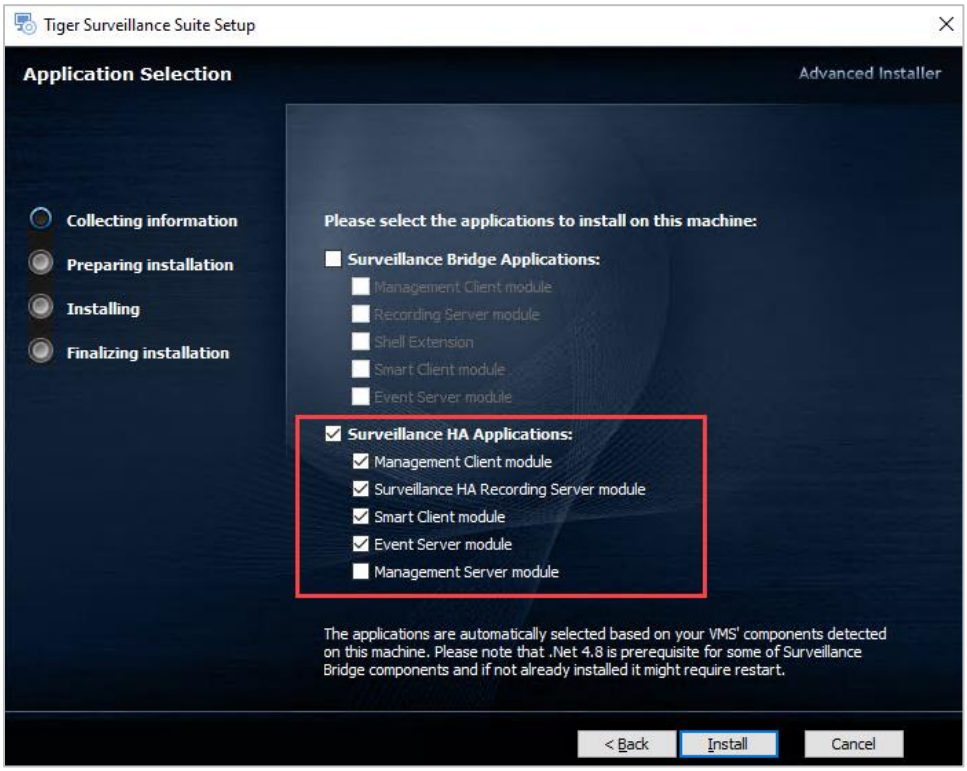
2. In the Tiger Surveillance Suite Setup installation wizard, click **Next**.



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 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 HA Applications section, then click **Install**.



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

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

Note: As visible in the installer itself, the .Net 4.8 software is a prerequisite for some Surveillance Bridge components and will also be installed, if not already present. It might require a system restart.

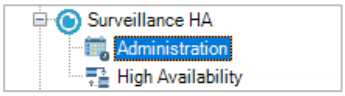
5. When the installation is complete, click **Finish**.

Activate Surveillance HA

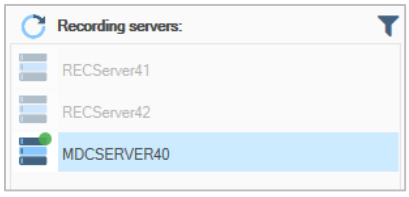
You can activate Surveillance HA using a software as a service (SaaS) license. You need to activate the product on each recording server, which you want to add in a high availability configuration. To enable more features once you have activated the product, simply repeat the activation procedure again.

To view the activation status of Surveillance HA on a recording server:

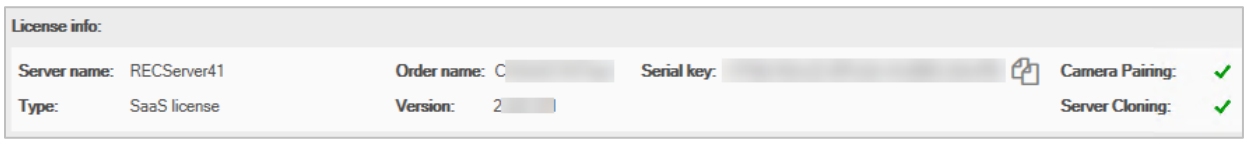
1. In the Navigation pane of your Management Client, click **Administration** under Surveillance HA.



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

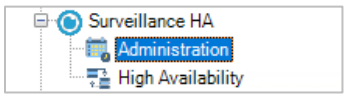


3. The License info pane displays the type of license, your serial key, the version of the product and the types of HA that you can configure for the specific server. If no such information is provided, you are yet to license your product.

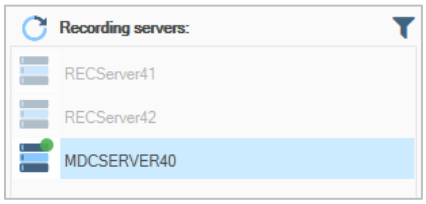


To activate a Surveillance HA on a recording server:

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



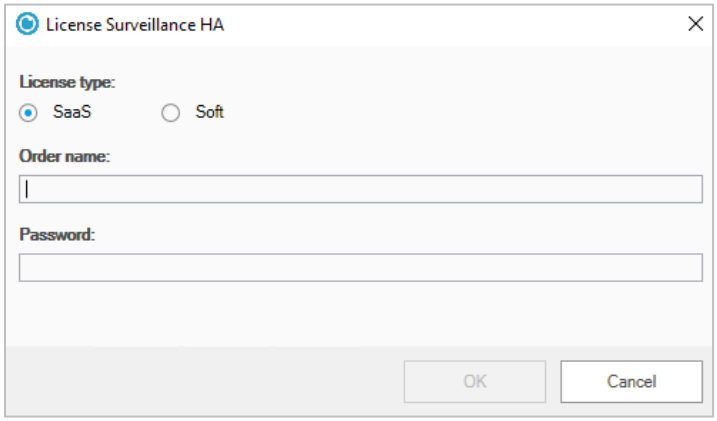
2. In the right pane under Recording Servers, click the recording server, which you want to activate.



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

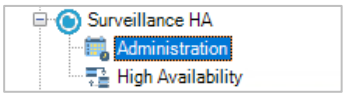


Upgrade Surveillance HA

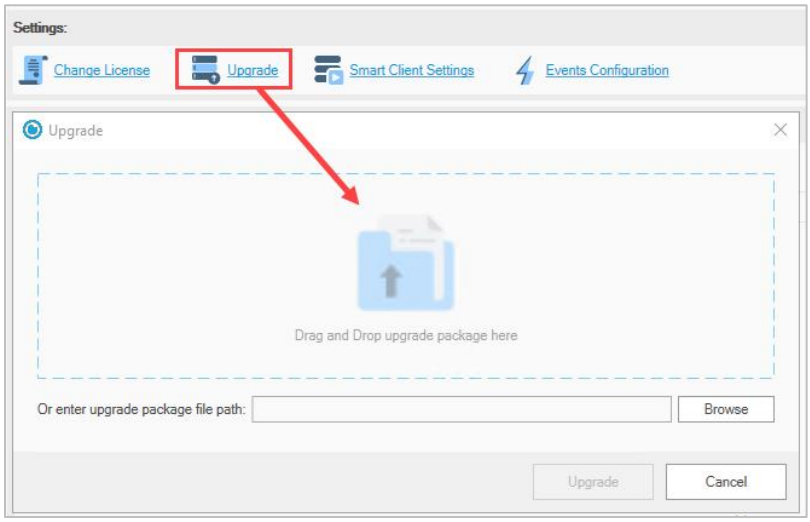
You can upgrade Surveillance HA when a new version comes out.

To upgrade Surveillance HA:

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



2. In the right pane, click on **Upgrade** and then Browse or Drag and Drop the upgrade package.



Uninstall Surveillance HA

You can uninstall Surveillance HA and any of its modules at any time.

When you uninstall Surveillance HA from a recording server, even if high availability is not first disabled, no further high availability services will be provided to the VMS as the partner recording server would not be able to exchange information any further.

However, if you uninstall Surveillance HA from the Management Client only, that would not disrupt the high availability services that have already been configured. Only their management (the ability to see and change the configuration) will be lost.

Uninstalling the Surveillance HA module from the Smart Client will simply hide the additional menu allowing you to switch the camera feed.

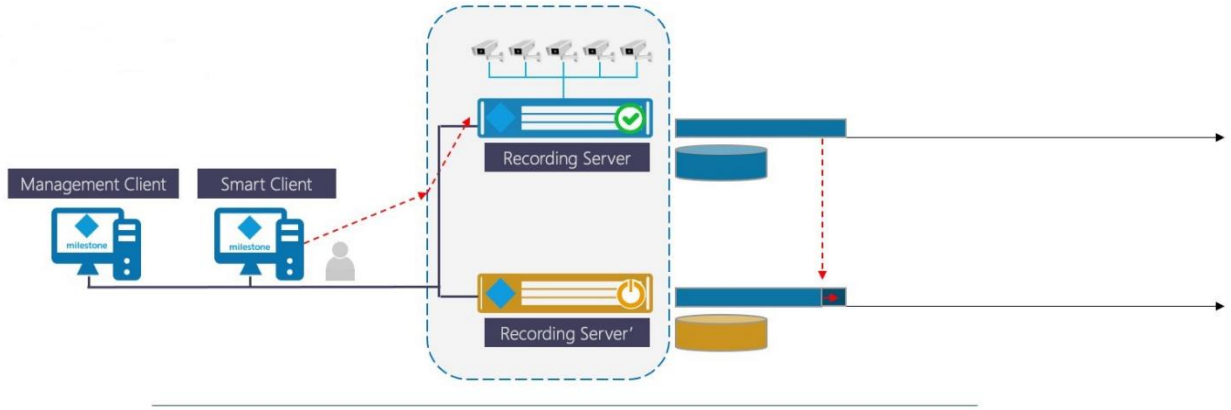
To uninstall Surveillance HA:

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

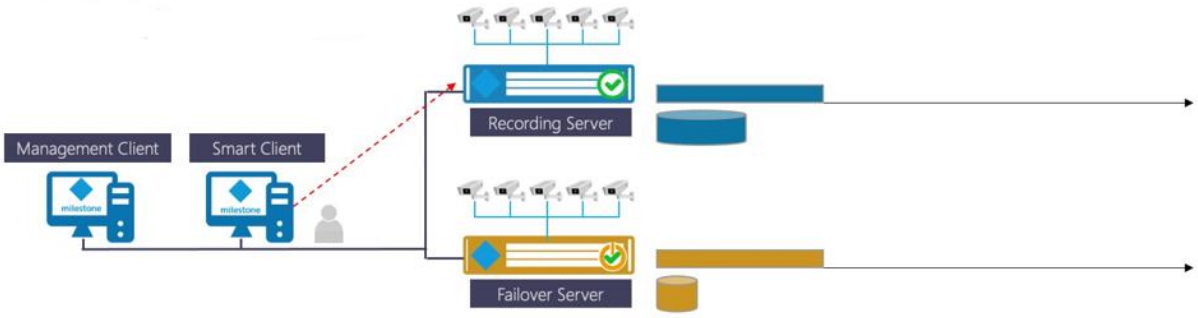
III. Manage High Availability

Surveillance HA provides you with yet another way to ensure against failure of a recording server or recording storages/archives. Apart from preventing data loss, the two high availability mechanisms of Surveillance HA guarantee continuity of service and transparent recovery.

