The Open Platform Company

White paper

Milestone Interconnect™

Prepared by:

John Rasmussen, Senior Technical Product Manager, Corporate Business Unit, Milestone Systems

Date: July 05, 2013

Table of Contents

Introduction 3

Target audience and purpose 3

The concept behind Milestone Interconnect 4

Technical overview 5

Applied use of Milestone Interconnect 7
- **Retail** 7
- **Transportation** 9
- **Companies offering centrally managed video surveillance** 11
- **City surveillance** 12

Milestone Interconnect Management 15
- **Prerequisites** 15
- **Adding remote sites** 15
- **Settings – remote systems and devices** 18
- **Updating remote site devices** 19
- **Remote recording and direct play back configuration** 19
- **User rights in XProtect Corporate** 24
- **Rules** 25

Milestone Interconnect and XProtect Smart Client Operation 26
- **Setup** 26
- **Live** 26
- **Play back remote recordings** 26
- **Play back recordings from central site and retrieval of remote recordings** 28

Milestone Interconnect in comparison to Edge Storage 34

Milestone Interconnect in comparison to Milestone Federated Architecture 34

System implementation considerations 37

Supported products 40

Licensing 41

Benefits and summary 42

Introduction

With the release of XProtect® Corporate 2013, Milestone Systems introduces Milestone Interconnect™.

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

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

- Support for using low maintenance and footprint XProtect products on dedicated hardware in e.g. vehicles.
- Cost-efficient deployment by interconnecting Milestone products designed for the SMB market which are easy to install in addition to supporting system configuration cloning
- Retrieval of video and audio recordings over an intermittent network connection to the remote system
- Retrieval of video and audio recordings from interconnected systems to the central XProtect Corporate system
- Direct play back of the remote system's recording
- Scheduled, event or user-activated retrieval of remote system's recordings to the central XProtect Corporate system
- Short and consistent login times regardless of the number of interconnected systems, remote system response time or network connection state
- Full XProtect Corporate camera rights for the interconnected cameras
- Remote Management of the interconnected systems

Due to its unique features, Milestone Interconnect is especially suited for specific verticals such as: retail chains, transportation, companies offering surveillance services or city surveillance.

Target audience and purpose

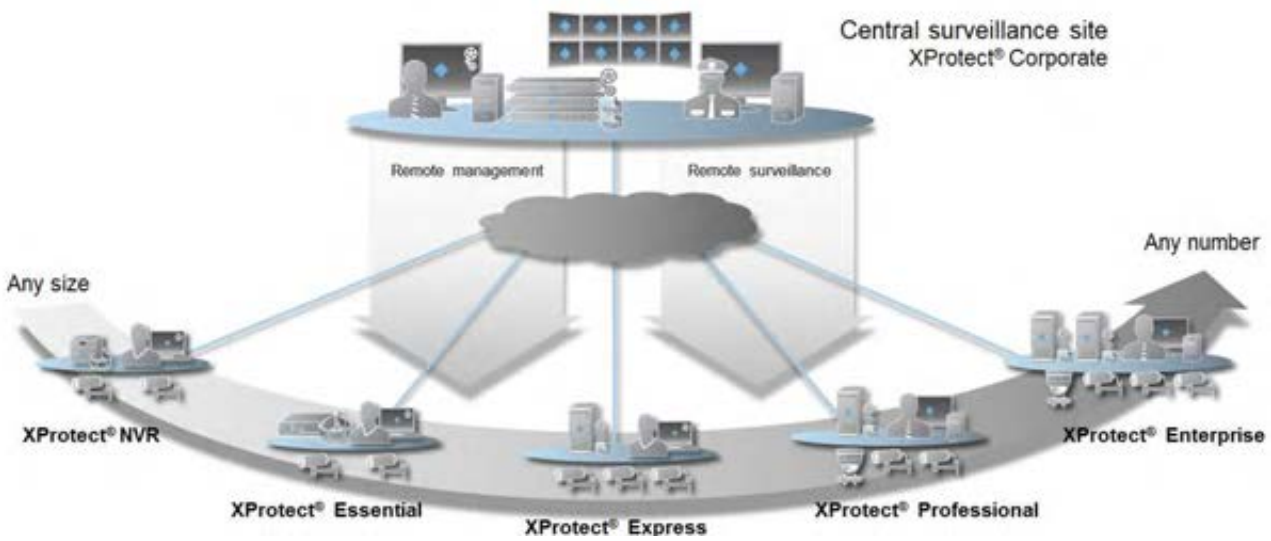
This white paper's target audiences are: surveillance system architects and designers, large-scale surveillance project consultants, companies, organizations, universities and governments with distributed surveillance projects or installations.

The purpose of this white paper is to provide a general overview of Milestone Interconnect; the concept behind it, its technical implementation, its benefits and the problems it solves.

This white paper should enable the reader to understand the architecture and technology behind Milestone Interconnect, as well as how to design and implement a distributed surveillance system by utilizing Milestone Interconnect. It is assumed that the reader has a general understanding of Milestone XProtect Corporate, its Management Client and XProtect® Smart Client and the other XProtect VMS products as well as a general understanding of network infrastructure.

The concept behind Milestone Interconnect

With Milestone Interconnect multiple remote sites running different XProtect products can be linked with a central XProtect Corporate site.



This offers central XProtect Corporate system users seamless access to live and recorded video and audio regardless if it is recorded at a remote site, in the central XProtect Corporate system or both.

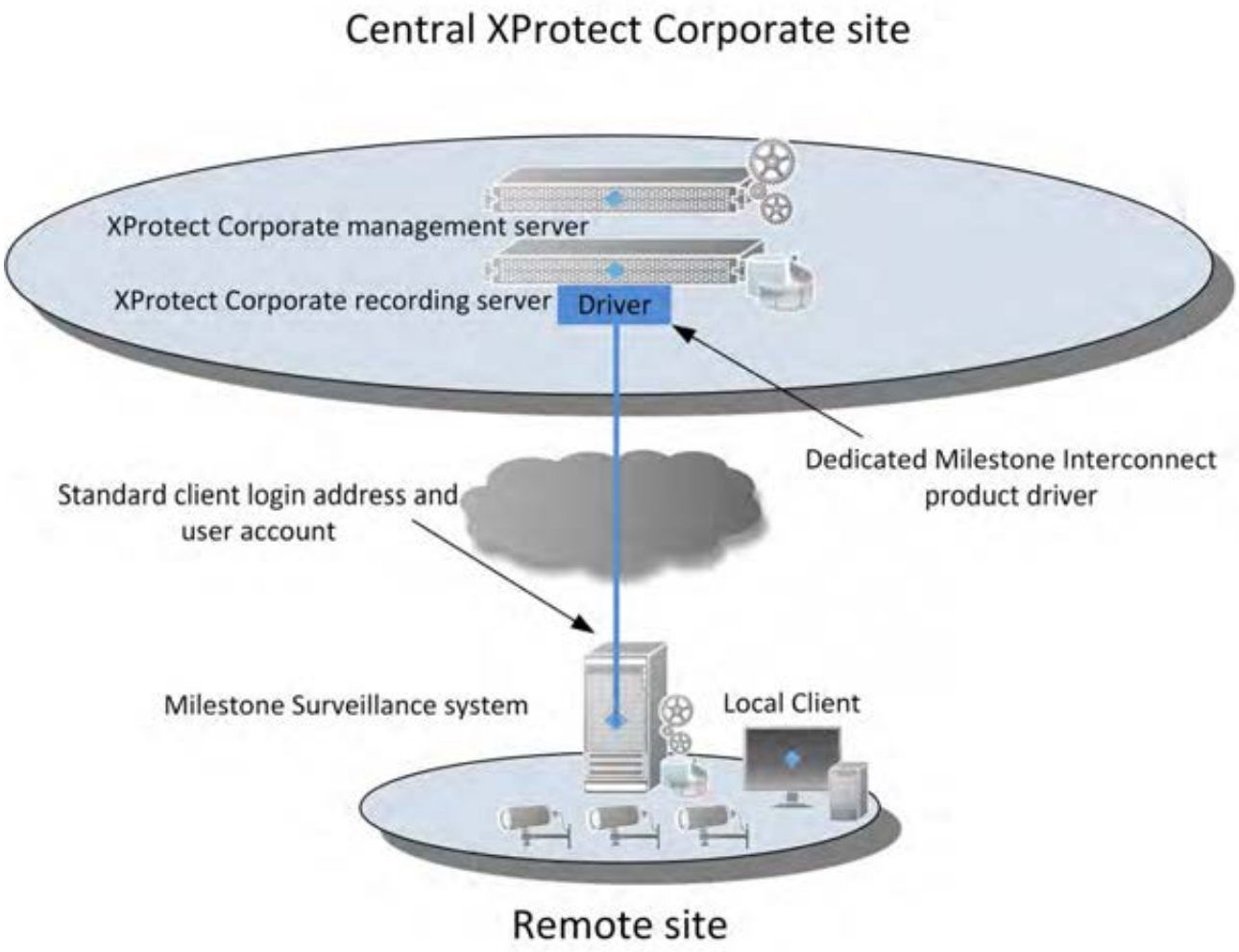
Furthermore, it offers the central XProtect Corporate users advanced functions for all the interconnected products when accessed through the central XProtect Corporate system such as: advanced rule and recording retrieval functionality, time based access rights, system status and monitoring, bookmarking, alarm management, etc. This capability works regardless if the remote site's VMS offers the advances functions or not.

If users need to access the remote system directly they can do it as usual for these products and they can use the standard functions the specific product offer.

Technical overview

The actual connection between the central XProtect Corporate site and the remote site is established through an XProtect Corporate recording server via a driver, exactly as connecting to a camera or a video encoder.

The following diagram shows how the central XProtect Corporate site and the remote site are interconnected via a dedicated device driver on the recording server.



Since the remote site is interconnected via the recording server, the remote system will in essence appear on the central XProtect Corporate site as a “multi-channel video encoder” with edge storage support.

All cameras on the interconnected remote sites will appear as any other camera connected directly into the central XProtect Corporate system, and can be used and administrated in the XProtect Corporate system in the same way as any camera

connected directly with the exception of changing the actual image settings for the camera, since this is controlled by the remote system.

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

- Short and consistent login time for clients regardless of number of interconnected systems and remote sites response time or online status
- Support for remote sites that are not online all the time, for instance surveillance systems in vehicles
- Ability to transfer recordings from remote sites to the central XProtect Corporate site
- Capacity to play back recordings directly from the remote site
- Full XProtect Corporate camera rights including time limited access rights
- Full MIP-SDK support via XProtect Corporate for the cameras on the remote site

Recording and storage wise there are three different ways this can be done; each having their own advantages and usage.

Option 1: Recording only takes place in the remote interconnected system
With this option all recording and play back is done locally in the interconnected system. Recording will be switched off completely in the central XProtect Corporate system and the recording servers will only function as a gateway to live and recorded video and audio from the remote system.

- Users accessing the interconnected system directly can view live and recorded video and audio
- Users accessing the interconnected system via the central XProtect Corporate system can view live and recorded video audio and use the advanced XProtect Corporate features

Option 2: Recording only takes place in the central XProtect Corporate system
With this option, recording is switched off in the remote interconnected system. All video is streamed to the central XProtect Corporate system and is recorded based on XProtect Corporates motion detection, events or schedule.

- Users accessing the interconnected system directly can only view live video and audio, but they cannot play back recordings
- Users accessing the interconnected system via the central XProtect Corporate system can view live and recorded video audio and use the advanced XProtect Corporate features

Option 3: Recording is done in both systems

With this option, recording and play back is done both at remote sites and at the central XProtect Corporate system. Recordings can furthermore on schedule, event or user request be transferred (copied) from the interconnected system to the central XProtect Corporate system. This makes it possible to transfer all or selected recordings from the interconnected system at a later time when bandwidth or connection is available or only transfer certain sequences requested by a user.

- Users accessing the interconnected system directly can view live and recorded video and audio
- Users accessing the interconnected system via the central XProtect Corporate system can view live and recorded video and audio as well as use the advanced XProtect Corporate features. Furthermore they also have access to requesting recordings not present in the central XProtect Corporate system to be transferred to it from the remote system.

