

White paper

# Milestone Interconnect™

Prepared by:

John Rasmussen, Senior Product Manager

Milestone Systems

Date: August 1, 2017

# Table of Contents

<b>Introduction.....</b>	<b>3</b>
<b>Purpose and target audience .....</b>	<b>4</b>
<b>The concept behind Milestone Interconnect.....</b>	<b>5</b>
<b>Technical overview .....</b>	<b>6</b>
<b>Recording and playback options.....</b>	<b>7</b>
<b>Scalable Video Quality Recording (SVQR) .....</b>	<b>9</b>
<b>Implementation of SVQR with Milestone Interconnect .....</b>	<b>9</b>
<b>Applied use of Milestone Interconnect.....</b>	<b>11</b>
<b>Retail .....</b>	<b>11</b>
<b>Transportation .....</b>	<b>12</b>
<b>Security companies offering centrally managed video surveillance.....</b>	<b>14</b>
<b>City surveillance.....</b>	<b>15</b>
<b>Milestone Interconnect Management.....</b>	<b>17</b>
<b>Prerequisites.....</b>	<b>17</b>
<b>Adding remote sites .....</b>	<b>17</b>
<b>Settings – remote sites and devices.....</b>	<b>20</b>
<b>Updating remote site devices.....</b>	<b>21</b>
<b>Interconnect playback configuration.....</b>	<b>21</b>
<b>User rights in XProtect Corporate .....</b>	<b>25</b>
<b>Rules.....</b>	<b>26</b>
<b>Milestone Interconnect and XProtect Smart Client Operation .....</b>	<b>27</b>
<b>Setup .....</b>	<b>27</b>
<b>Live .....</b>	<b>27</b>
<b>Playback remote recordings.....</b>	<b>27</b>
<b>Playback recordings from central site and retrieval of remote recordings .....</b>	<b>29</b>
<b>Milestone Interconnect in comparison to Edge Storage .....</b>	<b>33</b>
<b>Milestone Interconnect in comparison to Milestone Federated Architecture .....</b>	<b>34</b>
<b>Implementation considerations .....</b>	<b>36</b>
<b>Supported products .....</b>	<b>40</b>
<b>Licensing.....</b>	<b>41</b>
<b>Benefits and summary .....</b>	<b>42</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 a large-scale and geographically dispersed video surveillance installations where each independent surveillance site can be designed with the required functionality and price in mind, while still offering the benefits of a centralized surveillance installation.

Milestone Interconnect is in some aspects similar to Milestone Federated Architecture™, however the way the different sites communicate is different and it supports a wider selection of Milestone's VMS products while also offering several advanced features:

- Support for using low-end XProtect products on dedicated hardware e.g. in vehicles
- Cost-efficient deployment by interconnecting Milestone products designed for the SMB market
- Retrieval of video, audio and metadata recordings from interconnected sites, including over intermittent network connections, to the central XProtect Corporate site
- 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 number of interconnected sites, remote site response time or network connection state
- Full XProtect Corporate camera rights for the interconnected cameras
- Remote Management of the interconnected sites

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

- Retail chains
- Transportation installations
- 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
- The technical implementation
- The benefits
- The problems it solves

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

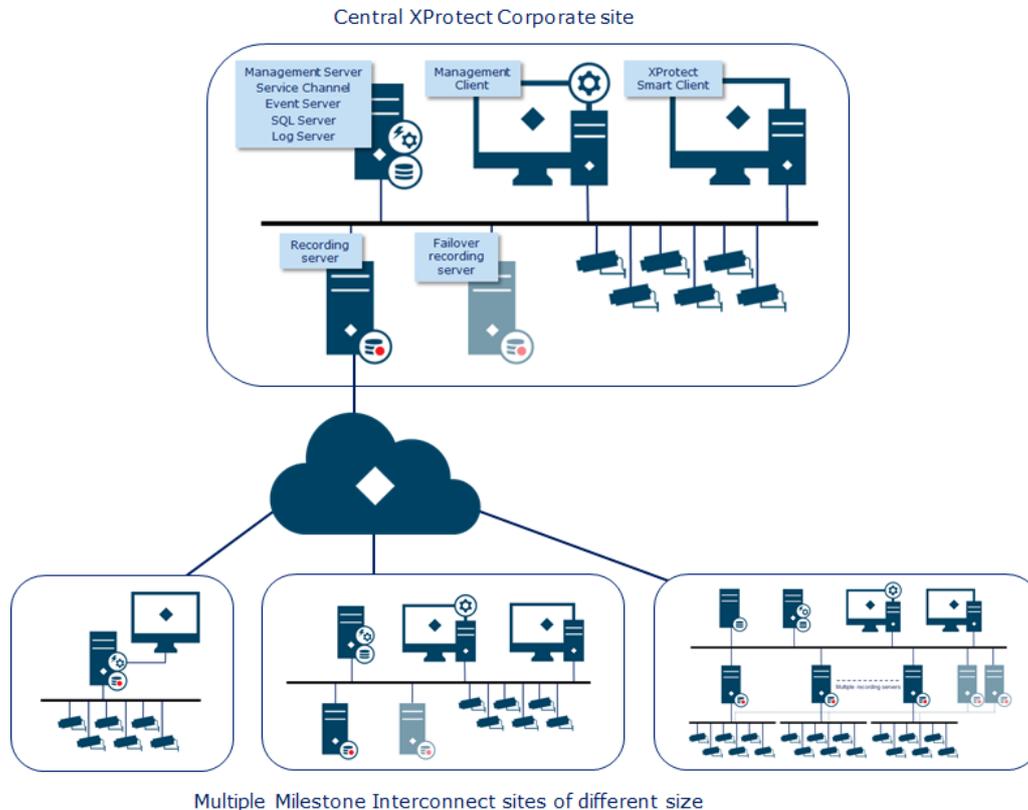
- Surveillance system architects and designers
- Large-scale surveillance project consultants
- Companies, organizations, universities, cities and governments with distributed surveillance projects or installations.

This white paper will enable 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 Management Client and XProtect® Smart Client as well as the other XProtect VMS and Husky products. The reader is also assumed to be having 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 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 for recordings recorded or retrieved to the central XProtect Corporate site
- Bookmarks<sup>2</sup>
- Alarms<sup>3</sup>

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

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

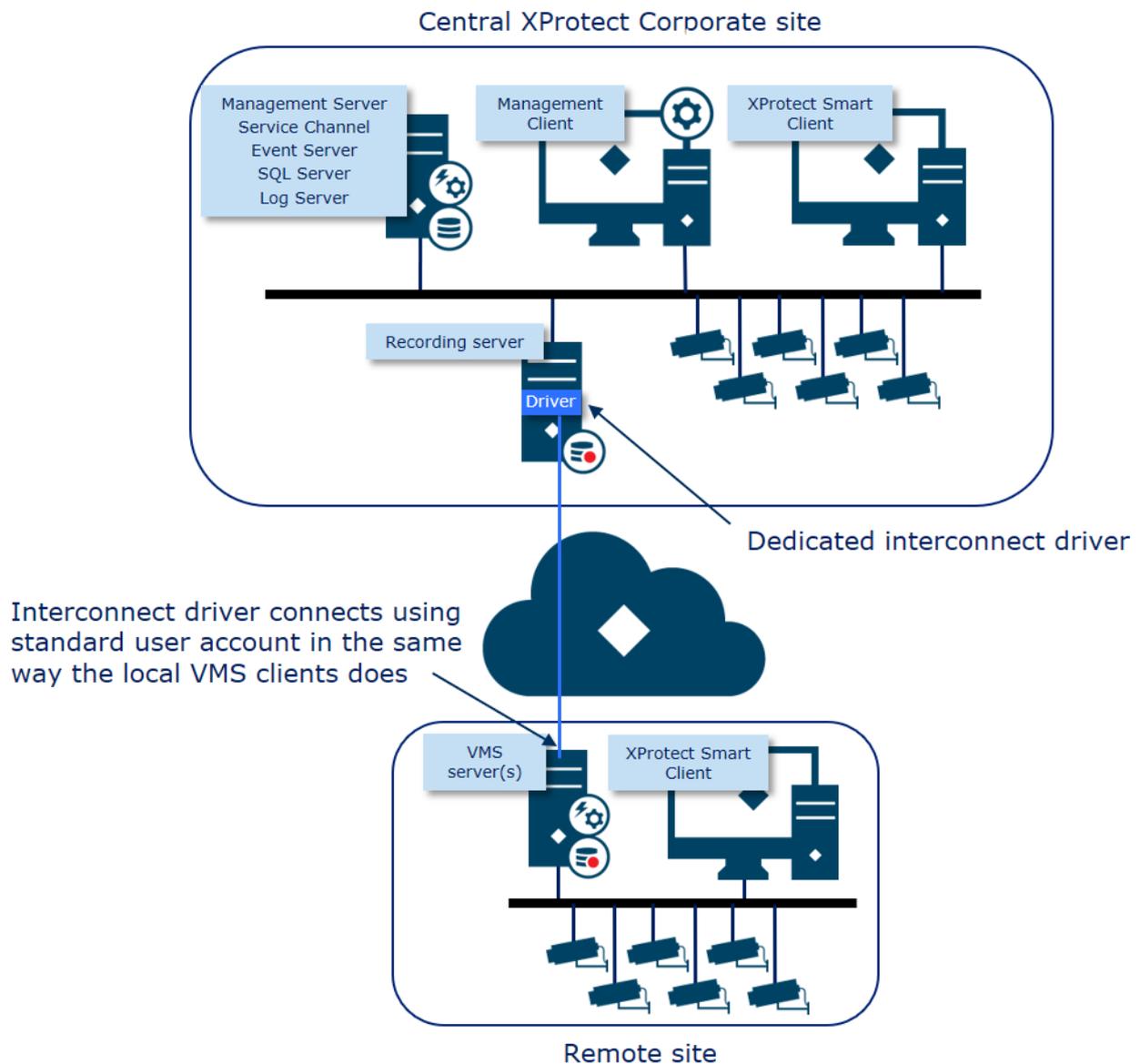
<sup>3</sup> Alarms triggered on remote sites cannot be viewed or managed centrally

When sites are interconnected to a central XProtect Corporate site, they can still be accessed and used locally with the same functionality the specific product offers, as before interconnecting the site.

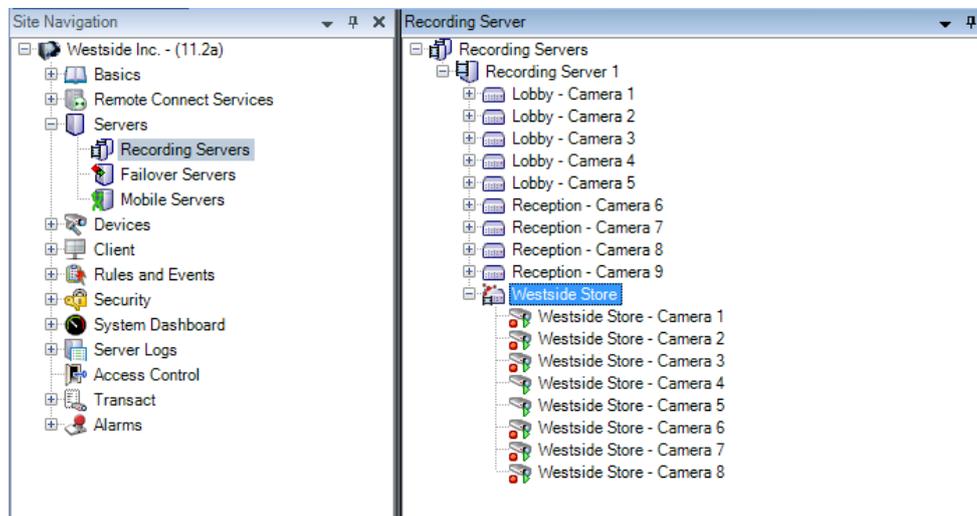
## Technical overview

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.

The below 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 will appear in the Management Client on the central XProtect Corporate site as a kind of “multi-channel video encoder” listing the cameras that can be accessed on the remote interconnected site.



As the interconnected cameras 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 directly connected camera. The only exception is changing the actual image settings for the camera. This is 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 regardless of 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 camera 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 provides different functions and usage cases.

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

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

**Option 1 user experience:**

- Users accessing the interconnected site directly can view live and recorded video, audio and metadata
- Users accessing cameras on the remote interconnected site via the central XProtect Corporate site can view live and recorded video, audio and metadata and use many of the advanced XProtect Corporate features, such as bookmarks, regardless of whether the product running the interconnect site supports this feature or not.

**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 is streamed to the central XProtect Corporate site and recorded based on the defined rules in the XProtect Corporates site.

**Option 2 user experience:**

- Users accessing the interconnected site directly can view live video, audio and metadata, but they cannot play back recordings
- Users accessing cameras from the remote interconnected site via the central XProtect Corporate site can view live and recorded video, audio and metadata and use many of the advanced XProtect Corporate features, such as bookmarks, regardless of whether the product running the interconnect site supports this feature or not

**Option 3: Recording is done in both sites**

With this option, recording and playback are done both on the remote site and on the central XProtect Corporate site. This allows recordings to be retrieved from the remote interconnected site and stored in the central XProtect Corporate site on a time schedule, defined events or by users manually retrieving recordings of interest using the XProtect Smart Client.

