

White Paper

---

# Milestone Interconnect™

---

**Prepared by:**

*John Rasmussen, Platform Architect*

# Table of Content

---

<b>Introduction</b>	<b>4</b>
<b>Purpose and target audience</b>	<b>5</b>
<b>The concept behind Milestone Interconnect</b>	<b>6</b>
<b>Technical overview</b>	<b>7</b>
Recording and playback options	9
<b>Scalable Video Quality Recording (SVQR)</b>	<b>10</b>
<b>Implementation of SVQR</b>	<b>11</b>
<b>Applied use of Milestone Interconnect</b>	<b>12</b>
Retail chains	12
Transportation	13
Security companies offering centrally managed video surveillance	15
City surveillance	17
<b>Milestone Interconnect Management</b>	<b>19</b>
Prerequisites	19
Adding remote sites	19
Settings – remote sites and devices	22
Updating remote site devices	23
Interconnect playback configuration	24
User rights in XProtect Corporate	29
Rules	30
<b>Milestone Interconnect and XProtect Smart Client operation</b>	<b>31</b>

---

---

Setup	31
Live	31
Playback remote recordings	32
Playback recordings from central site and retrieval of remote recordings	32
<b>Milestone Interconnect in comparison to Edge Storage</b>	<b>36</b>
<b>Milestone Interconnect in comparison to Milestone Federated Architecture</b>	<b>37</b>
Milestone Interconnect	37
Milestone Federated Architecture	38
<b>Implementation considerations</b>	<b>39</b>
<b>Supported products</b>	<b>43</b>
<b>Licensing</b>	<b>44</b>
<b>Benefits and summary</b>	<b>45</b>

---

## Introduction

Milestone Interconnect is a unique concept that allows all of Milestone's video management software (VMS) products to be interconnected with Milestone's premium VMS XProtect Corporate. This allows the design of large-scale and geographically dispersed video surveillance installations, where each independent surveillance site can be designed with the required functionality and cost in mind, while still offering the benefits of a centralized surveillance installation.

In some respects, Milestone Interconnect is similar to [Milestone Federated Architecture](#). However, the way the different sites communicate is different, and Milestone Interconnect supports a wider selection of Milestone's VMS products and offers several additional features:

- Support for using low-end XProtect products on dedicated hardware, for instance in vehicles
- Cost-efficient deployment by interconnecting Milestone products designed for the small and midsize business (SMB) market
- Retrieval of video, audio, and metadata recordings from interconnected sites to the central XProtect Corporate site, including over intermittent network connections
- Direct playback of the remote site's recording
- Scheduled, event, user-activated or automatic retrieval of remote site recordings to the central XProtect Corporate site
- Support for Scalable Video Quality Recording (SVQR)
- Short and consistent client login times regardless of the number of interconnected sites, remote site response time, or network connection state
- Full XProtect Corporate camera rights for the interconnected cameras

Due to its unique features, Milestone Interconnect is suited especially for specific verticals such as:

- Retail chains
- Transportation
- Companies offering surveillance services
- City surveillance

## Purpose and target audience

The purpose of this white paper is to provide a general overview of Milestone Interconnect and:

- The concept behind it
- The technical implementation
- The benefits it offers
- The problems it solves

This white paper's target audiences might include (but are not limited to) the following audiences:

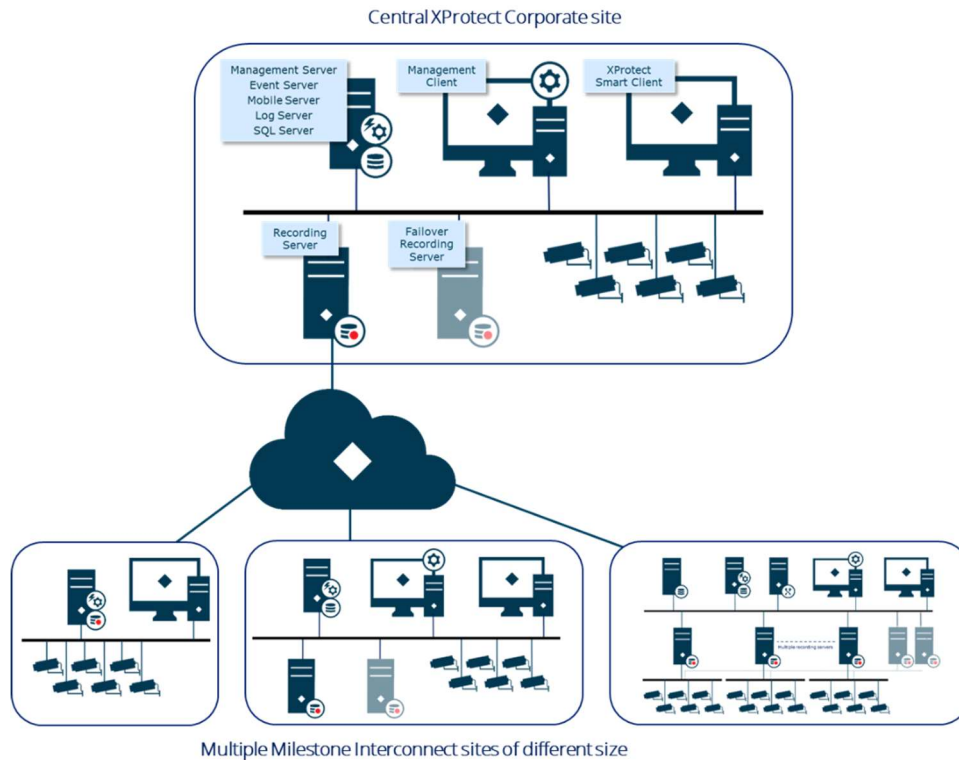
- Surveillance system architects and designers
- Large-scale surveillance project consultants
- Companies, organizations, universities, cities, and governments with distributed surveillance projects or installations

This white paper enables the reader to understand the architecture and technology behind Milestone Interconnect, as well as how to design and implement a distributed surveillance installation by utilizing Milestone Interconnect.

It is assumed that the reader has a general understanding of Milestone XProtect Corporate, the XProtect Management Client, and XProtect Smart Client, as well as the other XProtect VMS and Husky products. The reader is also assumed to have a general understanding of network technology and design.

## The concept behind Milestone Interconnect

With Milestone Interconnect, multiple remote sites running any XProtect product<sup>1</sup> can be interconnected with a central XProtect Corporate site.



This offers central XProtect Corporate site users seamless access to live and recorded video, audio, and metadata regardless of whether the recording is done on the remote site, on the central XProtect Corporate site, or on both.

Furthermore, it offers administrators and users on the central XProtect Corporate site, advanced functionality for all the interconnected sites, even when the VMS product running the interconnected site natively does not support this function, for instance:

- Advanced rules
- Recording retrieval functionality with support for SVQR
- Detailed and time-based user rights
- Evidence Lock recordings recorded or retrieved to the central XProtect Corporate site
- Create Bookmarks for interconnected cameras on the central XProtect Corporate site<sup>2</sup>
- Create Alarms for interconnected cameras on the central XProtect Corporate site<sup>3</sup>

The interconnected sites can be accessed and managed locally, like any standard stand-alone site.

<sup>1</sup> Except the free XProtect Essential+ product

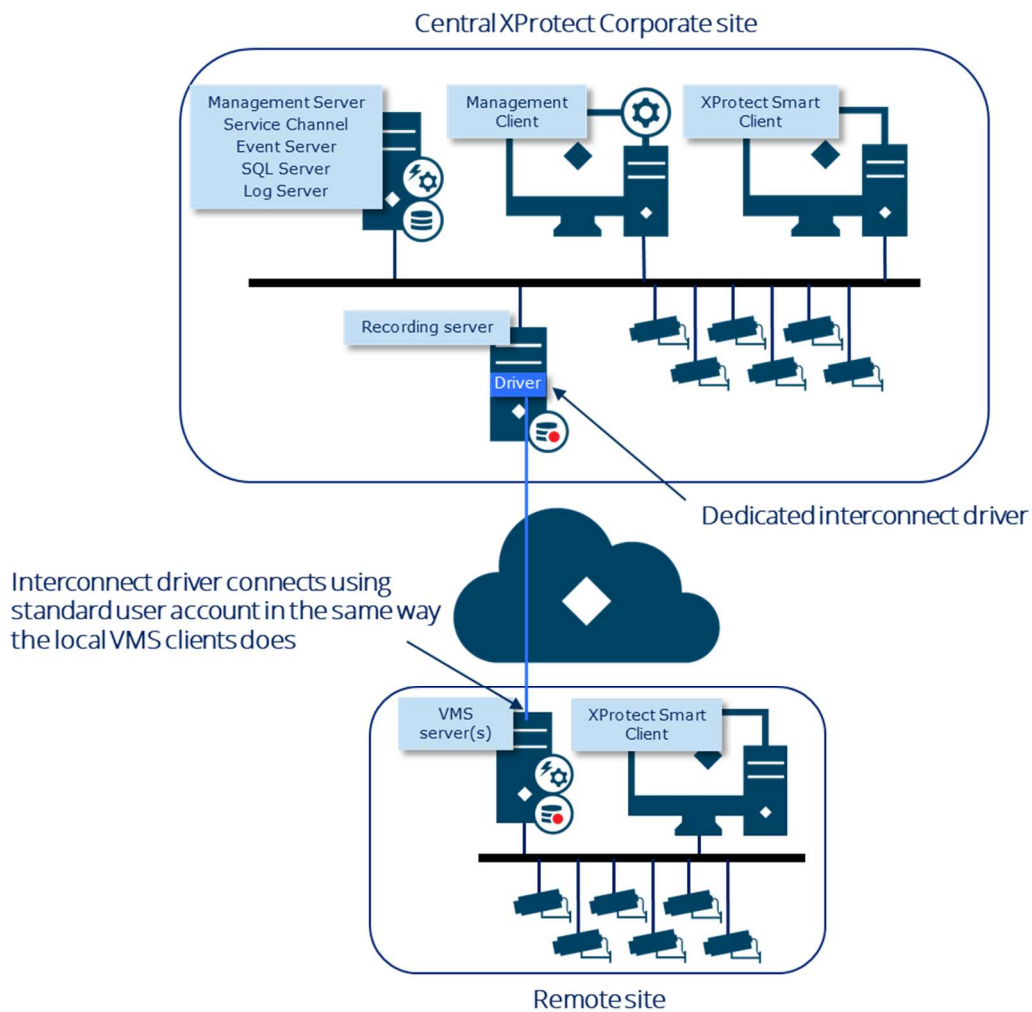
<sup>2</sup> Bookmarks created on remote sites cannot be viewed or managed centrally

<sup>3</sup> Alarms triggered on remote sites cannot be viewed or managed centrally

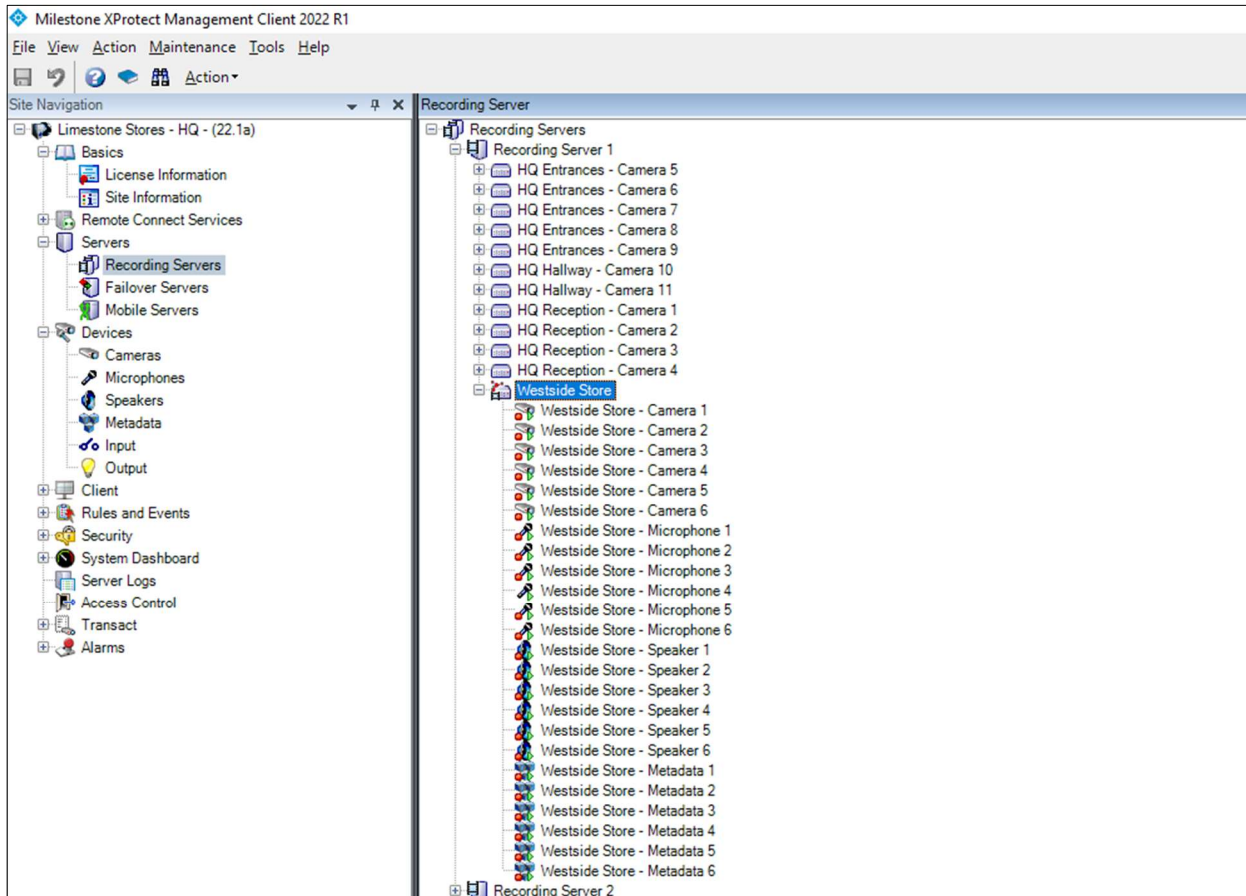
## Technical overview

The actual connection between the central XProtect Corporate site and the remote VMS site is established through a driver in the XProtect Corporate recording server, in the same way as when connecting to a network camera or a video encoder.

This diagram shows how the central XProtect Corporate site and the remote VMS site are interconnected via the dedicated driver in the XProtect Corporate recording server.



Since the remote site is interconnected via the recording server, the remote site appears in the XProtect Management Client on the central XProtect Corporate site as a kind of multi-channel video encoder, listing the cameras, microphones, speakers, and metadata devices that can be accessed on the remote interconnected site.



**XProtect Management Client**  
Interconnected site added to recording server

Because the interconnected cameras, microphones, speakers, and metadata devices are listed as if they were connected to a video encoder, they can be used and administrated in the central XProtect Corporate site in the same way as any standard camera that is connected directly. The only exception is changing the actual image, audio, or metadata settings on the devices. These settings are controlled on the remote site.

The main advantages of interconnecting remote sites via the XProtect Corporate recording servers are:

- Short and consistent login time for the XProtect clients and MIP SDK integrations, regardless of the number of interconnected sites and response time or online/offline state of the sites
- Support for remote sites that are not online all the time, for instance, surveillance in vehicles
- Support for playing back recordings directly from the remote site
- Support for retrieving recordings from remote sites to the central XProtect Corporate site
- Full XProtect Corporate device rights, including time-based access rights



## Recording and playback options

Milestone Interconnect offers three ways to configure recording and playback across the central and remote sites, each supporting different use cases and providing different functions.