Applied use of Milestone Interconnect

Retail

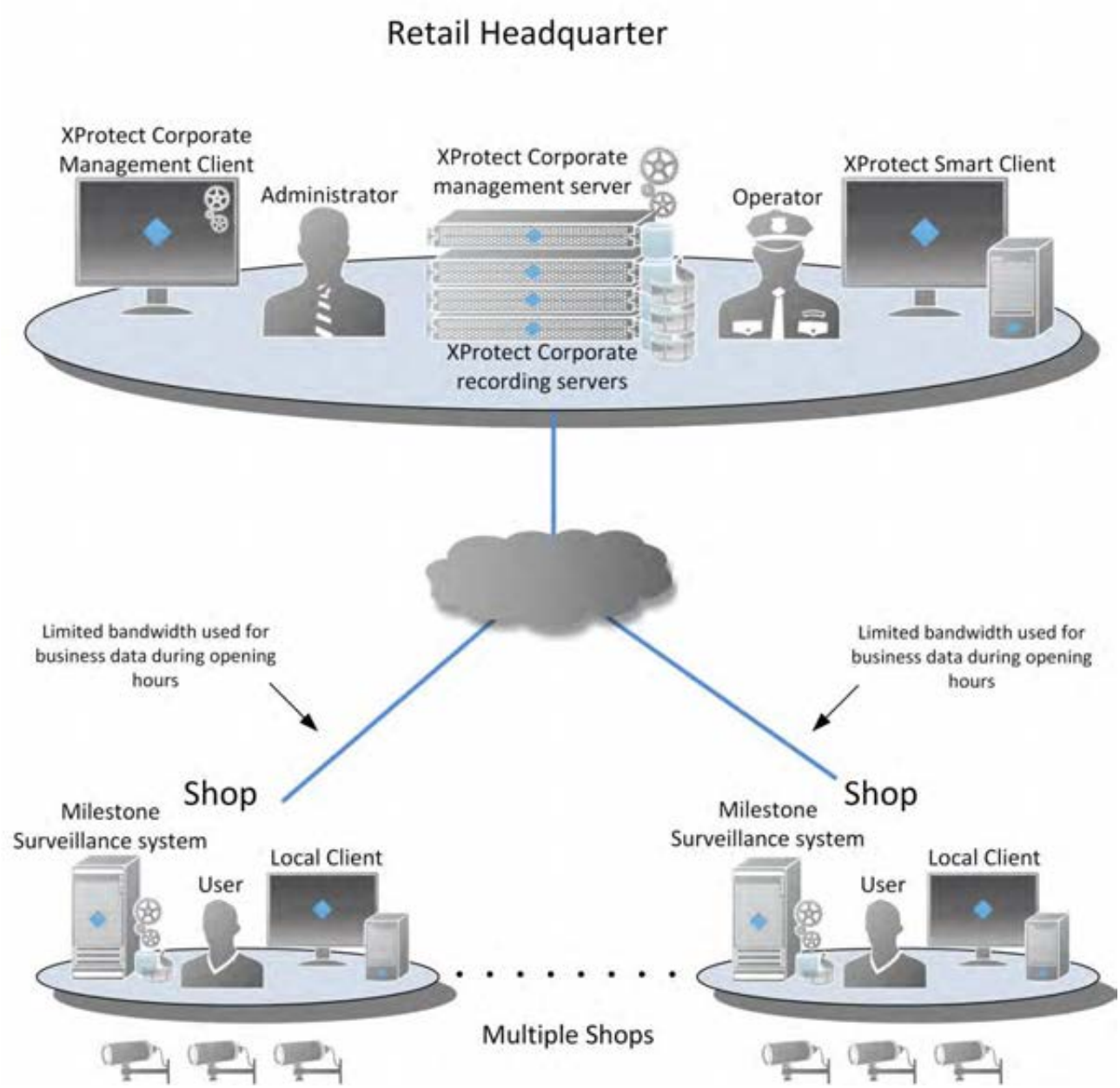
Retail chains with individual shops often need video surveillance in each shop for employee security and to counter theft and control internal fraud. However, they also have a wish to link these independent surveillance systems with the headquarters to form a large centralized surveillance system to lower operational costs and optimize administration, monitoring and fraud investigation.

Linking multiple surveillance systems is often not possible when using a simple or cheap solution, and using advanced surveillance systems across multiple sites can be quite expensive. An additional challenge is that the bandwidth between the shops and headquarters often are limited and may be used for business data during opening hours.

Milestone Interconnect offers an ideal solution for installations that cover multiple sites dispersed geographically, as the individual surveillance systems can be made-to-measure to satisfy the customer's needs which typically are:

1. **Price:** The surveillance system for the individual retail shops needs to be cost-efficient and simple since many local shops just require a few cameras and a basic functionality
2. **Connection:** Limited bandwidth to the different shops and bandwidth may be used for business data during opening hours
3. **Internal revenue:** Central access to the remote site for internal fraud investigation and evidence creating in the form of video and audio exports

4. **Deployment:** Easy deployment of the surveillance system on the remote sites with support for system cloning
5. **Management:** Central access to system administration and status monitoring



The retail needs are addressed by various Milestone Interconnect features:

1. With Milestone Interconnect, retail chains can build a cost-effective and geographically dispersed surveillance installation. Different sites can use different XProtect products designed for small or medium businesses while still obtaining a centralized surveillance system.
2. Milestone Interconnect offers flexible control of bandwidth usage when retrieving recordings from the remote sites. It features two settings that allow control of when

recordings can be retrieved from the remote site and the maximum bandwidth that may be used.

3. Since all remote sites are linked with the central XProtect Corporate site, any fraud investigation can be done from the headquarters. If there are any bandwidth limitations, investigators can request recording sequences to be transferred to the central XProtect Corporate site with a limited bandwidth or during off-peak hours. Once the video is transferred, it can be played back without bandwidth limitations.
4. Milestone Interconnect offers integrated access to remotely manage interconnected systems via a built-in remote management function.

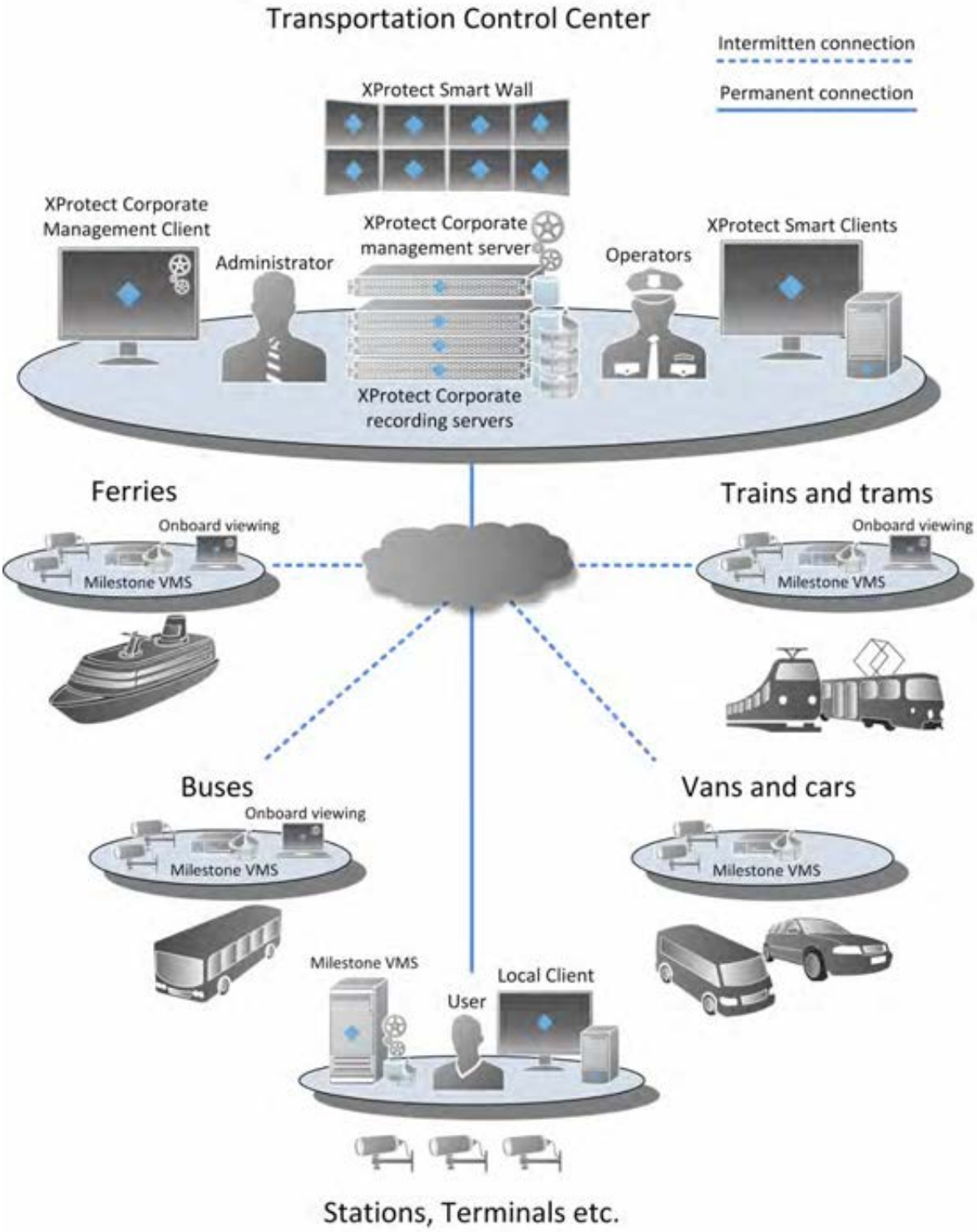
Transportation

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

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

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

1. **Connection:** It does not require a permanent high-speed wireless connection.
2. **Incident investigation:** There is no need for a manually process to physically retrieve recordings. Investigators can request transferal of recordings from the vehicles surveillance systems no matter if they are online or offline. They are then transferred once the vehicle is within network reach, for instance at a station, bus stop, ferry terminal, etc.
3. **Deployment:** It offers easy deployment of surveillance systems on remote sites with support for system cloning.
4. **Management:** When mobile systems are online, they can be accessed and administered centrally.
5. **Combined survailance:** Mobile onboard survailance systems can be combined with the stationary survailance in a cohesive security solution



The above needs are addressed by various Milestone Interconnect features:

1. With Milestone Interconnect there is no need to have a permanent high-speed connection as long as the vehicle has access to wireless hotspots at places such as bus or train stations, ferry terminals, etc.

2. Security operators can request that specific recordings are transferred from the vehicles to the central surveillance system even when the vehicle is offline. Once the vehicle comes online at a hotspot, the requested recordings are copied to the central system. Furthermore, this can be automated based on events or software integration via the MIP SDK.
3. Maintenance of the vehicles surveillance systems can be done remotely when the vehicle is online reducing the need for physical in-vehicle maintenance.

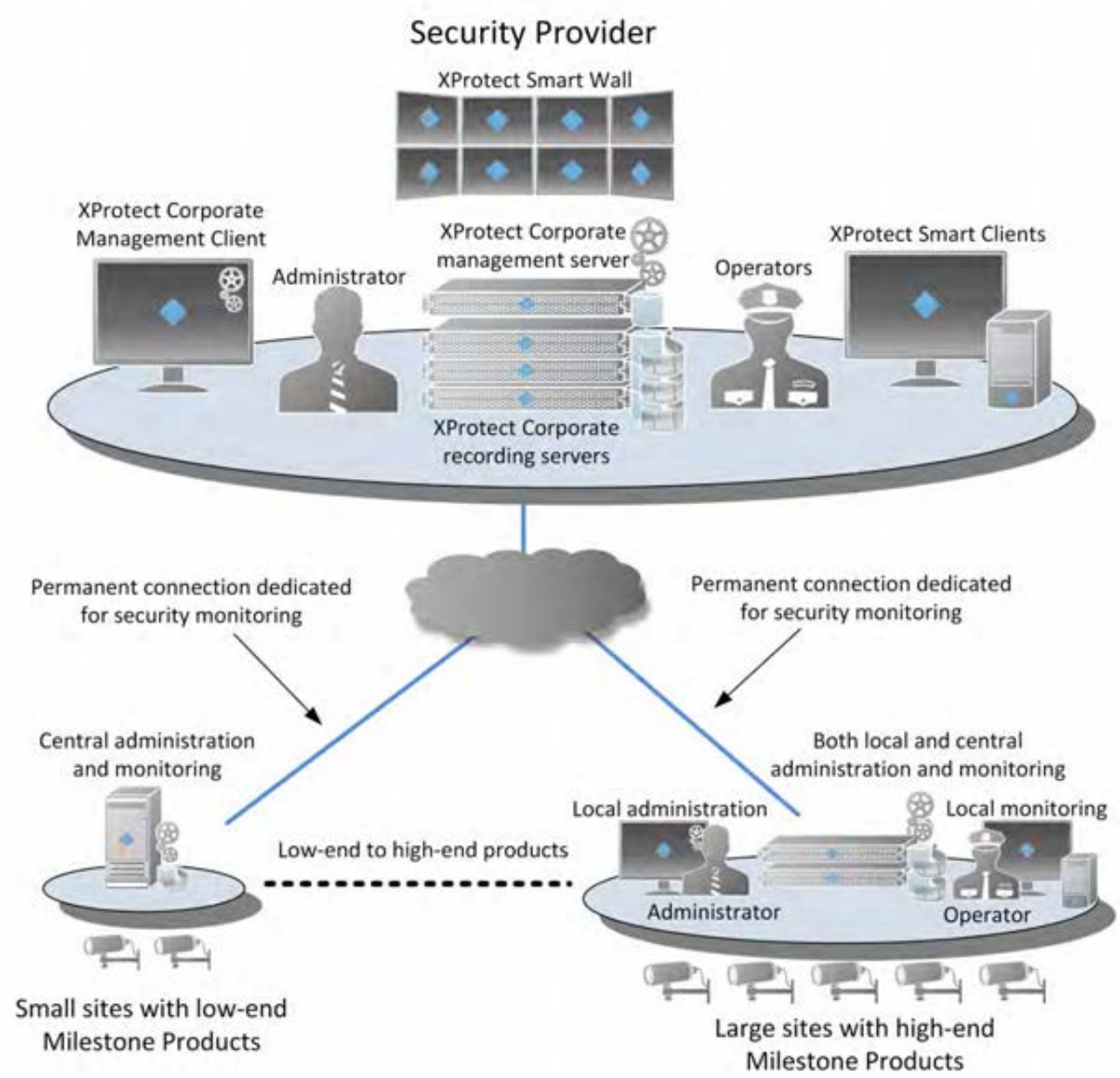
Companies offering centrally managed video surveillance

Companies offering onsite security, video surveillance and alarm services require a solution that gives them the possibility to satisfy their customers' needs by customizing a fully integrated system managed by a centralized monitoring and alarm system.