Server Cloning - the method relies on a simple procedure that clones in a Server Cloning a recording server already in use on your VMS network with a stand-by recording server. In case of a failover condition (power failure, system crash, planned shutdown, etc.) the serving node of the cluster fully transparently and within seconds transfers its role to the stand-by recording server, which takes over recording data from the attached devices. The recording storages/archives of the two nodes are in constant synchronization, ensuring the stand-by server not only takes over writing new data, but can serve to Smart Clients all the already written data.



Camera Pairing - the method pairs identical cameras on two active recording servers into a high availability unity. Should one of the recording servers or its recording storage/archive fail, Smart Clients' access can be automatically redirected to the current and past recordings of the same camera on the other recording server. Once the problem is resolved, missing data is transparently synchronized on the recovered recording server's recording storage/archive.



Choosing one of the methods depends on your workflow and existing infrastructure. While the Camera Pairing method is more flexible, it is not suitable for environments, in which the network connection between a camera and the recording servers cannot handle writing two streams concurrently. Additionally, you cannot deploy Camera Pairing, if your VMS recordings are encrypted.

Server Cloning

How it Works

Once the nodes are linked in a Server Cloning, Surveillance HA writes newly recorded data on both recording servers instead of just one. Data is then mirrored between the two members of the pool, thus ensuring that in case of failure, the surviving node has the latest information and can serve the Smart Client requests.

Surveillance HA provides you with all necessary tools to monitor and manage the Server Cloning.

Prerequisites for a Server Cloning Configuration

Before you clone two recording servers into a Server Cloning, make sure that each of the following requirements is met:

- both recording servers have the Surveillance HA product module installed and activated
- only one of the recording servers have any devices attached in the VMS

It is also recommended for each volume with recording storage/archive on the active node there is a matching volume with identical drive letter and the same or bigger size on the stand-by node

---

Note: You can clone the Server Cloning nodes if at least one of their recording storage/archive volumes match but after failover no existing data from unmatched drives will be accessible to Smart Clients and no new recordings will be saved on unmatched drives.

- there is an identical account with administrative privileges on both cluster nodes
- both recording servers can communicate with one another over the network

---

Note: You can establish a dedicated network connection between the two server nodes to guarantee optimal data and metadata transfer between them.

- the stand-by recording server sees all recording devices attached to the active one
- the startup type of the Recording Server service on both nodes is set to Manual

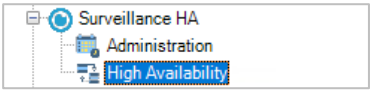
Configure Server Cloning

Before you proceed with the steps below, make sure that both your cluster nodes meet the requirements. Keep in mind that during the configuration procedure your recording server cannot record any data from attached devices. Once you finish the procedure, the cluster automatically takes over recording data.

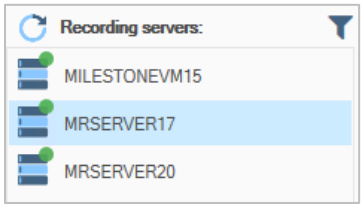
You can configure as many clusters as you want.

To configure Server Cloning:

1. In the Navigation pane of the Management Client, click **High Availability** under Surveillance HA.

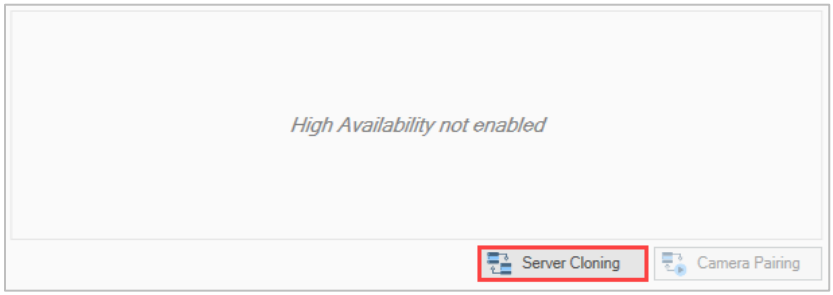


2. In the right pane under Recording Servers, click the recording server, which will play the role of the primary node in the Server Cloning, i.e. the recording server with devices already attached.

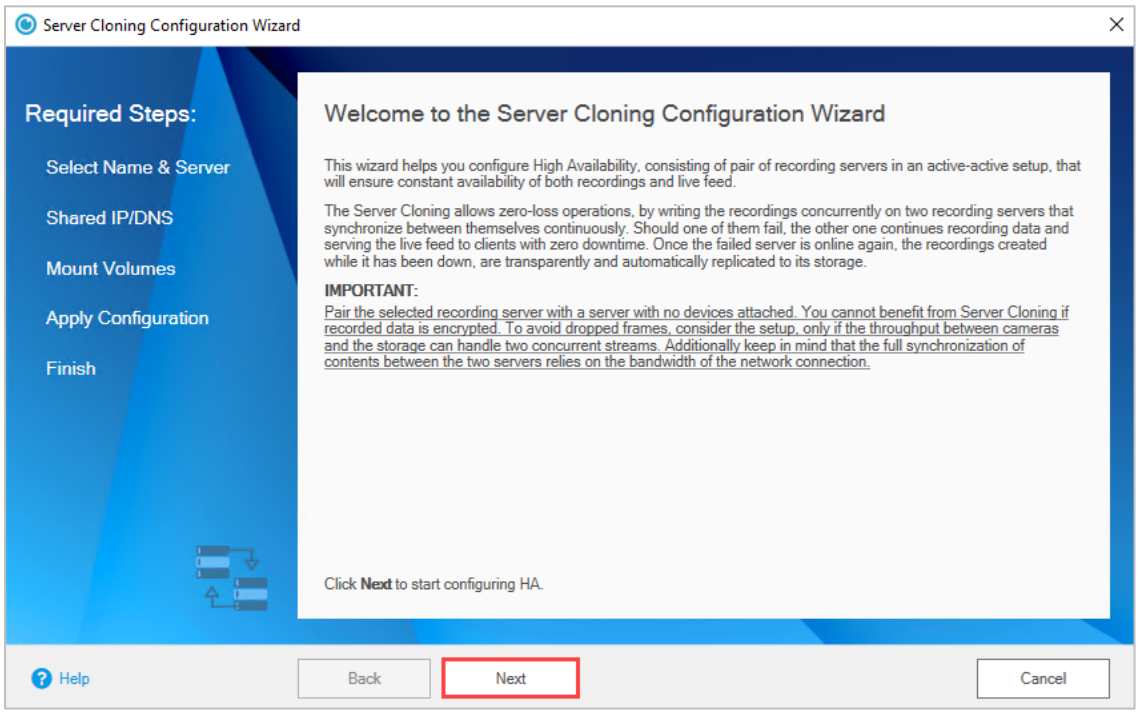


> **Note**: If a recording server is missing from the list, it is either already cloned in another cluster or does not match the requirements.

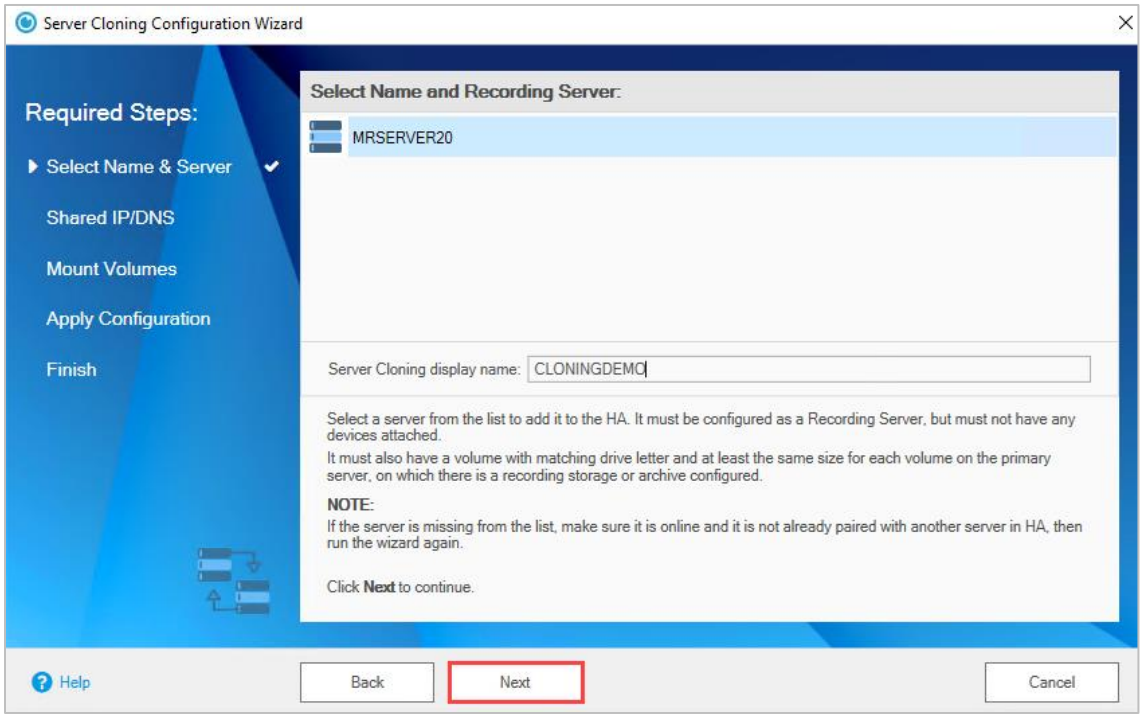
3. In the right pane, click **Server Cloning** to start the Configuration Wizard.



4. In the Welcome screen of the Server Cloning Configuration Wizard, click **Next**.



5. Select the recording server, which will play the role of the secondary node in the Server Cloning, i.e. the server with matching drives, but no devices attached and then click **Next**.