### Option 1: Recording only in the remote interconnected site

With this option, all recording and playback are done only in the remote interconnected site, and recording is switched off completely in the central XProtect Corporate site. Using this option, the XProtect Corporate recording servers function only as a gateway to live and recorded video, audio, and metadata from the remote site.

Option 1 user experience:

- Users who access the remote interconnected cameras, microphones, speakers, and metadata devices via the central XProtect Corporate site can view live and recorded video, audio, and metadata as normal
- Users on the central XProtect Corporate site can use many of the advanced XProtect Corporate features, such as XProtect Smart Wall, bookmarks, alarms, etc. regardless of whether the product running the interconnect site supports this feature or not
- Users who access the interconnected site directly can view live and recorded video, audio, and metadata and use their local system as normal

### Option 2: Recording only in the central XProtect Corporate site

With this option, recording is switched off in the remote interconnected site. All video, audio, and metadata are streamed to the central XProtect Corporate site and recorded based on the defined rules in the XProtect Corporates site.

Option 2 user experience:

- Users who access the remote interconnected cameras, microphones, speakers, and metadata devices via the central XProtect Corporate site can view live and recorded video, audio, and metadata as normal
- Users on the central XProtect Corporate site can use many of the advanced XProtect Corporate features, such as XProtect Smart Wall, bookmarks, alarms, etc. regardless of whether the product running the interconnect site supports this feature or not
- Users who access the interconnected site directly can view live video, audio, and metadata, but they cannot play back recordings because this is done only in the central XProtect Corporate site

### Option 3: Recording is done on both sites

With this option, recording and playback can be done both on the remote site and on the central XProtect Corporate site. This allows the central and remote sites to independently control what to record in each system. Furthermore, it allows recordings to be retrieved (copied) from the remote interconnected site at a later point and be stored in the central XProtect Corporate site.

One use of this type of setup could be if the central XProtect Corporate site loses connection to the remote site at times, and thus misses some recordings. In this case, the central XProtect Corporate site can be configured to retrieve the missing recordings automatically for the periods when communication with the remote site is unavailable.

Another reason for this type of setup could be that the central XProtect Corporate site is configured to view and record the video with a lower quality than on the remote site. This configuration can be useful for reducing the bandwidth load between the remote and central site, while still providing the user with situational awareness and access to retrieving high-quality recordings when needed. For this case, retrieval of recordings from the remote site can be controlled via time schedules, events, or manual requests by XProtect Smart Client users.

Option 3 user experience:

- Users who access the interconnected site via the central XProtect Corporate site can view live and recorded video, audio, and metadata recorded in the central XProtect Corporate site, but not immediately from the remote interconnected site
- Users on the central XProtect Corporate site can use many of the advanced XProtect Corporate features, such as XProtect Smart Wall, bookmarks, alarms, etc. regardless of whether the product running the interconnect site supports this feature or not
- Users can request recordings that are not present in the central XProtect Corporate site to be retrieved from the remote site
- Administrators can configure the central XProtect Corporate site to automatically retrieve recordings from the remote sites based on schedule, events, or automatically after the loss of communication with the remote site
- Users who access the interconnected site directly can view live and recorded video, audio, and metadata and use their local system as usual

## Scalable Video Quality Recording (SVQR)

SVQR is a technology that extends the functionality of Milestone Interconnect and enhances the existing synergies of recording video, both on the interconnected site and on the central XProtect Corporate site.

SVQR does this by making it possible to record high-quality video in the remote interconnected site while sending a second low-quality “reference” video stream to the central XProtect Corporate site where it can be viewed live and recorded.

In the event of an incident or investigation, the initial assessment can be made using the centrally recorded low-quality “reference” video, while allowing the user to quickly retrieve the high-quality video sequences from the interconnected site when needed.

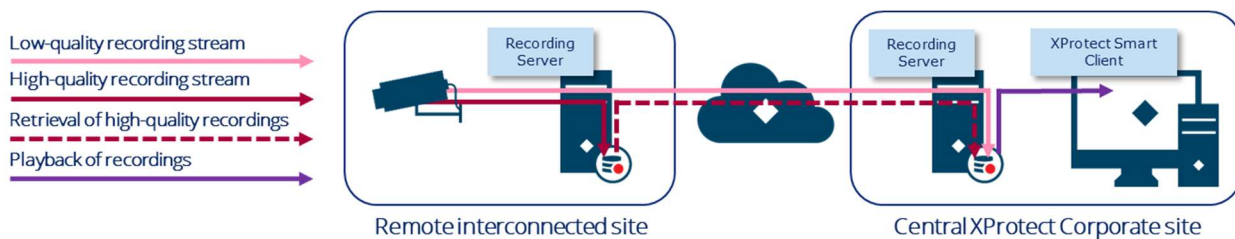
By recording high-quality video on the remote interconnected site and low-quality video on the central XProtect Corporate site, and having the function for central XProtect Corporate site users to retrieve the high-quality recordings when needed, SVQR significantly reduces the network and storage requirements and cost while still providing users of the central XProtect Corporate site with situational awareness and access to high-quality recordings when they need it.

## Implementation of SVQR

The use of SVQR requires at least two streams of different quality to be configured on the remote interconnected site (in the following example, the streams are referred to as low-quality and high-quality).

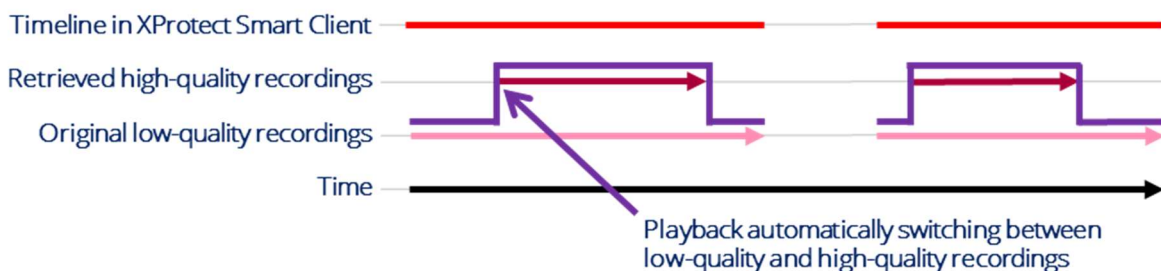
The high-quality stream is recorded on the remote interconnected site based on motion detection, events, schedule, or via manual control.

The low-quality stream is not recorded on the remote interconnected site, but simply relayed to the central XProtect Corporate site where it is recorded based on motion detection, events, schedule, or manual control.



When high-quality recordings are needed on the central site, for instance for conducting an investigation, the high-quality recordings can be retrieved by the users of the XProtect Smart Client, or alternatively, retrieved automatically on events.

The retrieved recordings are then stored in parallel with the existing low-quality recordings. During playback, the system will seamlessly and without user interaction switch between the low-quality and high-quality recordings. As illustrated, the client users will simply see the quality of the recordings go from low to high quality when they reach periods where high-quality recordings have been retrieved.



The same applies when recordings are exported. The quality of the recordings in the export will be the same as the quality experience when doing playback.

When high-quality recordings are retrieved, the existing low-quality recordings are not deleted or overwritten. The new high-quality are instead simply stored in parallel with the existing low-quality recordings. The reason for not deleting or overwriting the recordings is that it would break the digital signature of the existing recordings, making it look like the recordings had been tampered with. By placing the high-quality recordings in parallel with the existing recordings they will have their own digital signature, making it possible to verify the digital signatures of both the existing low-quality recordings and the retrieved high-quality recordings.

## Applied use of Milestone Interconnect

### Retail chains

Retail chains with individual shops often need video surveillance in each shop for employee security, to counter theft, and to control internal fraud. However, retail chains often also wish to link the independent surveillance sites in each shop with headquarters to form a large, centralized VMS, since it lowers operational costs and optimizes administration, monitoring, and fraud investigation.

Using XProtect Corporate or XProtect Expert in all the shops and then linking the sites together using Milestone Federated Architecture is often not desired, because the individual shops don't need the advanced functionality these products offer. Furthermore, using XProtect Corporate or XProtect Expert in all shops can be costly. Another reason for not using Milestone's Federated Architecture is that the bandwidth between the shops and the headquarters is often limited and used for critical business data during opening hours.

For these types of customers Milestone Interconnect is the ideal solution because it supports using the simpler low-cost VMS products in the many shops while at the same time allowing the shops to be connected to the headquarters' advanced XProtect Corporate system.

For retail customers, Milestone Interconnect answers customer needs in the following areas:

1. **Cost-effective**

With Milestone Interconnect, retail chains can build a cost-effective and geographically dispersed surveillance installation. Different sites can use different XProtect VMS or Husky products designed for small to medium businesses while still obtaining a centralized surveillance experience in the headquarters.

2. **Efficient bandwidth control:**

Milestone Interconnect offers efficient control of bandwidth usage, by configuring when

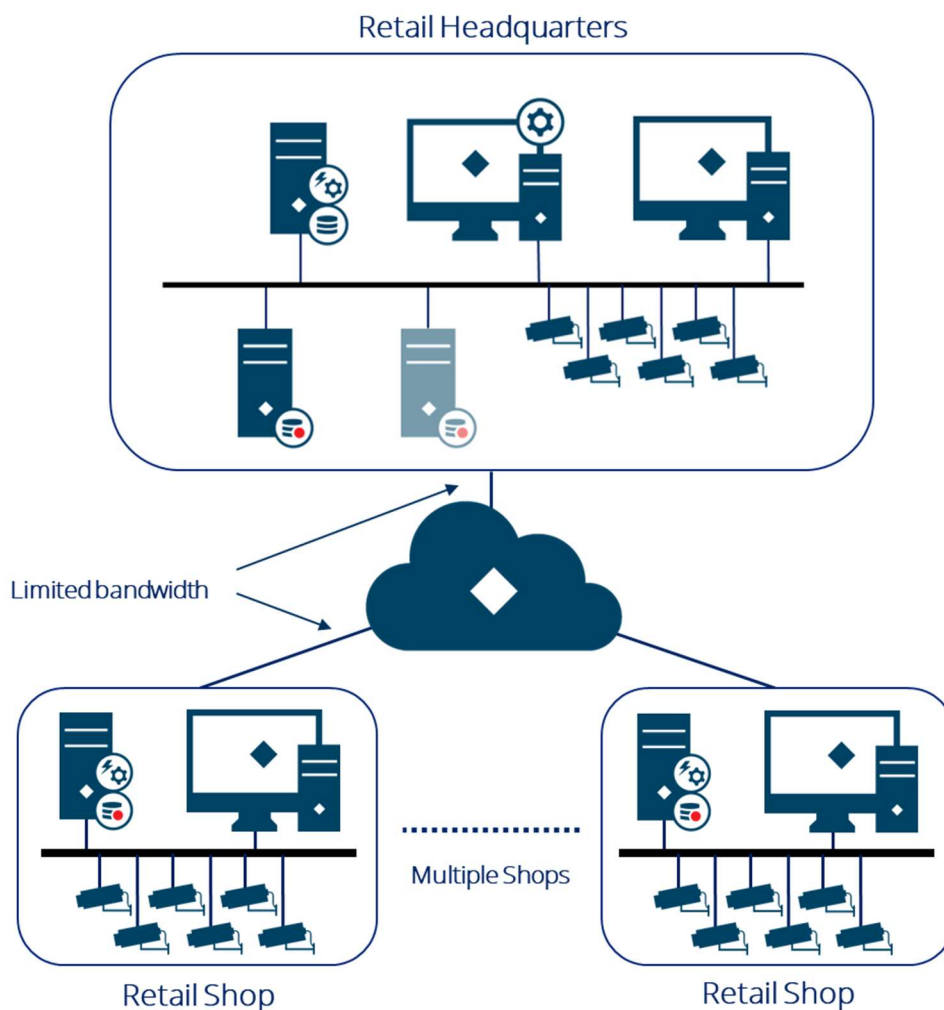
recordings are retrieved from the remote site and by setting the maximum bandwidth that can be used.

3. **Centralized management:**

Milestone Interconnect offers access to centrally monitor and manage the interconnected sites.

4. **Internal revision:**

Headquarters can have seamless access to the shops' VMS for investigating internal fraud and for exporting evidence. Should bandwidth limitations exist, the system can be configured so users instead can request recordings to be transferred to the central site, which then can be configured only to be done at a set maximum bitrate and/or time period.



## Transportation

Transportation companies need an extremely reliable and flexible solution that combines a standard surveillance installation on train stations, bus terminals, ferry terminals, or in any other buildings with onboard vehicle surveillance installations that are only connected to the surveillance network during certain times.

Mobile surveillance installations are generally a challenge since it requires either: a) permanent high-speed wireless access to the vehicles at all times - which is expensive, or b) a manual procedure to extract physically the recordings from the vehicle's onboard surveillance installation - which is slow and cumbersome.

Milestone Interconnect offers an ideal solution for transportation companies with distributed surveillance sites in buildings and vehicles. It does this by addressing the central challenges of handling intermittent connections to video surveillance installations in vehicles:

1. **Intermittent connection:**

Milestone Interconnect does not require a permanent high-speed connection to the vehicles as long as the vehicles have access to the VMS network from time to time, for instance via wireless hotspots at bus stops, train stations, ferry terminals, etc.

2. **Retrieve recordings for incident investigation:**

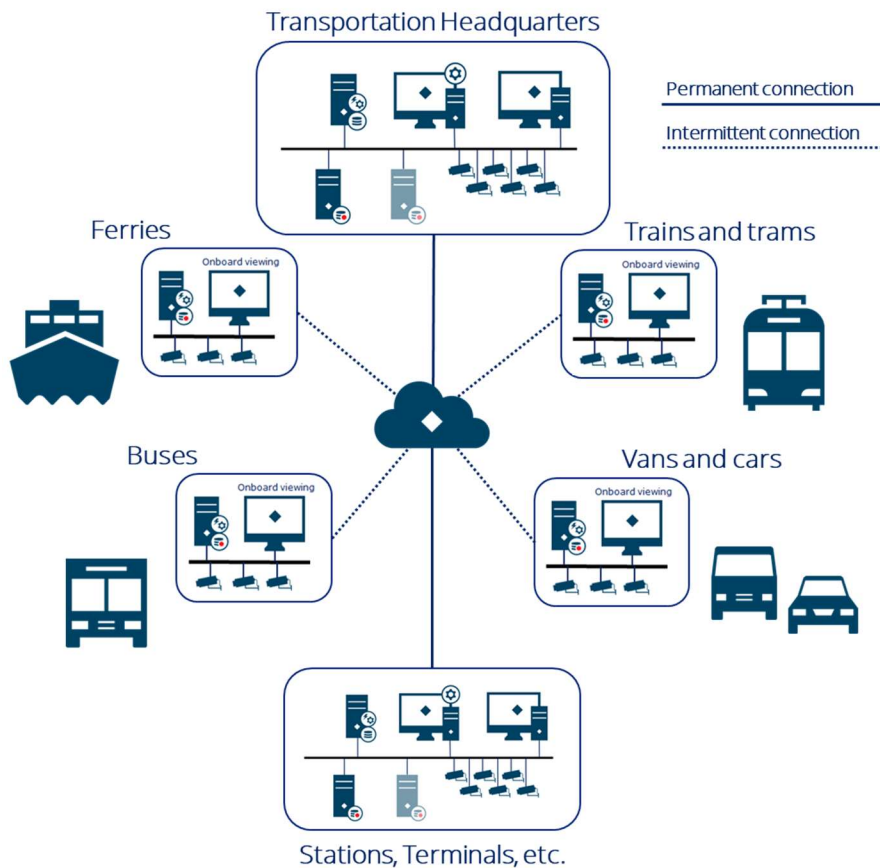
Milestone Interconnect does not need a manual procedure to retrieve recordings physically. Investigators can request recordings to be retrieved from the vehicles whether they are connected to the network or not at the time of the request. If recordings are requested while vehicles are out of network reach, the request is queued, and the needed recordings are transferred once the network is accessible again.