The surveillance solution must address all types of installations, from small surveillance systems with just a few cameras and no local monitoring to customers with several hundred cameras and staff dedicated to proactively monitor their installation.

Milestone Interconnect offers an ideal solution for security companies as it addresses the challenges for centrally managed video surveillance solutions.

1. **Products:** It supports a broad range of Milestone products from a simple installation with just a few cameras to more advanced solutions with an unlimited amount of cameras.
2. **Authentication:** Milestone Interconnect can be linked to remote systems using any type of Milestone XProtect user authentication for example: basic users, local Windows users or Windows Active Directory users. This makes the solution independent on creating AD trusts between the security company's central domain and the customer's local domain.
3. **Monitoring and Management:** Security companies can centrally monitor their customers' systems and quickly address any issues. There is no need to physically visit a customer's location or use non-integrated third-party solutions.
4. **Alarms:** Security companies can offer their customers an alarm functionality with integrated video surveillance which increases situational awareness, reduces response times and identifies false alarms.
5. **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 and distributed surveillance systems in for instance cities require a flexible and price-conscious solution that covers their needs in a highly fragmented and distributed surveillance environment consisting of systems owned and managed by different entities ranging from “single cameras on a pole” over small or medium-sized installations to high-security installations with thousands of cameras.

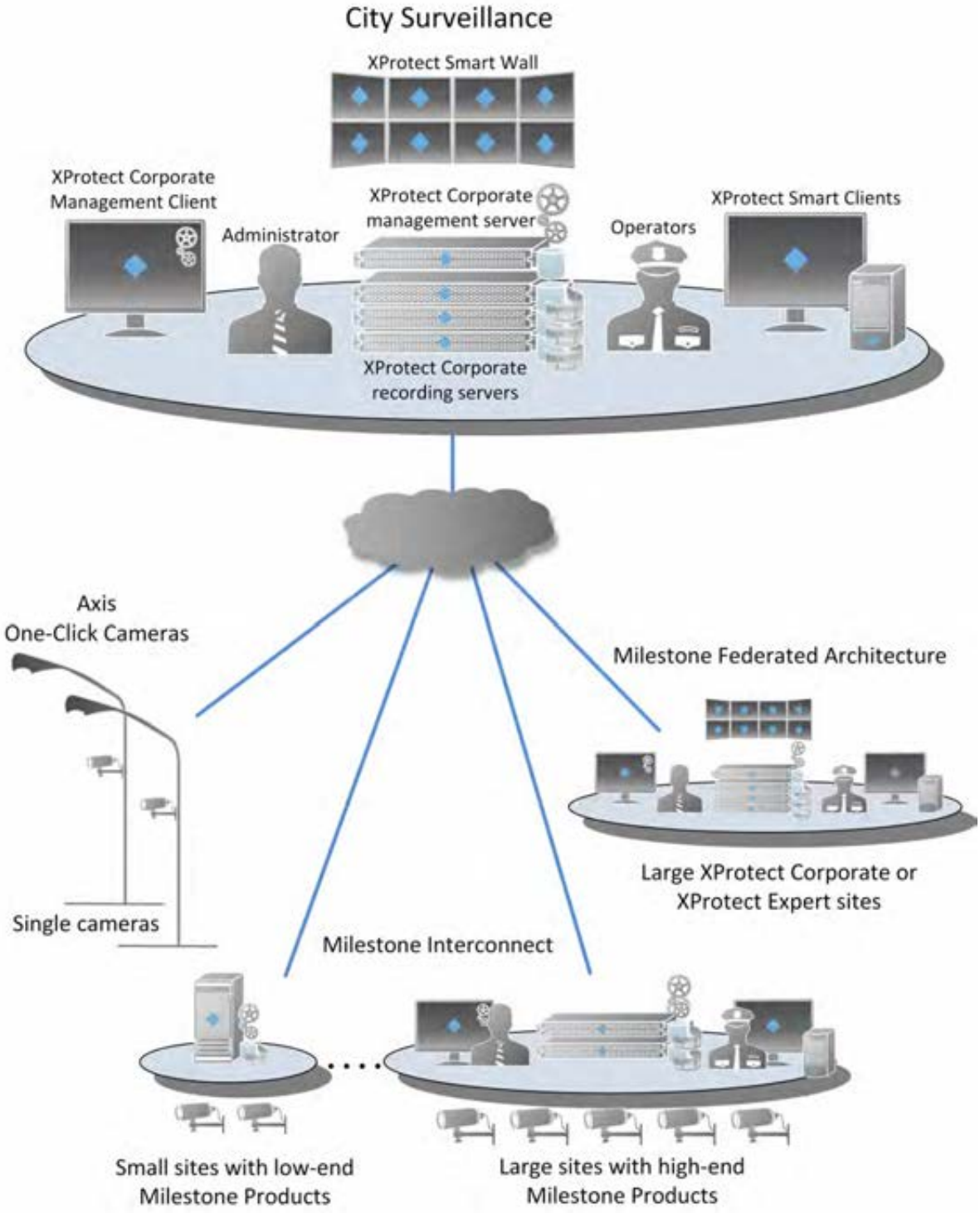
XProtect Corporate supports several technologies that address different types of installations.

1. Single camera: Remote Connect Services offers a simple solution for deploying cameras (Axis) on locations without a dedicated surveillance network infrastructure. The cameras can essentially "phone-home" over the public internet and create a secure and encrypted communication channel, even through unmanaged routers or firewalls.
2. Milestone Interconnect: can be used to connect multiple Milestone XProtect systems to the central XProtect Corporate site without requiring administrator rights or AD trusts on the remote system.
3. Milestone Federated Architecture: offers a solution to link a 1000+ camera high-end XProtect Corporate or XProtect Expert installation with a central XProtect Corporate site.

Each of these three technologies boasts specific strengths, features and uses. In addition to the information found on this Milestone Interconnect white paper, more information about Remote Connect Services and Milestone Federated Architecture can be found in the following links:

Remote Connect Services
http://www.milestonesys.com/SharePoint/White%20papers/Milestone_Remote_Connect_Services_Axis_One_Click.pdf

Milestone Federated Architecture
http://www.milestonesys.com/SharePoint/XProtectCorporate/4_0%20and%204_1/Whitepapers/Milestone_Federated_Architecture_w_synapsis.pdf



With these three different technologies, all installation types and sizes can be linked into one large central XProtect Corporate installation offering a unified city-wide surveillance solution.

Milestone Interconnect Management

Prerequisites

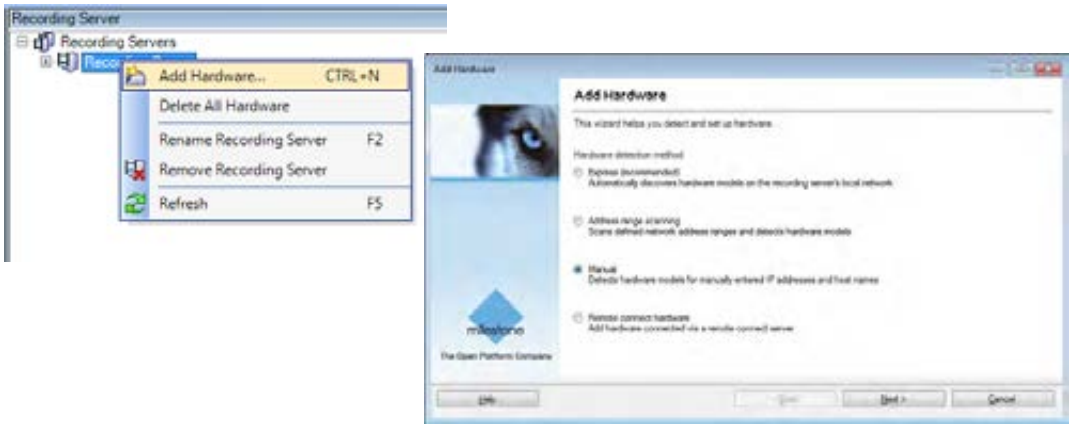
There are four basic prerequisites to use Milestone Interconnect:

- An installed and operational XProtect Corporate 2013 system
- An XProtect Corporate license including the total number of Milestone Interconnect device/camera licenses required
- A configured and working remote system including a user account (basic users, local Windows user or Windows Active Directory user) with rights for the devices that the central XProtect Corporate system should access
- Network connection between the central XProtect Corporate system and the remote systems with access or port forwarding to the ports used on the remote system

Note: The central XProtect Corporate system can only see and access devices the specified user account has access to. This allows local system administrators to control which devices should be made available to the central XProtect Corporate system and its users.

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.



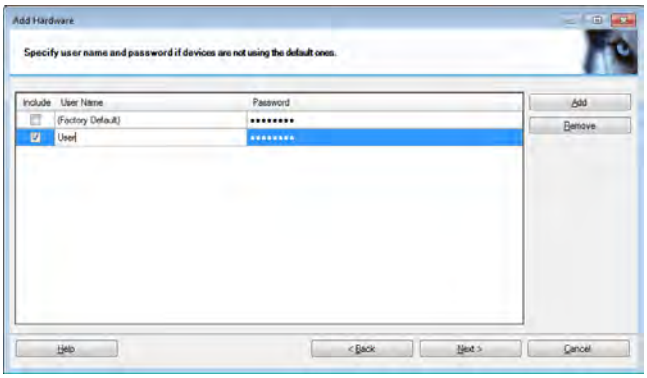
Note: Remote sites can only be added via the "Address range scanning" and "Manual" options.

Like when adding cameras the following must be specified in the wizard for it to detect the remote system: Address - or address scan range, driver (e.g. "Milestone SMB XProtect VMS Products and XProtect Enterprise") – or alternatively select auto-detect and the user account to connect with.

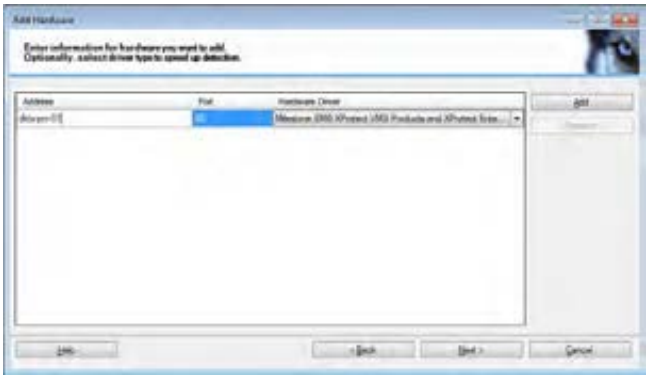
The user account with access rights to devices must be predefined on the remote system. Users can be either a basic users or a Windows user defined on the local Windows server/PC or a Windows user defined in a domain.

The “Add Hardware” wizard will run through the normal steps for detecting remote systems as it does when detecting standard cameras.