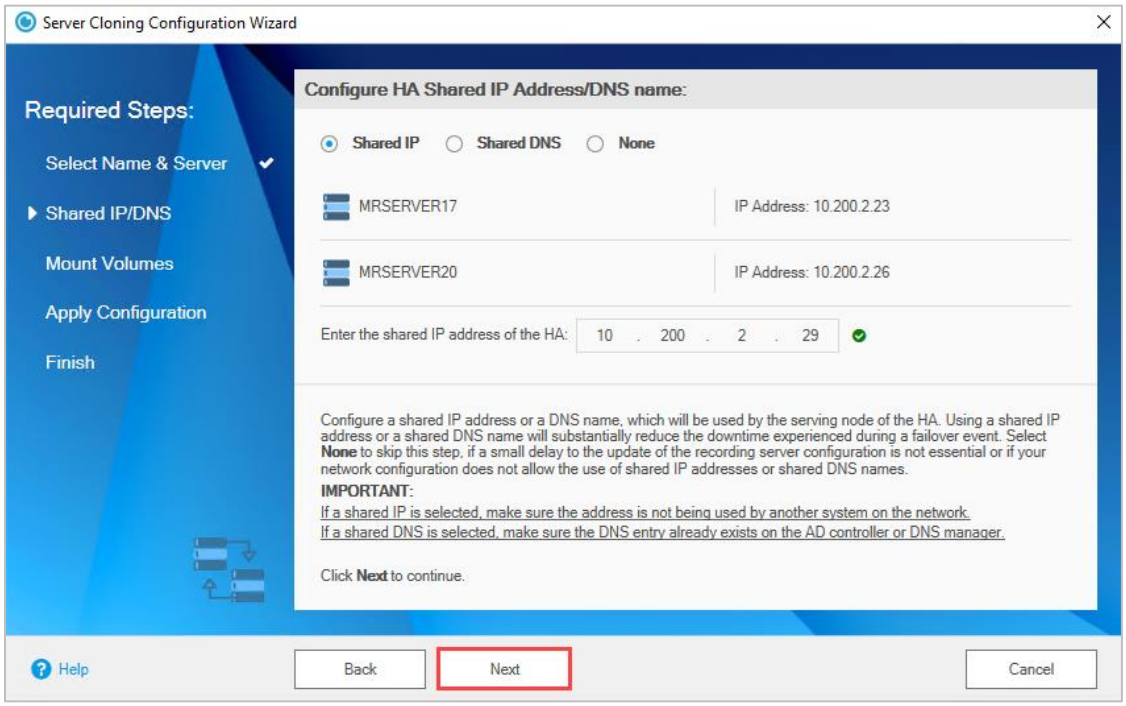
The Configuration Wizard will list both cluster nodes with their names and IP addresses and allows you to specify an IP address of the Server Cloning, which will be used to represent either of the two computers only in the VMS. Configuring a common IP address of the cluster speeds up the failover process as it saves time on registering the IP address of the stand-by node within the VMS before it takes over recording new data and serving existing recordings to Smart Clients.

6. Do one of the following:

- Click the **Shared IP** option and enter a shared IP address for the HA cluster, then click **Next**.

Note: The Configuration Wizard cannot verify whether the IP address you have entered is not already in use by another computer on the network. If the IP address is already in use, Surveillance HA will ignore it and use the individual IP addresses of the cluster nodes.

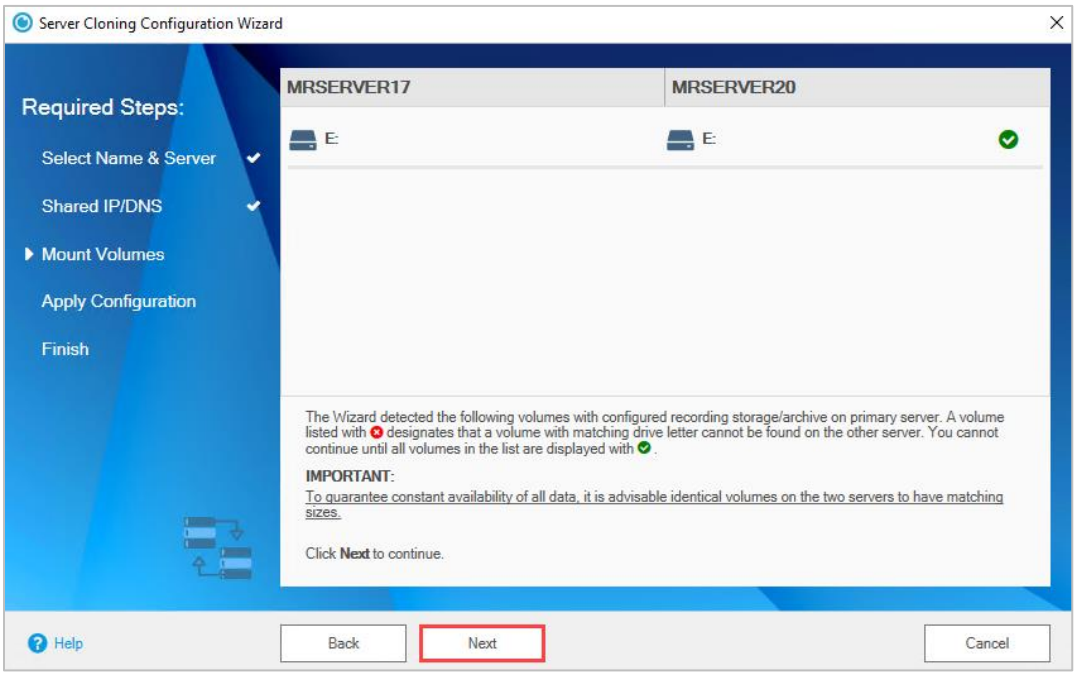
- Click the **Shared DNS** option and enter a shared DNS name, then click **Next**.
- Click **None** to let each cluster node use its own IP address within the VMS, then click **Next**.



The Configuration Wizard lists all volumes with configured recording storage and/or archive on the primary node and their equivalents on the secondary node of the cluster. If a matching volume has been detected on the stand-by node, it is displayed with this icon in the list . If no match has been found on the stand-by node, the respective volume is displayed with a warning sign .

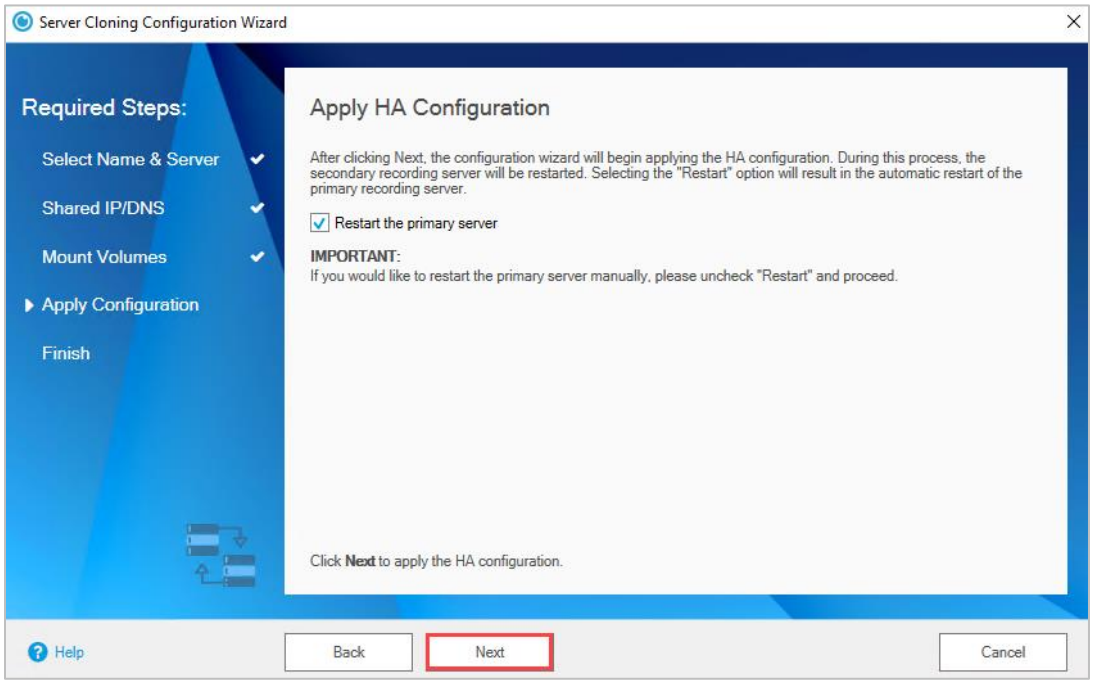
7. Do one of the following:

   - Click **Next** to configure the cluster with the available matching volumes on both nodes.
   - Click **Back** to configure any mismatching volumes on the stand-by nodes and then repeat this step again.

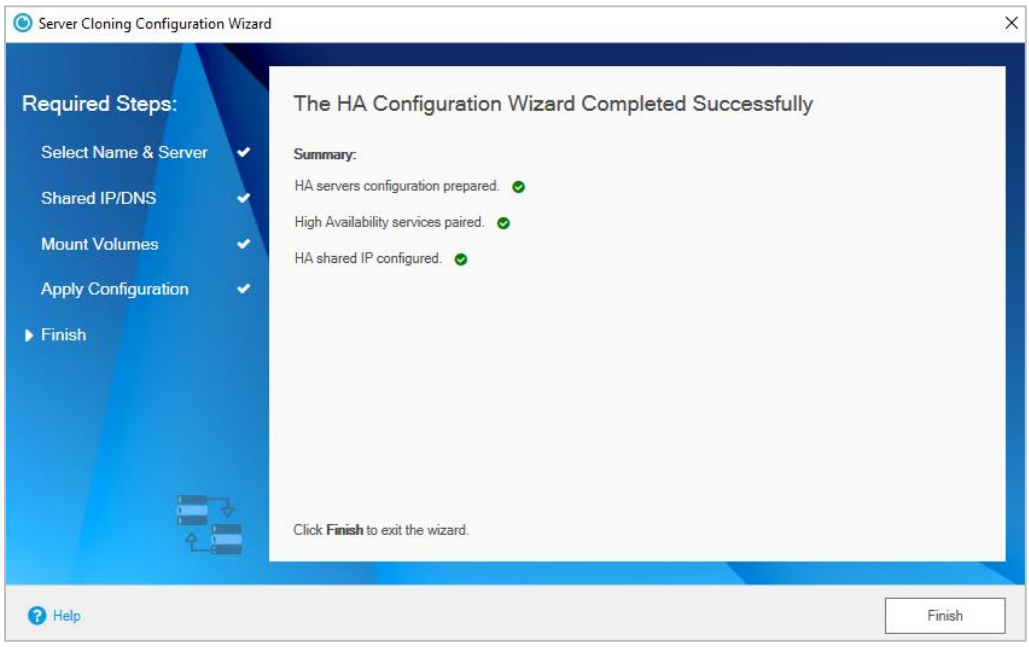


> **Note**: You cannot continue unless there is at least one matching volume found on both nodes.