Furthermore, the central XProtect Corporate site can be configured to retrieve recordings automatically from time periods where communication with the remote site is unavailable.

**Option 3 user experience:**

- Users accessing the interconnected site directly can view live and recorded video, audio and metadata
- Users accessing 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 from the remote interconnected site
- Users accessing the interconnected site via the central XProtect Corporate site can use many of the advanced XProtect Corporate features, such as

bookmarks, regardless of whether the product running the interconnect site supports this feature or not

- Users can request recordings 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 loss of communication with the remote site

## Scalable Video Quality Recording (SVQR)

SVQR is a technology that extends the functionality of Milestone Interconnect and enhances the existing synergies of recording video, audio and metadata 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.

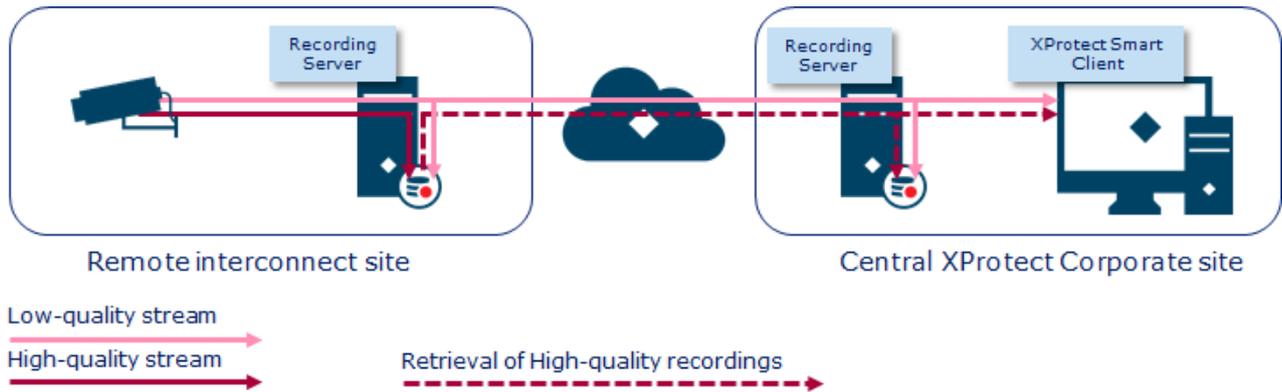
By recording high-quality video on the remote interconnected site and low-quality video on the central XProtect Corporate site, and having the function for central XProtect Corporate site users to retrieve the high-quality recordings when needed, SVQR significantly reduces the network and storage requirements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

## Implementation of SVQR with Milestone Interconnect

The use of SVQR requires at least two streams of different quality to be configured on the remote interconnected site – in the example below, 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.

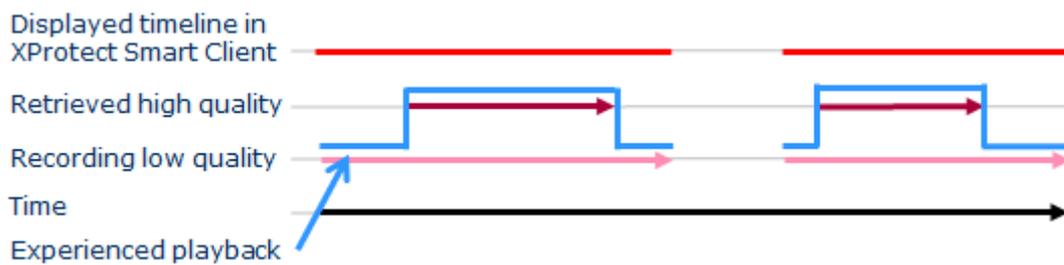
The low-quality stream is relayed from the remote interconnected site to the central XProtect Corporate site where it is recorded based on motion detection, events, or schedule.



When high-quality recordings are needed on the central site, for instance for doing an investigation, the high-quality recordings can be retrieved on request 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, and can be played back seamlessly with the existing low-quality recordings without the users needing to do anything. The 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 if the recordings are exported. The quality of the recordings in the export will be the same as the quality experience when doing playback.



*Timeline, recorded and retrieved tracks - highlighting the playback experience*

As can be seen above, the low-quality recordings are not deleted or overwritten when high-quality recordings are retrieved, but stored in parallel with the existing 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

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

Using the advanced XProtect Corporate product and Milestone Federated Architecture to link all the sites is often not desired as the individual shops don't need the advanced functionality of XProtect Corporate. Furthermore, using XProtect Corporate on all sites can be costly. Another reason for not using Milestone's Federated Architecture is that the bandwidth between the shops and the headquarter are often limited and used for critical business data during opening hours.

For these types of customers Milestone Interconnect is the ideal solution, as it supports using the simpler low-cost VMS products on many geographically dispersed sites while at the same time allowing them to be connected to the headquarters advanced XProtect Corporate VMS.

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.

- 2. Efficient bandwidth control:**

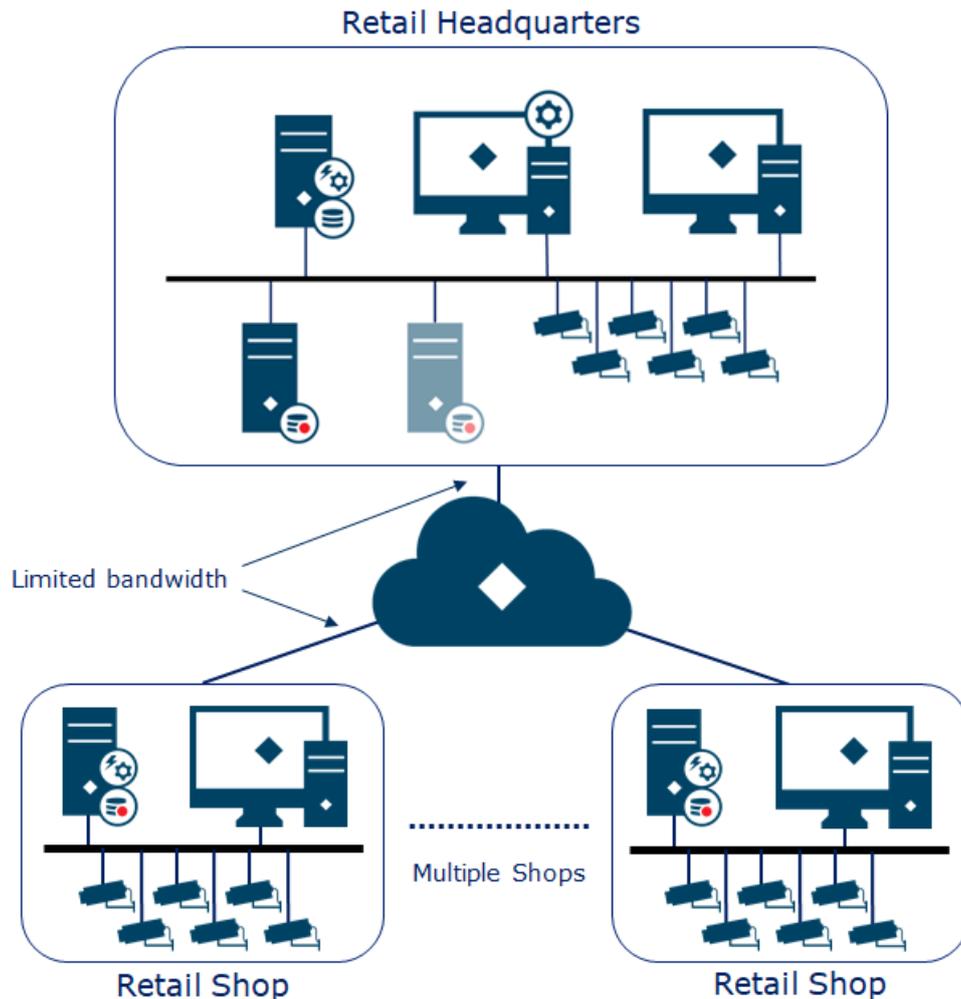
Milestone Interconnect offers efficient control of bandwidth usage since it is possible to program when recordings are retrieved from the remote site and what is the maximum bandwidth that can be used.

- 3. Centralized Management:**

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

#### 4. **Internal revision:**

Headquarters have seamless central access to the shops' VMS for investigating internal fraud and for exporting evidence. Should bandwidth limitations exist, investigators can request recording sequences to be retrieved to the central XProtect Corporate site using a preset bandwidth limit, or schedule the retrieval to occur after opening hours.



## 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 an on-board vehicle surveillance installation that is only connected to the surveillance network during certain times.

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

Milestone Interconnect offers an ideal solution for transportation companies with distributed surveillance sites in buildings and vehicles since it addresses the central challenges of video surveillance 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:**

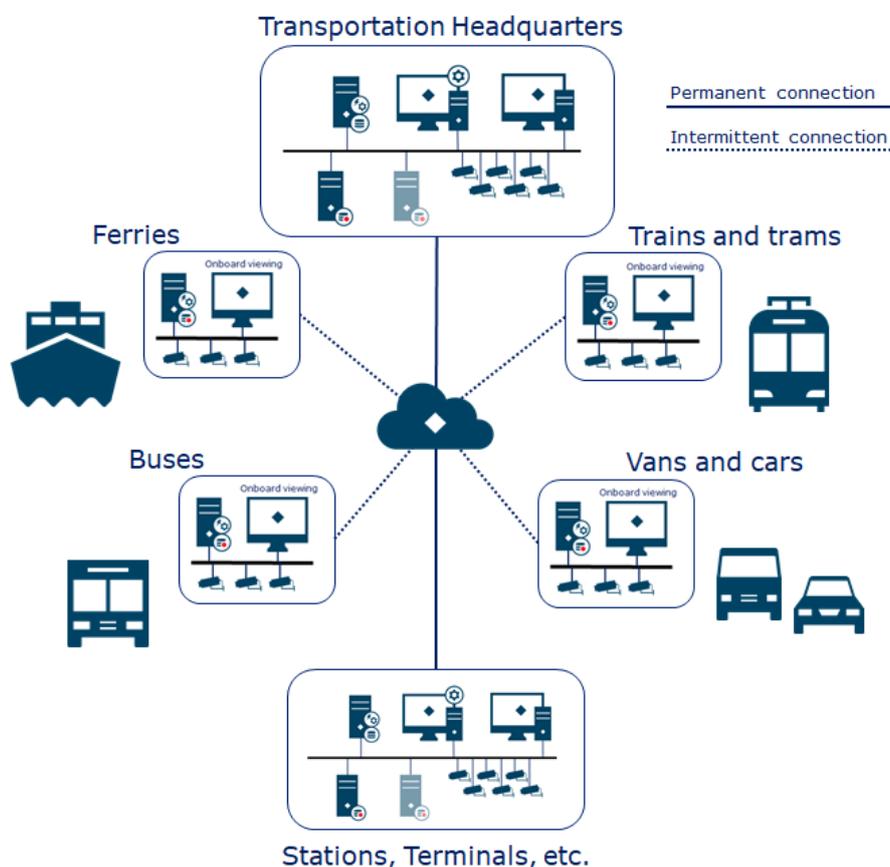
Milestone Interconnect does not need a manual procedure to physically retrieve recordings. Investigators can request recordings to be retrieved from the vehicles no matter if they are connected to the network or not at the time of the request. If recordings are requested while vehicles are out of network reach, the request is queued and the 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 sites to provide a comprehensive 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 a VMS installed on a customer site and provide access to the following specific functions:

- 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 the specific features listed above, the solution must also support a mix of installations of different size, choice of XProtect VMS or Husky product.