3. **Management:**

When the vehicles are online, the VMS in them can be accessed and administered centrally, reducing the need for physical in-vehicle maintenance.

#### 4. Combined surveillance:

With Milestone Interconnect, the VMS in the vehicles can be combined with stationary surveillance installations to provide a complete security solution.



#### Security companies offering centrally managed video surveillance

Companies offering physical onsite security combined with centrally managed video surveillance and alarm services require a VMS solution that can tie the security company's central VMS installation together with the VMS installations on the customer sites and provide access to the following specific functionality:

- Access to live and recorded video, audio, and metadata both locally for the customer and centrally for the security company
- User permissions to control what the customer can access locally and what the security company's users can access centrally
- Receive events from the customer VMS in the central security company VMS
- Trigger alarms in the security company VMS based on received events from the customer VMS installations
- Remotely maintain and administrate the customer VMS installations

In addition to these specific features, the solution must also support a mix of installations of different sizes and choice of XProtect VMS or Husky products.

With these requirements in mind, Milestone Interconnect is the ideal solution for such security companies because it offers the following:

1. **Wide product support:**

Milestone Interconnect supports all paid XProtect VMS and Husky products and installations of any size – from simple installations with only a few cameras to more advanced installations with an unrestricted number of cameras.

2. **Flexible authentication:**

Milestone Interconnect can connect to remote sites using the following authentication methods: Basic users, local Windows users, or Windows Active Directory users. Furthermore, if the customer uses a domain in their IT installation, Milestone Interconnect doesn't require an AD trust to be created between the customer's domain and the security company's domain.

3. **Central monitoring and management:**

Security companies can centrally monitor their customers' sites and quickly address any detected issues. Furthermore, the customer's installations can be managed centrally without needing to physically visit the customer site.

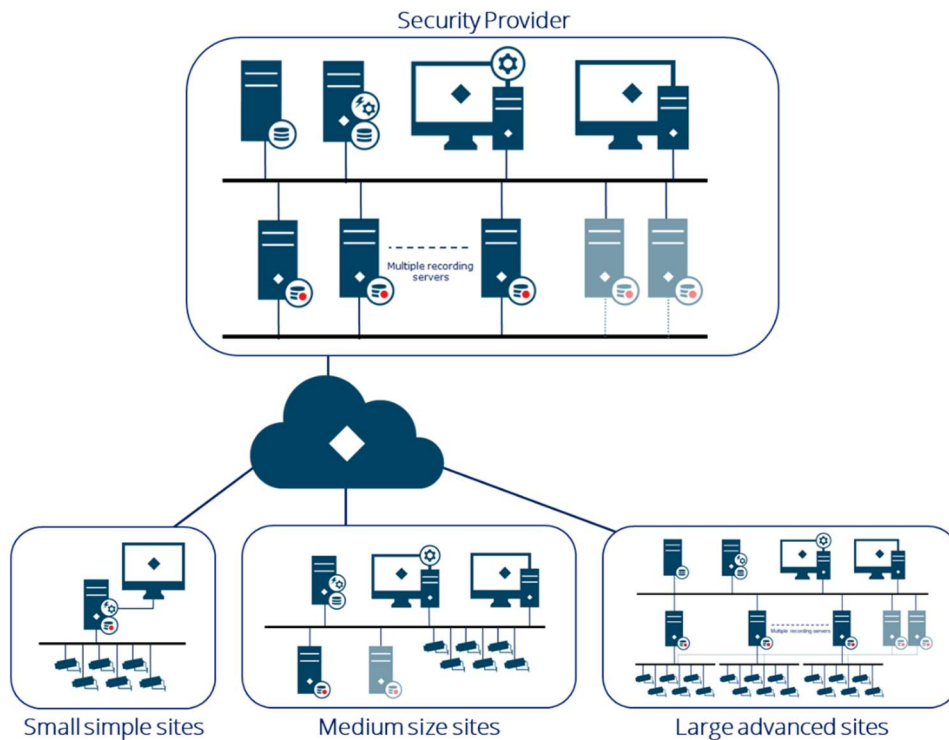
4. **Central alarm management:**

Security companies can offer their customers centralized alarm management with integrated video surveillance, which increases situational awareness, reduces response times, and can, with access to cameras, be used to identify false alarms.



### 5. Network connection:

Milestone Interconnect works with intermittent connections, low bandwidth connections, or connections where a certain percentage of the bandwidth is reserved for other purposes. This is done by support for scheduled retrieval functionality with bandwidth throttling and retrieval retry/resume functionality ensuring transfer of all requested recordings.



### City surveillance

Large, distributed city surveillance installations require a flexible and price-conscious solution that covers their needs in a highly fragmented and distributed surveillance environment, consisting of sites owned and managed by different entities ranging from individually installed cameras over small or medium-sized installations to advanced high-security installations with thousands of cameras.

XProtect Corporate addresses these needs by offering several ways to connect these cameras and surveillance sites.

#### 1. Individual cameras:

Individually mounted cameras throughout the city can be attached to the VMS in the same way as cameras connected to the local network. When attaching cameras outside the local security network to the VMS it is recommended to use HTTPS to secure the communication.

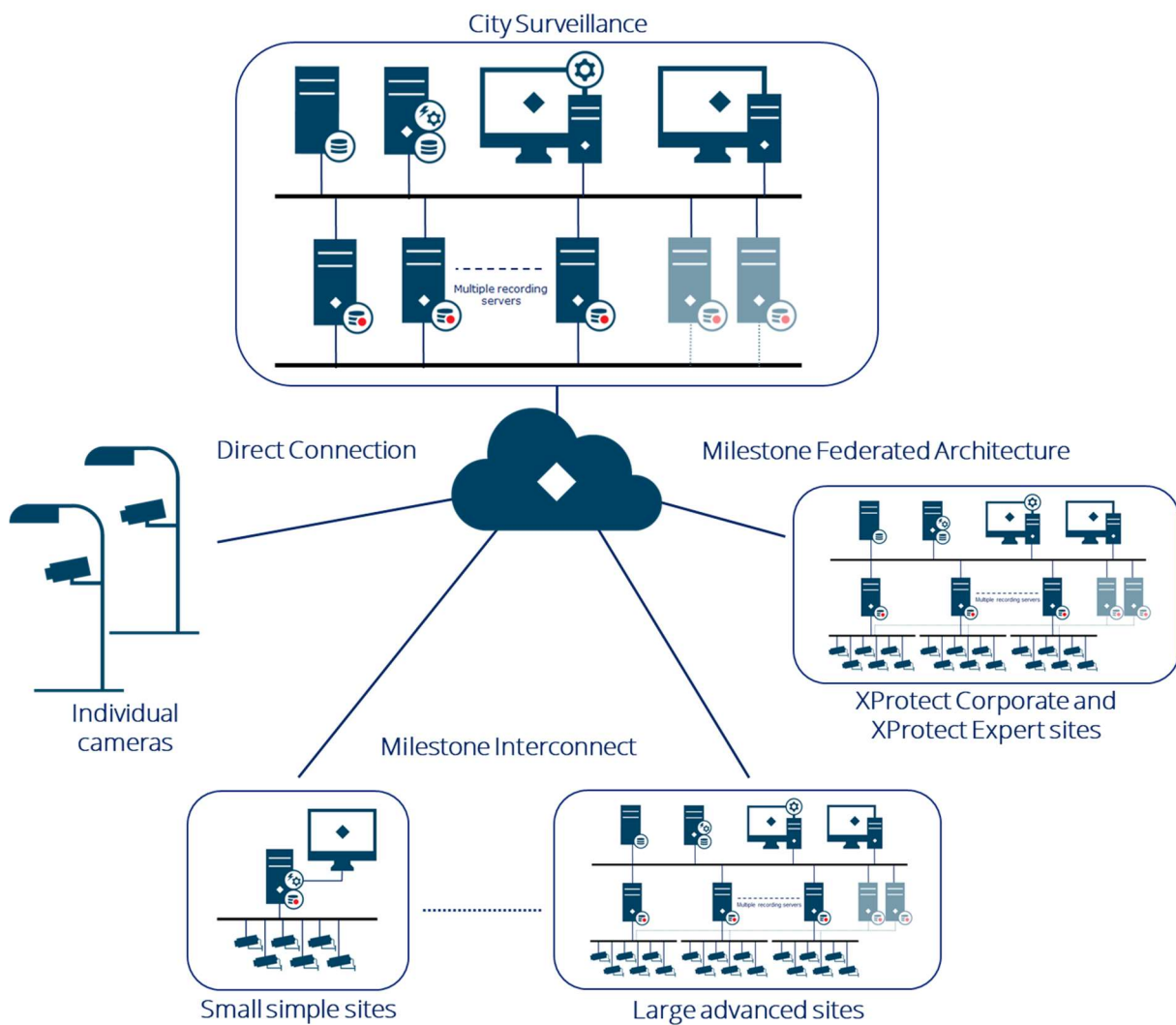
#### 2. Milestone Interconnect:

Milestone Interconnect allows multiple sites running XProtect VMS and Husky products to be

connected to a central XProtect Corporate site without needing administrator rights or AD trusts on the remote sites.

### 3. Milestone Federated Architecture:

Milestone Federated Architecture offers a solution to link XProtect Corporate and XProtect Expert sites with a central XProtect Corporate site. If the remote sites are not part of the Domain of the central site, a domain trust must be created.



Each of these three ways to attach cameras and sites to a central XProtect Corporate site offers specific strengths, features, and use cases.

In addition to the Milestone Interconnect information covered in this white paper, more information about the general VMS architecture and Milestone Federated Architecture can be found here:

- [XProtect VMS - System Architecture Guide for IT Professionals](#)
- [Milestone Federated Architecture](#)

# Milestone Interconnect Management

## Prerequisites

The following prerequisites are needed to configure Milestone Interconnect:

### Central site

- An installed and operational XProtect Corporate system
- An XProtect Corporate license that includes Milestone Interconnect camera licenses for the number of interconnected cameras – One license per interconnected and enabled camera

### Remote site

- An installed and operational paid version of the XProtect VMS or Husky product
- A configured role and user account with permissions for the devices and functions that the central XProtect Corporate site should have access to
  - **Note:** The central XProtect Corporate site can only access devices that the user account for the Milestone Interconnect connection has access to. This allows the remote site's administrators to control which devices are available to the central XProtect Corporate site

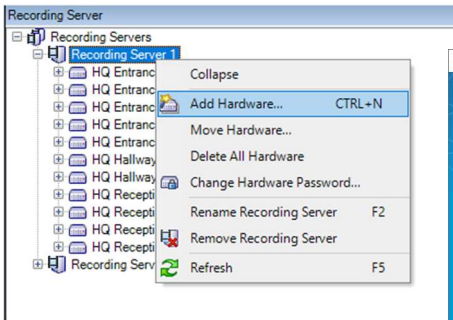
### Network

- A working network connection between the central XProtect Corporate site and the remote site
  - **Note:** Once the remote site has been added to the central XProtect Corporate system, it is OK that the network connection to the remote site is intermittent
- If communication is done over internal secure networks where NAT and firewalls are enabled in the path towards the remote VMS, then use port forwarding to ensure communication with the remote VMS.

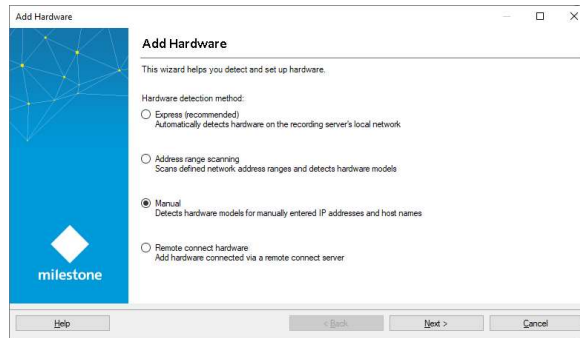
If the communication is done over nonsecure networks or the public internet, then use a VPN.

## Adding remote sites

Remote sites are added to the central XProtect Corporate site via the XProtect Corporate recording servers, in the same way, cameras and video encoders are added by using the '*Add Hardware*' wizard.



XProtect Management Client  
Add Hardware to recording server



XProtect Management Client  
Add Hardware – Manual option

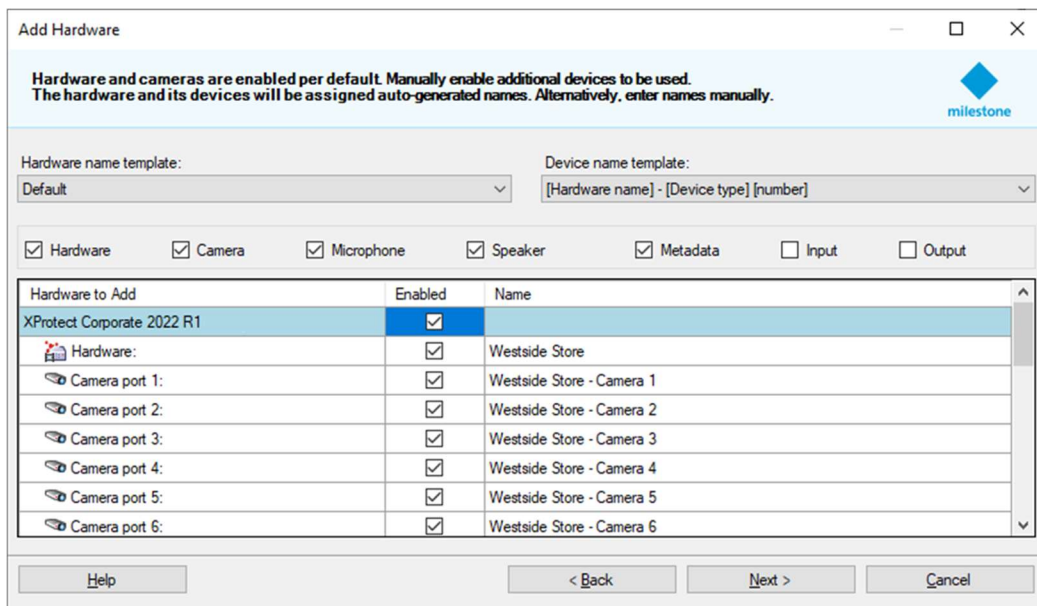
**Note:** Remote sites can only be added using the 'Address range scanning' and 'Manual' options.

Like adding cameras, the following must be specified in the wizard to detect the remote site:

- Address - or address scan range
- Port
- Use HTTP or HTTPS
- Select Milestone Interconnect driver to use – for example, 'Milestone XProtect VMS Interconnect'
- User account to authenticate with

**Note:** The XProtect VMS cannot be autodetected, so the driver must be selected manually.

On the 'Add Hardware' wizard's step where the detected devices can be named, the wizard will use the remote site's server and device names by default.