8. Click **Next** to apply the configuration of the Server Cloning. Leave the “Restart the primary server” check box enabled if you can afford to restart the primary node now or clear the box to leave it for later.



The Configuration Wizard displays a summary of the Server Cloning configuration it has applied.



9. Click **Finish** to exit the Configuration Wizard and let the VMS operate with the cluster instead of the individual recording servers. The server you initiated the cloning from will be reported and stay as the Primary node of the clone while the additional server will be reported as Secondary.

   The storage pool created on both cluster nodes is mounted on the respective computer with the drive letter previously used by the volume containing the recording storage/archive. The volume itself remains mounted on the respective node, but now using the first available drive letter.

Manage the Server Cloning

You can manage the Server Cloning in the following ways:

- fine-tune the Server Cloning
- configure a dedicated connection between the two server nodes for copying data
- manually switch the roles of the serving and stand-by node in the cluster
- manage the synchronization of data between the nodes in the cluster
- disable the Server Cloning

Fine-tune the Server Cloning

Surveillance HA offers you several options for fine-tuning the operation of the Server Cloning:

- allow faster failover between cluster nodes by turning on continuous monitoring and updating of VMS' camera database on both nodes
- use synchronous or asynchronous recording of camera data on the pool
- force the VMS to rebuild its database each time the active and stand-by node switch places
- prevent unnecessary failover due to lag of network communication between the two cluster nodes

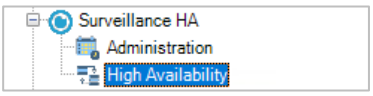
Enable or Disable Extend Missing Data

Extend data is used when one of the servers is being restarted for example or is unavailable for another reason. In such cases, the system puts placeholder data that is later replaced by the actual camera data as long as the other recording server is still functioning.

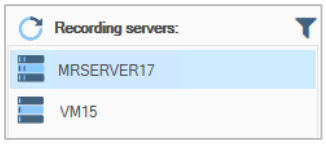
The setting is enabled by default and filling up gaps in the recording timeline later would not be possible if this setting was disabled.

To enable/disable Extend Missing Data:

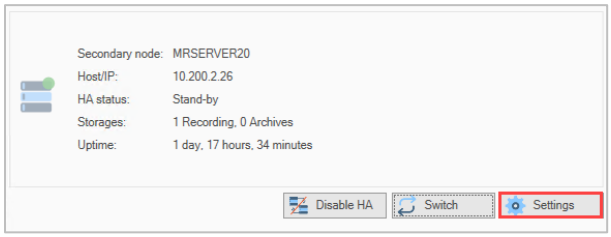
1. In the Navigation pane of the Management Client, click **High Availability** under Surveillance HA.



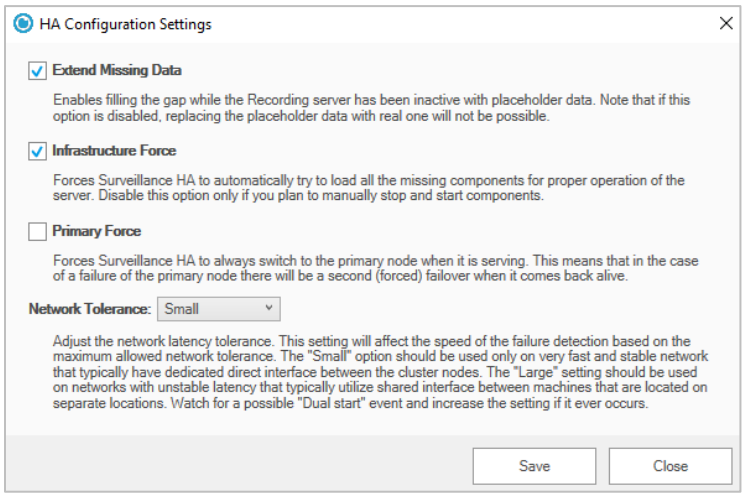
2. In the right pane under Recording Servers, click the Server Cloning, for which you want to enable or disable placeholder data.



3. In the right pane, click **Settings**.



4. In the HA Configuration Settings dialog, do one of the following:



- to allow placeholder data, select the Extend Missing Data check box and click Save.
- to disable placeholder data, clear the Extend Missing Data check box and click Save.

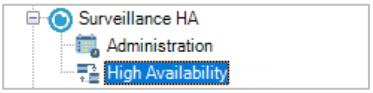
Enable or Disable Infrastructure Force

With this setting enabled, the system will be trying to start the VMS component services if needed, meaning that if a recording server stops for whatever reason, Surveillance HA will try to revive it periodically.

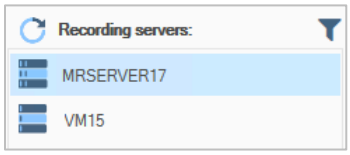
The setting is enabled by default.

To enable/disable Infrastructure Force:

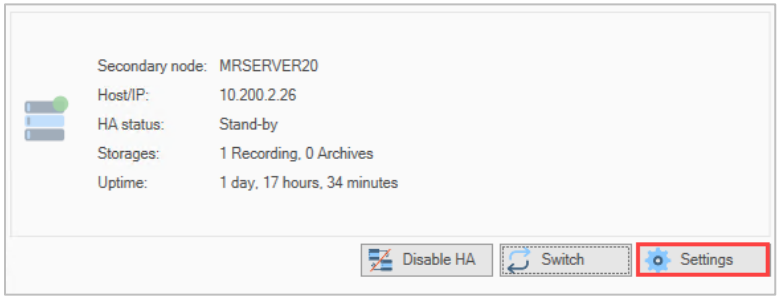
1. In the Navigation pane of the Management Client, click **High Availability** under Surveillance HA.



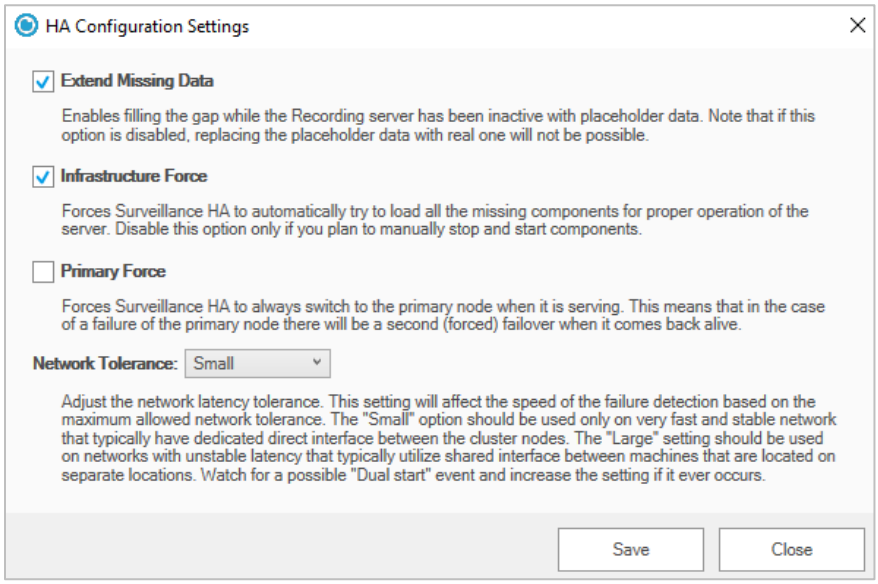
2. In the right pane under Recording Servers, click the Server Cloning, for which you want to enable or disable synchronous replication.



3. In the right pane, click **Settings**.



4. In the HA Configuration Settings dialog, do one of the following:



- to enable recording server's revival at need, select the Infrastructure Force check box and click Save.
- to disable recording server's revival at need, clear the Infrastructure Force mode check box and click Save.

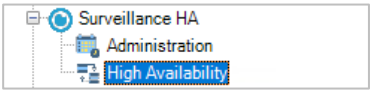
Enable or Disable Primary Force

In both Server Cloning and Camera Pairing clusters one of the nodes acts as serving and the other node acts as stand-by within the cluster, the Smart Client is connected to only one of the nodes, the currently active one. In case the primary one fails, the other one takes over the primary role. Once the originally primary node comes back online, if this setting is enabled, it will get back the primary role and the Smart Client will be rerouted to the original cluster node. If the setting is disabled, the originally stand-by node will continue being primary until it fails for some reason.

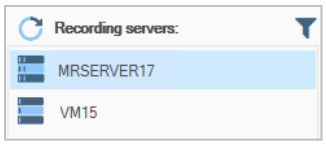
The setting is disabled by default.

To enable/disable Primary Force:

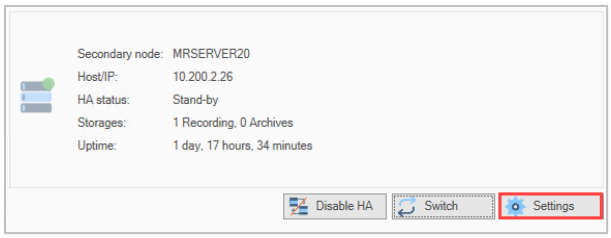
1. In the Navigation pane of the Management Client, click **High Availability** under Surveillance HA.



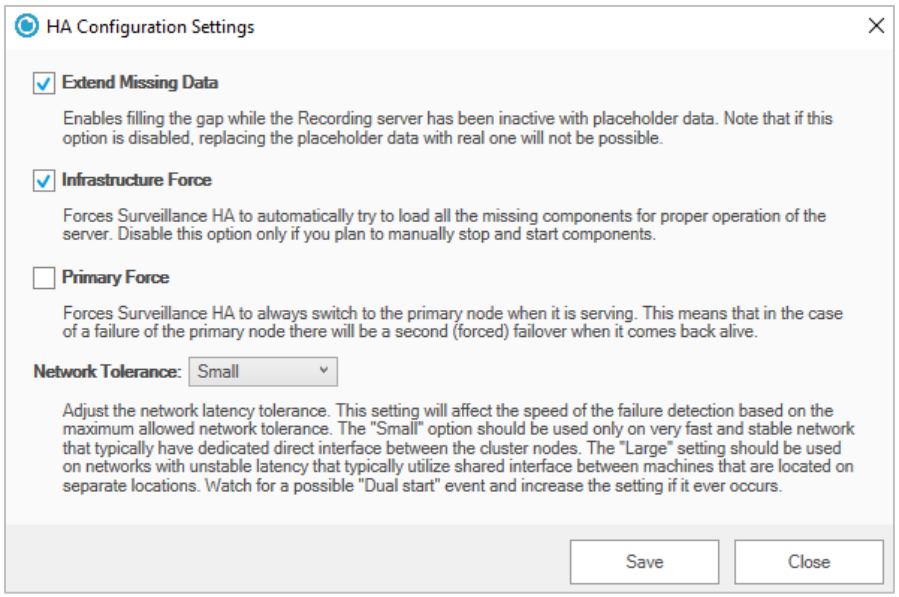
2. In the right pane under Recording Servers, click the Server Cloning, for which you want to enable or disable forced rebuilding of the database.