With all these requirements in mind, Milestone Interconnect is the ideal solution for such security companies as 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 all XProtect VMS user authentication methods: Basic users, local Windows users or Windows Active Directory users. Furthermore, should the customer use 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:**

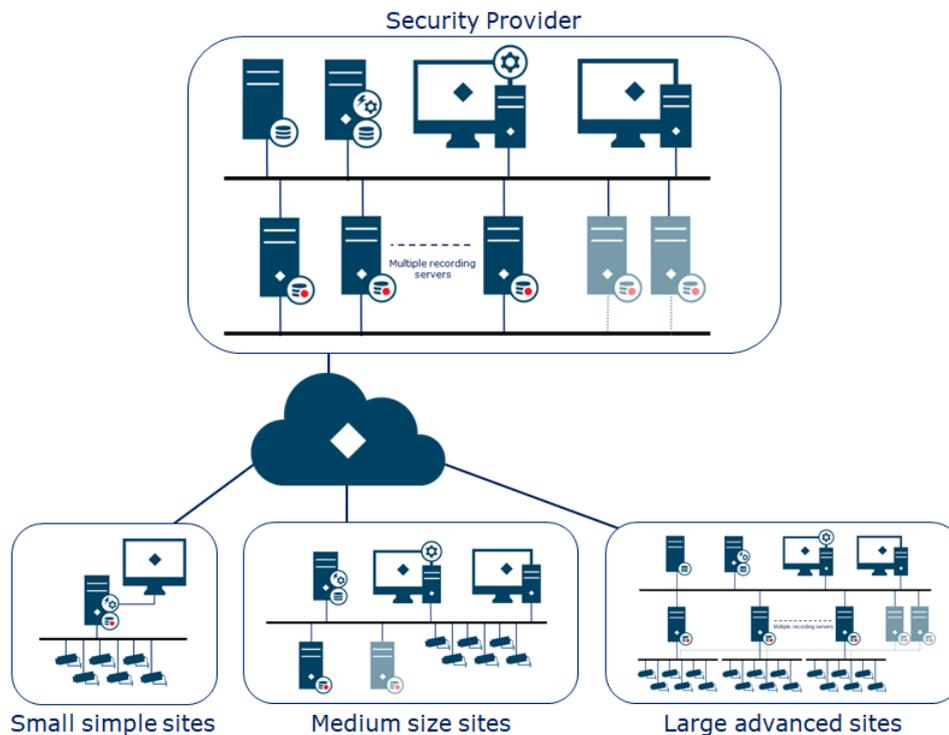
Security companies can centrally monitor their customers' sites and quickly address any detected issues. Furthermore, the customers installations can be managed centrally without needing to physically visit the customer site.

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 identifies 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, by allowing a scheduled and robust retrieval functionality with bandwidth throttling.



## 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:

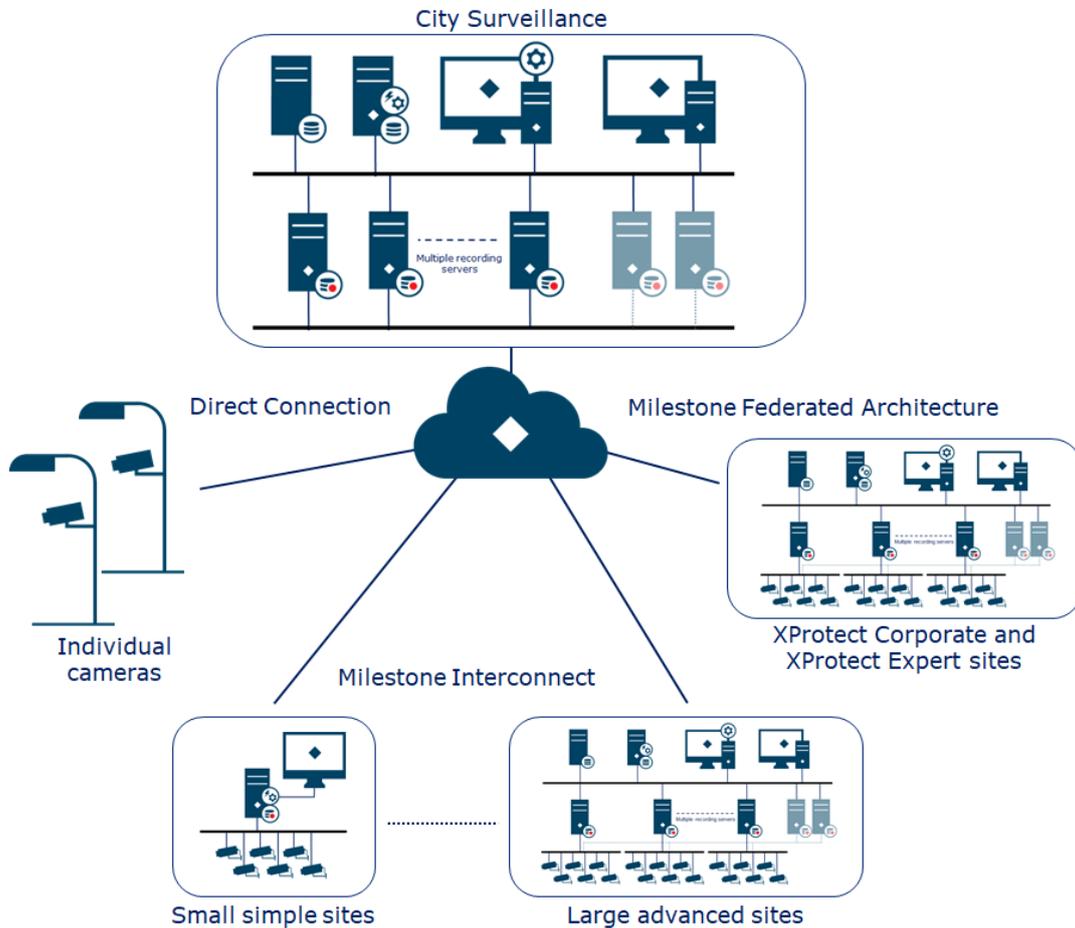
Individually mounted cameras throughout the city can be attached to the VMS in the same way as cameras connected to the local network. When attaching cameras outside the local security network to the VMS it is recommended to use HTTPS to secure the communication.

### 2. Milestone Interconnect:

As described in this whitepaper, 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:

Offers a solution to link large advanced 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

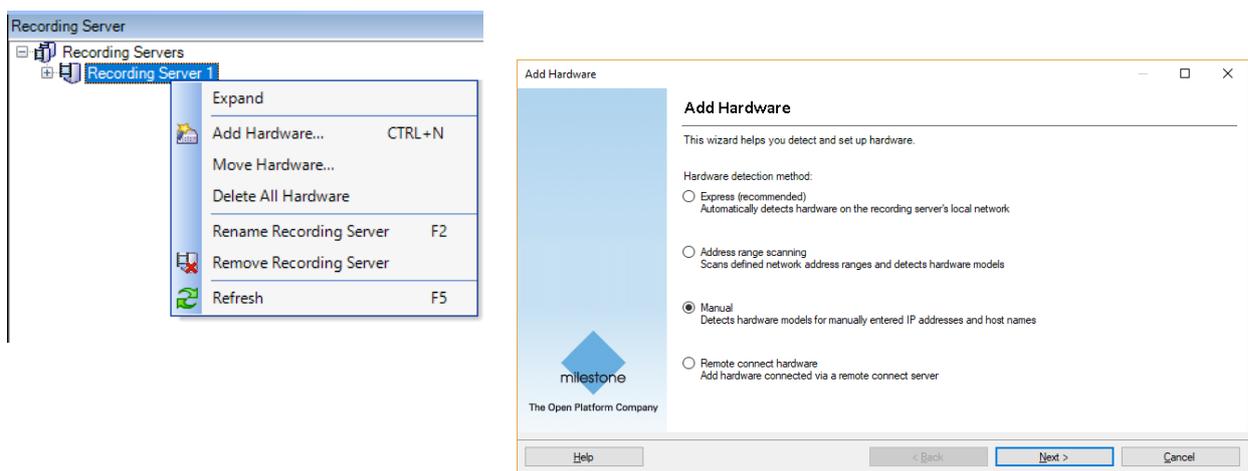
There are four basic prerequisites for using Milestone Interconnect:

- An installed and operational XProtect Corporate 2013 or newer VMS
- An XProtect Corporate license that includes the total number of Milestone Interconnect camera licenses required
- A configured and working XProtect VMS or Husky products based surveillance installation at the remote site, including a user account/role (basic users, local Windows user or Windows Active Directory user) with permissions for the devices and functions that the central XProtect Corporate site should access
- A network connection between the central XProtect Corporate site and the remote sites - with port forwarding in relevant routers or firewalls to the ports used on the remote site

**Note:** The central XProtect Corporate site can only see and access devices that the specified user account used for the Milestone Interconnect connection, has access to. This allows remote site's local administrators to control which devices are available to the central XProtect Corporate site and for its users.

## Adding remote sites

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

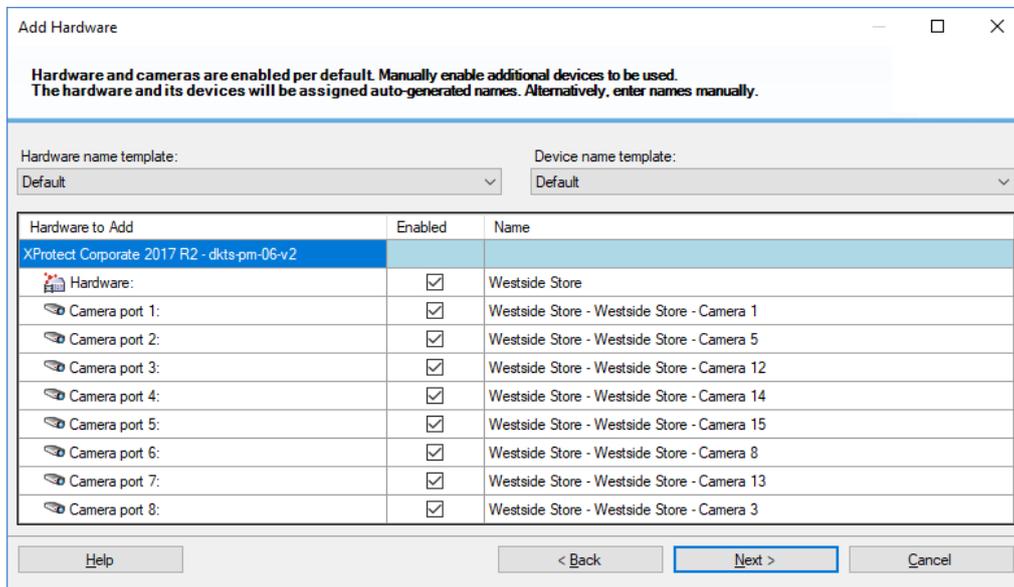


**Note:** Remote sites can only be detected and added using the **Address range scanning** and **Manual** options.

Like adding cameras, the followings must be specified in the wizard in order to detect the remote site: Address - or address scan range, specific Milestone Interconnect

driver (e.g. **Milestone XProtect VMS Interconnect** driver) – or alternatively select auto-detect and the user account to connect with.

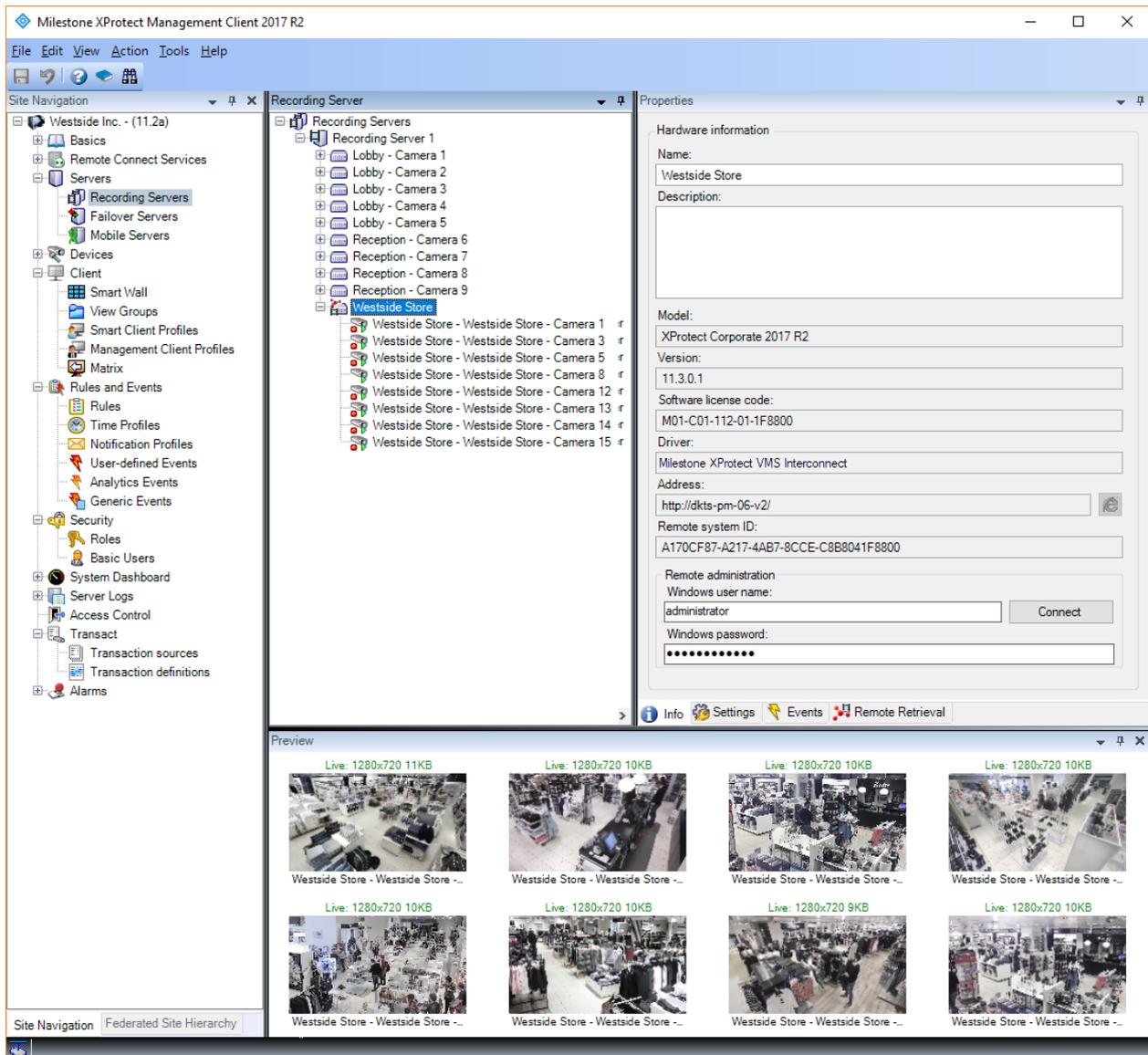
On the Add hardware wizard's step where the detected devices can be named, the wizard will use the remote site's server and device names by default.