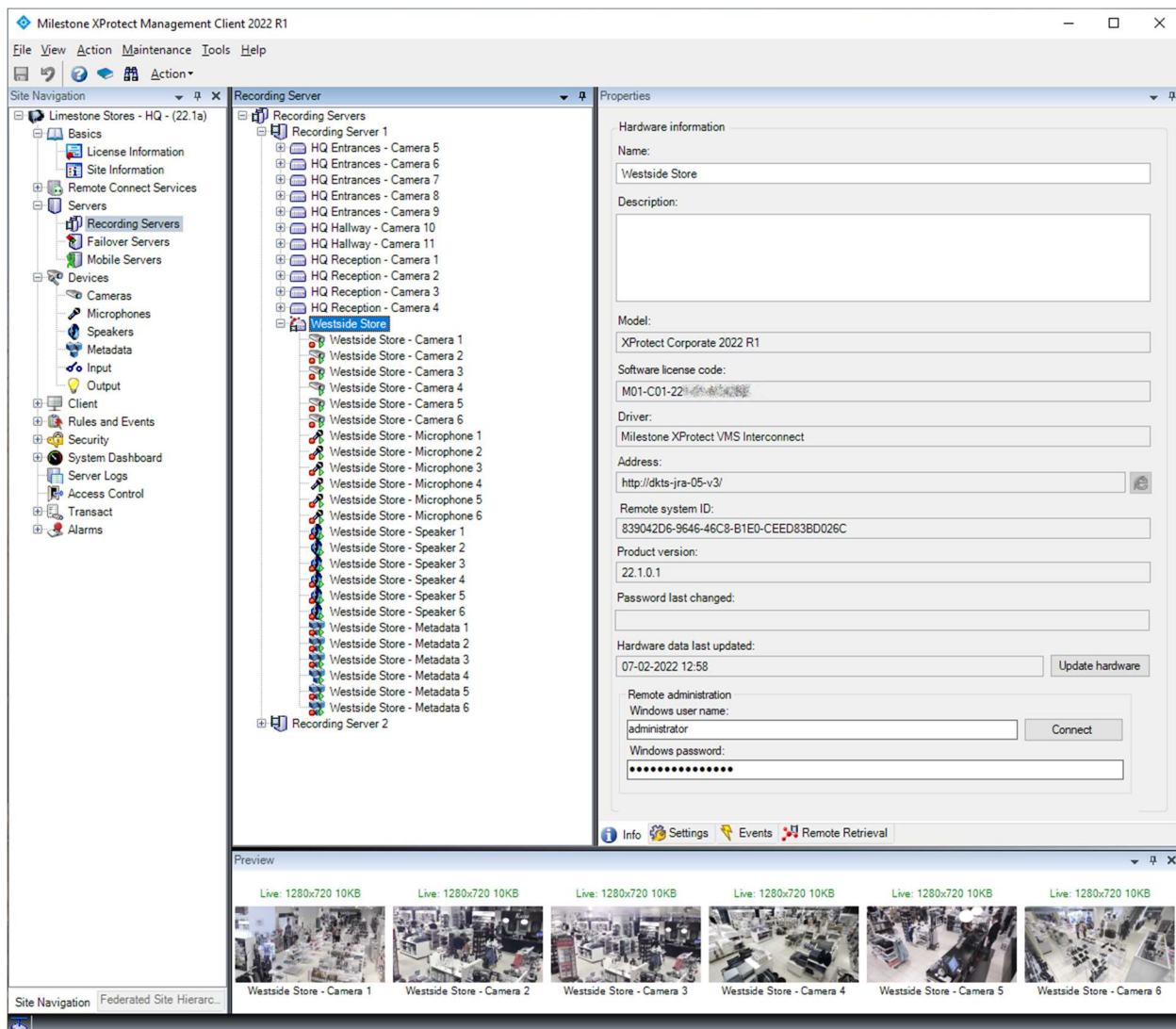


XProtect Management Client  
Add Hardware – Enable devices and set names

These default auto-assigned names can be changed for the central XProtect Corporate site in the Add Hardware dialog or later by using the standard functions of the XProtect Management Client like for normal cameras. Doing this will not change the names on the remote site. In this way, you can ensure that cameras will have unique names in the central site, even though cameras may reuse the same names across the interconnected sites.

If needed later, the original names of the devices on the remote site can be seen by selecting the device's 'Settings' tab in the XProtect Management Client.

When the remote site has been added to a recording server, it is listed the same way standard cameras and video encoders are.



### XProtect Management Client Remote site added

At this point, it is worth remembering that the cameras, microphones, speakers, and metadata sources listed for the interconnected system are the ones the central XProtect Corporate has been granted

access to by the administrator of the remote site (via the user account used for connecting to the remote site).

Therefore, if all the expected devices are not listed, or certain functions are missing, the permissions for the user and role must be checked by the administrator on the remote site. Similarly, if new devices are added to the remote site, and the central site should have access to these, the “interconnect” user permissions must be updated to grant access to the new devices. Finally, an update function must be done on the central site to update the configuration with the new devices.

### Settings - remote sites and devices

The interconnected remote site has a few tabs for displaying site information and for configuring settings, events, and remote recording retrieval.

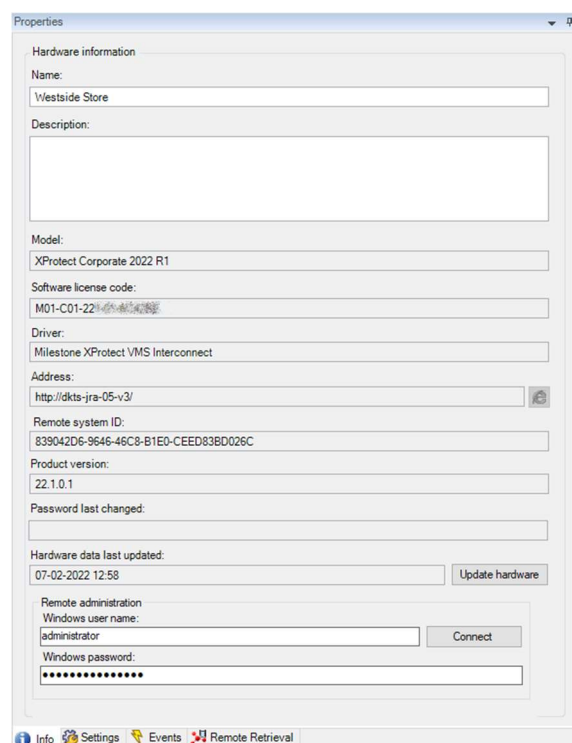
The *'Info'* tab displays certain details of the interconnected remote sites like: Product (*model*), Version, Software License Code (SLC), etc.

Furthermore, it has an *'Update Hardware'* function which refreshes the configuration to match what can be accessed on the interconnected site. This function must be used if changes are made on the interconnected site, such as adding a new camera that should be available to the central site.

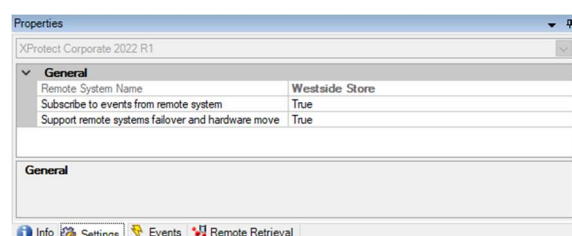
Finally, via Windows remote desktop, access to the server running the management server on the remote site is available. This requires remote desktop to be enabled on the remote site, and the administrator to know the Windows credentials for the server.

If the name of the remote site has been changed in the central XProtect Corporate site, the *'Settings'* tab will display the remote site's original name. The same applies to cameras and other devices when selecting the *'Settings'* tab for these.

On the *'Settings'* tab, it is also possible to disable subscription to events, failover, and move hardware updates. If not using events, failover, and only having one recording server on the remote site, disabling these can be used to reduce the communication with the remote site to an absolute minimum.



XProtect Management Client  
Interconnected site – Info tab



XProtect Management Client  
Interconnected site – Settings tab



The 'Events' tab lists the system events that are available from the remote interconnected site. The events that are supported depend on the specific XProtect VMS or Husky product used on the remote site.

Events available for the individual devices can be seen on the device's 'Events' tab

See the [Milestone Interconnect Compatibility](#) site for supported products, versions, and events.

The 'Remote Retrieval' tab allows the user to set the maximum total bandwidth of recordings that can be retrieved from the remote site for all devices retrieved in parallel.

Furthermore, the time interval allowing retrieval of recordings can be specified.

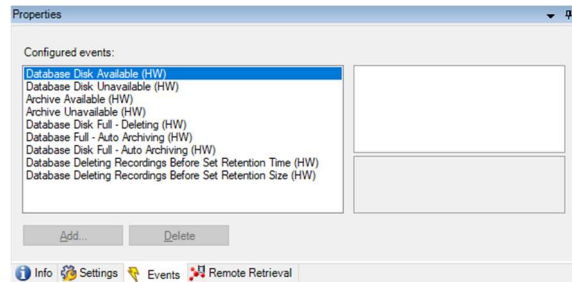
Finally, the number of devices to retrieve recordings from in parallel can also be set here. The default is eight devices in parallel, but this can be increased to better utilize the bandwidth, if a lot of bandwidth is available.

**Note:** The 'Remote retrieval' settings only apply to retrieval of recordings from the remote site's database to the central XProtect Corporate site's recording server's database. The settings do not apply in case the remote site is configured for direct playback (see "Remote recording and direct playback configuration" section). In that case, remote recordings played back in the clients will be retrieved as fast as possible to give a smooth and responsive experience in the clients.

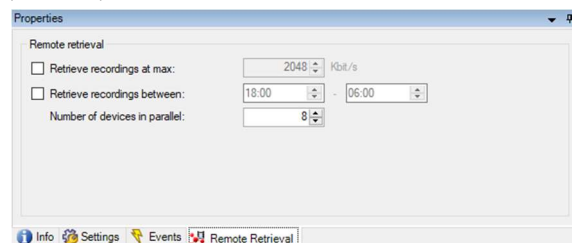
### Updating remote site devices

If the configuration of an interconnected site has been changed, for instance by adding or removing cameras or events, the configuration in the central XProtect Corporate site must be updated to reflect the actual configuration of the interconnected site.

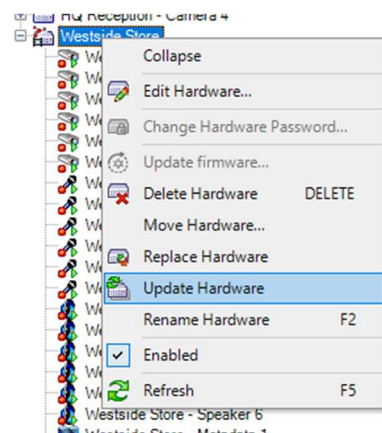
The update must be done manually by selecting the hardware device representing the remote site, and on the 'Info' tab, clicking the 'Update hardware' button. Alternatively, right-click the hardware device representing the remote site and select 'Update Hardware'.



XProtect Management Client  
Interconnected site – Events



XProtect Management Client  
Interconnected site – Remote Retrieval tab



XProtect Management Client  
Interconnected site – Update Hardware

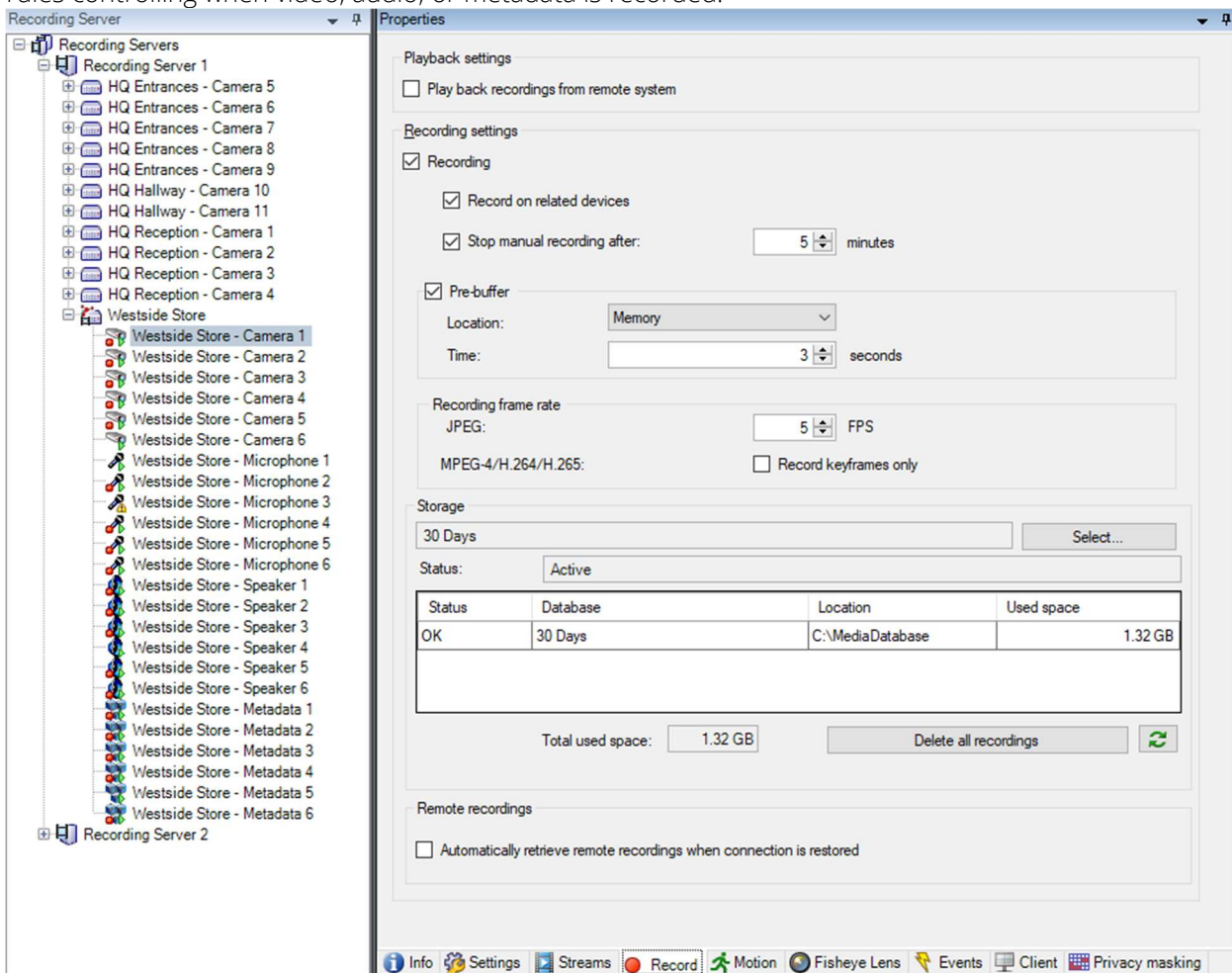
Both actions will open a dialog that refreshes the configuration and lists a summary of any detected changes.

## Interconnect playback configuration

### Playback from the central XProtect Corporate site

When selecting a camera, microphone, speaker, or metadata device attached to the remote site, it is possible to select if recordings should be played back from the remote site or from the central XProtect Corporate site.

When recordings are set to be done in the central XProtect Corporate site, the standard XProtect Corporate recording settings can be used like for normal cameras. The same applies when creating rules controlling when video, audio, or metadata is recorded.



The screenshot displays the XProtect Management Client interface. On the left, a tree view shows 'Recording Servers' with two servers listed: 'Recording Server 1' and 'Recording Server 2'. Under 'Recording Server 1', various devices are listed, including cameras (HQ Entrances - Camera 5-9, HQ Hallway - Camera 10-11, HQ Reception - Camera 1-4) and a 'Westside Store' section with cameras (1-6), microphones (1-6), speakers (1-6), and metadata (1-6). 'Recording Server 2' is also listed.

The main window shows the 'Properties' dialog for a selected device. It is divided into several sections:

- Playback settings:** A checkbox for 'Play back recordings from remote system' is currently unchecked.
- Recording settings:**
  - 'Recording' is checked.
  - 'Record on related devices' is checked.
  - 'Stop manual recording after:' is set to 5 minutes.
  - 'Pre-buffer' is checked, with 'Location' set to 'Memory' and 'Time' set to 3 seconds.
  - 'Recording frame rate' is set to 5 FPS.
  - 'MPEG-4/H.264/H.265:' has 'Record keyframes only' unchecked.
- Storage:**
  - 'Storage' is set to '30 Days'.
  - 'Status' is 'Active'.
  - A table shows recording status and space usage:
 

Status	Database	Location	Used space
OK	30 Days	C:\MediaDatabase	1.32 GB
  - 'Total used space:' is 1.32 GB.
  - 'Delete all recordings' button is visible.
- Remote recordings:** A checkbox for 'Automatically retrieve remote recordings when connection is restored' is unchecked.