3. In the right pane, click **Settings**.



4. In the HA Configuration Settings dialog, do one of the following:



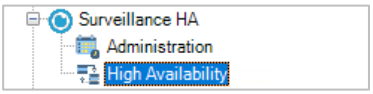
- to enable primary node enforcement, select the Primary Force check box and click Save.
- to disable primary node enforcement, clear the Primary Force mode check box and click Save.

Configure Tolerance of Network Communication Between Nodes

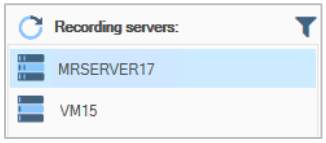
For detecting a failover condition, Surveillance HA relies on constant communication between the two cluster nodes. Depending on the network connection they use to communicate with one another, it is a response from one node to be delayed and force a failover, when actually the respective node is online and healthy. To let you fine-tune possible interruptions in the communication, Surveillance HA introduces three levels of network communication tolerance, letting Surveillance HA know how much it should wait after failing to connect to the other node before entering a failover procedure.

To configure the network communication tolerance between nodes:

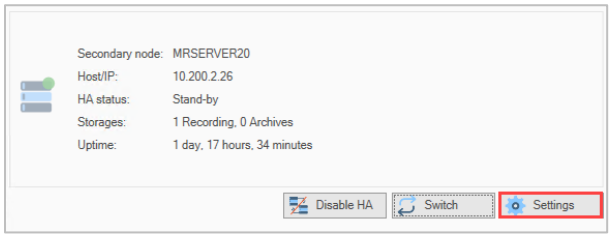
1. In the Navigation pane of the Management Client, click **High Availability** under Surveillance HA.



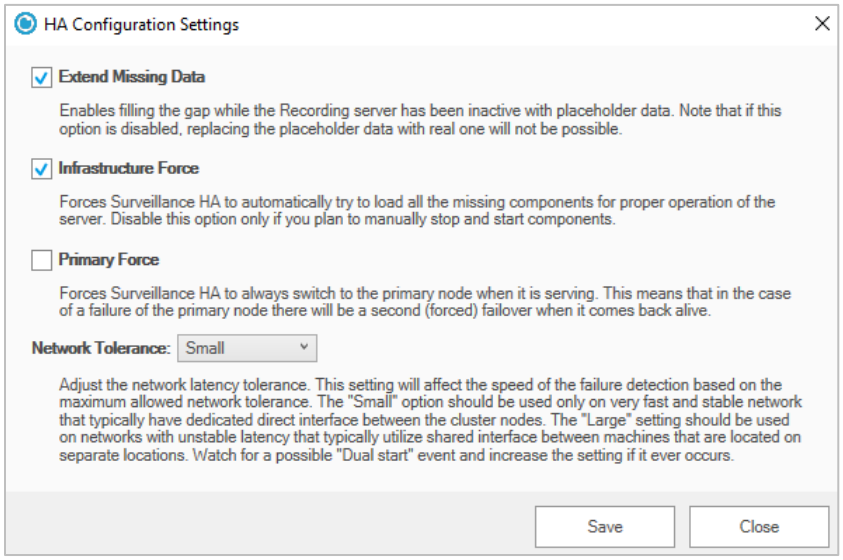
2. In the right pane under Recording Servers, click the Server Cloning, for which you want to configure network communication tolerance.



3. In the right pane, click **Settings**.



4. In the Network tolerance drop-down box of the Settings dialog, select the level of tolerance suitable for your network and then click **Save**.



Configure Dedicated Network Connection Between Cluster Nodes

By default, the two nodes of the Server Cloning communicate using the network interface with which they are visible on your VMS network. In case both nodes have additional network cards installed, you can configure a dedicated connection between them and thus ensure faster mirroring of recorded data in the pool.

To configure a dedicated network connection between cluster nodes:

1. On the serving node, start the **Registry Editor**.

   Note: To start Registry Editor, on the Start menu click Run and in the dialog type regedit.

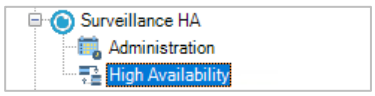
2. Navigate to:
   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tiger Technology\ha\hasvc\settings
3. Right-click the **my_address** string value and select **Modify**.
4. In Value data, enter the **IP address** of the network card for the dedicated connection on your computer and click **OK**.
5. Right-click **other_node_address** string value and select **Modify**.
6. In Value data, enter the **IP address** of the network card for the dedicated connection on the stand-by node and click **OK**.
7. Restart the Surveillance HA service, by executing the following in Command Prompt:
   - **net stop tiersvc**
   - **net start tiersvc**
8. Repeat the above steps on the stand-by cluster node.

Manually Switch the Active and Stand-by Roles Within the Cluster

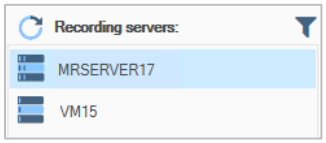
To allow you to perform maintenance operations on your current active recording server, Surveillance HA allows you to force the failover between nodes in the cluster. Once the maintenance operation is completed, you can revert the cluster node roles again.

To force the failover between cluster nodes:

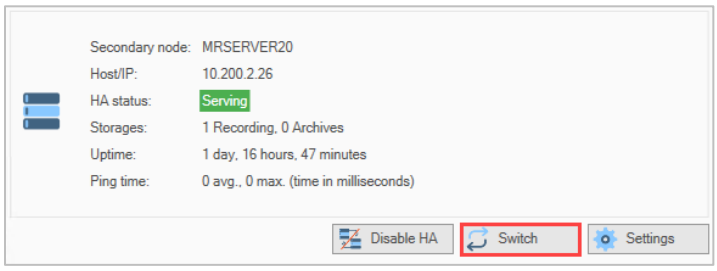
1. In the Navigation pane of the Management Client, click **High Availability** under Surveillance HA.



2. In the right pane under Recording Servers, click the Server Cloning whose node roles you want to switch.

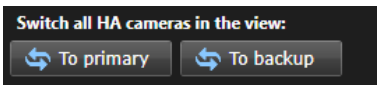


3. In the right pane, click **Switch**.



Surveillance HA switches the roles of the two nodes and displays the currently stand-by node with a greyed out icon.

If you have installed the Surveillance HA Smart Client module, you can perform this action in the VMS' Smart Client as well:



Monitor the Synchronization of Data Between the Cluster Nodes

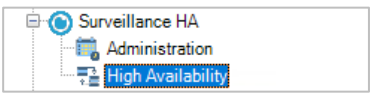
While Surveillance HA takes care to automatically synchronize the contents of the pool on both cluster nodes, when failover occurs, it is possible either of the two to contain different data. That is why Surveillance HA provides you with two methods for manually synchronizing the contents of both pools:

- synchronize the contents of the stand-by node, by adding any missing recordings available only on the active node
- synchronize the contents of the pools on both cluster nodes in order to make them identical

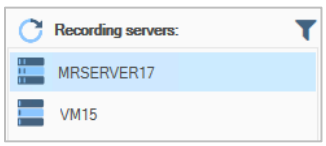
To benefit from either of the above two options, both cluster nodes must be online. You can view the pool data synchronization status on both nodes in the progress bar of the respective pool. For more information, refer to **Error! Reference source not found.**.

To synchronize the contents of the cluster nodes:

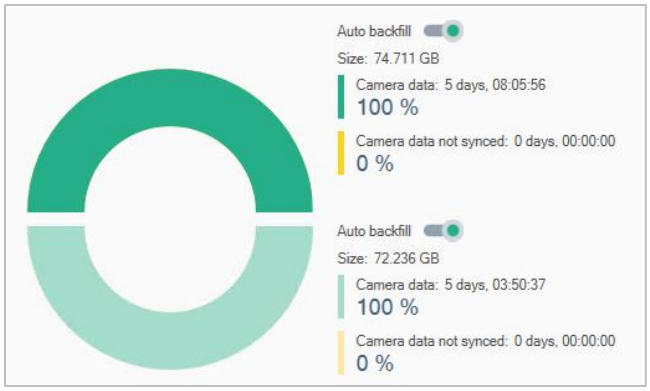
1. In the Site pane of the Management Client, click **High Availability** under Surveillance HA.



2. In the right pane under Recording Servers, click the Server Cloning.



3. In the right pane, you can see how much of the data is replicated and you have the option to enable/disable data backfill:

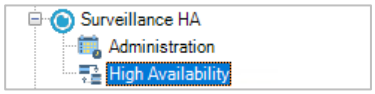


Disable the Server Cloning

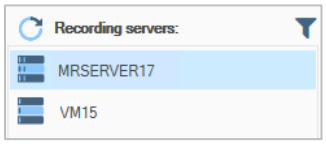
You can disable the Server Cloning at any time in order to replace the stand-by node with another computer or use it as an ordinary recording server instead.

To disable a Server Cloning:

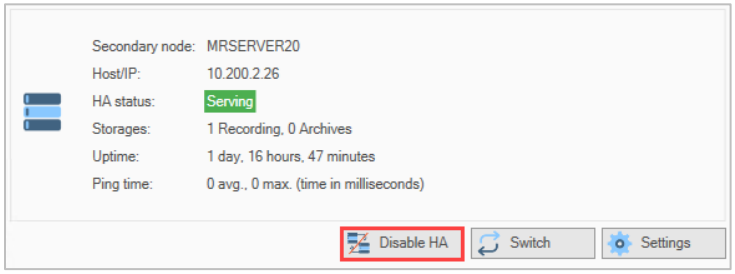
1. In the Navigation pane of the Management Client, click **High Availability** under Surveillance HA.



2. In the right pane under Recording Servers, click the Server Cloning you want to disable.



3. In the right pane, click **Disable HA**.



Surveillance HA disables the Server Cloning and registers the primary node with its attached devices in the VMS. The secondary node is available to be cloned in another Server Cloning or used as a regular recording server.