These default auto-assigned names can be changed in the central XProtect Corporate site using the XProtect Management Client as for normal cameras. Doing so will not change the names on the remote site. In this way you can ensure, that each camera will have a unique name in the central site, even though cameras use the same names in the interconnected sites.

If seeing the original names of the remote site's devices is necessary, it can be seen on the device's **Settings** tab.

When the remote sites have been added to the recording server, they will be listed the same way standard cameras and video encoders are.



Because access to devices and functions is controlled using standard user accounts/roles on the remote sites, it is possible for the remote sites administrator to control which cameras and functions the central XProtect Corporate site has access to.

This means that if a user account/role used to connect to the remote site is now granted access to a subset of the cameras and functions, only these will be listed/allowed in the central XProtect Corporate site.

This ensures that the remote sites' administrator has full control over what can be accessed and done on his or her VMS installation, which provides peace of mind for the administrator knowing that the central site can only be accessed as agreed on.

## Settings – remote sites and devices

The interconnected remote site has a couple of tabs dedicated for displaying site information and for configuring events and remote recording retrieval settings.

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

Furthermore, it gives access to manage the remote site via Windows remote desktop support.

Use of the remote desktop feature require that remote desktop is enabled on the server/PC running the remote site, and that a Windows user account for the remote site is specified.

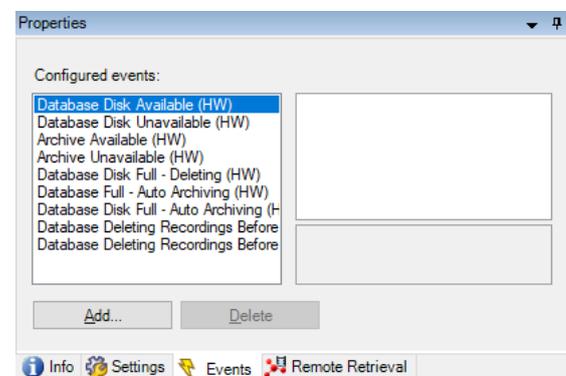
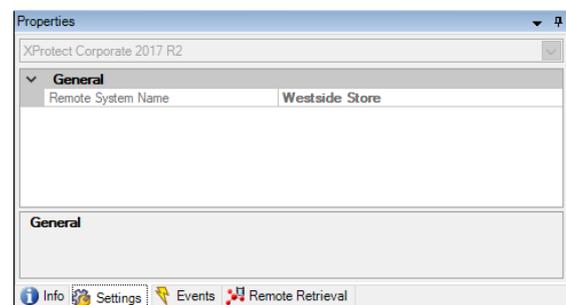
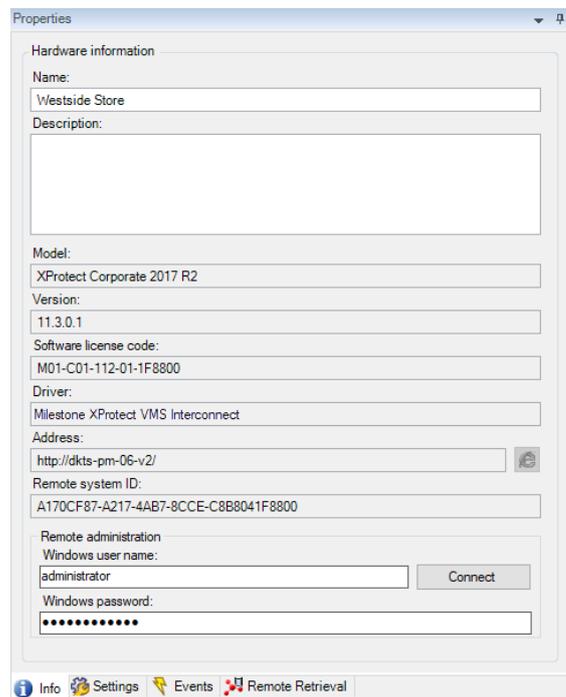
If using XProtect Express+, XProtect Professional+, XProtect Expert or XProtect Corporate, it is also possible to manage the remote sites by connecting the XProtect Management Client directly to the remote site.

If the name of the interconnected 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.

The **Events** tab allows the user to select which events from the remote site should be usable in the central XProtect Corporate site.

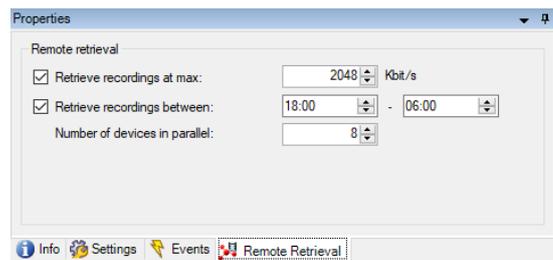
The list of supported events depends on the XProtect VMS or Husky product that runs on the remote interconnected site.

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



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

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



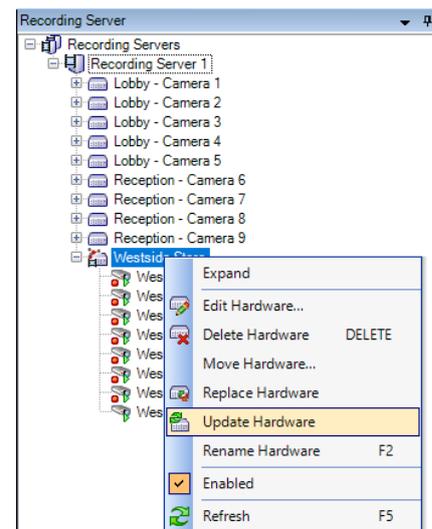
Finally, the number of devices to retrieve recordings from in parallel can also be set here. The default is set to eight devices in parallel, but this can be increased in order to better utilize the bandwidth, if a lot of bandwidth is available.

**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 needs to be updated to reflect the actual configuration of the interconnected site.

The update must be done manually by right-clicking the hardware device representing the remote site and selecting **Update Hardware**. This will open a dialog that lists a summary of detected changes.

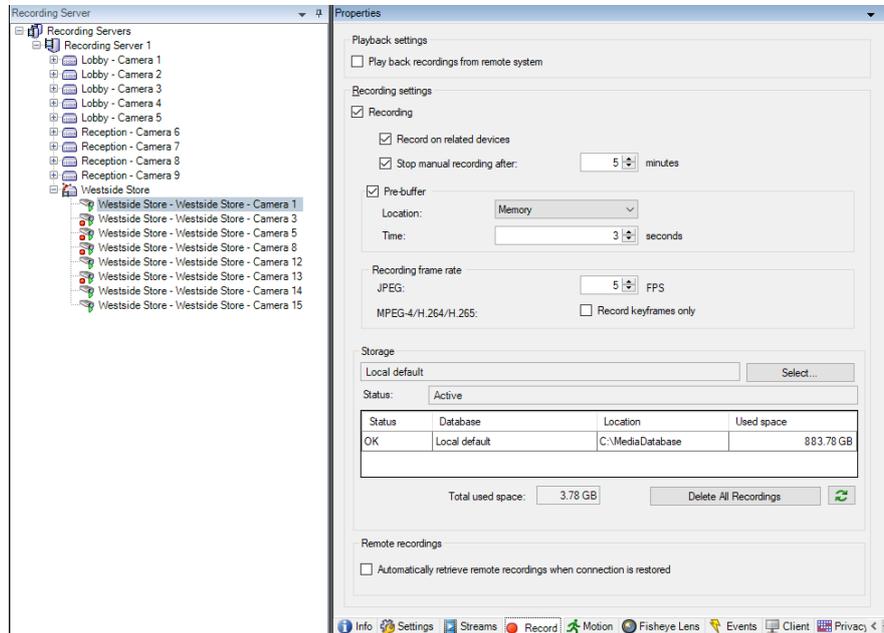


## Interconnect playback configuration

### Playback from the central XProtect Corporate site

When selecting a camera, microphone, speaker or metadata device, 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 as for normal cameras. The same applies when creating rules controlling when video, audio or metadata is recorded.

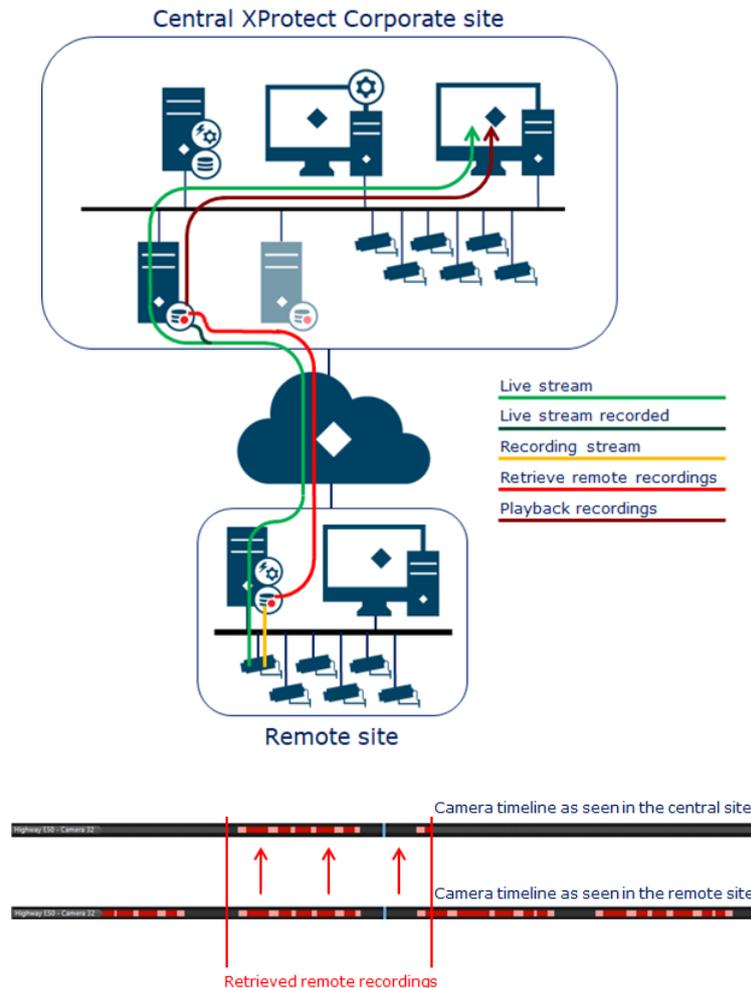


In addition to standard recording on rules, the remote interconnected site can be used as a kind of "edge storage" device for recovering missing recordings in case of network or recording server issues by checking the **Automatically retrieve remote recordings when connection is restored** checkbox.

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 remote and central sites, Scalable Video Quality Recording (SVQR) can be used to record low-quality recordings on the central XProtect Corporate site, and to retrieve high-quality recordings from the remote site later on event or request (See the SVQR section).

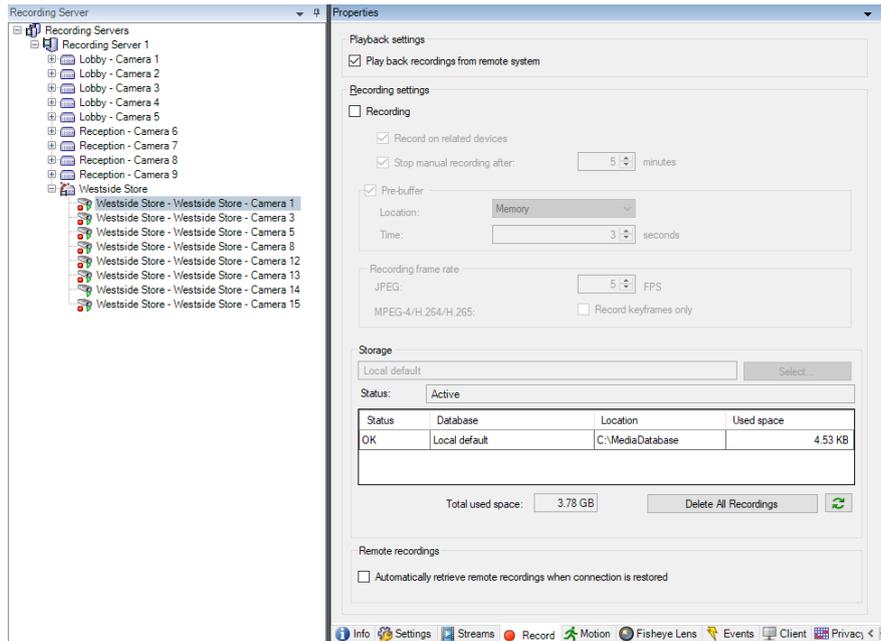
By default, the central XProtect Corporate site starts requesting live streams of video, audio and metadata. If live streams are not needed in the central XProtect Corporate site or only needed when a client requests it, the rule system can be used to configure that the live stream is not started, or only started when live streams are requested by clients.