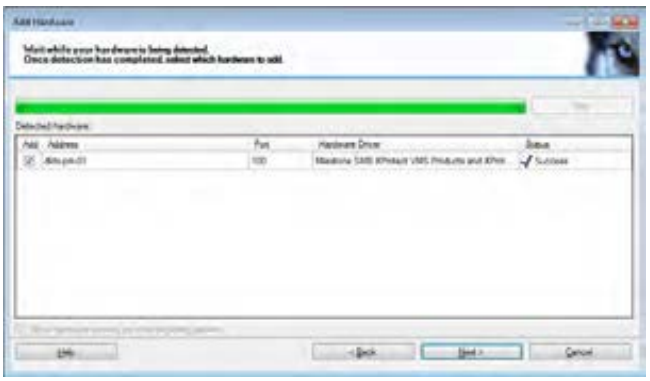
1



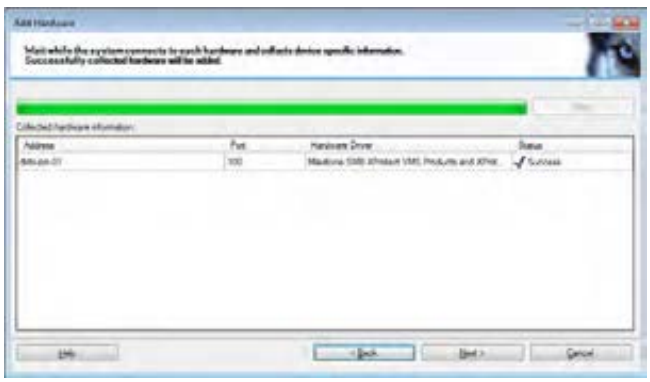
2



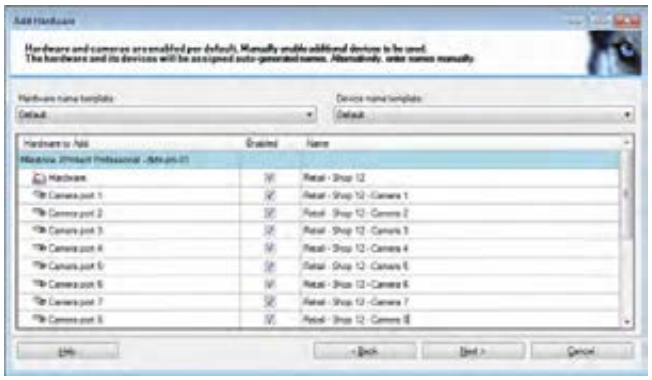
3



4



5

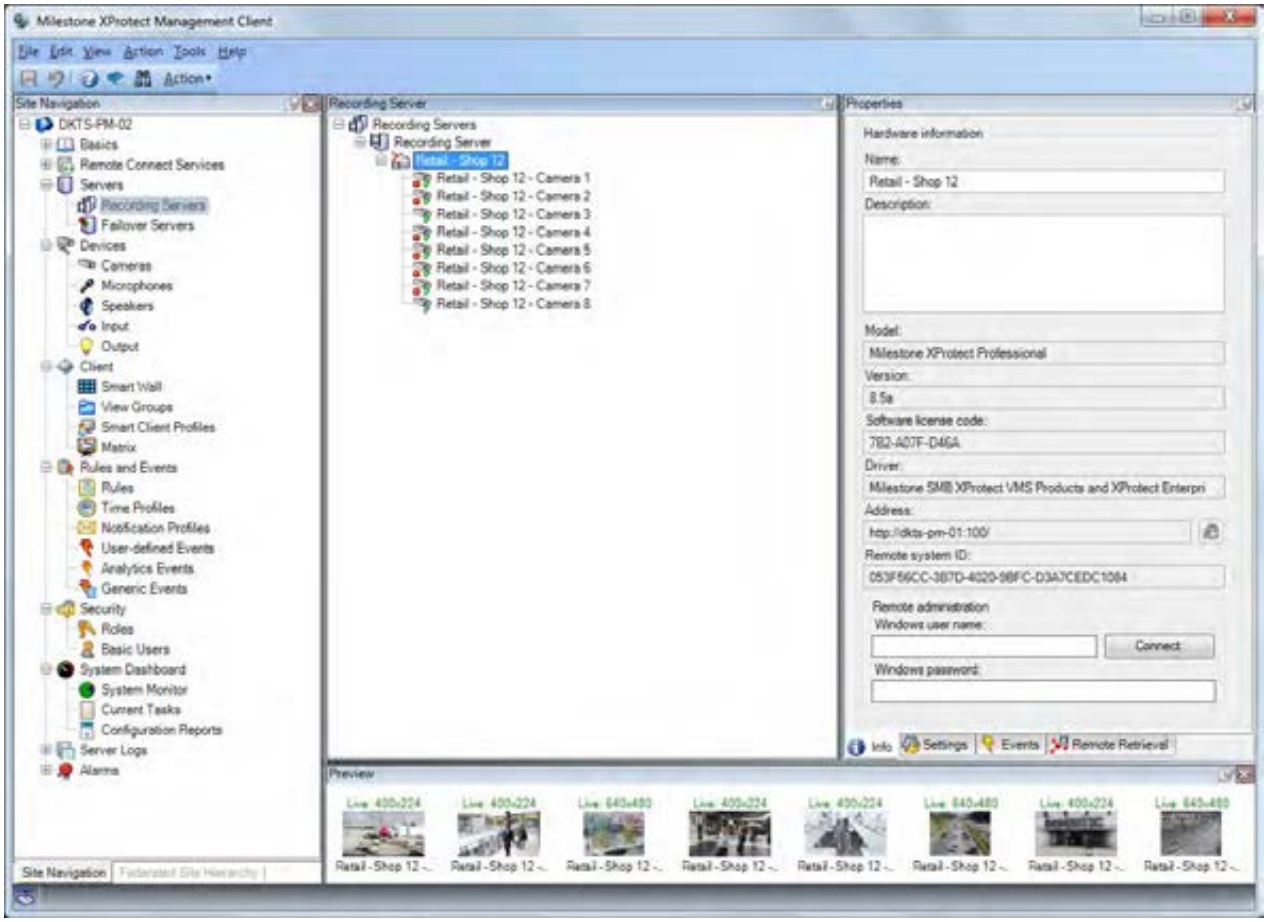


6

On the wizard’s step (5) where the detected devices can be named, the wizard uses by default the remote system’s server and device names.

These auto assigned names can be changed in the central XProtect Corporate system as for normal cameras. Doing so will not change the names on the remote system.

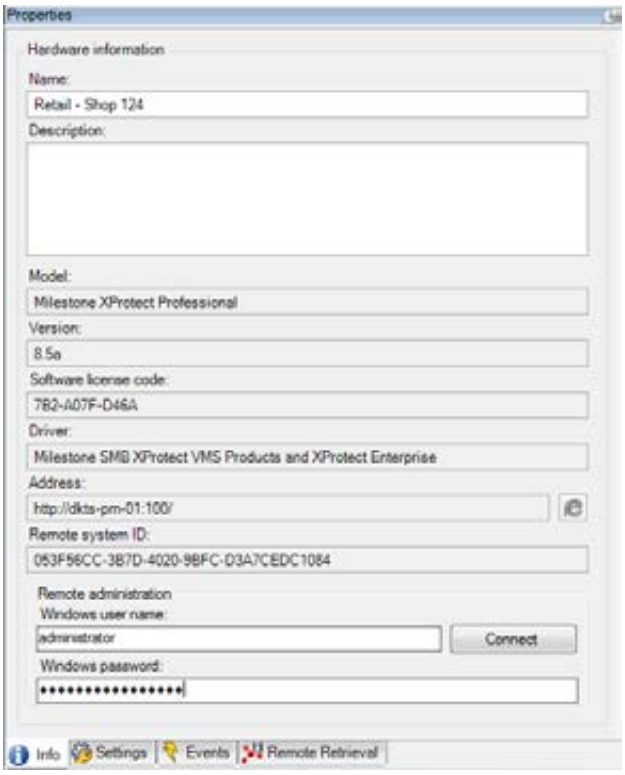
If it is necessary to see the original names of the remote system's devices, they can be seen on the device's "Settings" tab.
Once the remote systems have been added to the recording server, they will be listed the same way as standard cameras and video encoders.



The central XProtect Corporate site will have access to cameras, microphones, speakers and their functionalities (live, playback, PTZ, talk to speaker etc.) as specified for the user on the remote system. This means that if a user's account only grants access to a subset of cameras or functions, only these will be listed or allowed.

Access to devices and functions are controlled via standard user accounts on the remote systems; therefore, it is possible for the remote system administrator to control which cameras and functions the central XProtect Corporate site has access to. This ensures that the local administrator has full control of access rights to the local system and does not need rely that the central XProtect Corporate site doesn't access more cameras than agree on.

Settings – remote systems and devices



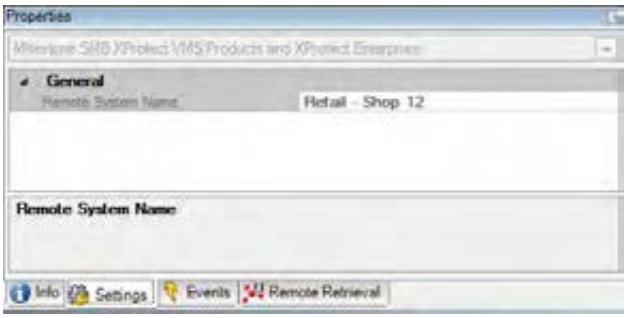
The interconnected remote system has a couple of tabs dedicated to display system information and for configuring events and remote recording retrieval settings.

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

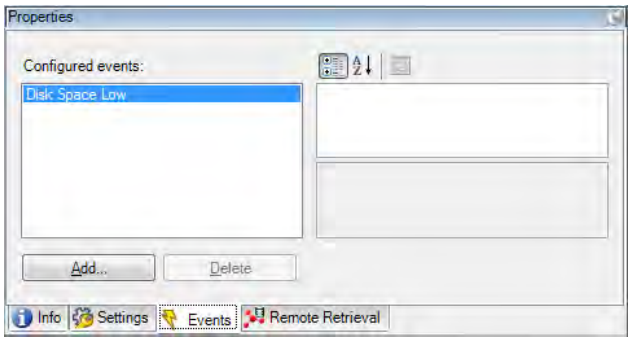
Furthermore it gives access to manage the remote system via built-in remote desktop support.

This requires that a Windows account for the remote system is specified and remote desktop connections are enabled on the server/PC running the remote system.

Note: The user account required to open a remote desktop session to the remote system is the Windows user account for the server - not the user account used to interconnect the remote system with the central XProtect Corporate site.



If the device name has been changed in the central XProtect Corporate system, the “Settings” tab will display the remote system’s original name.



The “Events” tab gives access to select events from the remote system that should be usable in the central XProtect Corporate system.

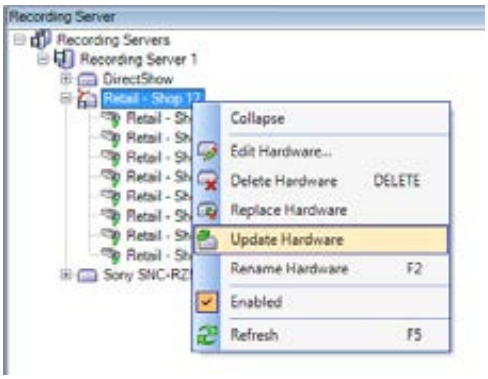
The list of supported events depends on what the interconnected remote system supports. See the supported products section for details.

The “Remote Retrieval” tab gives access to set the maximum bandwidth that remote recordings can be retrieved with as well as the specifying the time interval they can be retrieved within.

Note: The “Remote retrieval” settings only applies to retrieval of recordings from the remote system’s database to the central XProtect Corporate site’s recording server’s database. They do not apply in case the remote system is configured for direct play back. 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 system has been changed, for instance, by adding or removing cameras or events, the configuration in the central XProtect Corporate system needs to be updated to reflect the actual configuration of the interconnected system.



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

Remote recording and direct play back configuration

Recording in the central XProtect Corporate site

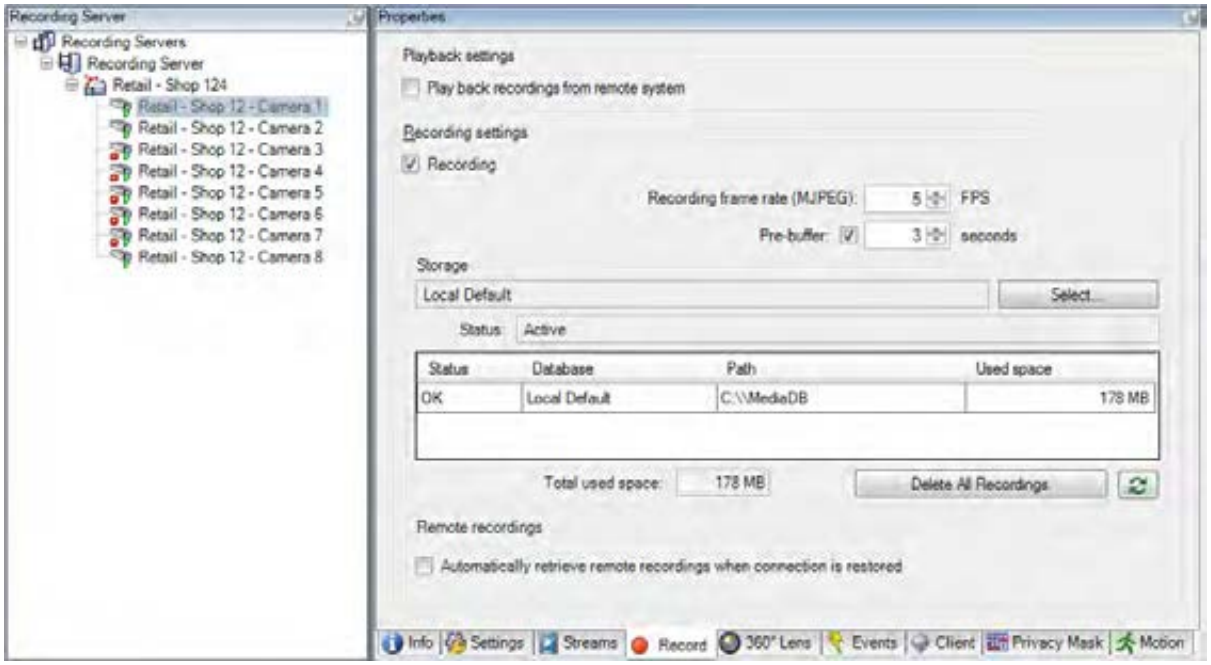
When selecting a camera, microphone or speaker it is possible to select if the device should be recorded in the central XProtect Corporate system, or if the device should be recorded and played back directly from the remote system.

Note: Configuration of the remote system’s recording settings must be done directly in the remote system.

When a remote system is initially interconnected to the central XProtect Corporate site, the default setting for its devices is to record and play back video and audio on the central XProtect Corporate system.