The bottom toolbar includes icons for Info, Settings, Streams, Record, Motion, Fisheye Lens, Events, Client, and Privacy masking.

### XProtect Management Client

Interconnected Camera – Record tab – Central site recording

In addition to standard recording on rules, the remote site can be used as a kind of “edge storage” device for recovering missing recordings in case of network or recording server issues by selecting the ‘Automatically retrieve remote recordings when connection is restored’ checkbox.



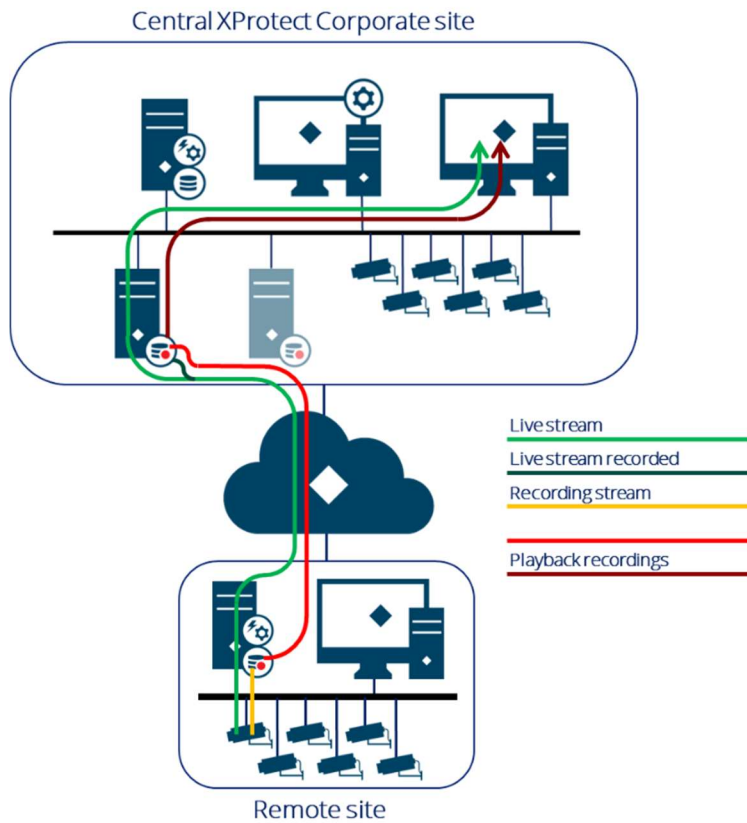
In addition to the automatic recording retrieval function, it is also possible to use the rules to trigger retrieval of recordings and for users of the XProtect Smart Client to request recordings to be retrieved.

Furthermore, when recording on both the central and remote sites, Scalable Video Quality Recording (SVQR) can be used to record low-quality recordings on the central XProtect Corporate site, and then later retrieve high-quality recordings from the remote site, for instance on certain events or on manual user request (See the SVQR section).

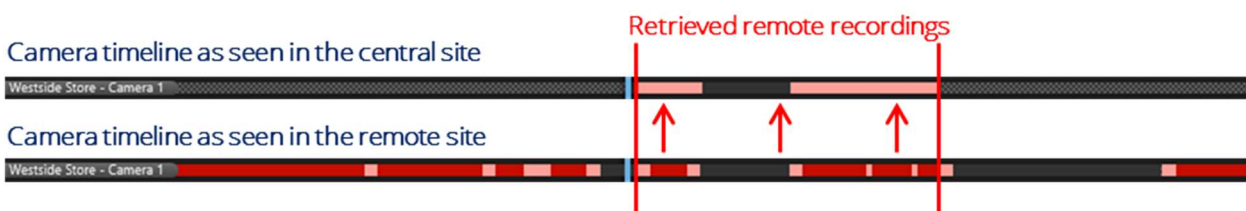
By default, the central XProtect Corporate site always starts streaming live video, audio, and metadata from the remote site to the central XProtect Corporate site. If the live streams are not always needed in the central XProtect Corporate site, for instance, if the central XProtect Corporate site should not record by default, the rule-system can be used to configure the live stream not to start, or maybe only to start when live streams are requested by clients. Doing so will reduce the network traffic from the remote site to the central site to a minimum.

With recording enabled in the central XProtect Corporate system, the timeline for users connected to the central site will not necessarily be the same as for users connected directly to the remote site. This is because each site records by its own rules and because recordings can be retrieved (copied) from the remote site to the central site.

This drawing illustrates that both sites have their own media database in their recording servers and thus may record different amounts of media.

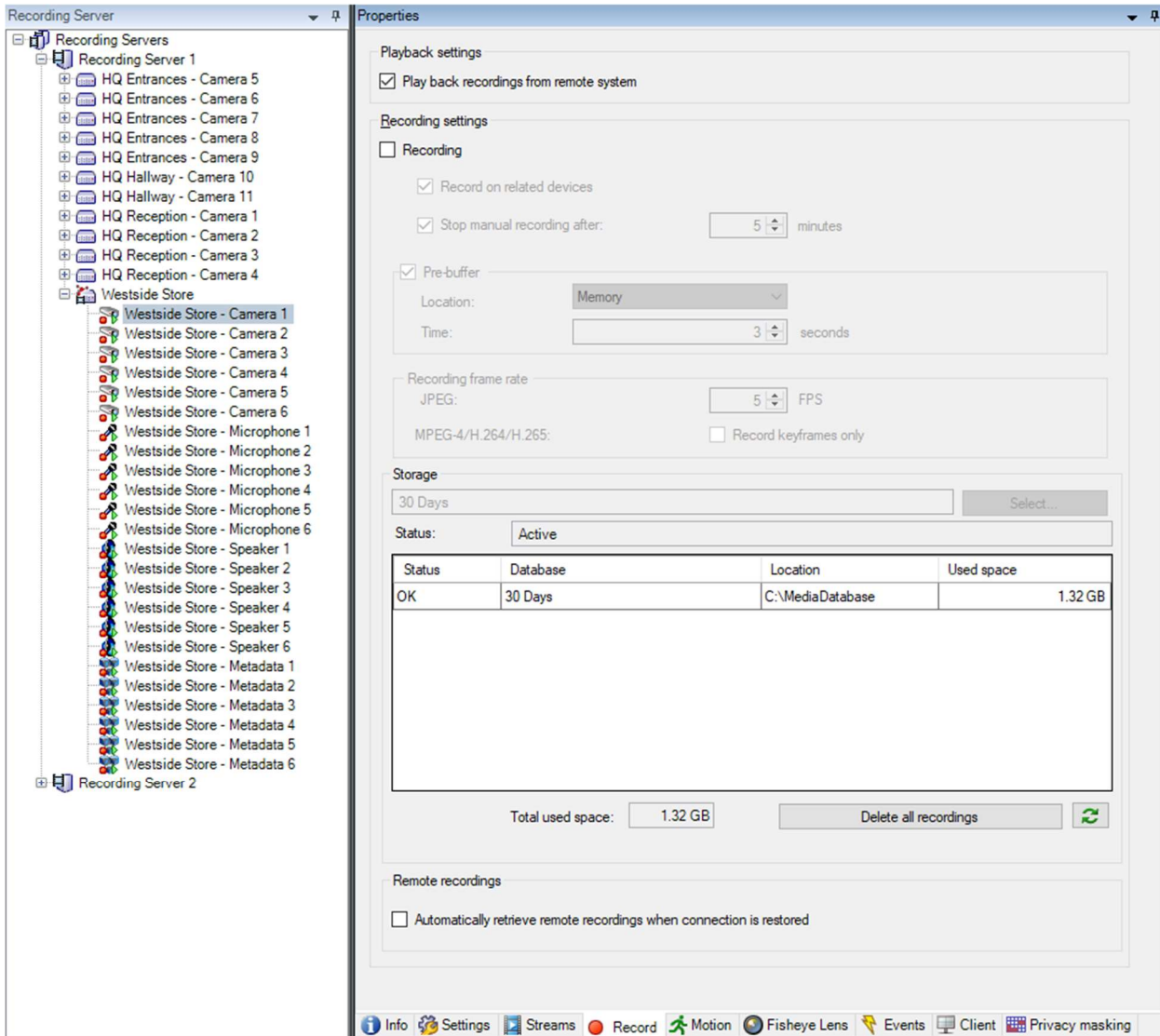


The timeline illustrates the difference in recorded media on the central XProtect Corporate site and the remote interconnected site. For this specific illustration, recording is enabled on the central XProtect Corporate site, but no rules have been configured to trigger recording – The users, however, can retrieve recordings when needed.



## Playback from the remote interconnected site

Selecting to playback recordings directly from the remote interconnected site can be done from the interconnected device's 'Record' tab by selecting the 'Play back recordings from remote site' checkbox. This will also disable recording of the device in the central XProtect Corporate site's recording server.



The screenshot shows the 'Recording Server' configuration window. On the left, a tree view shows 'Recording Server 1' and 'Recording Server 2'. Under 'Recording Server 2', 'Westside Store' is expanded, showing various camera, microphone, speaker, and metadata devices. The 'Properties' window on the right is configured as follows:

- Playback settings:**  Play back recordings from remote system
- Recording settings:**
  - Recording
  - Record on related devices
  - Stop manual recording after: 5 minutes
  - Pre-buffer
    - Location: Memory
    - Time: 3 seconds
  - Recording frame rate: 5 FPS
  - MPEG-4/H.264/H.265:  Record keyframes only
- Storage:** 30 Days, Select... button
- Status:** Active
- Table:**

Status	Database	Location	Used space
OK	30 Days	C:\MediaDatabase	1.32 GB
- Total used space:** 1.32 GB, Delete all recordings button, Refresh button
- Remote recordings:**  Automatically retrieve remote recordings when connection is restored

At the bottom, there is a navigation bar with icons for Info, Settings, Streams, Record, Motion, Fisheye Lens, Events, Client, and Privacy masking.

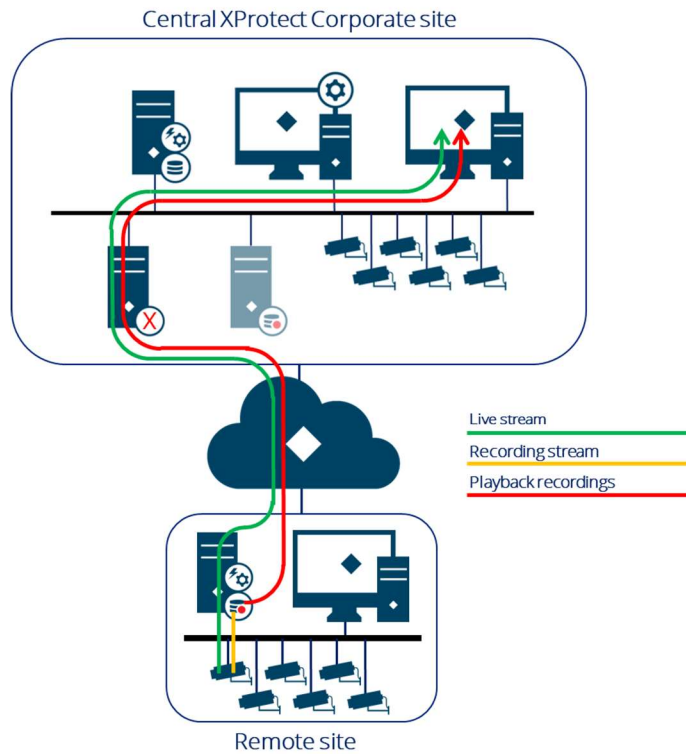
### XProtect Management Client

Interconnected Camera – Record tab – Remote interconnected site recording

Clients playing back recordings with this configuration will still communicate with the recording server on the central XProtect Corporate site. However, the recording server will retrieve recordings from the remote interconnected site's recording database rather than fetching it from its own recording database.

Selecting to play back recordings from the remote site also disables the function to retrieve recordings from the remote site because the device doesn't have a media database on the central site.

This drawing illustrates that only the remote site has a media database in the recording server and thus is the only system that can record.



The timeline illustrates that users experience the same timeline no matter if connected to the central or remote site.

Camera timeline as seen in the central site



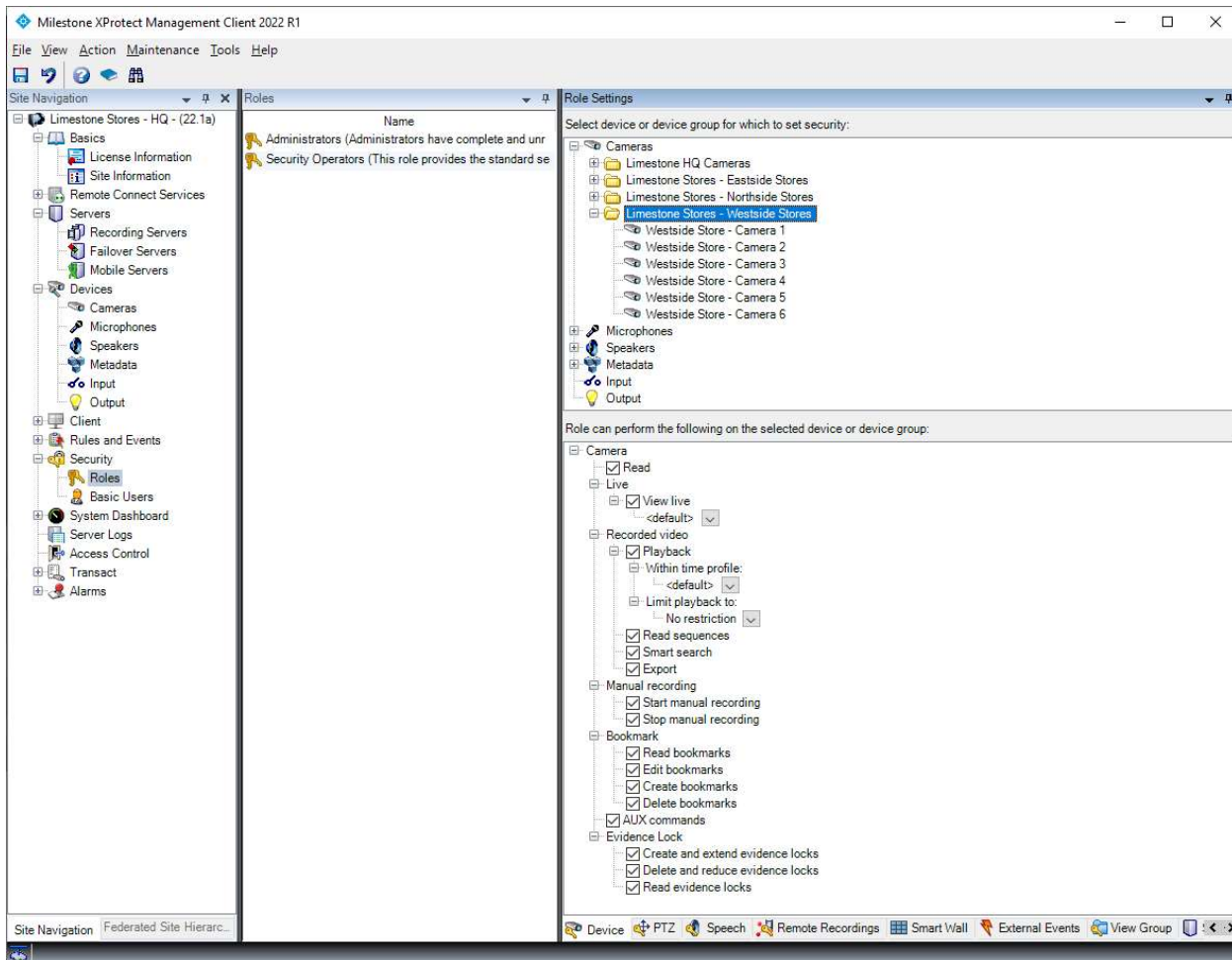
Camera timeline as seen in the remote site



The timelines are identical as all recordings are played back from the remote site

## User rights in XProtect Corporate

Configuration of user rights for the interconnected devices (cameras, microphones, speakers, metadata, inputs, and outputs) are done in the same way as for regular devices, by creating a “Role” and assigning access to the devices and functions.