With this central recording configuration, the timeline for users connected to the central site will not be the same as for users connected to the remote site. This is because each site records under its own rules and because recordings can be retrieved from the remote site to the central site.

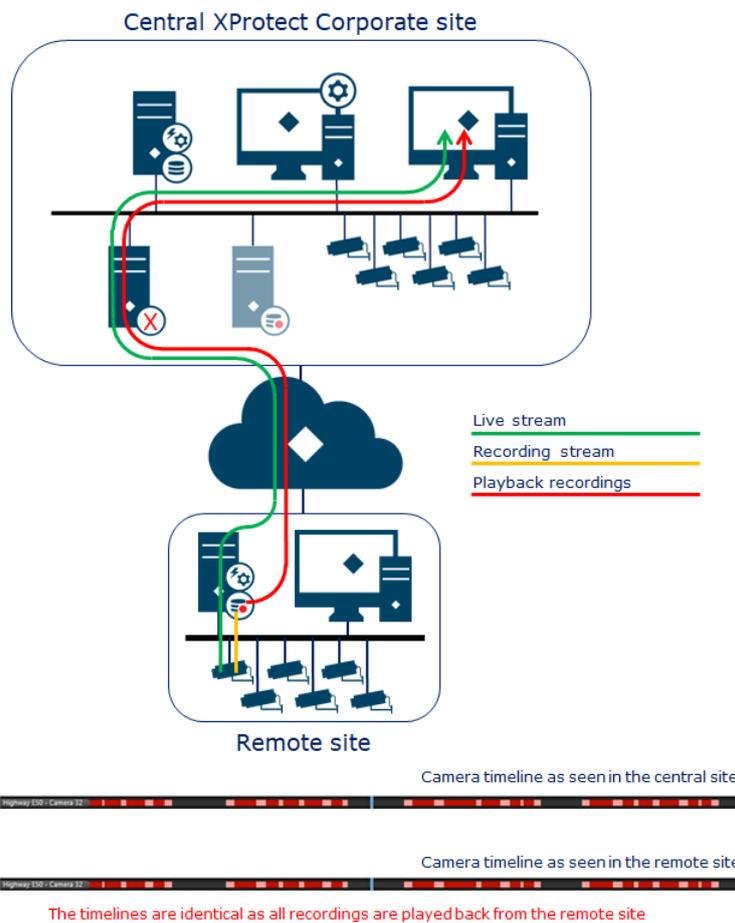


### Playback from the remote interconnected site

Selecting to playback recordings directly from the remote interconnected site can be done from the device's **Record** tab by checking 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.



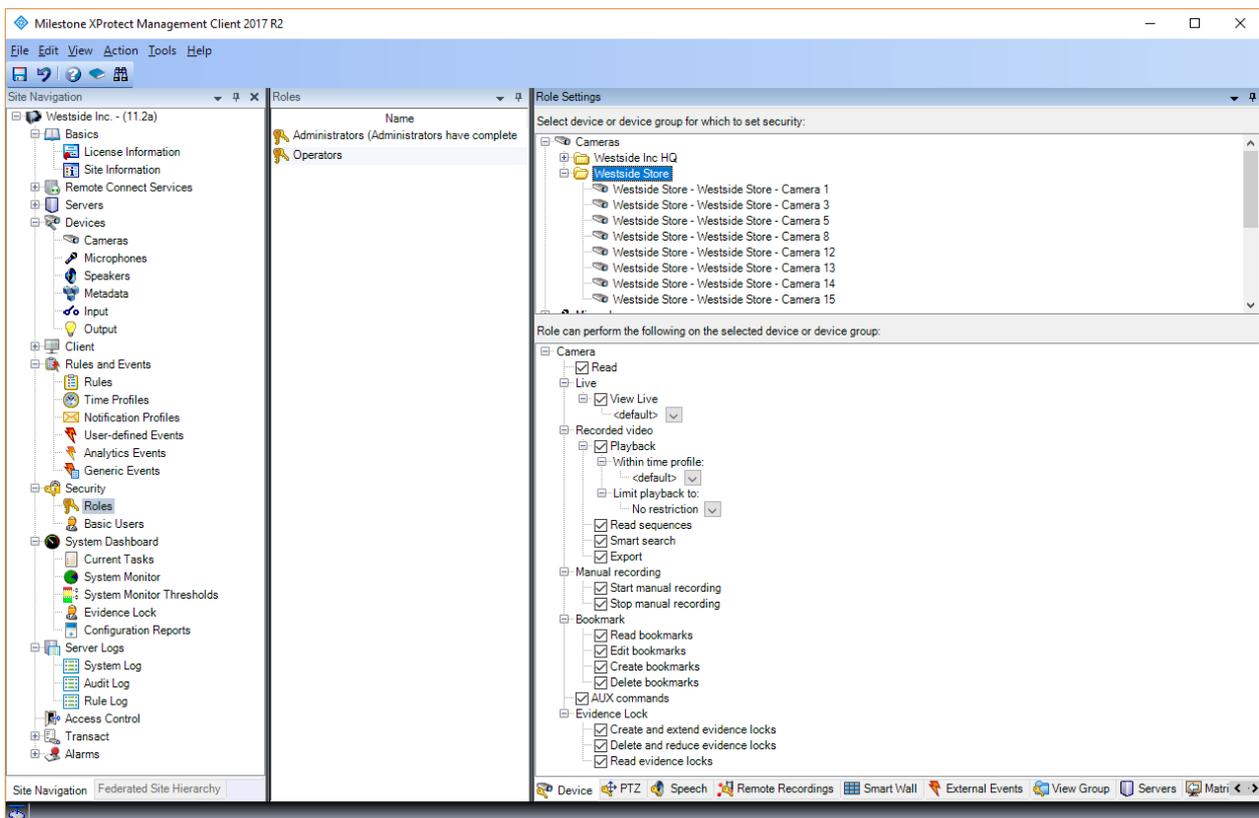
Clients playing back recordings with this configuration, will still communicate with the recording server on the central XProtect Corporate site - however, the recording server will retrieve recordings from the remote interconnected site's recording database rather than fetching it from its own recording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



With this configuration, the timeline for the central site operator will be the same as for an operator on the remote site. Furthermore, there are no recording databases for the camera in the central site at all; therefore, remote recordings can only be played back from the remote site and not be retrieved and stored in the central site.

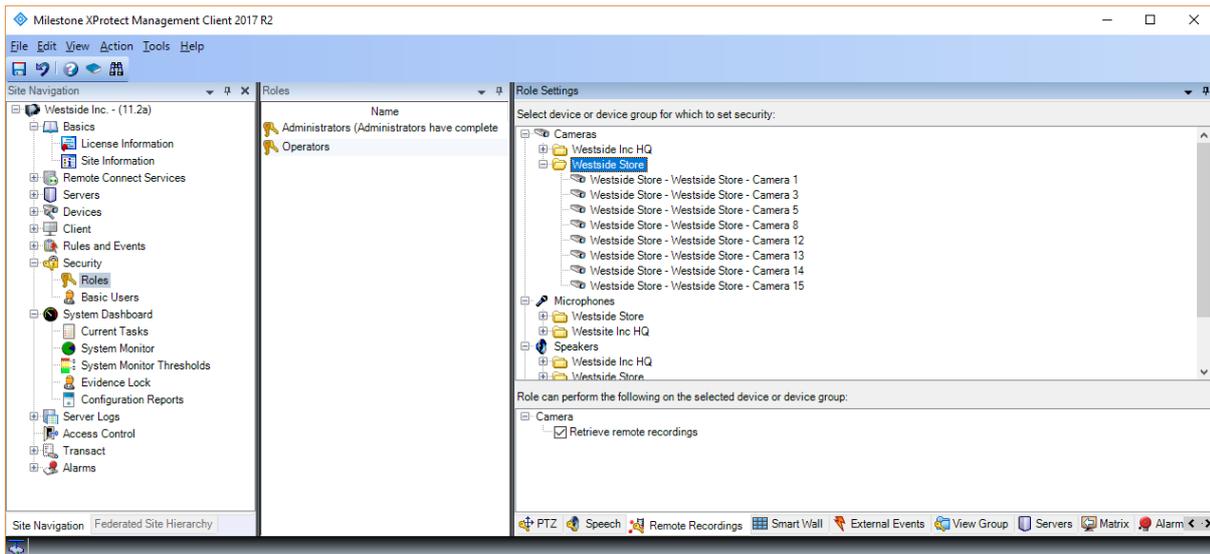
## User rights in XProtect Corporate

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 its access to the devices and functions on them.



The bookmark function also works on interconnected cameras regardless if they are recorded in the central XProtect Corporate site, 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 devices, which also works on interconnected devices even though the interconnected remote site itself does not support time-limited access rights.

In addition to the standard device rights described above, the interconnected devices also have a dedicated tab called **Remote Recordings**. On this tab the rights to retrieve remote recordings can be set, allowing users of the clients to create remote recordings retrieval jobs for the selected devices.

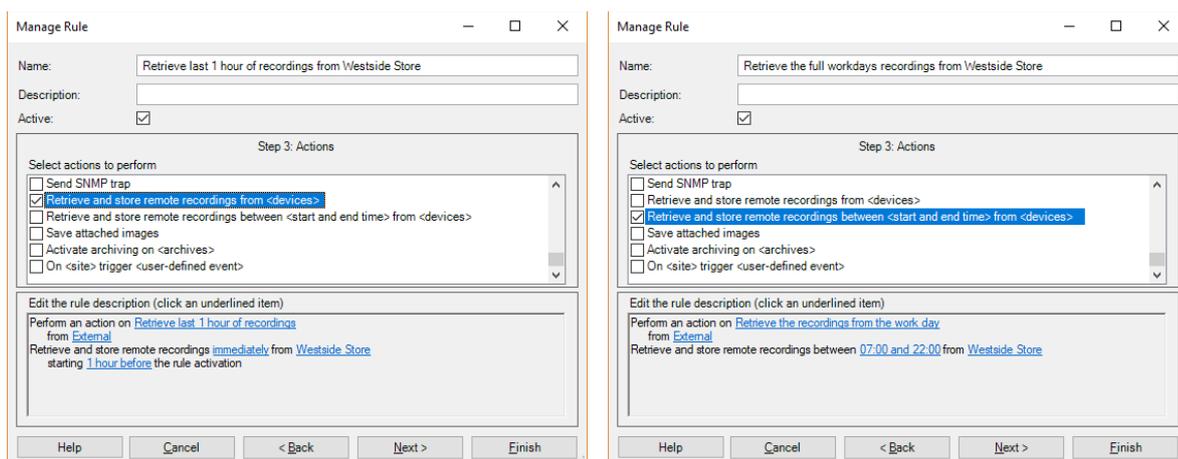


## Rules

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 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 setup of the rules are done in the XProtect Management Client using the **Manage Rule** wizard. Here are two examples of rules that retrieve the last hour of recordings (left) and retrieve recordings between 07.00 and 22.00 (right) from a group of cameras on an event.



If the recordings need to be retrieved following a specific schedule, the rules can be configured to start on a standard XProtect Corporate time profile.