Monitor the Server Cloning

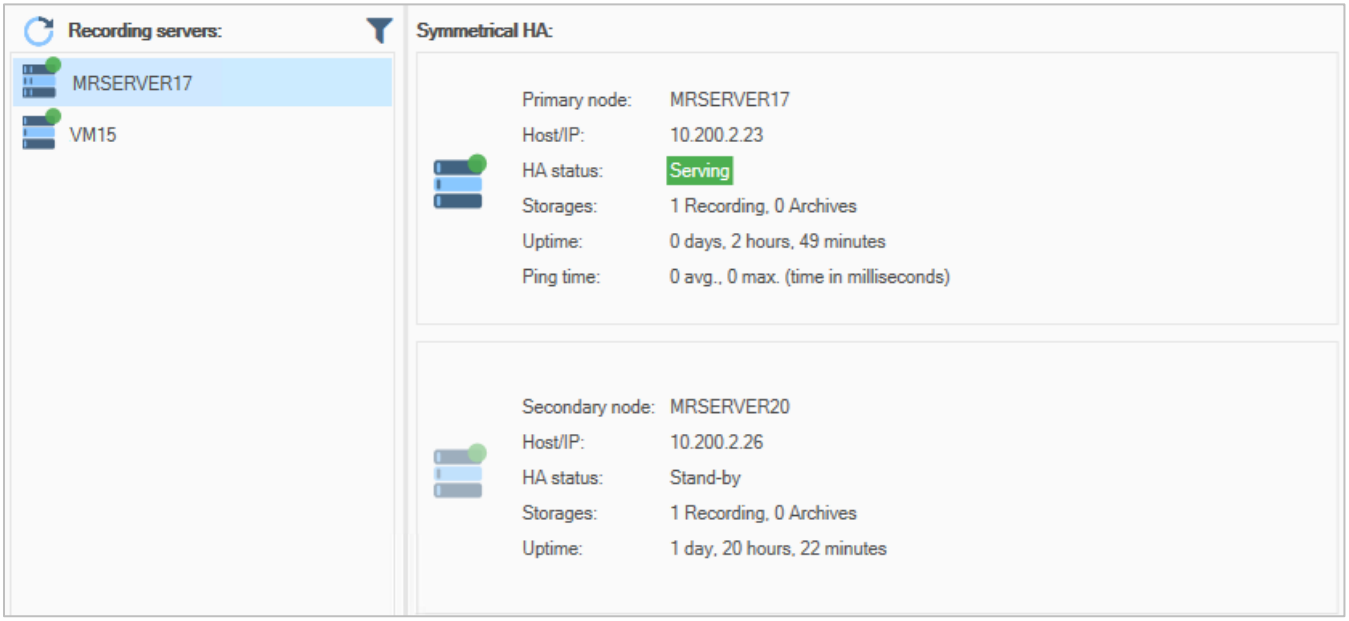
The High Availability page of the Surveillance HA module in the Management Client module provides you with all information necessary to keep track of the status of the cluster nodes, the cluster itself and the synchronization of data between pools on the two nodes.

Monitor the Nodes

You can easily discern between the currently serving node of the cluster and the stand-by one by their icons. Additionally, the color indicator of the icon designates the cluster node status:

	The cluster node is online and operating normally. This icon stays on the left if the first node is currently serving and moves to the right when the second node takes the lead.
	The cluster node is online, but one or more of the components necessary for fully transparent failover is missing. This icon may designate missing volume, on which there is recording storage/archive configured, for example.
	The cluster node is offline or there is no network connection to it.

The name of the cluster is the name of the originally active node by default and can be changed during the HA setup. Once the nodes enter a cluster, they do no show up as individual Recording servers in the VMS menu anymore:



Camera Pairing

Camera Pairing Prerequisites

To deploy Camera Pairing, the following requirements must be met:

- The camera must be added through the VMS on two recording servers on the same network and managed by the same Management Server.
- Encryption on both recording servers' storage and archives must be disabled.

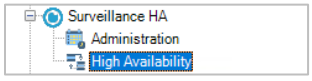
Configure Camera Pairing

Before configuring Camera Pairing, you must decide which one of the recording servers that are concurrently writing data from one and the same camera will be your primary server and which one will be secondary. The division between primary and secondary server is strictly nominal and concerns the Camera Pairing settings and Smart Client settings. Should these differ on the two servers, the settings that are valid are the ones configured on the primary server. By design, the server from which you pair the camera is considered primary and the one on which a matching camera has been found is considered secondary. Note that a primary server for one camera can be a secondary for another, if you initiate the pairing of the second camera from the second server.

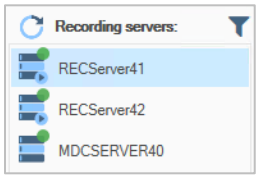
You can unpair an HA camera at any time, keeping in mind that the camera will continue writing concurrently on the storages of both recording servers, but should one or the other fails Smart Clients will not be automatically redirected to the stream/past recordings of the other server and missing data cannot be automatically synchronized.

To pair a camera on two recording servers:

1. In the Site Navigation of Management Client, click **High Availability** under Surveillance HA.



2. In the right pane under Recording Servers, click the recording server, which will play the role of primary server in the Camera Pairing.

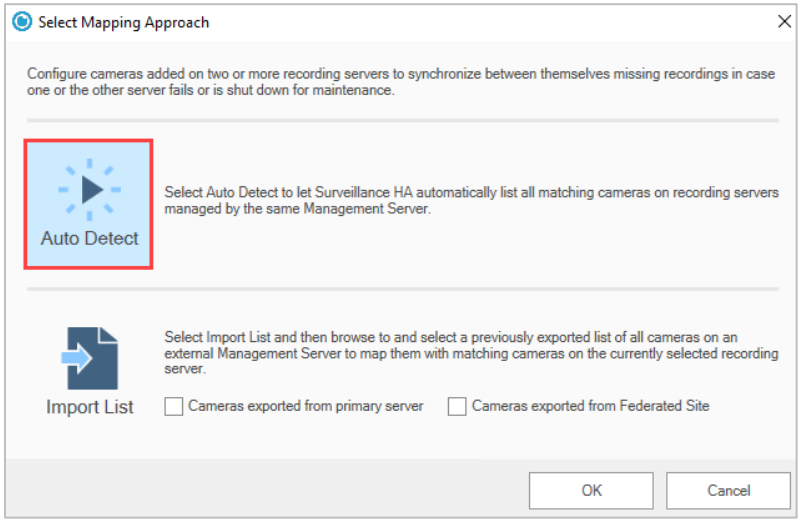


Note: If a recording server is missing from the list, it is already paired in a Server Cloning.

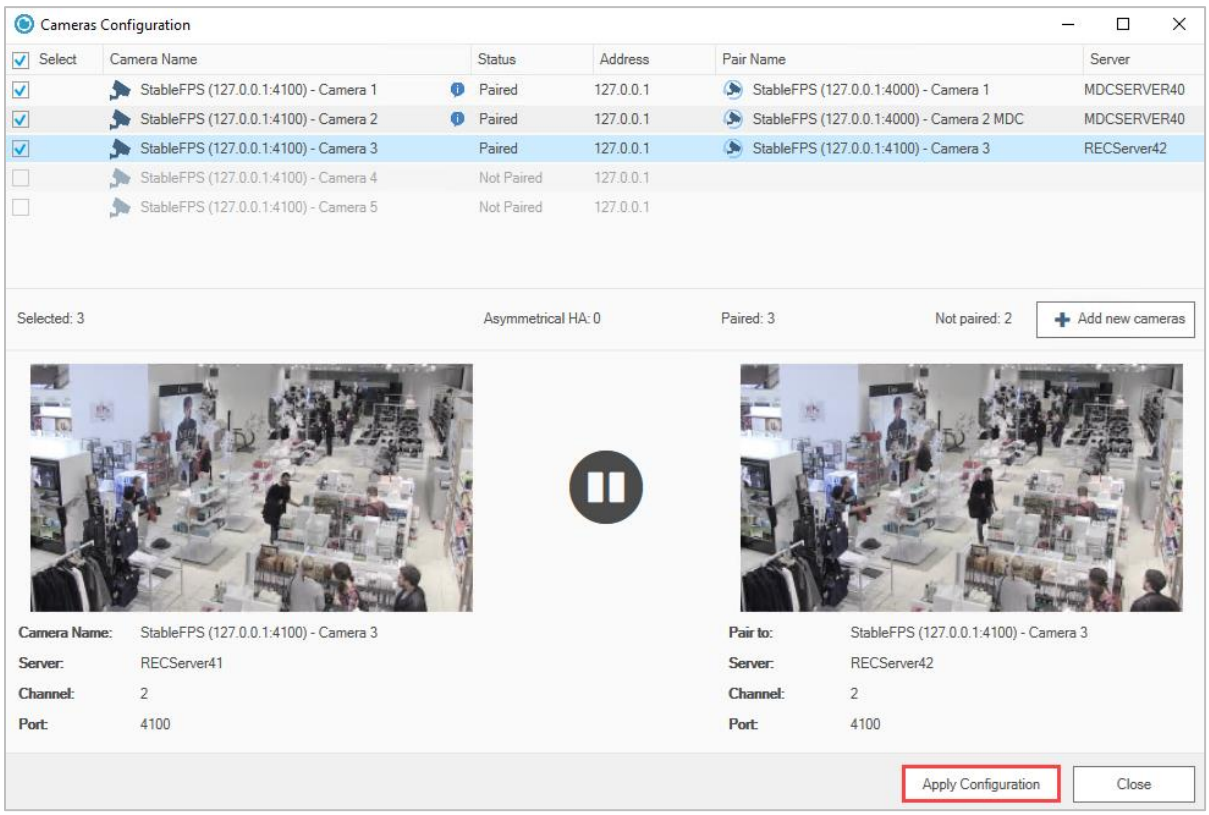
3. In the right pane, click **Camera Pairing**.

Note: If the option is greyed out, then the selected server is not licensed for Camera Pairing. Check the Activate Surveillance HA section for further instructions.