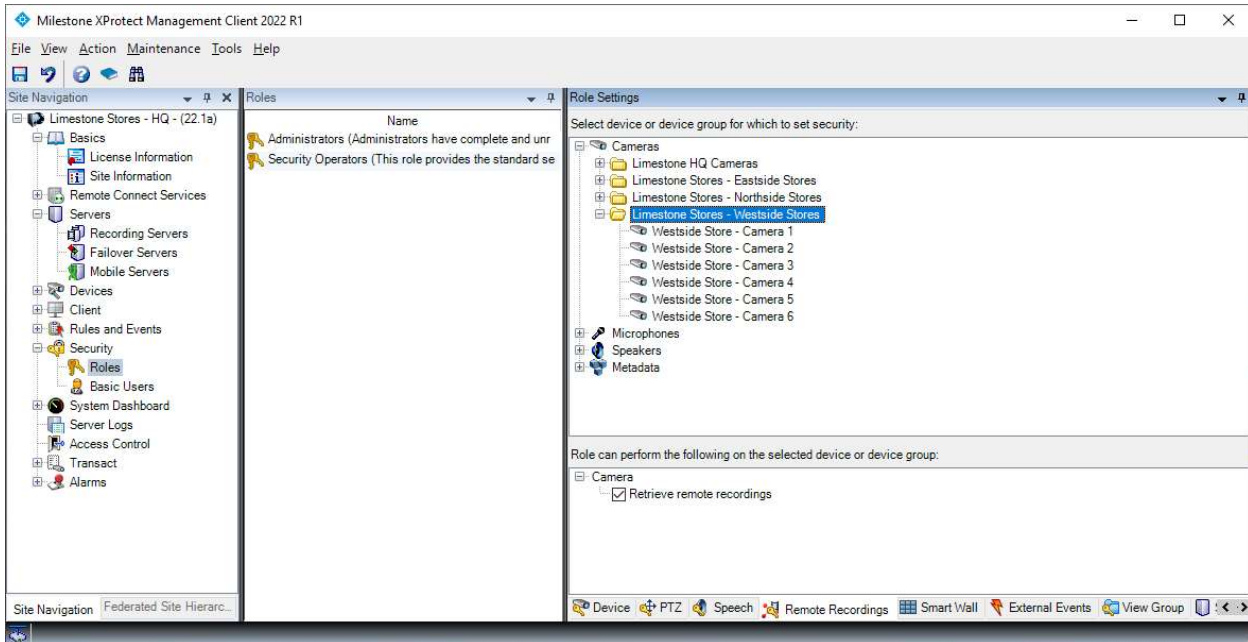


### XProtect Management Client

#### Roles – Device permissions

The bookmark function works on interconnected cameras whether they are recorded in the central XProtect Corporate site, in both sites, or only in the remote site. The same applies for the function to time-limit access to live and playback of video, audio, and metadata, which also works on interconnected devices even though the interconnected remote site itself may not support time-limited access rights.

In addition to the standard device rights, the interconnected devices also have a dedicated tab called 'Remote Recordings'. On this tab the rights to retrieve remote recordings can be enabled, allowing users to retrieve recordings from the devices on the remote site.



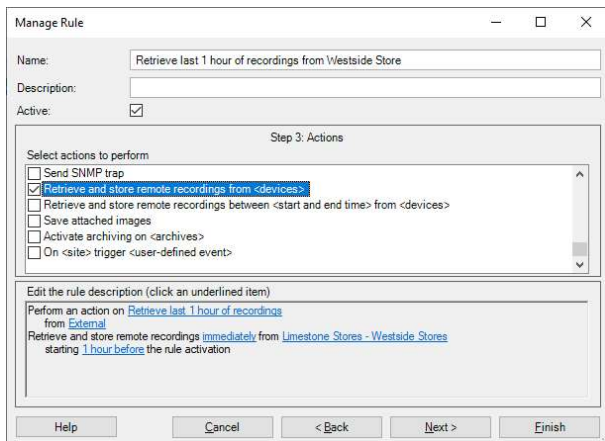
XProtect Management Client  
Roles – Remote Recordings permissions

### Rules

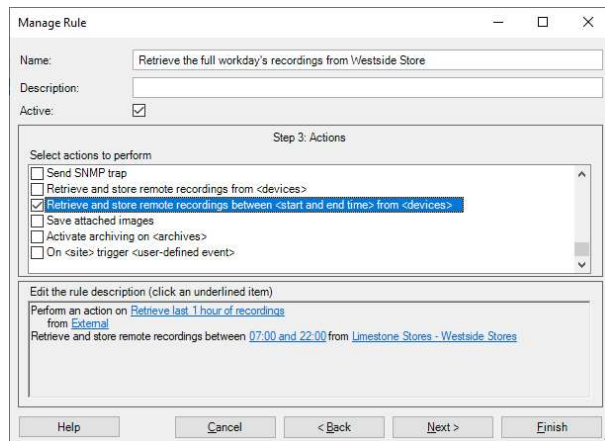
For interconnected devices configured to record in the central XProtect Corporate site, the rule system can be used to retrieve recordings from the remote site on events and/or on a time schedule.

When retrieving remote recordings, it is possible to select to retrieve recordings from a specific time interval or a set time before an event or schedule occurred.

The rules are set up in the XProtect Management Client using the 'Manage Rule' wizard. Below are two examples of rules that retrieve the last hour of recordings (left) and retrieve recordings between 07.00 and 22.00 from a group of cameras on an event.



XProtect Management Client  
Manage Rule – Retrieve recordings from n-time before event



XProtect Management Client  
Manage Rules – Retrieve recordings from a defined time period



## Milestone Interconnect and XProtect Smart Client operation

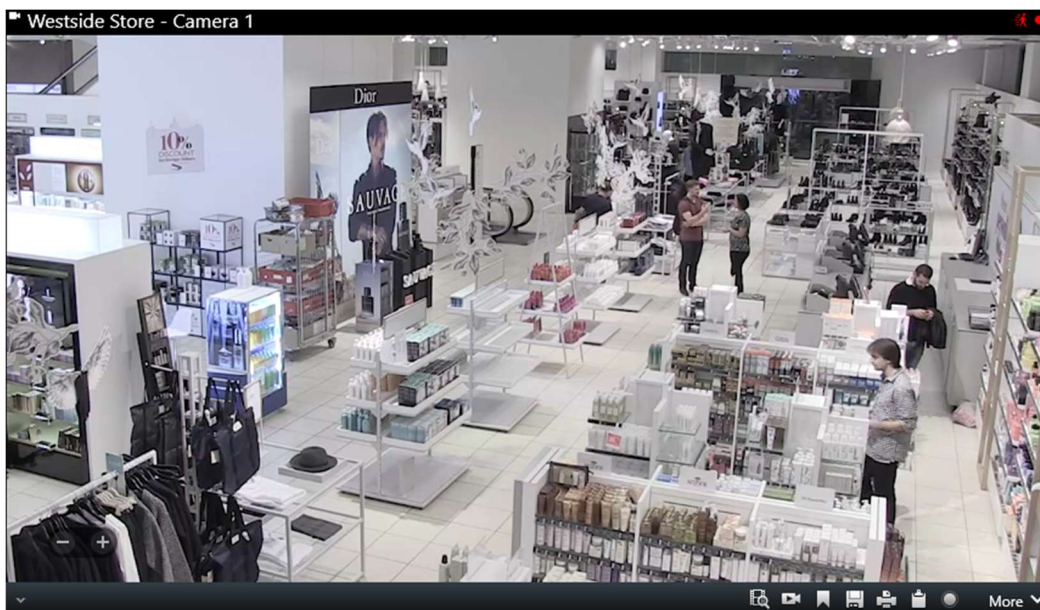
### Setup

Interconnected cameras appear in the XProtect Smart Client's list of cameras like any other regular cameras, and they have the same properties and are added to views the same way regular cameras are.

### Live

Interconnected cameras are displayed live in the views the same way as regular cameras are, and have the same functions on the camera toolbar as regular cameras do regardless of whether they are recorded in the central XProtect Corporate site, on both sites, or only at the remote interconnected site.

The screenshot shows an interconnected camera in the XProtect Smart Client in live mode, showing the camera toolbar with available functions.

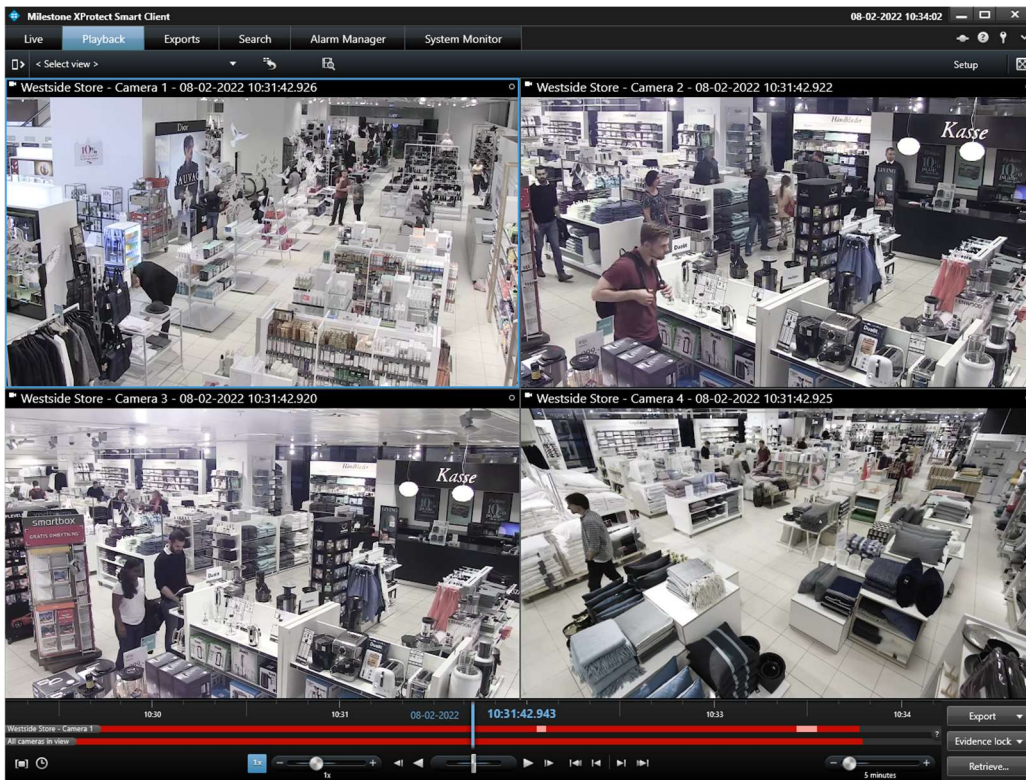


XProtect Smart Client

Interconnected camera shown in XProtect Smart Client

## Playback remote recordings

When interconnected cameras are configured to play back recordings directly from the remote site, they appear in the XProtect Smart Client and show the timeline just like any other regular camera.



XProtect Smart Client  
Playback recordings directly from remote interconnected site

When interconnected cameras are configured to be played back directly from the remote site, the recordings are retrieved directly from the remote site's database and there will not be a media database on the central site recording server. With this configuration, the timeline for both the operators on the central XProtect Corporate site and the remote site's operators will be identical, and it will not be possible to retrieve remote site recordings.

Furthermore, direct playback of remote recordings requires the remote site to be online. If the remote site is offline, the client will report an error for the cameras. Finally, any configured remote retrieval bandwidth limits or time restrictions will not apply with this configuration.

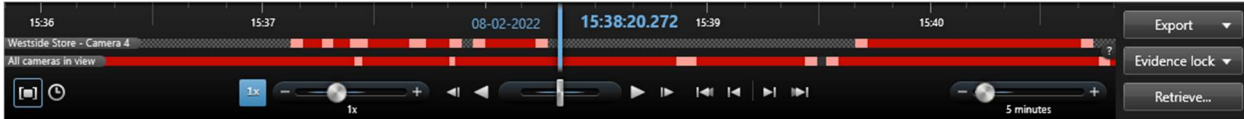
## Playback recordings from the central site and retrieval of remote recordings

When interconnected cameras are configured to record and play back recordings in the central XProtect Corporate site, the camera will appear in the XProtect Smart Client just like any regular camera.

However, if the XProtect Smart Client operator has user rights to retrieve remote recordings, the camera timeline will display additional information and will offer a function to retrieve the remote recordings.





This is indicated by a grey pattern in the normally black space between recordings to indicate there might be recordings on the remote site that can be retrieved by the XProtect Smart Client operator.

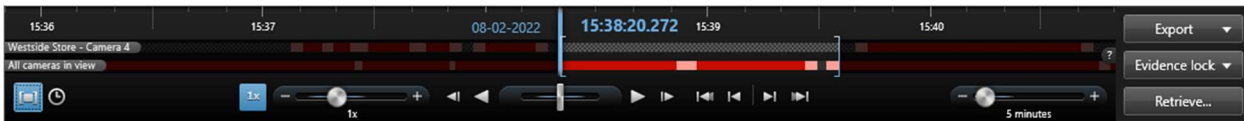


#### XProtect Smart Client

Playback – Timeline indicating remote recordings may be available

Retrieving recordings from the remote site is done by selecting the time period and the cameras to retrieve from in the same way as when selecting a time period to export.

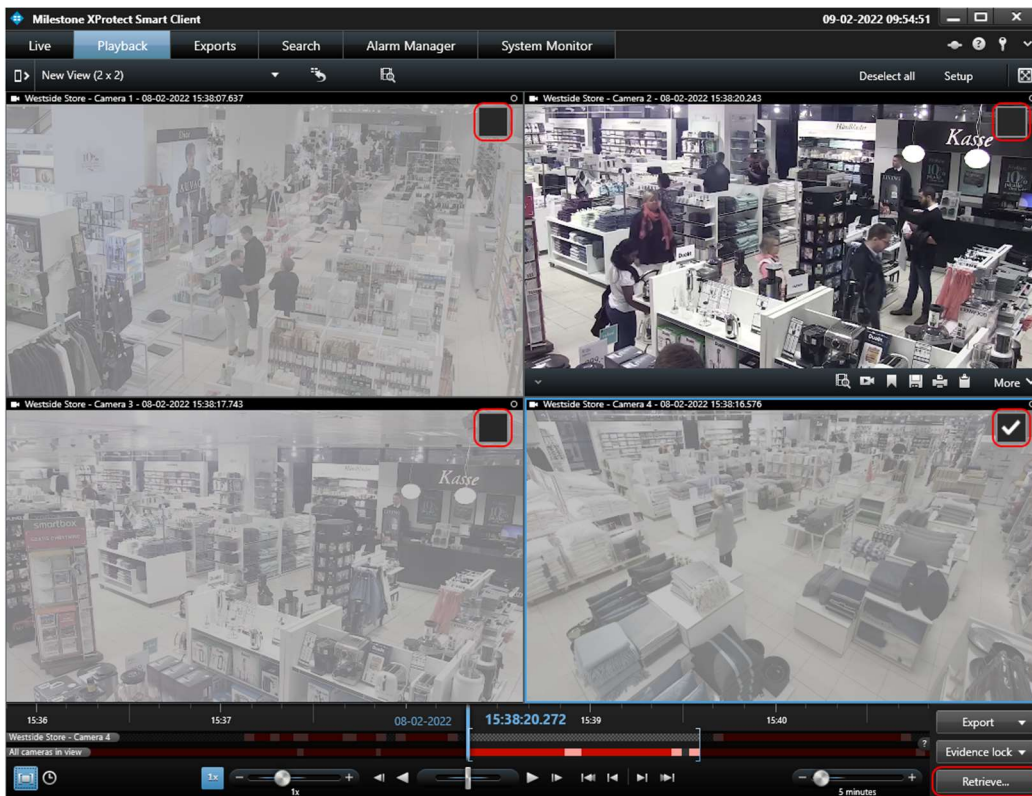
Either – Click the  button and select the desired timespan graphically on the timeline, or click the  button and enter the desired timespan directly.