# Milestone Interconnect and XProtect Smart Client Operation

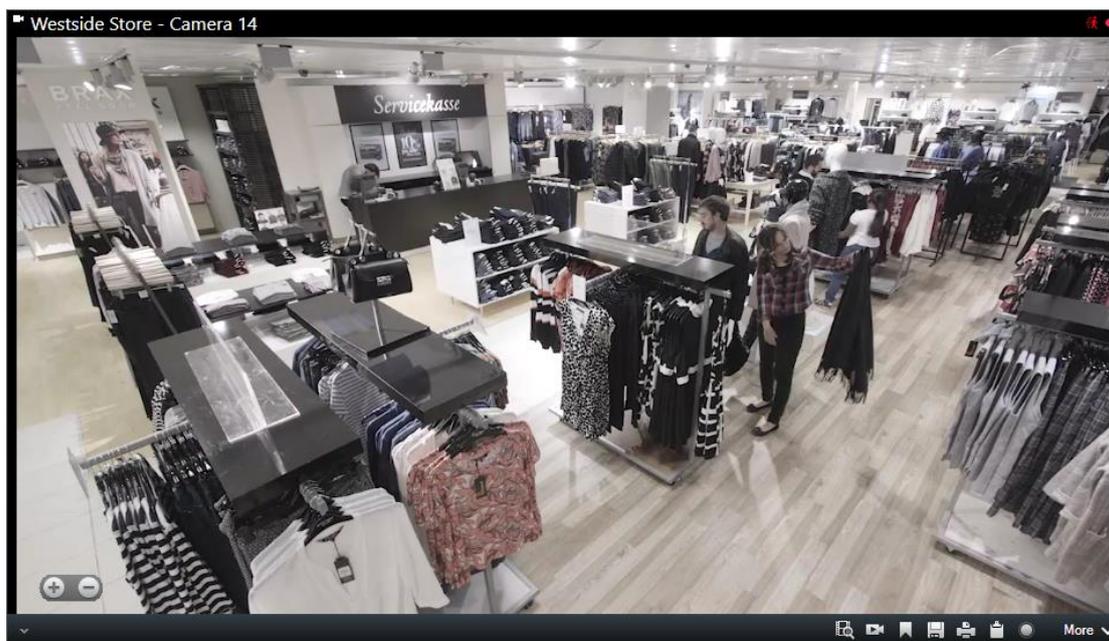
## Setup

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

## Live

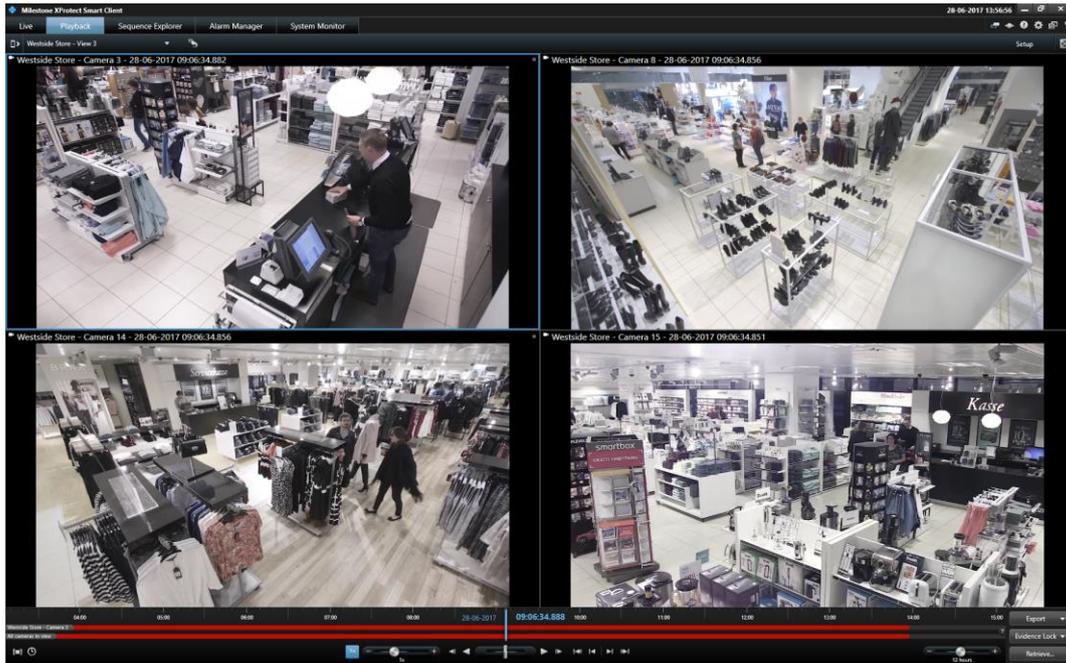
Interconnected cameras are displayed live in the views the exact same way as regular cameras are and have the same functions on the camera toolbar as regular cameras do regardless if they are recorded in the central XProtect Corporate site, both sites, or the remote interconnected site.

Below screenshot shows an interconnected camera in the XProtect Smart Client's live mode showing the camera toolbar with available functions.

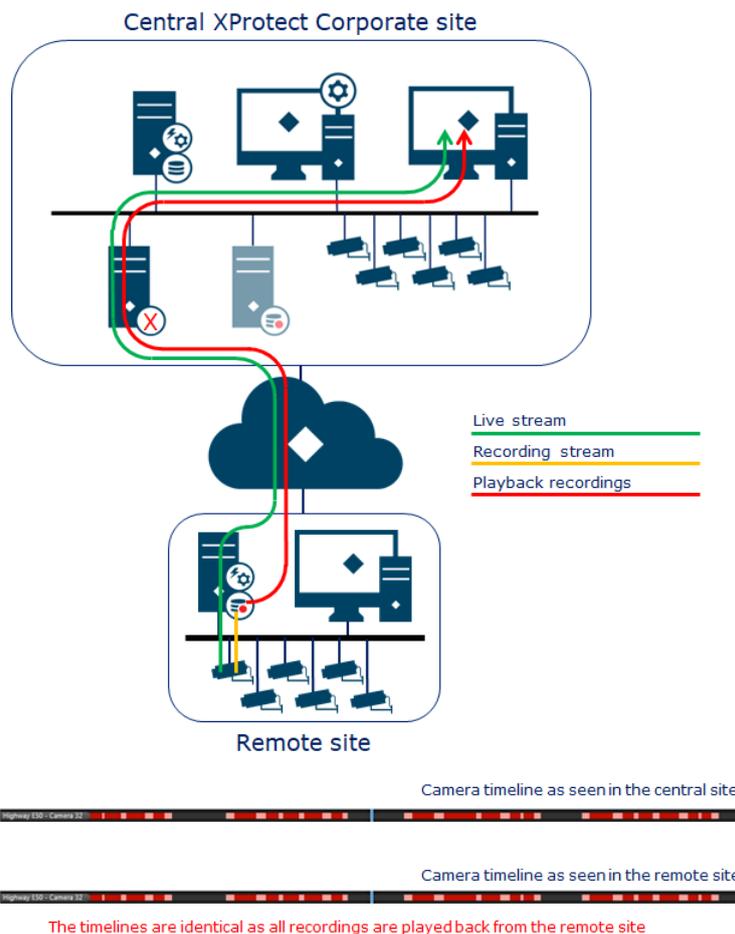


## Playback remote recordings

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



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 won't be a media database on the central site recording server.

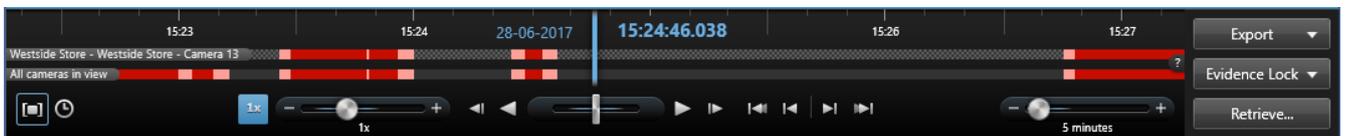


With this configuration, the timeline for the operators on both the central XProtect Corporate site and remote site's operators will be identical and it will not be possible to retrieve remote site recordings. Furthermore, any configured remote retrieval bandwidth limits or time restrictions will not apply when configuring the central site for direct playback of remote recordings.

**Note:** 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.

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

When interconnected cameras are configured to record and playback 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.



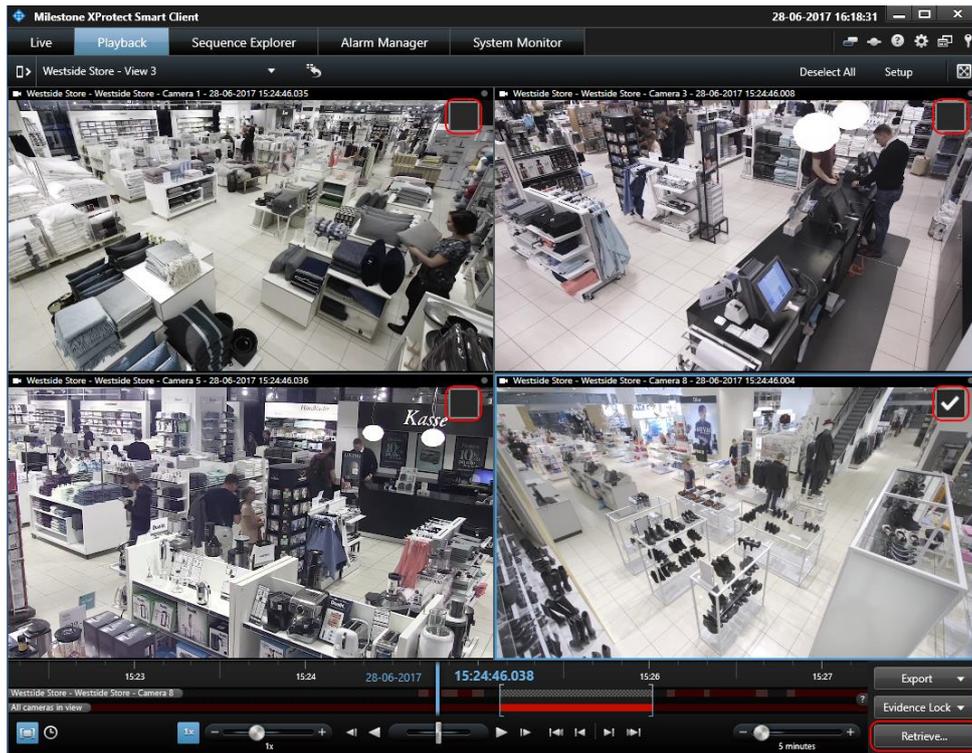
For these interconnected cameras where the operator has **Retrieve remote recordings** user rights, the remote recordings can be retrieved. Selecting the time period and the cameras to retrieve recordings from is selected in the same way as when selecting time periods to export.

Either – Click the  button and select the desired timespan graphically on the timeline...

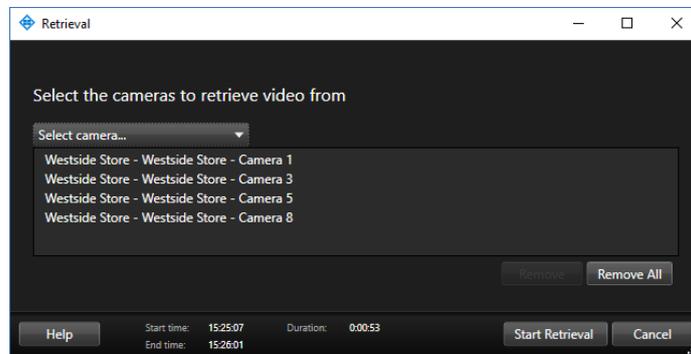


...or by clicking the  button and entering the desired timespan directly.

Once 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 checked by default).



Once the timespan and cameras in the view have been selected, the retrieval job can be created by clicking the **Retrieve** button. This will open the **Retrieval** dialog where additional cameras can be selected.



Clicking the **Start Retrieval** button will create the retrieval job. The created job will be indicated on the timeline by a lighter grey pattern as shown below.

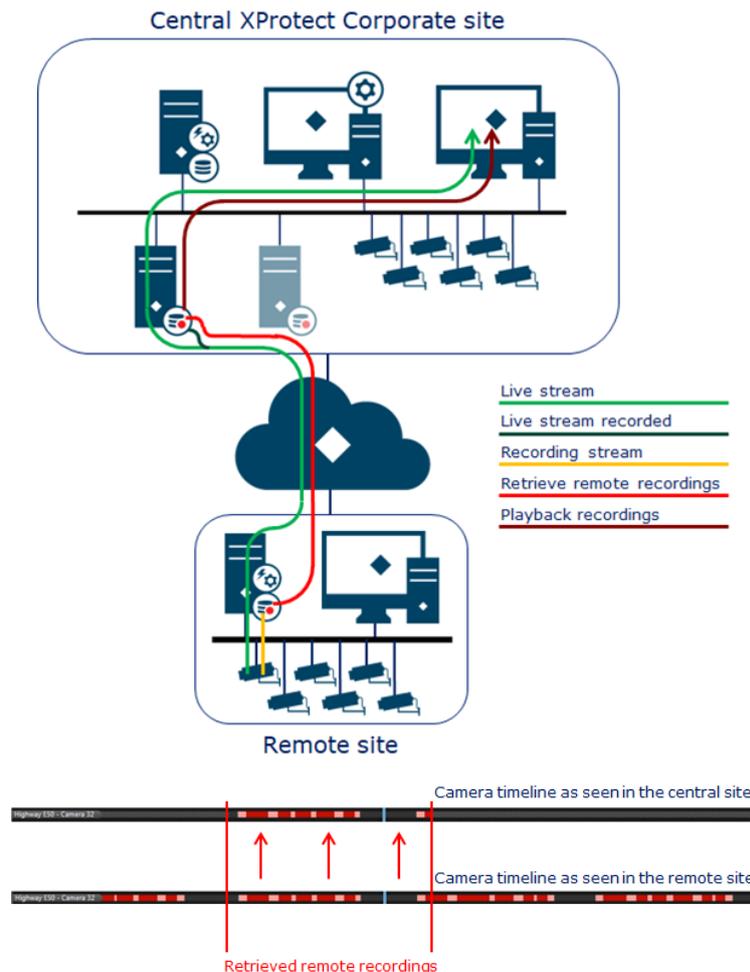
Sequence requested:



Sequence retrieved:

When the retrieval job is complete, the timeline will show the retrieved recordings with the standard red color and areas that didn't have any recordings on the remote site by showing these segments with the standard black unpatterned background.