When recordings are set to be done in the central XProtect Corporate system, the standard XProtect Corporate recording settings (including the “Automatically retrieve remote recordings when connection is restored” setting) can be used as for any standard

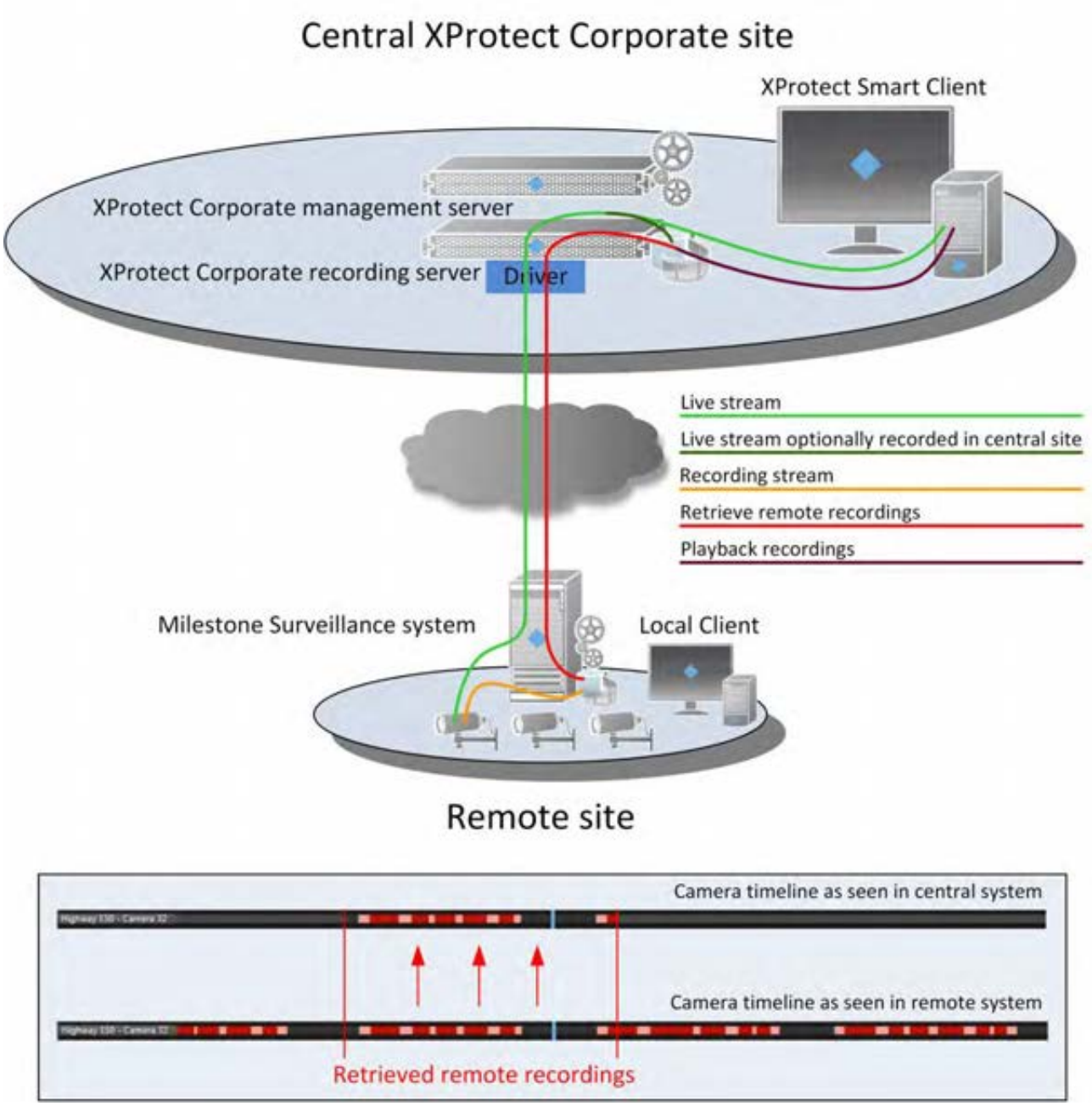
cameras with Edge Storage support. This also applies for creating rules controlling when video is recorded.



In addition to recording in the central XProtect Corporate system, the remote system can be used as a kind of “edge storage” device for recovering missing recordings should there have been a network or server issue. The missing recordings can be retrieved automatically if the connection is lost to the remote system; this is enabled by checking the “Automatically retrieve remote recordings when connection is restored” checkbox.

If live video or audio is not needed in the central XProtect Corporate system or only needed when someone monitors it, the rule system can be configured not to start the live stream or to start it only upon request.

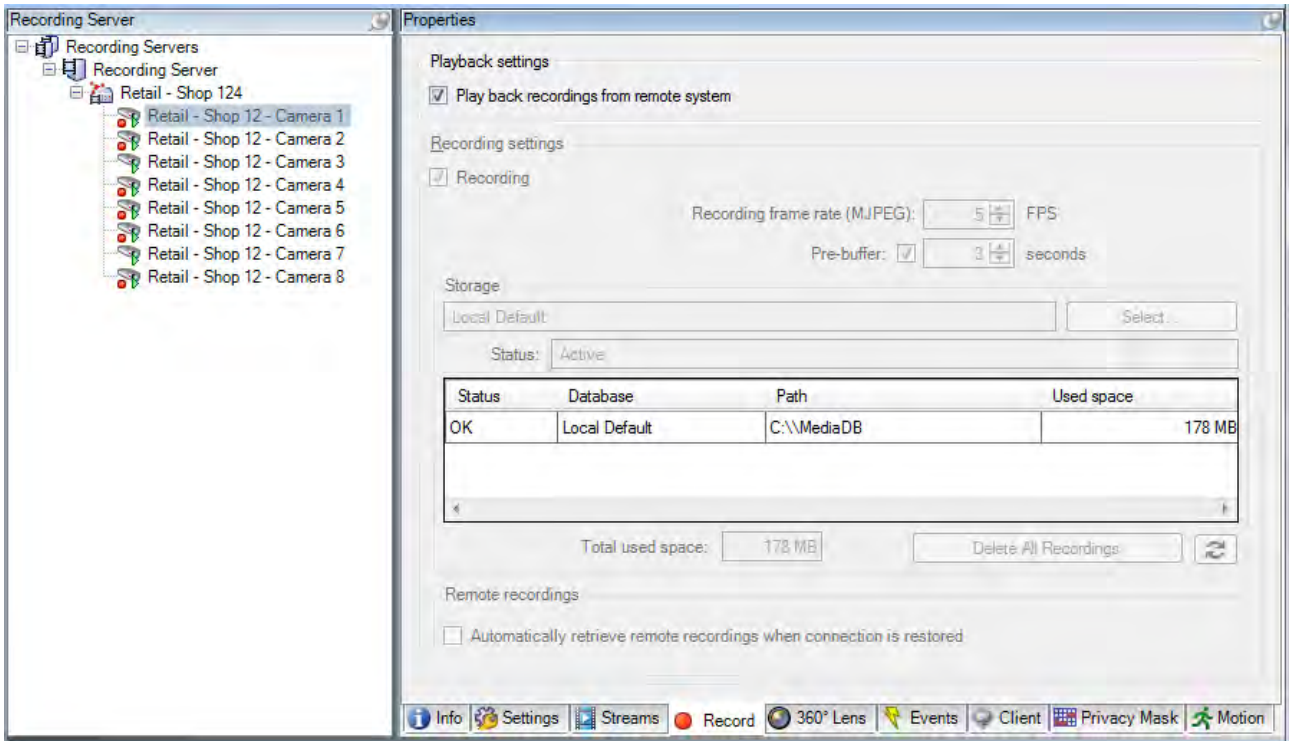
Furthermore, setting audio and video to be recorded in the central XProtect Corporate system in addition to the remote system, makes it possible to utilize the function to transfer recordings from the remote system to the central XProtect Corporate system. The transfer of recordings can be initiated on manual request from a Smart Client operator, on system or device events, on schedule or a combination of these.



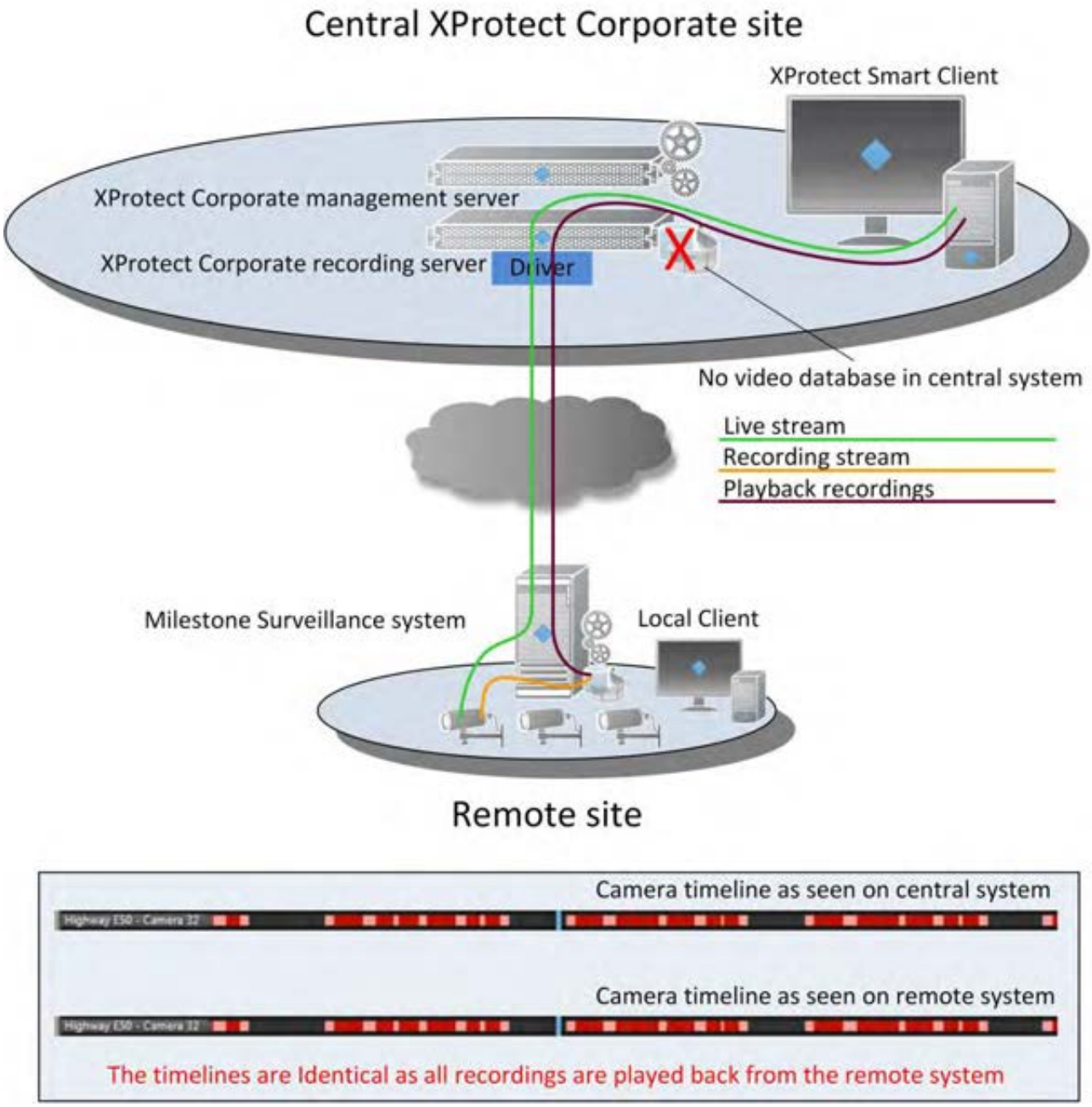
With this configuration, the timeline for the central site operator will not be the same as for an operator on the remote system. This is due to the fact that each system records by its own rules and because recordings can be retrieved from the remote system.

Direct remote system play back

Selecting to play back recordings directly from the remote system is done on the device's "Record" tab, by checking the "Play back recordings from remote system" checkbox. This will also disable recording of the device in the central XProtect Corporate site's recording server.