#### XProtect Smart Client

Playback – Time period selected on timeline

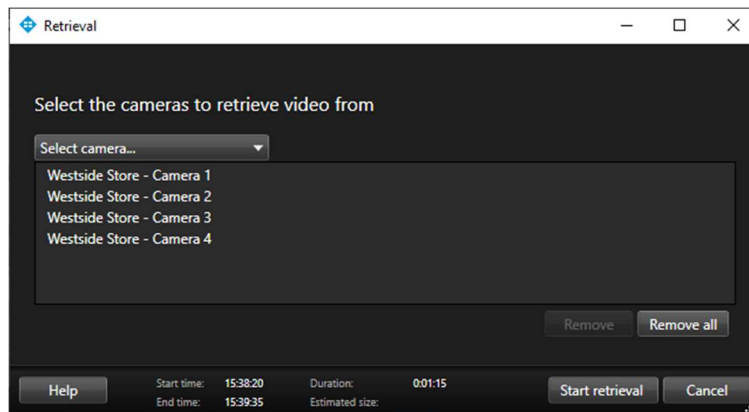
When the time span has been selected, the cameras to retrieve recordings from can be selected by clicking on the checkboxes displayed for each camera (the current camera is selected by default).



#### XProtect Smart Client

Playback – Selected timespan and cameras to retrieve from

When the timespan and cameras in the view have been selected, the retrieval job is created by clicking the 'Retrieve...' button. This will open the 'Retrieval' dialog where additional cameras can be selected if needed. Clicking the 'Start Retrieval' button will create the retrieval job.



XProtect Smart Client  
Retrieve recordings – select cameras to retrieve from

The created job will be indicated on the timeline by a lighter grey pattern, as shown here.

XProtect Smart Client  
Playback – Selected timespan before retrieval



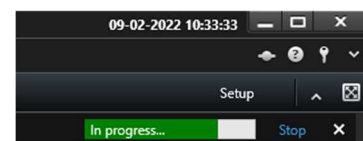
XProtect Smart Client  
Playback – Selected timespan after retrieval

When the retrieval job is complete, the timeline will show the periods with retrieved recordings with a light red color and periods that didn't have any recordings on the remote site with the standard dark grey background.



If a bandwidth and time limitation have been set for retrieving recordings from the remote site, the remote recordings will be retrieved when the retrieval time-period allows it and with the maximum bandwidth specified. If these limitations have not been set, the recordings will be retrieved immediately and at the highest speed possible.

## Retrieval Jobs

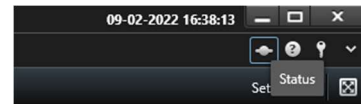
When a retrieval job is created, it will display the progress in the top of the XProtect Smart Client in the same way as export jobs are.



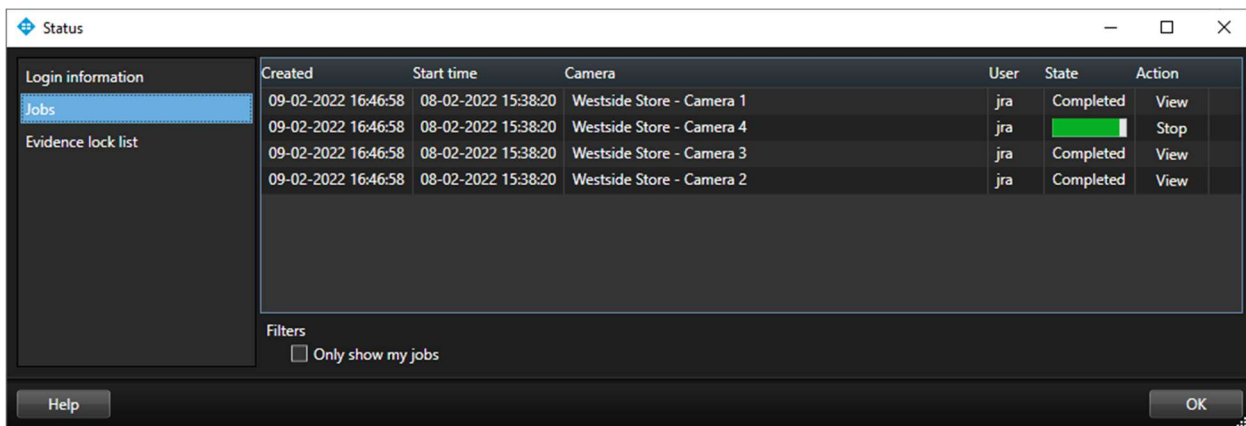
XProtect Smart Client  
Retrieval progress

Hide the jobs shown by clicking on the  button or remove the individual jobs from the list by clicking on the  button (it will not cancel the retrieval job). To cancel an ongoing job, click the **Stop** button.

For a complete overview of all jobs, pending, in progress, stopped, or completed, the 'Jobs' overview can be used. It can be found by opening the 'Status' dialog and selecting the 'Jobs' tab.

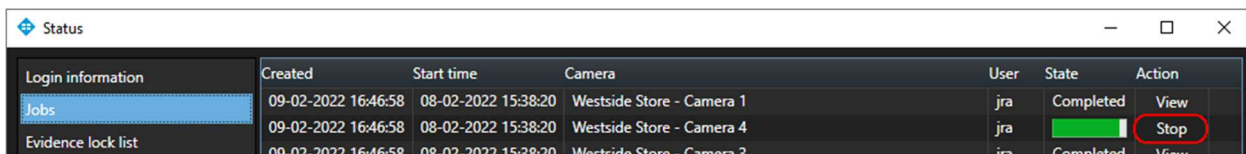


XProtect Smart Client  
Status dialog button



XProtect Smart Client  
Status - Jobs

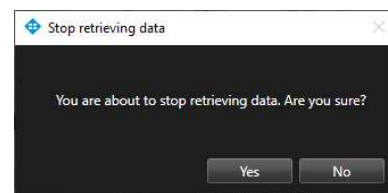
If necessary, the ongoing or pending retrieval jobs can be canceled by clicking on the **Stop** button.



XProtect Smart Client  
Status dialog - Jobs; Stop action

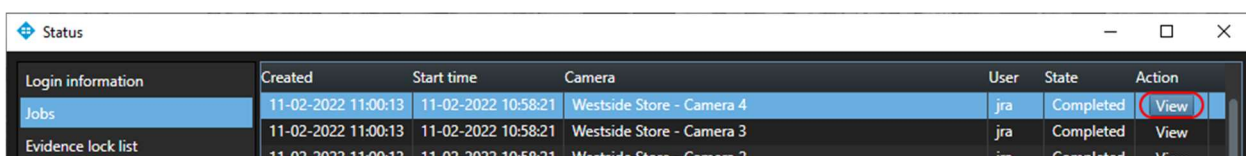
Users will be prompted to confirm that the retrieval should be stopped.

**Note:** If an ongoing retrieval job is stopped, the recordings that have already been retrieved will not be deleted from the central site's media database.



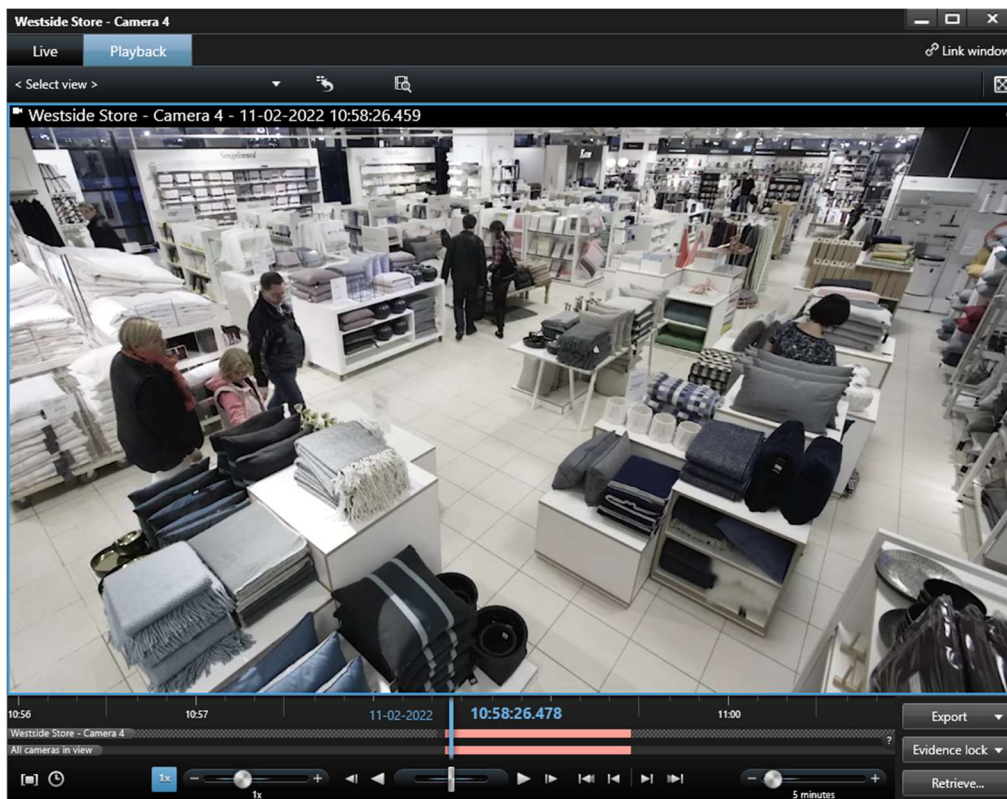
XProtect Smart Client  
Stop retrieving data - confirm action

If the operator wants to view the retrieved recordings, this can be done by clicking the **View** button.



XProtect Smart Client  
Status dialog - View retrieved recordings

When clicked, a floating playback window will open showing the camera at the beginning of the retrieved time period. The operator can now play back the recordings easily or export them for other purposes.



XProtect Smart Client  
Floating window – playback from start time of retrieved recordings

## Milestone Interconnect in comparison to Edge Storage

Cameras with Edge Storage have built-in storage or storage directly associated with the camera, where the camera can store video, audio, and metadata. When a Milestone surveillance site is interconnected, the complete remote surveillance site, including cameras, microphones, speakers, and metadata devices and the associated media databases can be seen as a kind of “multi-channel video encoder” with Edge Storage support connected to the central XProtect Corporate site.

Since Milestone Interconnect is implemented in general the same way as Edge Storage for cameras, it offers the same basic functions and benefits as Edge Storage, plus some more advanced functions such as direct playback from the remote site, system events and status monitoring.

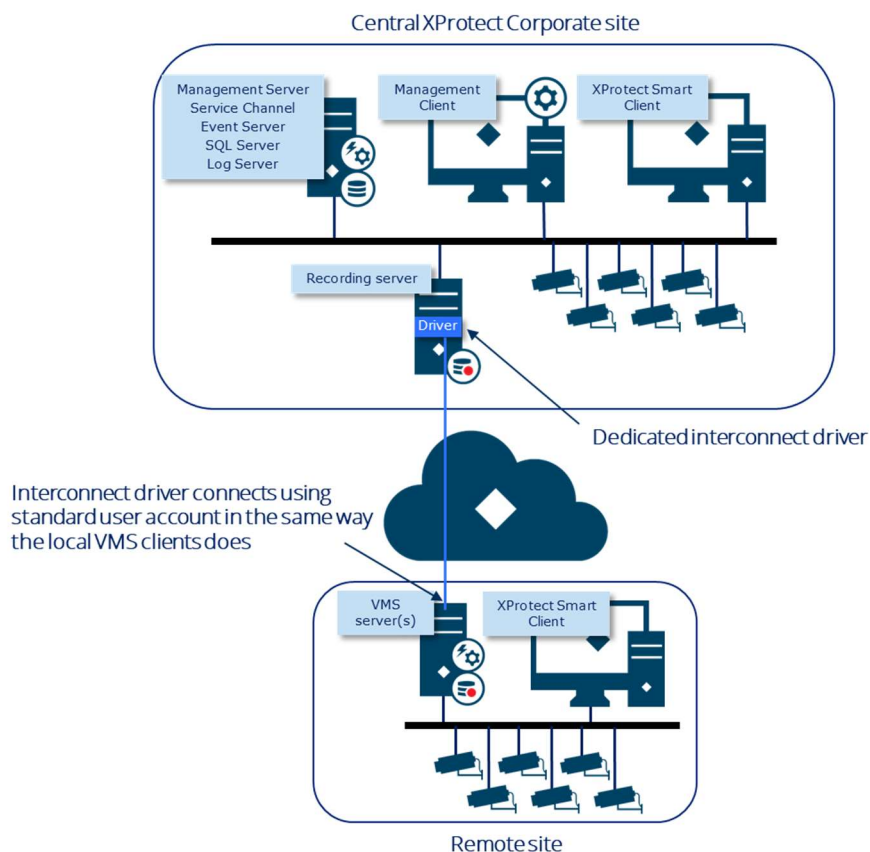
## Milestone Interconnect in comparison to Milestone Federated Architecture

Milestone Interconnect and Milestone Federated Architecture may be seen as two different solutions to the same problem. However, even though they offer the same basic functionality of building a large, centralized VMS consisting of multiple VMS sites, they in fact offer different functionalities, and complement each other in various ways, each with its own specific strengths and use cases.

### Milestone Interconnect

With Milestone Interconnect, the connection to the remote sites is made through a dedicated driver in the central XProtect Corporate site's recording server.

This enables the interconnected site to appear like a kind of video encoder with Edge Storage support, which offers users of the Smart Client the possibility to play back recordings directly from the remote site. Alternatively, if also recording in the central site, it retrieves recordings from the remote sites.