The drawing below displays the central and remote site streams as well as the remote recordings retrieval connection for interconnected cameras that are set up to be recorded in both the central and remote sites and played back in the central XProtect Corporate site.



As can be seen, this configuration has a much more complex stream flow than the direct remote site playback configuration. This is because there are recording databases in both the central and remote sites and because there is support for retrieving recordings from the remote site.

With this configuration, the timeline for the central site operator will not be the same as for an operator on the remote site. This is because each site records under its own rules and because recordings can be retrieved from the remote site.

If **Remote Retrieval** limitations have been set for the remote site in the XProtect Management Client the remote recordings will be retrieved when the retrieval time-

window 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.

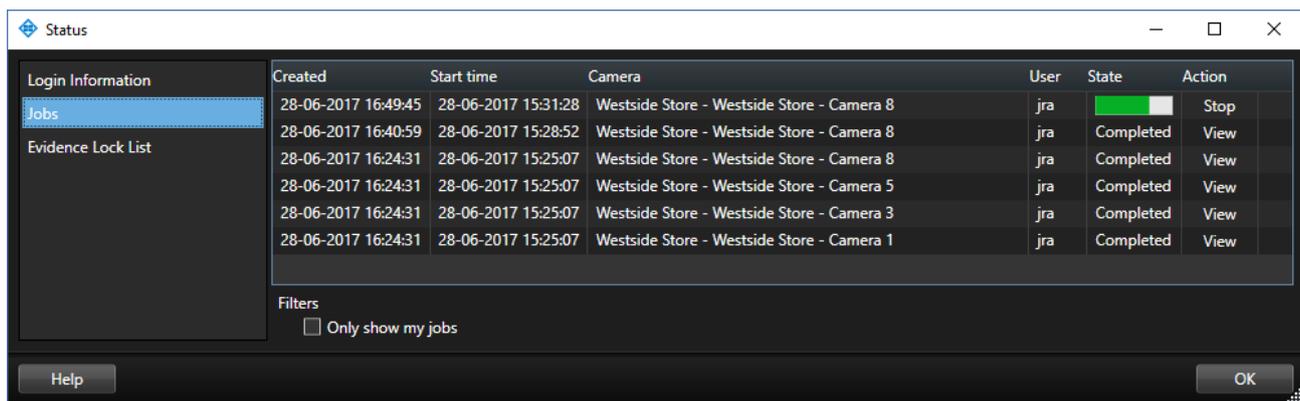
### Retrieval Jobs

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

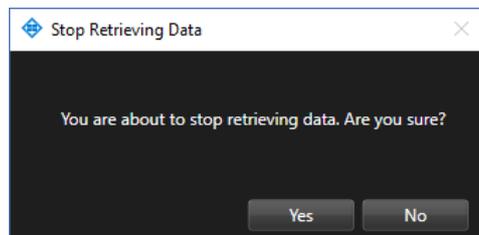
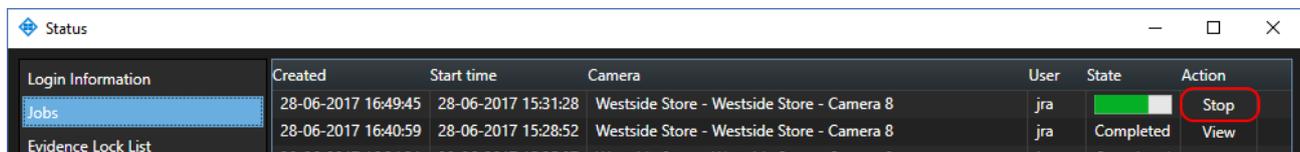


You can hide all shown jobs by clicking on the  button or remove the individual jobs from the list by clicking on the  button (it will not cancel the retrieval job) To cancel an ongoing job click the **Stop** button.

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.



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



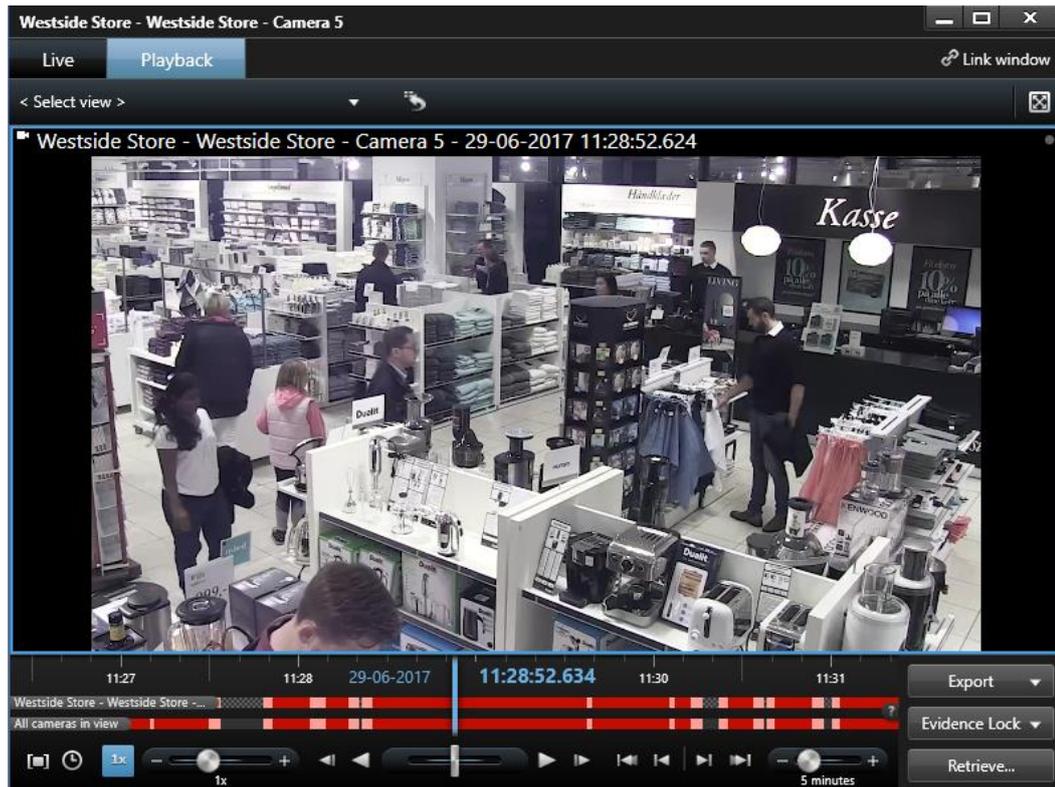
Users will be prompted to confirm that the retrieval should be stopped.

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

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

Login Information	Created	Start time	Camera	User	State	Action
Jobs	29-06-2017 12:58:53	29-06-2017 11:28:52	Westside Store - Westside Store - Camera 8	jra	Completed	View
Evidence Lock List	29-06-2017 12:58:53	29-06-2017 11:28:52	Westside Store - Westside Store - Camera 5	jra	Completed	View

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



## Milestone Interconnect in comparison to Edge Storage

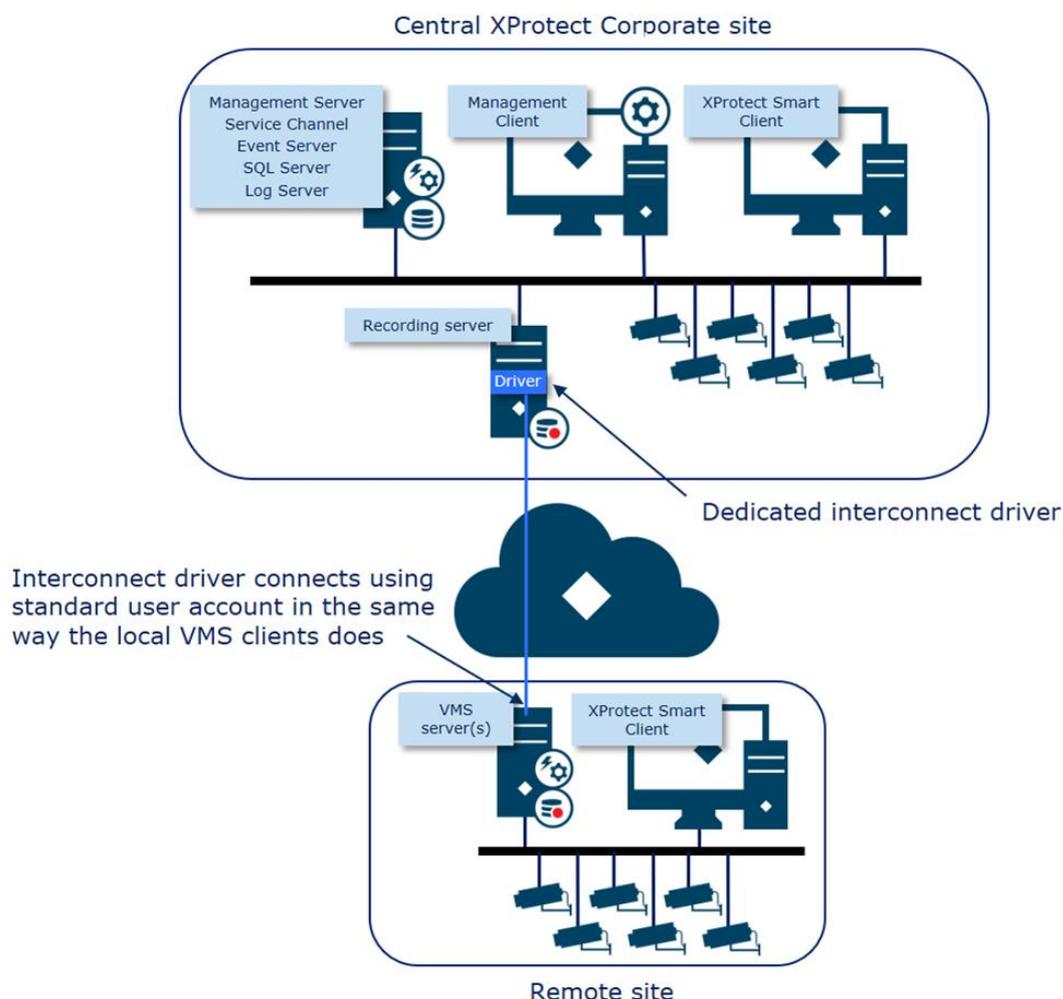
Cameras with Edge Storage have built-in storage or storage directly associated with the camera, where the camera stores the video recordings. When a Milestone surveillance site is interconnected, the complete remote surveillance site including cameras, microphones, speaker and metadata devices and the 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 principally is implemented the same way Edge Storage for cameras is, 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 need. However, even though they offer the same basic functionality of building a large centralized VMS consisting of multiple sites running a VMS, they in fact offer different functionalities, complement each other in various ways and each has its own specific strengths and uses.

The connections in Milestone Interconnect are made through a dedicated driver in the central XProtect Corporate site's recording server. This enables the interconnected site to appear as a kind of video encoder with Edge Storage support, offering users of the Smart Client the possibility to playback or retrieve recordings from the remote sites.



Milestone Interconnect has the benefit of having the recording server handling the connection and authentication on the interconnected sites. Therefore, clients do not have to connect and authenticate on multiple sites when logging in.

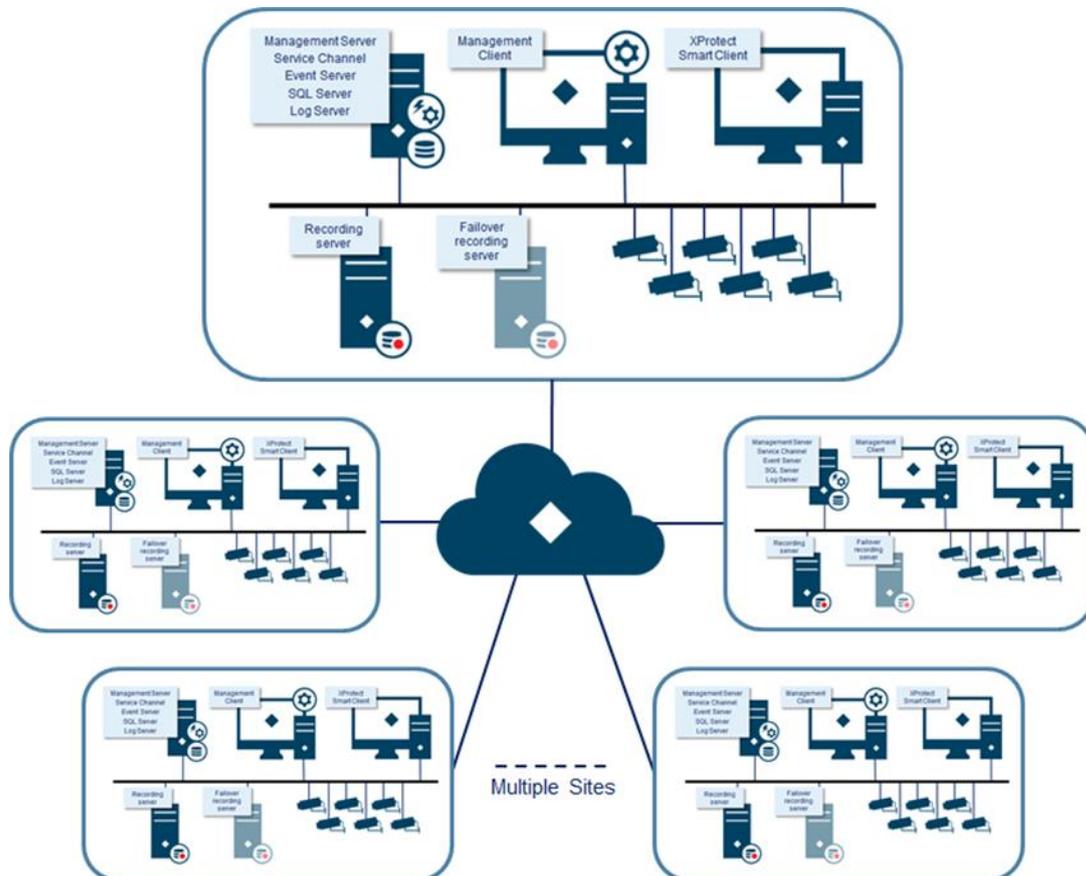
Additionally, it is also possible to set up connections to remote sites running on other domains than the central XProtect Corporate site, or connect to remote sites that are not permanently online. Moreover, and most importantly, it offers the functionality of retrieving recordings from a remote site to the central XProtect Corporate site or to playback the recordings from the remote sites directly.