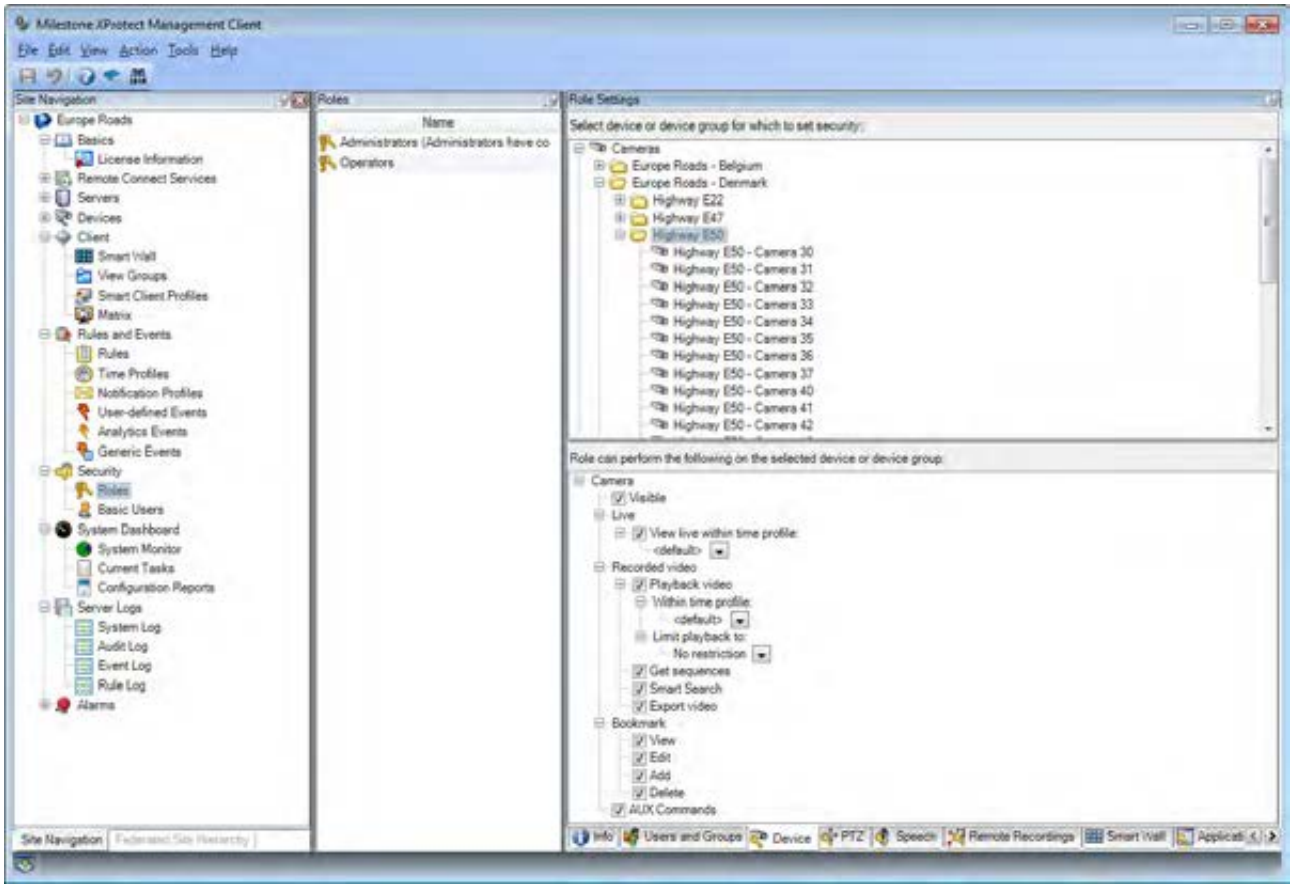
Clients requesting recorded audio and video for play back will in this case still send the request to the central XProtect Corporate site's recording server; nevertheless, the recording server will instead of fetching them from its own recording database retrieve them from the interconnected remote system's recording database.



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

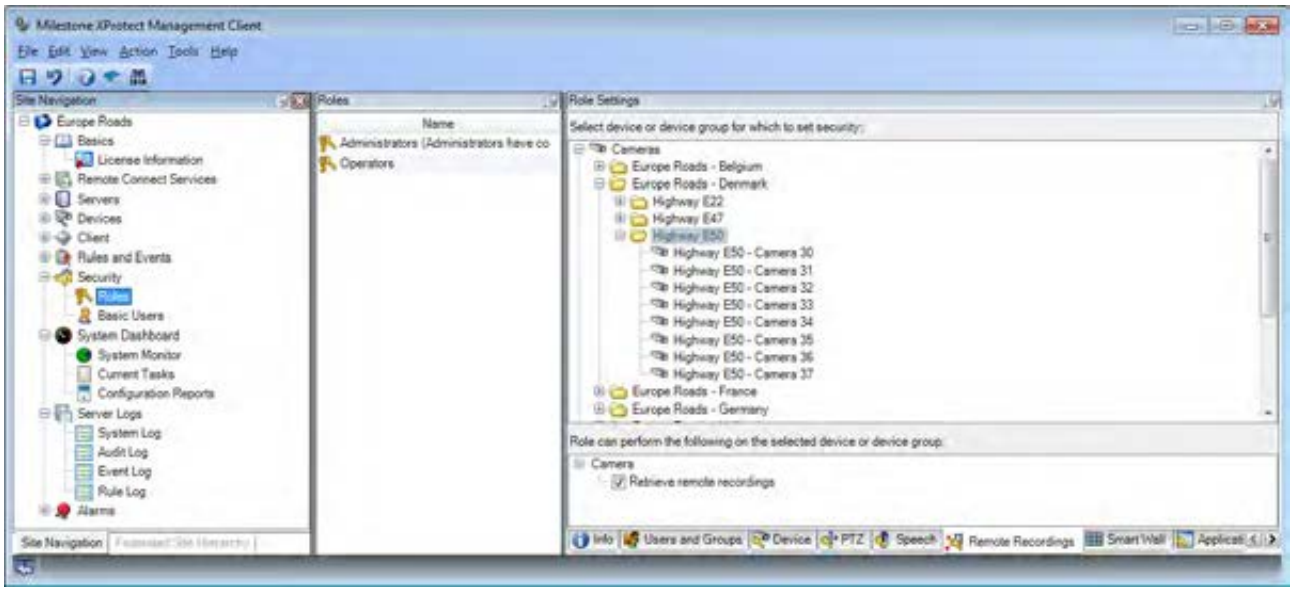
User rights in XProtect Corporate

Configuration of user rights for the interconnected cameras is done the same way as for regular cameras, by creating a “Role“ and assigning this role access to functions on the cameras.



The bookmark function also works on interconnected cameras; consequently, access rights to this function can be also set. The same applies to time-limited access to live and playback which also works on interconnected cameras even though the interconnected remote system 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 cameras.

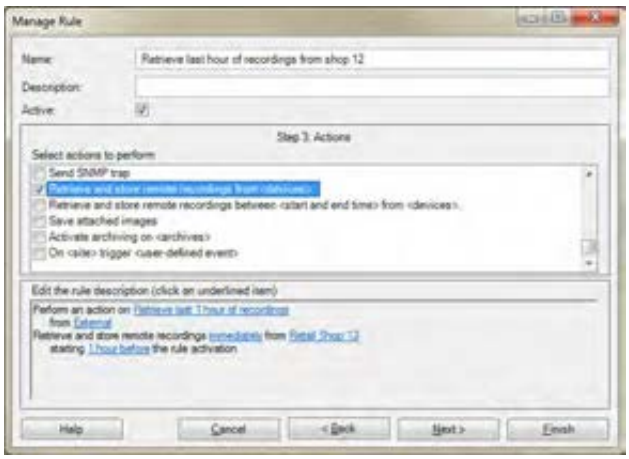


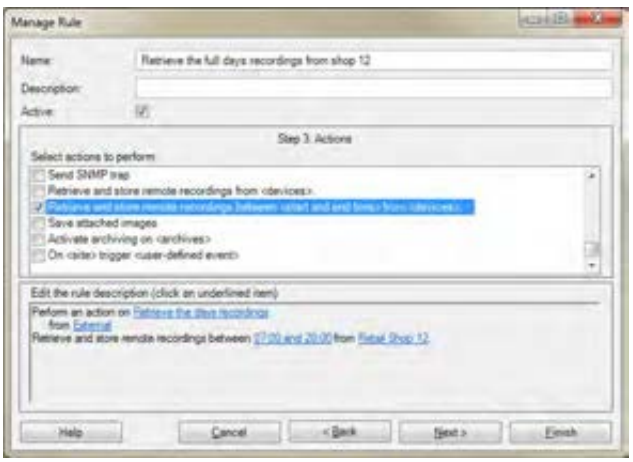
Rules

The rule system for interconnected cameras configured to record in the central XProtect Corporate system can be used to retrieve recordings from the remote system 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.

Example of two rules retrieving the last hour of recordings (left) and retrieving recordings between 07.00 and 20.00 (right) from a group of cameras on an event.





If the recordings need to be retrieved on a schedule, the rules should just be changed 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 standard camera; they have the same properties and are added to views in the same way.

Live

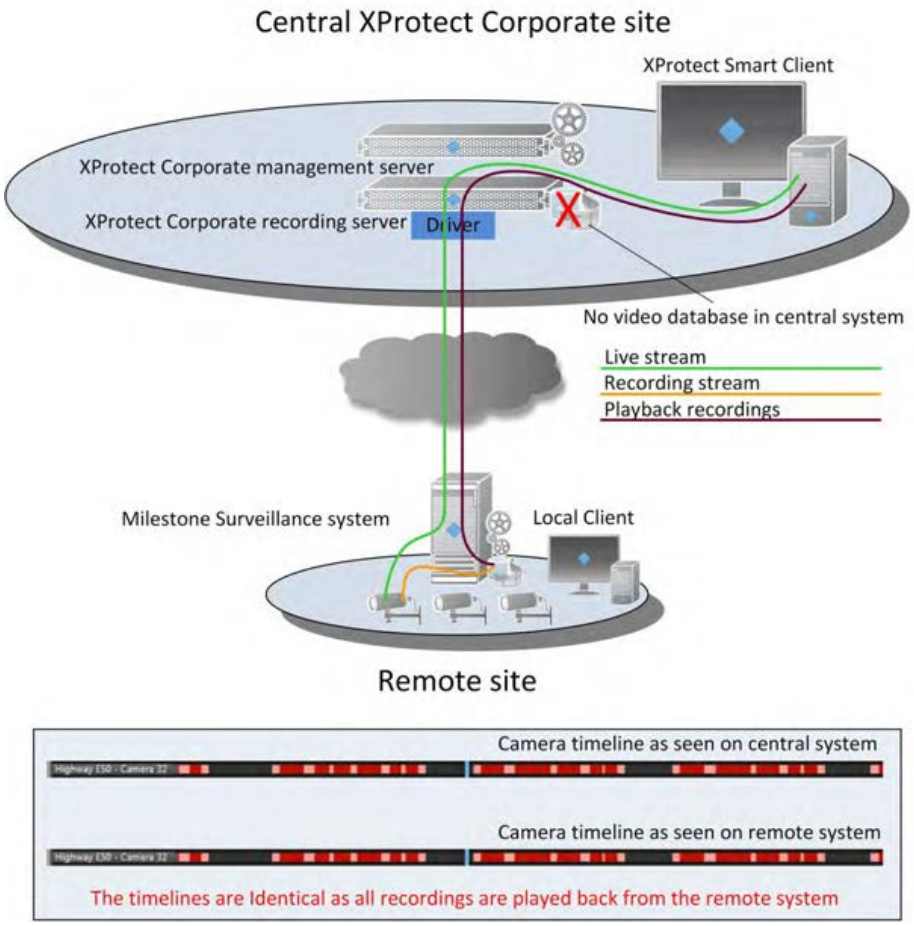
Interconnected cameras are displayed live in the views in the exact same way as regular cameras and have the same functions on the camera toolbar as regular cameras such as: bookmarks, print, snapshots, etc.

Screenshot of an interconnected camera in the XProtect Smart Client's live mode showing the camera toolbar and its functions

Play back remote recordings

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

When interconnected cameras are configured to be played back directly from the remote system the recordings are retrieved directly from the remote system's database as describe on the below drawing.



With this configuration, the timeline for the central site operator will be the same as for an operator on the remote system. Furthermore, there is not a recording database for the camera in the central site therefore remote recordings can only be played back from the remote site and not retrieved and stored in the central site.

Play back of the remote recordings will override any set remote recording retrieval bandwidth limits or time restrictions. If these limitations should apply it requires the interconnected camera to be configured to be played back from the central system's database. The limitations will then apply to scheduled, event or manual retrieval of remote recordings.

Note: Direct play back of remote recordings requires the remote system to be online. If the remote system is offline the client will report an error for the cameras.

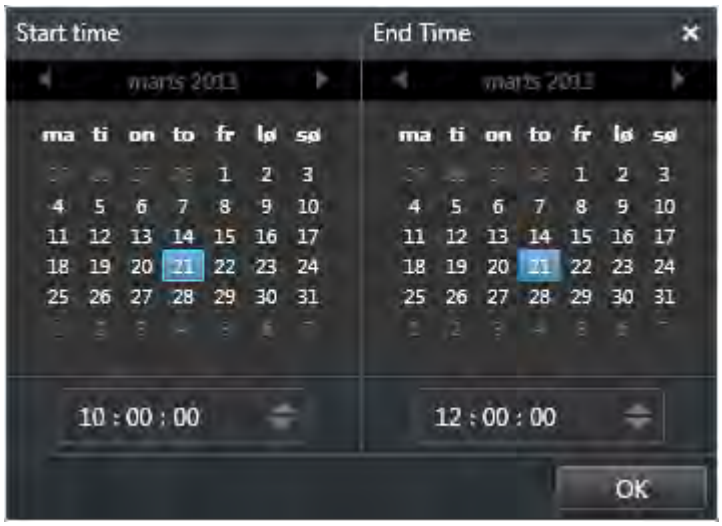
Play back recordings from central site and retrieval of remote recordings

When interconnected cameras are configured to record and play back recordings in the central XProtect Corporate system, the camera will appear in the XProtect Smart Client 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 offer a function to retrieve the remote recordings. This is visualized by the normally black space between recordings now displaying a grey pattern instead, indicating there might be recordings on the remote system that can be retrieved by the XProtect Smart Client operator.