Furthermore, it has the benefit that the recording server handles the connection and authentication on the interconnected sites. This means that cross-domain trust is not needed should the sites be joined to different domains. It also means that the clients do not have to connect and authenticate to multiple

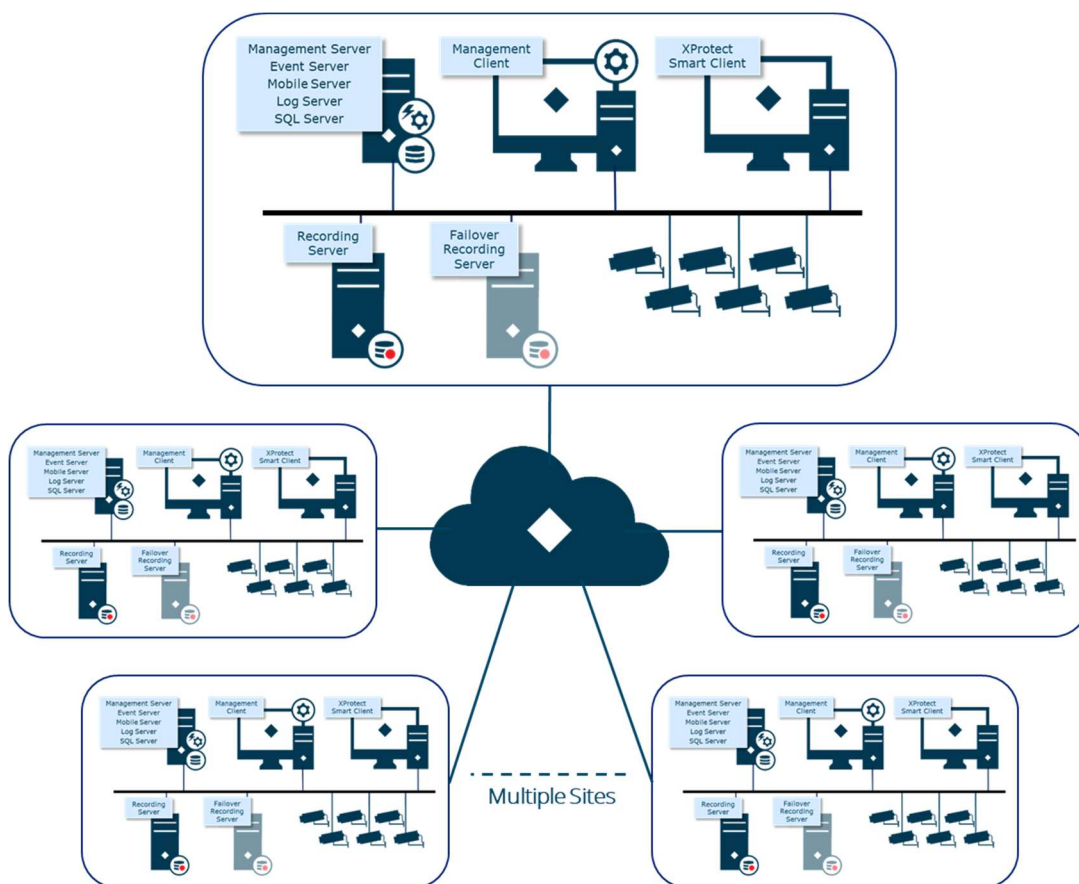


sites when logging in. Finally, it is also possible to interconnect remote sites that are not permanently online.

### Milestone Federated Architecture

Milestone Federated Architecture allows multiple individual XProtect Corporate and XProtect Expert sites to be interconnected in a parent/child hierarchy of federated sites. Each individual site in the federated hierarchy is a standard XProtect Corporate or XProtect Expert installation, complete with a management server, SQL server, recording server(s), failover server(s), and a number of cameras.

**Note:** XProtect Expert can only be added as a child in a federated hierarchy.



When the individual sites are added to a federated hierarchy, they appear as one complete VMS installation to administrators and users, while still being as manageable as independent XProtect Corporate or XProtect Expert sites.

The connection between different sites in the federated hierarchy is not a permanent connection but can be seen more like a link to the other sites. In this way, clients that log in on a site that has children will be informed that there are children that it must also connect to and authenticate on.

This means that even though the VMS from the operator's point of view in the clients appears as one large VMS, the clients authenticate and retrieve the configuration from each site individually. Therefore, Milestone Federated Architecture requires all sites to be online when the clients log in and authenticate. If sites are not online, the clients will experience a longer log-in time because attempts to connect to the unresponsive sites must first time out before login is completed. Furthermore, the client cannot establish a connection automatically to the sites that did not respond during login. The operator in the client must log out and retry to log in manually to get access to the sites that were not responsive.

Finally, as clients always communicate directly with the child sites, and thus receive live and recorded media directly from the child sites, media recorded on the child sites cannot be retrieved or copied from the child sites to the central parent site.

For more information, see the [Milestone Federated Architecture](#) whitepaper.

## Implementation considerations

In the scenarios where recordings are played back directly from the remote site or retrieved to the central XProtect Corporate site, there are several things to consider for optimal performance and user experience.

### **Retrieve recordings from remote sites when bandwidth in certain periods is reserved for other data**

As an example, a retail chain has several shops that record video in each shop's local VMS. To provide the VMS users in the retail chain's headquarters access to investigate incidents and internal fraud in the shops, the local VMS in the shops are interconnected to the HQ site. However, during the shops' opening hours, the network connection between the shops and HQ is reserved for business-related data. Therefore, in these periods, the bandwidth should not be used to transfer video recordings from the shops. Live viewing is permitted, but only if something critical happens.

With such a configuration, the challenges are:

- Limit the bandwidth use from the interconnected site to when nobody views the cameras
- Limit the CPU load on the central HQ site's recording server when live video is viewed
- Limit when recordings can be transferred from the shops to HQ
- Ensure enough time and bandwidth to retrieve the recordings in a timely fashion

To address these concerns, the following is recommended:

- Disable the live-feed rule for the interconnected cameras in the central XProtect Corporate site. If this is not done, the central XProtect Corporate site will automatically connect to the interconnected sites and continuously retrieve a live video stream, using bandwidth for no reason

- If users in the central XProtect Corporate site need to view live video from the interconnected cameras, a new rule can be created to start the live video feed when a user in a client requests live video
- In the central XProtect Corporate system, disable motion detection for the interconnected cameras to reduce CPU load when users view live video
- Disable recording rules for the interconnected cameras to minimize disk load when users view live video
- Configure the period in which recordings can be retrieved from the shops – for instance, outside business hours
- Ensure the retrieval bandwidth limit and retrieval period for the interconnected sites are configured with enough bandwidth and a long enough period to allow the remote recordings to be retrieved in a proper timeframe.
  - If too little time and bandwidth are allocated, there is a risk that retrieval jobs will queue up with a risk of recordings being deleted before they are transferred. Users will also experience that it takes a very long time before the requested recordings are available
  - **Note:** A remote recordings retrieval job that has started will continue until it is completed, even if it goes beyond the configured period allowed for retrieving the recording. If these jobs mustn't continue into a period where the bandwidth is needed for other traffic (for instance, no more retrieval after 8.00 am), the retrieval time window should be set so that any active jobs for certain can be completed before this time (for instance, end the retrieve time window at 6.00 am – allowing 2 hours for completing ongoing jobs)
- In the central XProtect Corporate site, the recording retention on the interconnected cameras must be set long enough to allow further playback or investigation.
  - To avoid concerns about disk usage combined with keeping the retrieved recordings for as long as possible, the storage container can be set to 365 days (or more), but limited in size. In this way, the VMS will try to keep the recordings for at least a year, but still automatically delete the oldest recordings if the storage limit is reached.

Following these recommendations, the recording server requirements on the central HQ site can be kept low, requiring only enough CPU and network bandwidth to act as a gateway for live viewing and retrieving recordings from the interconnected site.

### Retrieve recordings from remote sites without a permanent network connection

In a transportation scenario where a vehicle, for instance a train, is temporarily out of network reach for the duration of a trip, and there is a wish to transfer all recordings from the train to a central site, once the train is again within network reach (for instance at a terminal or depot), it can be a challenge to:

- Limit the bandwidth used for streaming live video, audio, and metadata from the VMS in the train to the central site during periods when the train is within the network connection
- Ensure that there is enough time and bandwidth to retrieve recordings in a timely fashion when the train has a network connection to the central site



- Ensure the recordings in the train are not deleted before there has been enough time to be retrieved by the central site

To address these concerns, the following is recommended:

- Disable the live-feed rule for the interconnected cameras in the central XProtect Corporate site. If this is not done, the central XProtect Corporate site will connect to the interconnected site as soon as there is a network connection and retrieve a live video stream from the remote site, using bandwidth unnecessarily
- In the central XProtect Corporate site, the recording retention on the interconnected cameras must be set long enough to allow further playback or investigation. To avoid concerns about disk usage combined with keeping the retrieved recordings as long as possible, the recording storage container can be set to 365 days (or more) but limited in size. In this way, the VMS will try to keep the recordings for at least a year, but still automatically delete the oldest recordings if the storage limit is reached
- The retention settings and available storage space in the train's VMS must be sufficient to store recordings for a long enough period to ensure that requested recordings can be transferred to the central site before they are deleted in the train's VMS
  - For example, if recordings in a train can only be stored for one day, there is a risk that the recordings will be deleted before they have been retrieved by the central XProtect Corporate site
- It should be ensured that enough time and bandwidth are available to transfer requested recordings from the train to the central site when the train is connected to the network – for instance at terminals or depot
  - If too little time or bandwidth is available, the retrieval jobs will simply queue up and at some point, the train's VMS will start deleting recordings before they are retrieved

Following these recommendations will ensure that requested recordings can be transferred from the trains to the central site before they are deleted in the trains.

#### **Retrieve recordings from remote sites over a network connection with plenty of bandwidth**

Continuing the example with trains that for periods are out of network reach, but this time have plenty of bandwidth available when connected to the network, for instance at terminals or depots. It can be experienced that when transferring the recordings from the VMS in the train to the central site, the bandwidth available on the network is not utilized fully, causing the transfer to take too long time.

In this case, it is recommended that the number of parallel transmissions for the interconnected site are raised from the default eight to, for instance, sixteen. This will cause the bandwidth to be utilized better, ensuring a faster transmission of recordings. This, however, comes with the price of a higher load on the storage system of both the remote and central sites. If the storage system is not fast enough to handle this extra load, there is a risk that live video from the cameras on both sites will not be recorded with the desired framerate.

To address this the following is recommended:

- Ensure that the disk performance in both ends can cope with this higher transfer load
- Split the storage definition and recording in the central site over more disks and storage containers so that:
  - One storage container/disk in the recording server is used for the live recording of standard, directly connected cameras
  - Another storage container/disk is used for the remote interconnected cameras.  
**Note:** for this recommendation to be valid, it requires that the remote cameras are not also recorded in the central site, but only have recordings transferred from the remote sites
- Find a balance between utilizing the network bandwidth and loading the storage system, by reducing the number of devices retrieved in parallel, or by reducing the allowed bandwidth to ensure that all video is recorded

While the recording of new media from the cameras connected to the central site might be at stake if the storage system is overloaded, there is no risk of losing any of the retrieved recordings, because more recordings are not transferred until the retrieved recordings are successfully stored in the media database.

### Play back recordings directly from interconnected remote sites

In a city surveillance scenario where several sites are interconnected to the city's central site and configured for direct playback of the recordings on the remote sites, the challenges are:

- Ensuring there is enough bandwidth to play back the recordings directly from the remote sites
- Limit and distribute the network and CPU load across multiple recording servers
- Limit the disk requirements for the recording servers in the city's central XProtect Corporate site

To address these concerns, the following is recommended:

- Disable motion detection in the central XProtect Corporate site's recording servers to reduce CPU load when viewing live video
- Ensure there is enough upstream bandwidth available on the remote interconnected site, and enough downstream bandwidth available on the central XProtect Corporate site for simultaneously viewing the desired number of interconnected cameras – for instance viewing six cameras at the same time in live or playback
- If interconnecting many remote sites to the central site and having many users on the central site viewing cameras at the same time, it can be beneficial to add the remote sites across several recording servers, because this will distribute the network and CPU load across more servers

- There is no need for high-performance recording disks in the central site's recording servers because the remote interconnected cameras are recorded on and played back directly from the remote sites. If the central site's recording servers are not used for recording any cameras at all, the OS' system disk can be configured as the default-recording disk for the recording server because nothing will be recorded on it.

Following these recommendations will ensure the central site's recording server requirements are kept to a bare minimum, requiring only enough CPU and network bandwidth to act as a gateway for live viewing and playback of recordings from the interconnected sites.

#### **Recording interconnected cameras in the central XProtect Corporate site**

If the central XProtect Corporate site is configured to record interconnected cameras in its recording servers, the same recording server requirements and configuration guidelines apply like when recording standard cameras.

## **Supported products**

The current list of supported products, versions, and features supported can be seen here:

<https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/interconnect/milestone-interconnect-compatibility/>



## Benefits and summary

Milestone Interconnect is a unique concept that allows all paid versions of Milestone XProtect VMS and Husky products to be interconnected with Milestone's premium software XProtect Corporate. It allows the deployment of a central surveillance systems interconnected with multiple geographically dispersed sites in a flexible and cost-efficient way. Furthermore, it provides access to the advanced surveillance functions of XProtect Corporate for all interconnected sites regardless of what products are installed on the remote sites, creating a comprehensive and powerful security solution.

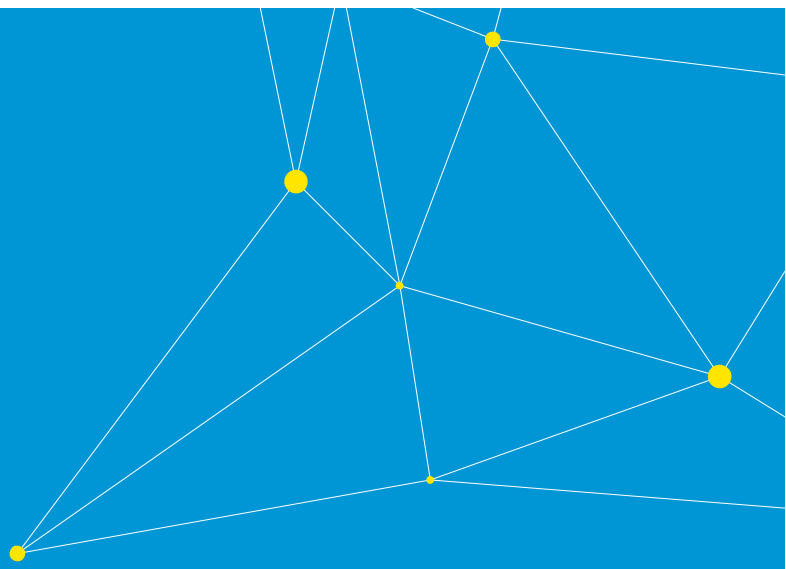
Milestone Interconnect complements Milestone Federated Architecture, and both technologies are designed to excel in their respective areas. For instance, Milestone Federated Architecture is designed primarily for a tight connection of fewer, but larger sites, while Milestone Interconnect is optimized to connect many smaller, distributed sites that are connected through low-bandwidth or intermittent connections.

Milestone Interconnect offers several powerful capabilities, such as:

- **Cost-efficient multi-site deployment**  
Allows customers to freely select what XProtect product to use per site to meet the specific needs and budget of the sites, including the possibility to use different XProtect products across the sites
- **Cross-domain support**  
Milestone Interconnect does not require sites to be on the same domain or have domain trust configured when the central and remote sites are on different domains, or when they are not joined to a domain at all
- **Intelligent video storage management**  
With support for Scalable Video Quality Recording (SVQR), Milestone Interconnect enables optimal use of remote and central video storage and available network bandwidth with a choice to store video recordings remotely, centrally, or combined with flexible retrieval of the remotely stored video
- **Flexible retrieval**  
Optimizes the use of available network bandwidth by controlling the maximum bandwidth usage allowed and by scheduling the retrieval to preserve bandwidth for critical business systems
- **Proactive monitoring**  
The central site receives notifications when there are issues in any of the connected sites. This way, administrators can identify errors proactively and ensure a problem-free and stable operation

Although Milestone Interconnect can be used by any business or organization with the need to optimize its surveillance operations across multiple sites or locations, Milestone Interconnect is particularly relevant to:

- **Retail** – Interconnecting different stores and branches into a common central site, enabling cost-efficient monitoring 24/7 and centralized evidence management
- **Transportation** – where remote sites are installed onboard vehicles, enabling continuous fleet monitoring, efficient evidence handling, and seamlessly correlated surveillance with stationary surveillance installations at stations, waiting areas, etc.
- **Alarm Centers and Monitoring Stations** – can use Milestone Interconnect to offer video monitoring as a service to their clients
- **City surveillance** – interconnecting different geographic areas and organizational units into a common central surveillance site



Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 500,000 sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.