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 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.

Milestone Federated Architecture is connected via the XProtect Corporate management servers in a so-called federated hierarchy. The connection between different sites in the federated hierarchy is not a permanent connection, but a link to the other sites. In this way, clients that logs in know there are more sites in this hierarchy, which they should connect to and authenticate on.



This means that even though the VMS from the operator's point of view in the clients appears as a one large VMS, the clients actually authenticate and retrieve the configuration from each site individually. Furthermore, live and recorded audio and video is retrieved directly from the recording servers on each site.

Milestone Federated Architecture requires all sites to be online when the clients log in and authenticate. Otherwise, the clients will experience a longer log in time as connections attempts to the unresponsive sites must first timeout before login is completed.

After log in, the client cannot establish a connection automatically to the sites that did not respond, as they are contacted only during login. The operator in the client will therefore have to log out and retry to login manually in order to get access to the sites that were not responsive.

For more information, see [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 a number of things to consider for optimal performance and user experience.

### **Retrieve recordings from remote sites with a permanent network connection**

In the previous retail scenario for example, the challenges with such configuration is to:

- Limit the bandwidth use from the interconnected site when nobody views the cameras
- Limit the CPU load on the central site's recording server
- Ensure there is enough time and bandwidth to retrieve the recordings in a timely fashion

In order 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 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 rule can be created to start the live video feed when a user in a client requests live video
- Disable the built-in motion detection in the central XProtect Corporate site to reduce CPU load

- Disable recording rules for the interconnected cameras to minimize disk load. With this configuration it is still possible to retrieve recordings from the remote sites
- Ensure the retrieval bandwidth limit and retrieval time period settings for the interconnected sites are configured with enough bandwidth and long enough time to allow the remote recordings to be retrieved in a proper timeframe. If this is not done, the VMS will build up a longer queue of remote retrieval jobs. Alternatively, if there are no bandwidth concerns leave the two settings disabled
- A remote recordings retrieval job that has already started will continue until it is completed, even if it goes beyond the configured time for retrieving the recordings. If it is critical that these jobs do not continue into a period where the bandwidth is needed for other traffic (e.g. no more retrieval after 8.00 am), the retrieval time window should be set so that the active job can be completed before this time (e.g. 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 as long as possible, the recording storage container can be set to 365 days (or more) with a set size limit – e.g. 200 GB. 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 200 GB limit is reached.

Following the above recommendation, the recording server requirements 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 over a network connection with large bandwidth**

In the previous transportation scenario where a ferry or a vehicle arrives at its garage or harbor and transfer the recordings to the central site, it can be experienced that the full bandwidth is not utilized fully. In this case we recommend that you raise the number of parallel transmissions from the default 8 to for instance 16.

By increasing this number, the bandwidth will be better utilized ensuring a faster transmission of recordings.

However, it 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.

In order to address this the following is recommended:

- Ensure that the disk performance in both ends can cope with this load.
- Split the storage definition and recording in the central site over more disks and "storage containers" so that:
  - One storage container/disk is used for the live recording of standard cameras running on the recording server
  - Another storage container/disk is used for the remote cameras.
  - Note: for this recommendation to be valid it requires that you never record the remote cameras live in the central site
- 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 video from the connected cameras might be at stake if the storage system is overloaded, there is no risk of losing any of the retrieved recordings, as new recordings are not transferred until the retrieved recordings are successfully stored in the media database.

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

In the transportation scenario for example, the challenge is to:

- Limit the bandwidth use for streaming live video, audio and metadata from the interconnected site
- Limit the CPU load on the central site recording server
- Ensure that there is enough time and bandwidth to retrieve the recordings in a timely fashion when the vehicle or vessel are within reach of a network connection to the central site
- Ensure the recordings on the interconnected site are not deleted before there has been enough time to retrieve it from the central XProtect Corporate site

In order 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
- Disable the built-in motion detection in the central XProtect Corporate site to reduce CPU load
- Recording retention on the interconnected cameras in the central XProtect Corporate site must be set long enough to allow for playback or investigation to be done, or alternatively the Evidence Lock feature can be used to protect important recordings against deletion
  - If there are concerns about disk usage or if there is a wish to keep the retrieved recordings as long as possible, the recording storage container can be set to 365 days (or more) with a set size limit – e.g. 200 GB. 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 200 GB limit is reached

- Recording retention settings and available disk space on the remote interconnected site must be sufficient to allow the recordings to be requested and retrieved to the central XProtect Corporate site before they are deleted from the remote site. For example, if the remote site can only store the recordings for one day there is a risk that they will be deleted before they had been retrieved by the central XProtect Corporate site
- There should be enough calculated and allocated time and bandwidth on the network connections to allow the requested recordings to be retrieved from the different vehicles to the central XProtect Corporate site. If there is not enough time and bandwidth available, the retrieval jobs will simply queue up and the VMS on the remote site will ultimately delete the recordings before they get a chance to be retrieved.

Following the above recommendations will ensure the recording server requirements on the central XProtect Corporate site are kept low, requiring only enough CPU and network bandwidth to retrieve recordings from the interconnected sites.

### **Playback recordings directly from interconnected remote sites**

In the city surveillance scenarios for example, the challenge with such configuration is to:

- Ensure there is enough bandwidth to playback the recordings directly from the remote site
- Limit and distribute the network and CPU load across multiple recording servers
- Limit the disk requirements on the central XProtect Corporate site.

In order to address these concerns, the following is recommended:

- Disable the built-in motion detection in the central XProtect Corporate site to reduce CPU load
- Ensure there is enough upstream bandwidth available on the remote interconnected site, and enough downstream bandwidth available on the central XProtect Corporate site for live viewing and playing back the required amount of remote interconnected cameras
- Consider connecting to remote sites via multiple XProtect Corporate recording servers to distribute the network and CPU load
- As the remote interconnected cameras record and playback directly from the remote site, there is no need for high performance recording disks in the central XProtect Corporate recording server. If the central XProtect Corporate recording server is not used for recording any regular cameras, the OS system disk can be configured as the default-recording disk for the recording server as nothing will be recorded on it.

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

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

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

## Supported products

The current list of supported products, versions and features supported can be seen here: <http://www.milestonesys.com/our-products/milestone-interconnect/milestone-interconnect-compatibility/>

# Licensing

Milestone Interconnect is licensed differently than the standard hardware devices which require a hardware device license per IP device/video-encoder/camera/MAC address

For more information on standard licenses: <http://www.milestonesys.com/analogtoip>

With Milestone Interconnect a “*Milestone Interconnect Camera license*” is required per interconnected and enabled camera on the central XProtect Corporate site. As this is per interconnected and enabled camera, it means that a license isn’t necessarily needed for all cameras present on the interconnected remote site. Only cameras that the central XProtect Corporate site has access permissions to and that are enabled need a Milestone Interconnect Camera license.

Interconnected remote sites themselves do not require additional licenses. Support for Milestone Interconnect is included in the interconnected site’s VMS license.

The Milestone Interconnect camera licenses are purchased the same way regular hardware device licenses are, and they are included in the license file used for XProtect Corporate.

The Management Client’s license page gives an overview of the purchased and activated camera licenses for regular hardware devices and interconnected cameras., It will also provide information about new temporary non-activated cameras and expired and missing licenses for all device types.

**Milestone XProtect Management Client 2017 R2**

Site Navigation: Westside Inc. - (11.2a)

- Basics
  - License Information**
  - Site Information
- Remote Connect Services
  - Axis One-click Camera Connection
- Servers
  - Recording Servers
  - Fallover Servers
  - Mobile Servers
- Devices
  - Cameras
  - Microphones
  - Speakers
  - Metadata
  - Input
  - Output
- Client
  - Smart Wall
  - View Groups
  - Smart Client Profiles
  - Management Client Profiles
  - Matrix
- Rules and Events
  - Rules
  - Time Profiles
  - Notification Profiles
  - User-defined Events
  - Analytics Events
  - Generic Events
- Security
  - Roles
  - Basic Users
- System Dashboard
  - Current Tasks
  - System Monitor
  - System Monitor Thresholds
  - Evidence Lock
  - Configuration Reports
- Server Logs
- Access Control
- Transact
- Alarms

**Milestone Care**

Your current level:

Milestone Care ID:

[Edit details...](#) [Access Milestone Care portal...](#)  
[End user license agreement](#) [Information about Milestone Care...](#)

**Installed Products**

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 2017 R2	M01-C01-112-01-6C4920	Unlimited	N/A	N/A
Milestone XProtect Smart Wall	M01-P03-100-01-6C4D5D	Unlimited	Unlimited	
Milestone XProtect Access	000-0000-0000	Unlimited	Unlimited	
Milestone XProtect Transact	000-0000-0000	Unlimited	Unlimited	

**License Overview - All sites** [License Details - All Sites...](#)

License Type	Activated
Hardware Device	42 out of 512
Milestone Interconnect Camera	42 out of 512
Access control door	0 out of 1000
Transaction source	0 out of 1000

**License Details - Current Site: Westside Inc.**

License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Hardware Device	9	0 out of 5	0	0	0
Milestone Interconnect Camera	8	N/A	0	0	0
Access control door	0	N/A	0	0	0
Transaction source	0	N/A	0	0	0

Enable automatic license activation

Activate License Manually...

Site Navigation Federated Site Hierarchy

Last activated: 9. juni 2017 09:53:25 Information refreshed: 30. juni 2017 16:04:11

## Benefits and summary

Milestone Interconnect is a unique concept that allows all Milestone XProtect VMS and Husky products to be interconnected with Milestone's premium software XProtect Corporate. It allows to deploy central surveillance across geographically dispersed sites in a flexible way, by combining cost-efficient remote XProtect VMS and Husky products with the advanced surveillance functions of XProtect Corporate in one 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 tight connection of fewer, but larger sites, while Milestone Interconnect is optimized to connect smaller distributed sites connected through low-bandwidth or intermittent connections.

Milestone Interconnect offers a number of powerful capabilities, such as:

- **Supports all Milestone XProtect VMS and Husky products**  
Allows customers to select the most efficient VMS solution for local sites with the possibility to mix different products and meet the specific needs of each site
- **Cost-efficient multi-site deployment**  
This is made possible by allowing the customer to use any Milestone VMS product on the remote sites fitting their needs and budget. Furthermore, Milestone Interconnect does not require common or trusted domains between the central site and the remote sites
- **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
- **Remote management of interconnected sites**  
Reduces the need for costly onsite visits by technicians and service personnel
- **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.

Thanks to its built-in flexibility, Milestone Interconnect can be used in a number of different verticals and contexts. Although Milestone Interconnect can be used in 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 in to 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 in to a common central surveillance site.

The underlying drivers for any business or organization deploying Milestone Interconnect is the wish to reduce the cost of the initial investment, optimize security operations and increase the security level with fewer resources and reduced operational and maintenance costs.

### **About Milestone Systems**

Founded in 1998, Milestone Systems is the global industry leader in open platform IP video management software. The XProtect platform delivers powerful surveillance that is easy to manage, reliable and proven in thousands of customer installations around the world. With support for the widest choice in network hardware and integration with other systems, XProtect provides best-in-class solutions to video enable organizations – managing risks, protecting people and assets, optimizing processes and reducing costs. Milestone software is sold through authorized and certified partners. For more information, visit [www.milestonesys.com](http://www.milestonesys.com)

Milestone Systems Headquarters, DK

Tel: +45 88 300 300

Milestone Systems US

Tel: +1 503 350 1100