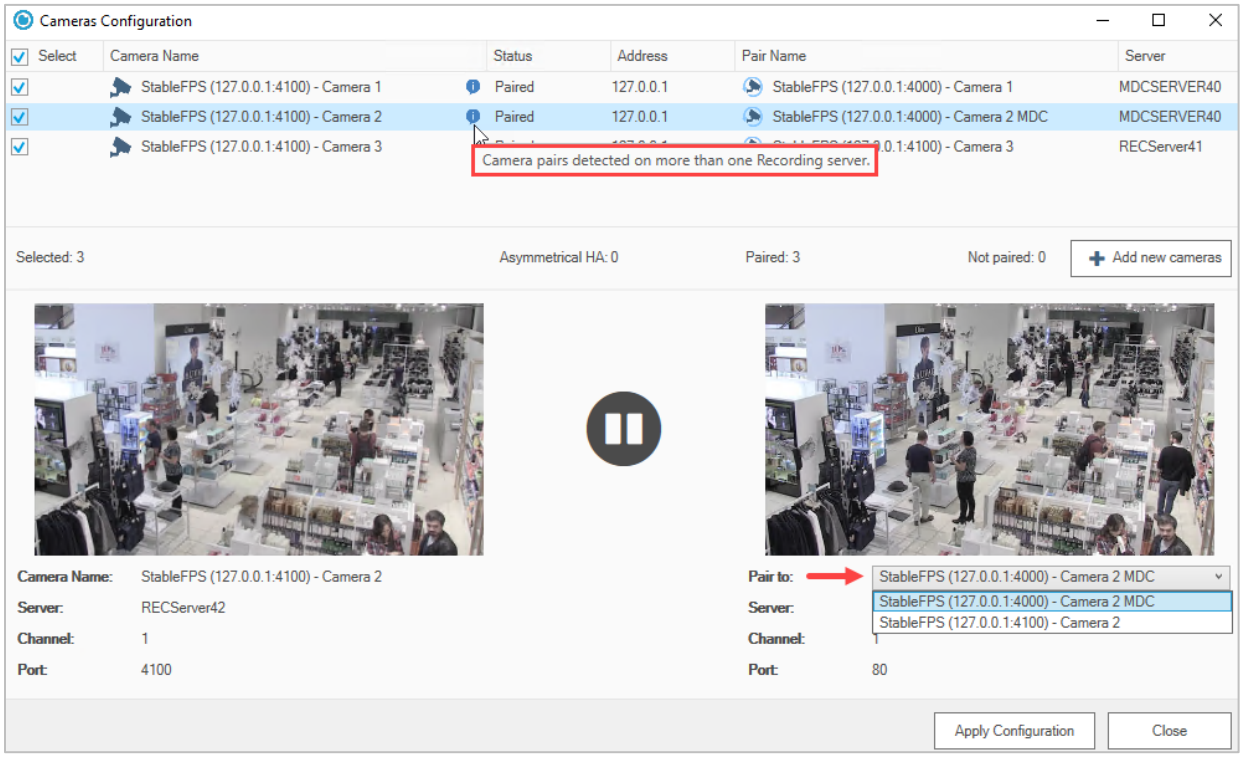
4. In the Select Mapping Approach dialog, select **Auto Detect** and then click **OK**.



The left pane of the Cameras Configuration dialog lists all cameras on the selected recording server and the right pane lists all matching cameras found on other recording servers. By default, the check box of each camera with a match found is selected. Cameras with no matches are greyed out in the list. You can sort the columns of the list in ascending or descending order.



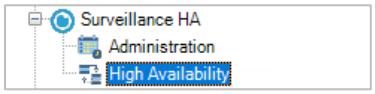
5. (optional, if a matching camera has been found on more than one server) To pair a camera available on two or more servers, select the camera in the list and in the pane below select the desired recording server in the drop-down box just below the player.



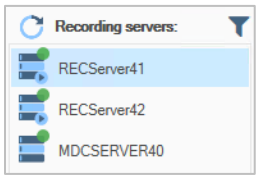
6. Clear the check boxes of the matching cameras that you do not want to pair in a Camera Pairing and click **Apply Configuration**.

To unpair a camera:

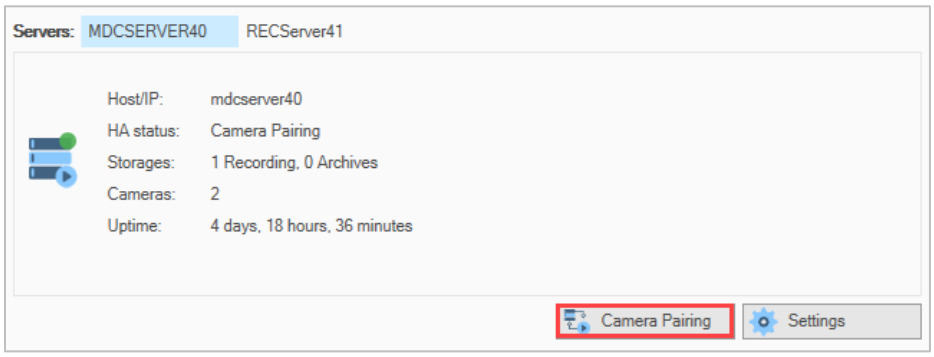
1. In the Navigation pane of the Management Client, click **High Availability** under Surveillance HA.



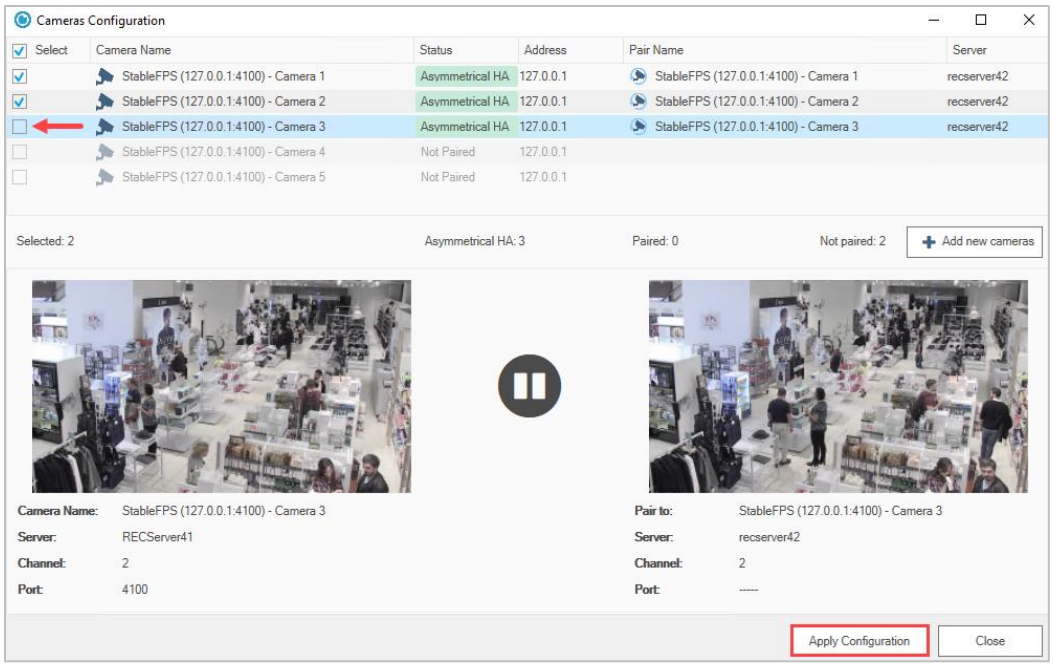
2. In the right pane under Recording Servers, click the recording server, whose camera(s) you want to unpair.



3. In the right pane, click **Camera Pairing**.

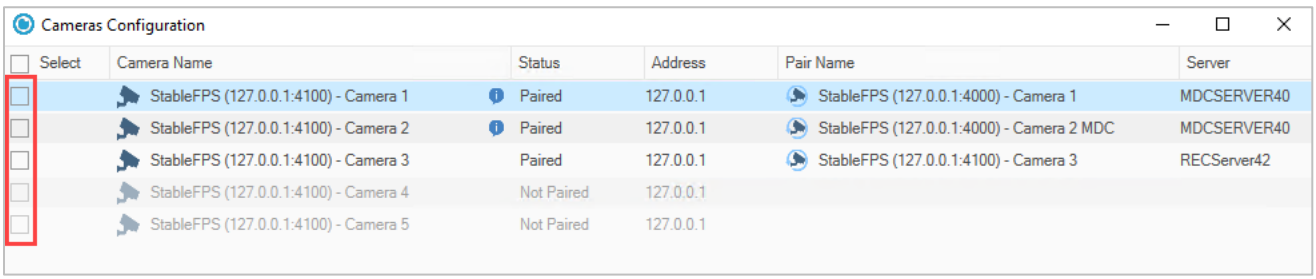


4. In the Cameras Configuration dialog, clear the check boxes of the cameras that you want to unpair and then click **Apply Configuration**.



To Disable Camera Pairing:

If you unpair all the available camera on the list, you effectively disable the Camera Pairing.



Configure Camera Pairing Settings on the Server

Surveillance HA provides you with several settings that optimize your workflow when Camera Pairing is enabled. The settings are valid for all cameras paired on the selected recording server, i.e. the primary server. If a camera on the selected server is paired in Camera Pairing on another server, the other server's settings are valid for this camera.

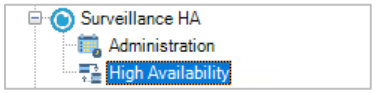
Extend Missing Data

Normally, without Surveillance HA's Camera Pairing configuration, should a recording server stop recording, the timeline of the camera remains blank and cannot be filled with the missing recordings later on. One of the features of Camera Pairing is that it is capable of backfilling missing recordings in the timeline of a camera by synchronizing it with the recordings from the other recording server. To be able to do so, Surveillance HA creates an empty placeholder file, filling in the gap when the recording has been interrupted. This placeholder data is then replaced by the equivalent recordings from the same camera, when the Camera Pairing synchronizes its content.

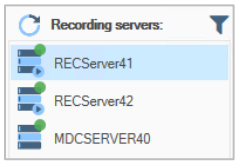
By default, extending missing data is enabled on both recording servers. You can select to disable it on the secondary server, for example, if your workflow does not require both timelines to be uninterrupted.

To enable/disable extension of missing data on a recording server:

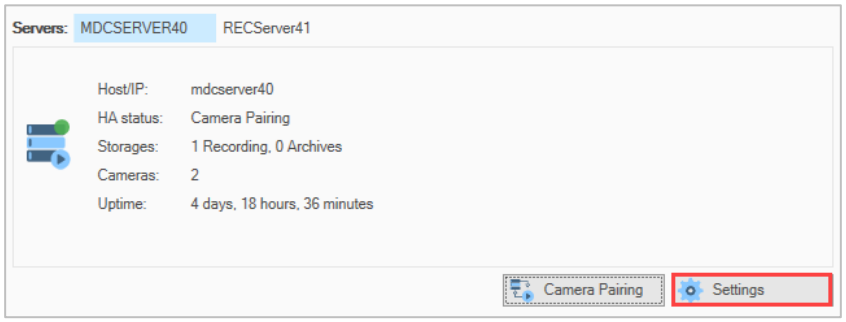
1. In the Navigation pane of the Management Client, click **High Availability** under Surveillance HA.