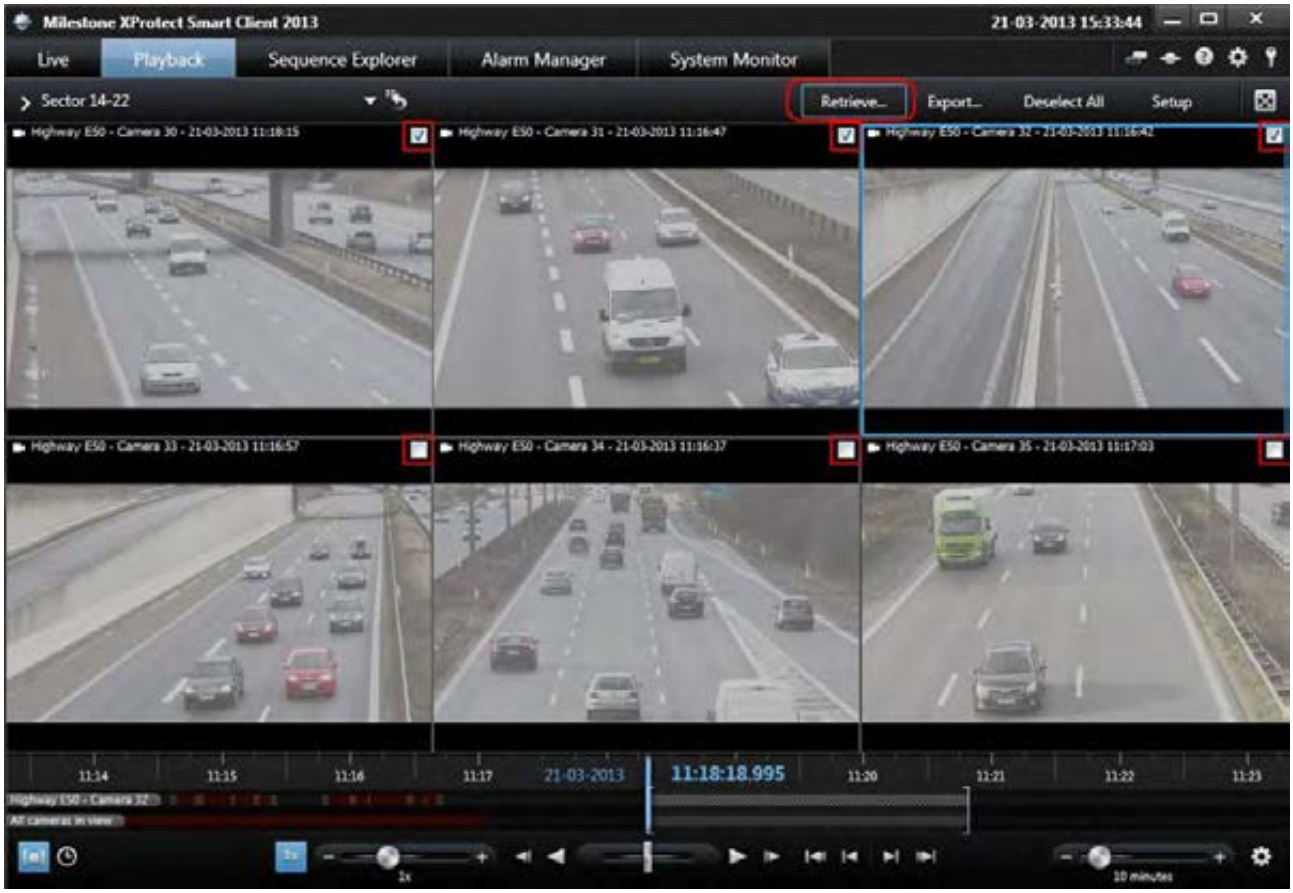
For these interconnected cameras where the operator has "Retrieve remote recordings" user rights, the remote recordings can be retrived much like when selecting video to export.

Either - Select the desired timespan graphically on the timeline

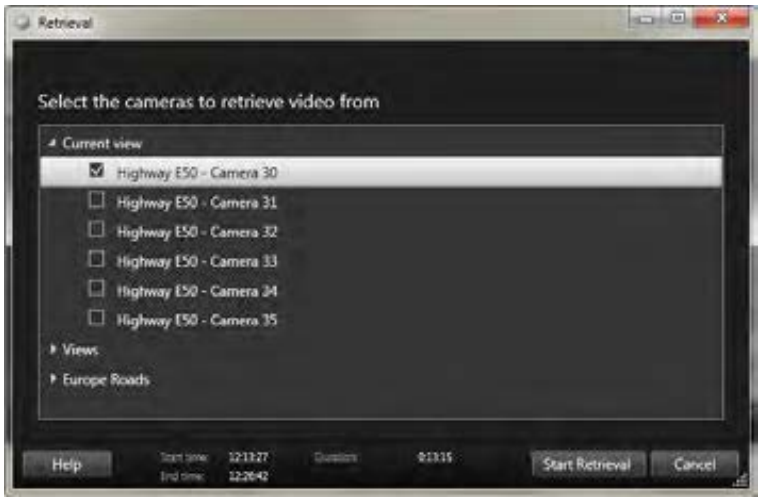
Or by entering directly the desired timespan by clicking the button and setting the start/end time



Once the time span has been set, the cameras from which the recordings will be retrieved can be selected by clicking on the checkboxes displayed for each camera (the current camera is checked by default).



Once the timespan and cameras have been selected the retrieval job can be created by clicking the “Retrieve…” button which will open the “Retrieval” dialog where additional cameras than the ones in the view can be selected.



Clicking the “Start Retrieval” button will create a retrieval job.

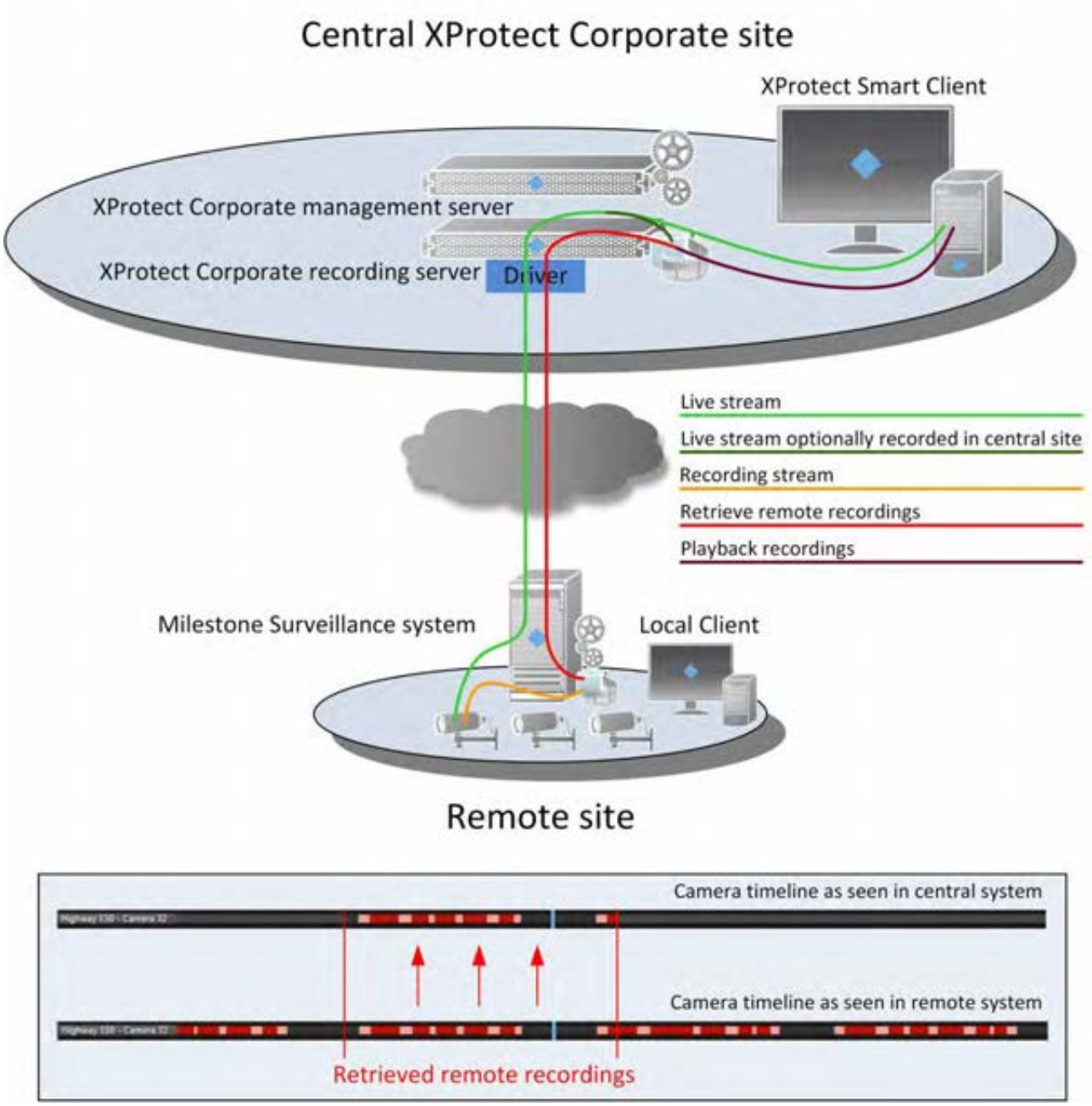
Once a remote recording retrieval job has been created it will be indicated on the timeline by a lighter grey pattern as shown below.

Sequence requested:

Sequence retrieved:

As shown above, 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 system by showing these segments with the standard black unpatterned background.

The drawing below shows the central and remote system streams as well as the remote recordings retrieval connection for interconnected cameras that are set up to be recorded and played back in the central XProtect Corporate site. As it is shown, it is a more complex flow than the direct remote site play back set up, since there are recording databases in both the central and remote systems and because there is support for retrieving recordings from the remote site.

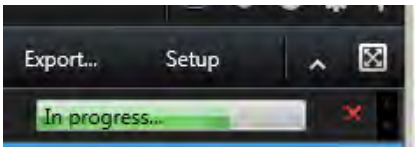


With this configuration, the timeline for the central site operator will not be the same as for an operator on the remote system. This is due to the fact that each system records by its own rules and because recordings can be retrieved from the remote system.

If “Remote Retrieval” limitations have been set for the remote system in the 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 highs possible speed.

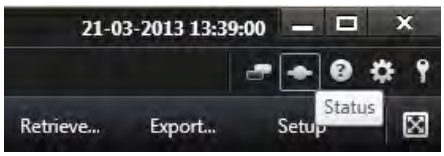
Retrieval Jobs

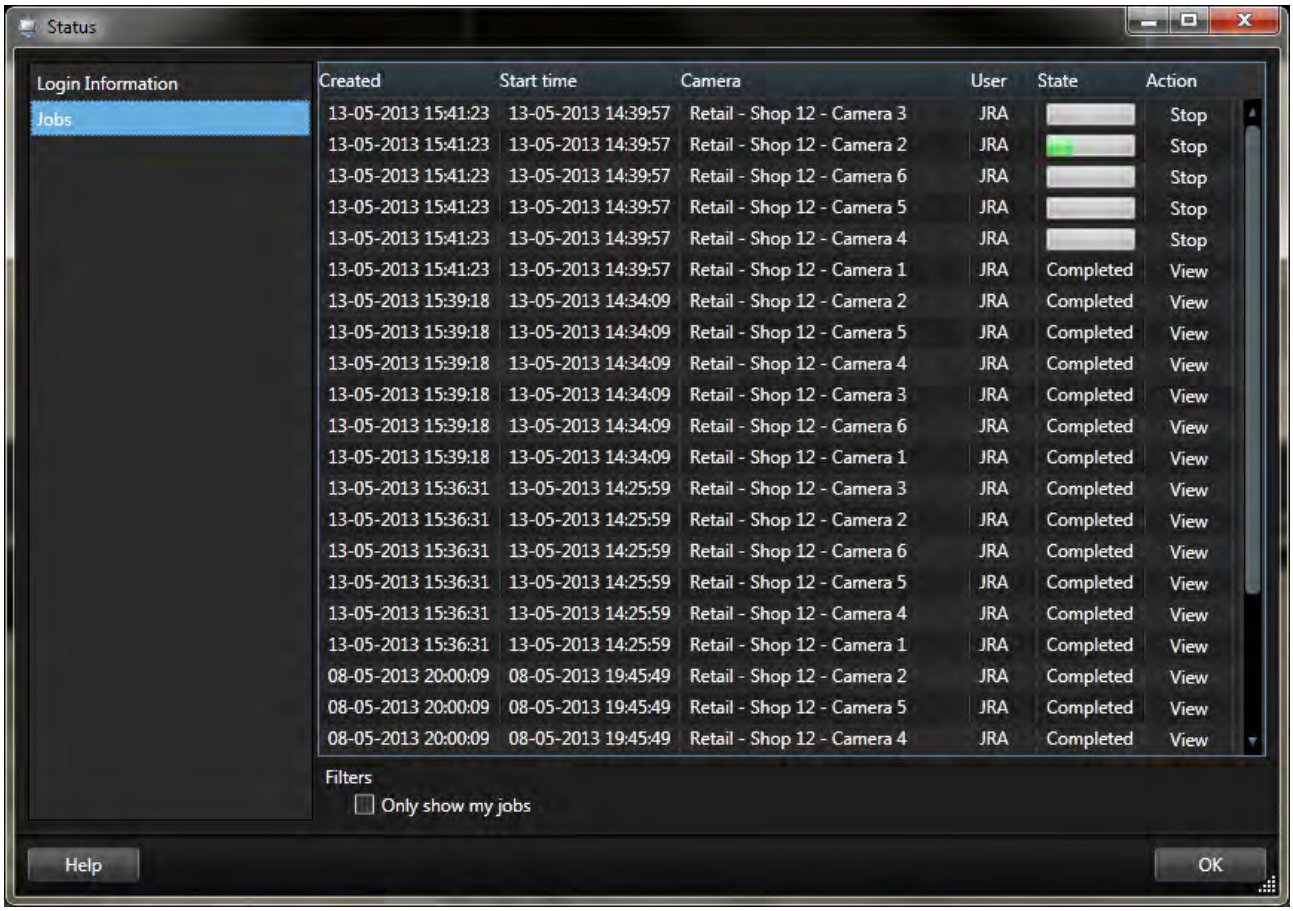
When a retrieval job is created, it will display its progress in the top of the XProtect Smart Client in the same way as export jobs are.