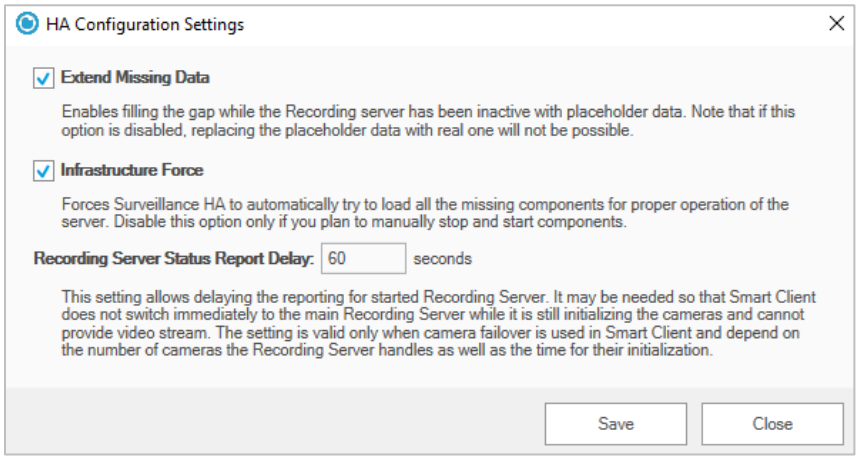
2. In the right pane under Recording Servers, click the recording server, whose Camera Pairing settings you want to configure.



3. In the right pane, click **Settings**.



4. In the HA Configuration Settings dialog, do one of the following:



- Select the “Extend Missing Data” check box, to allow the server’s camera timeline to be backfilled with recordings from the paired camera on the other recording server.
- Clear the “Extend Missing Data” check box, to prevent the server’s camera timeline to be backfilled with recordings from the paired camera on the other recording server.

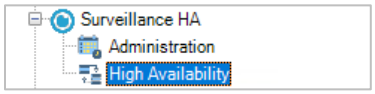
5. Click **Save**.

Infrastructure Force

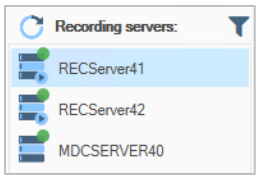
Surveillance HA’s Camera Pairing configuration is designed to attempt to overcome all interruptions in the operation of any of the components comprising a healthy unity - the recording server, its storages and the cameras. Thus, even if you have deliberately unmounted a volume with a configured recording storage in order to defragment it, for example, Surveillance HA may attempt to mount it on the recording server and interrupt the maintenance operation. In this case it is advisable to disable Surveillance HA’s infrastructure force and manually stop and start the components.

To enable/disable infrastructure force:

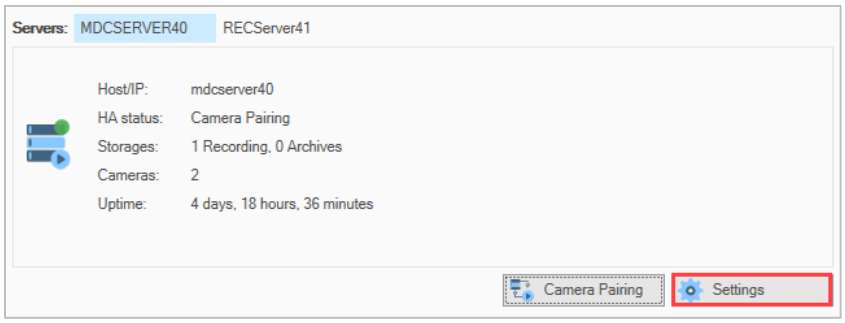
1. In the Navigation pane of the Management Client, click **High Availability** under Surveillance HA.



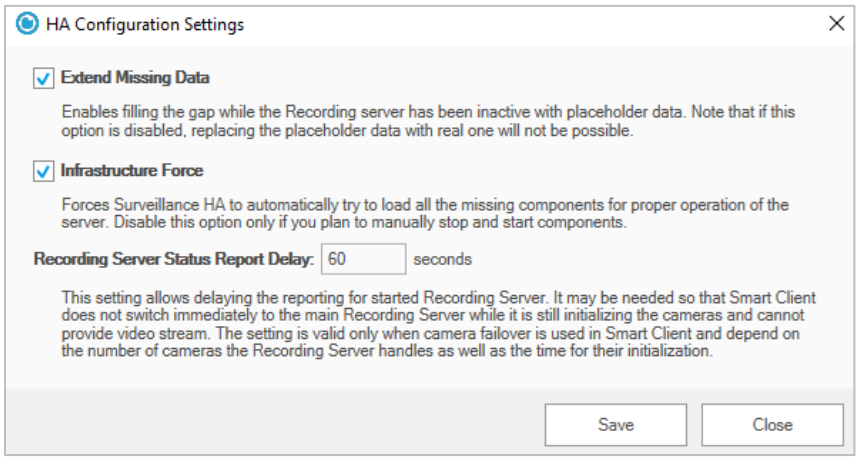
2. In the right pane under Recording Servers, click the recording server, whose Camera Pairing settings you want to configure.



3. In the right pane, click **Settings**.



4. In the HA Configuration Settings dialog, do one of the following:



- Select the “Infrastructure Force” check box, to let Surveillance HA attempt automatically start each component in a recording unity whenever this s possible.
- Clear the “Infrastructure Force” check box, to prevent Surveillance HA from attempting to automatically start each component in a recording unity and manually stop/start the respective components yourself.

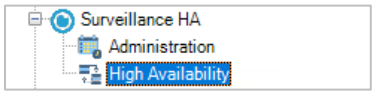
5. Click **Save**.

Reported Delay of the Recording Server Status

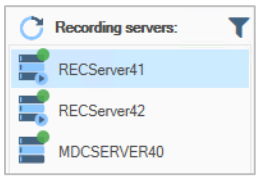
When a recording server is back online, as soon as Surveillance HA detects this, it displays the server’s cameras streams even though not all necessary devices may have been mounted on the recording server yet. Thus, if Smart Clients attempt to always access the streams of this server’s cameras, the timeline will display empty frames instead of the actual recordings accessible through the alternative server in the Camera Pairing. To prevent this you can specify a delay in automatically switching to the streams/recordings of a recording server, specifying the time needed for it to mount all necessary devices after it has been started. By default, this is set to 60 seconds on each server.

To configure the delay in reporting a recording server's status:

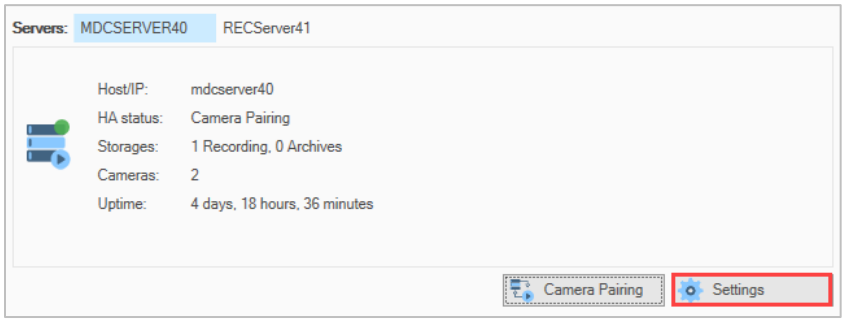
1. In the Navigation pane of the Management Client, click **High Availability** under Surveillance HA.



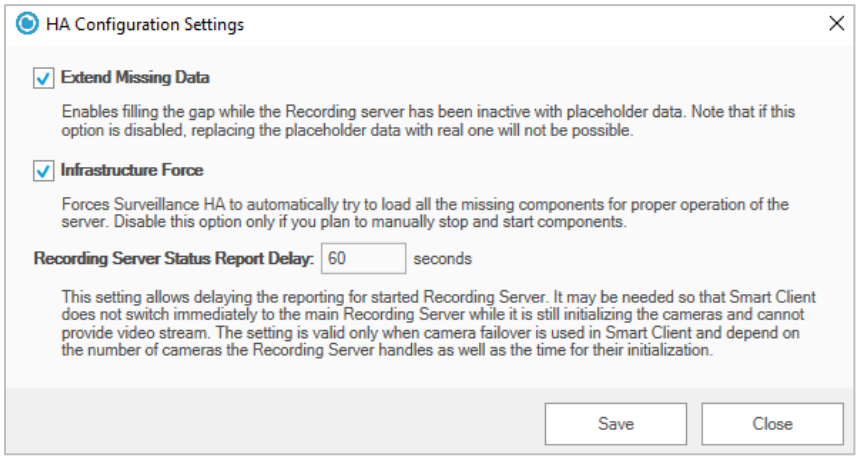
2. In the right pane under Recording Servers, click the recording server, whose Camera Pairing settings you want to configure.



3. In the right pane, click **Settings**.



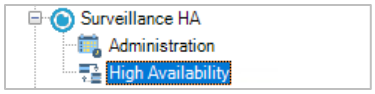
4. In Recording Server Status Report Delay enter the desired time in seconds and click **Save**.



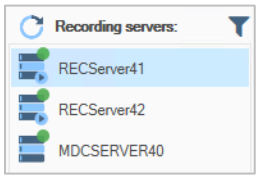
As long as the extension of missing data is enabled on a recording server, should a gap in any of its cameras' timeline occur, once the problem with the server or its storage is resolved Surveillance HA can backfill data by synchronizing it with the equivalent recordings from the other recording server. This can be done either manually (see **Error! Reference source not found.**) or automatically. The automatic method queues for synchronization all recordings, i.e. you cannot select which ones to synchronize or to prioritize. Additionally, the automatic synchronization of recordings starts as soon as circumstances allow and this can burden your network. That is why this option is disabled on both recording servers, by default.

To enable/disable automatic backfilling of timeline gaps:

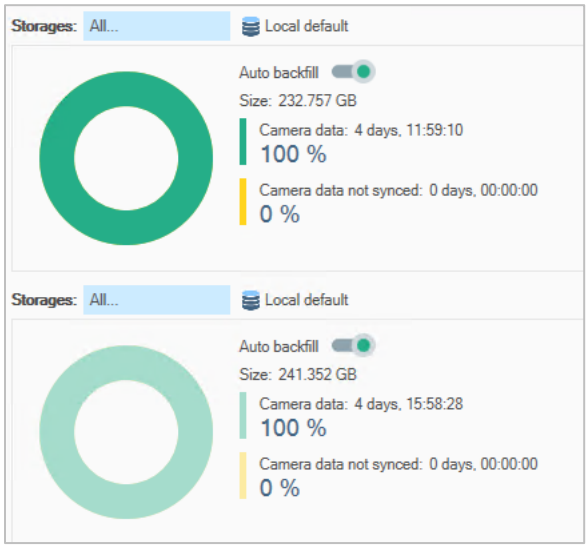
1. In the Site Navigation of the Management Client, click **High Availability** under Surveillance HA.



2. In the right pane under Recording Servers, click the recording server, whose Camera Pairing settings you want to configure.



3. In the right pane click the Auto backfill button to enable/disable the backfill of missing data on one or all of the servers listed.



Surveillance HA lists all recording storages/archives, on which matching cameras on both servers are recording.

Revisions Record

Revisions			
Date	**Description**	**Page(s)**	**Version**
08 Apr. 2023	Initial Draft		

Tiger Surveillance

About This Guide

The Surveillance HA 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