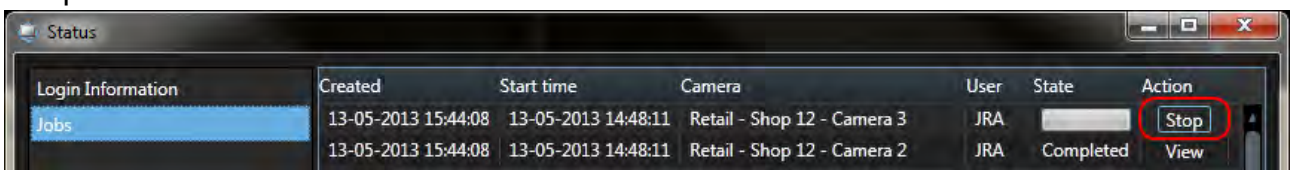
All shown jobs can be hidden by clicking on the button or for the individual jobs the button.

For a complete overview of all jobs, pending, in progress, stopped or completed, the "Jobs" overview can be used. It is 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 system's video database.

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

Once clicked a floating playback window will be displayed showing the camera at the start of the retrieved time period allowing the operator to easily play back the recordings or exporting them.

Milestone Interconnect in comparison to Edge Storage

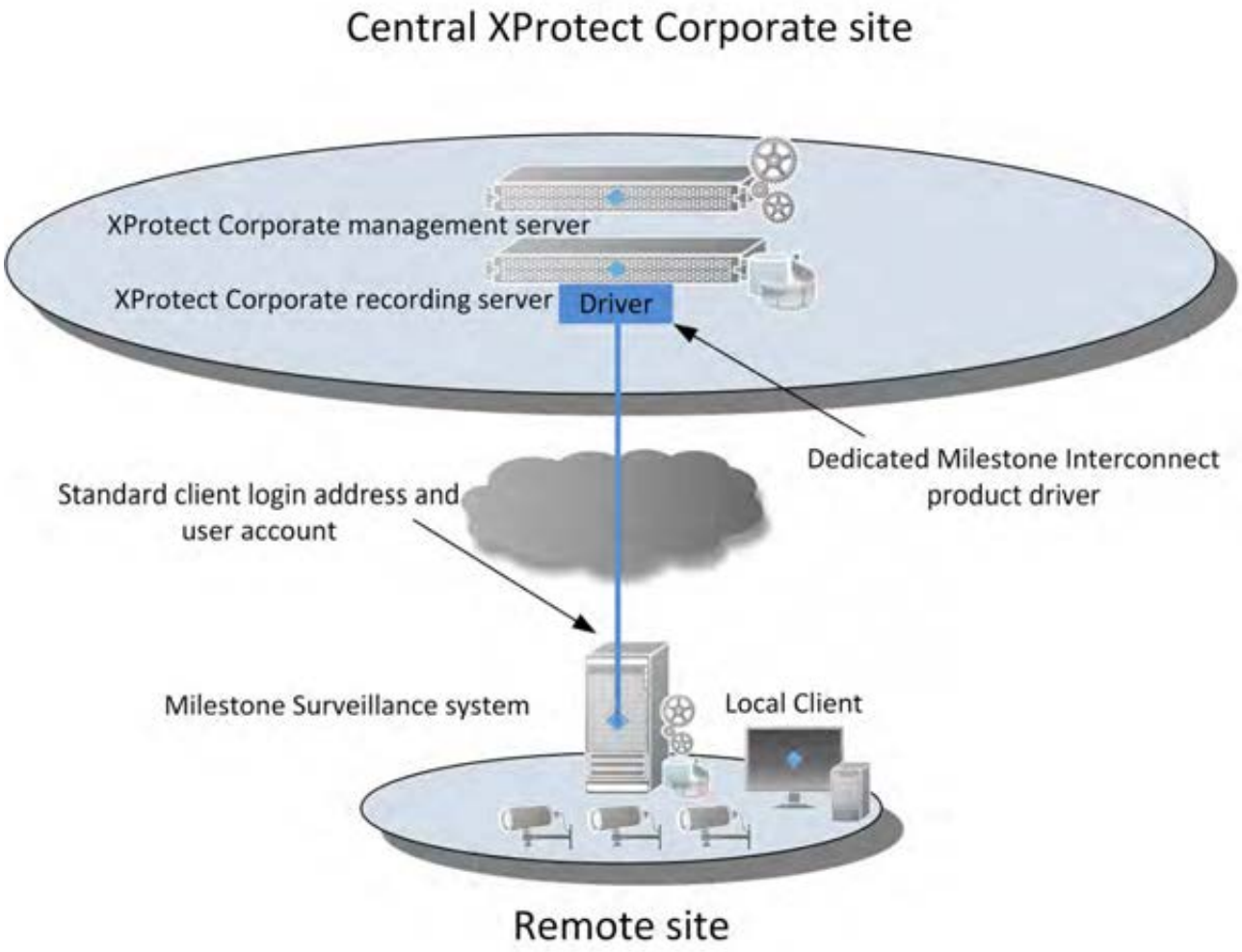
Cameras with Edge Storage have built-in storage or storage directly associated with the cameras which it is where the camera records its video. When a Milestone surveillance system is interconnected, the complete remote surveillance system including cameras and video databases can be seen as a kind of “multi-channel video encoder” with Edge Storage support from the central XProtect Corporate system.

Since Milestone Interconnect is implemented in the same principal way as Edge Storage on cameras, it offers the same basic functions and benefits as Edge Storage. However, it also adds more advanced functions like direct play back from the remote system, system events, status monitoring and alarms.

Milestone Interconnect in comparison to Milestone Federated Architecture

Milestone Interconnect and Milestone Federated Architecture may be seen as two different solutions with the same functionality. Even though they offer the same basic functionality of building a large centralized system constituted by multiple systems, they actually complement each other in different ways and they each have their 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 cameras to appear as a kind of Edge Storage camera connected to the central XProtect Corporate system, offering user of the Smart Client the functionality to play back or retrieve recordings from the remote systems.

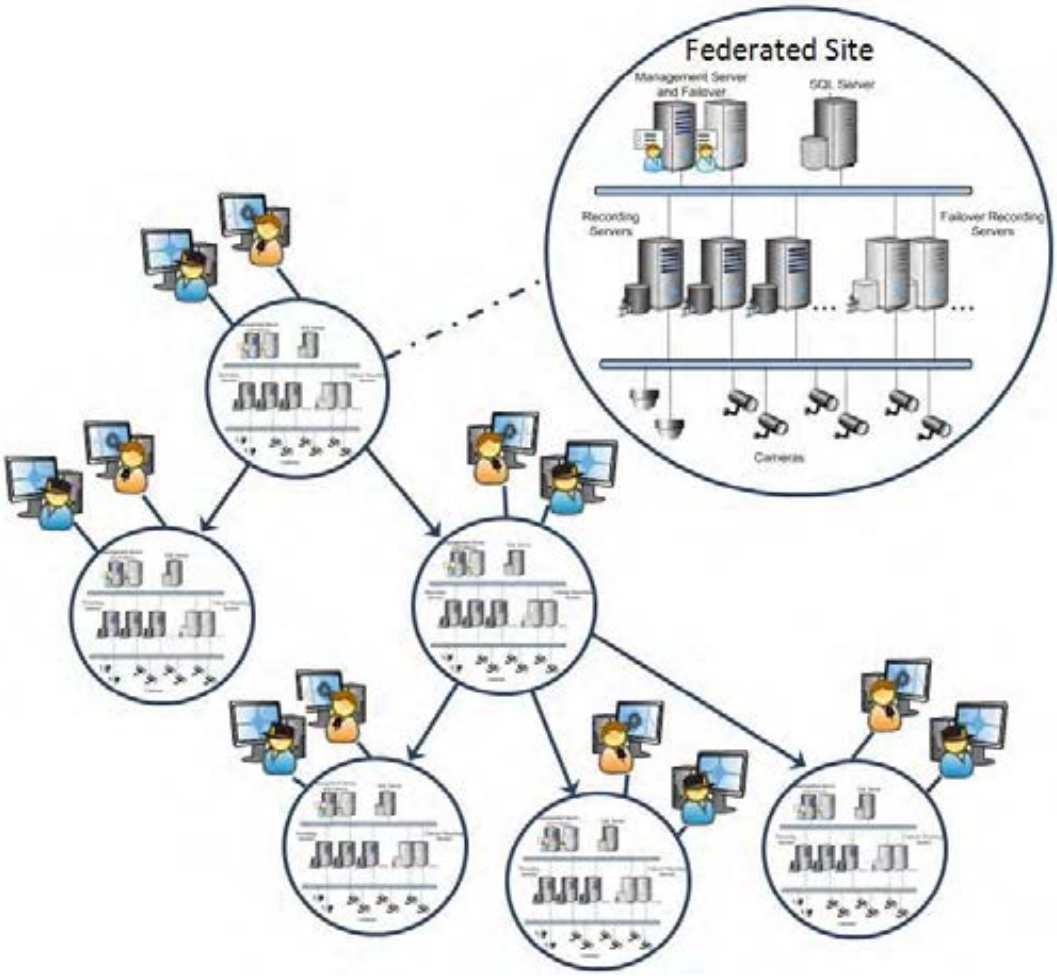


Milestone Interconnect has the benefit of having the recording server handling the connection and authentication on the interconnected systems so clients do not have to connect and authenticate on multiple systems when they login. Additionally it is also possible to set up connections to remote sites running on other domains than the central XProtect Corporate site or remote systems that are not permanently online. Moreover, and most importantly it offers the functionality to transfer recordings from a remote system to the central XProtect Corporate system or play back the recordings from the remote systems directly.

Milestone Federated Architecture allows multiple individual XProtect Corporate systems 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 system, complete with management server, SQL server, recording server(s), failover server(s), and a

number of cameras. When the individual systems are added to a federated hierarchy, they appear as one complete system to administrators and users, while still being as manageable as independent XProtect Corporate or XProtect Expert systems.

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 so clients logging in know there are more sites in this hierarchy that they should connect to and authenticate on.



This means that even though the system from the operator's point of view in the clients appears as one large system, the clients actually authenticate and retrieve the configuration from each system 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 to the not responding sites must timeout before login is completed. Furthermore, once logged in the client will not be able to automatically establish a connection to the not responding sites as they only are contacted during login. The operator in the client will therefore manually have to log out and retry login to get access to the sites previously was not responding.

For more information on Milestone Federated Architecture:
http://www.milestonesys.com/SharePoint/XProtectCorporate/4_0%20and%204_1/Whitepapers/Milestone_Federated_Architecture_w_synapsis.pdf

System implementation considerations

In the scenarios where recordings are played back directly from the remote site or transferred to the central XProtect Corporate system, there are a number of things that should be considered for optimal performance and user experience.

Transfer recordings from remote sites with a permanent network connection
(For example the retail scenario on page 7)

The challenges with this configuration are to:

- Limit the bandwidth use from the interconnected system when nobody views the cameras
- Limit the CPU load on the central systems recording server
- Ensure there is enough time and bandwidth to transfer 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 system. If this is not done, the XProtect Corporate system will connect to the interconnected system and continuously retrieve a live video stream, using bandwidth for no reason
- If users in the central XProtect Corporate system need to view live video from the interconnected cameras a rule can be created that starts the live video feed when a user in a client requests live video
- Disable the built-in motion detection in the central XProtect Corporate system to reduce CPU load
- Disable recording to minimize disk load, it is still possible to retrieve recordings
- Ensure the retrieval bandwidth limit and retrieval time period settings on the interconnected system are configured with enough bandwidth and a long enough time period to allow the remote recordings to be transferred in a proper time frame.

Otherwise, the system will build up a longer and 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 period for transferring 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 transfer time window at 6.00 am – allowing 2 hours for completing ongoing jobs)
- Recording retention on the interconnected cameras in the central XProtect Corporate system must be set long enough to allow further play back or investigation If users are concerned about disk usage or if there is a wish to keep the transferred recordings as long as possible, the recording storage container can be set to 365 days (or more) and a set size limit – e.g. 200 GB. In this way the system will automatically delete the oldest recordings once 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 system.

As recordings from the remote site are transferred one camera at a time (per interconnected site) the disk system can also be any standard disk system consisting of single disks or a disk array configured with any type of RAID configuration.

Transfer recordings from remote sites without a permanent network connection
(For example the transportation scenario on page 7)

The challenge with this configuration is to:

- Limit the bandwidth use from the interconnected system
- Limit the CPU load on the central system recording server
- Ensure that there is enough time and bandwidth to transfer the recordings in a timely fashion
- Ensure the recordings on the interconnected system are not deleted before there has been enough time to transfer them to the central XProtect Corporate system.

In order to address these concerns the following is recommended:

- Disable the live-feed rule for the interconnected cameras in the central XProtect Corporate system. If this is not done, the XProtect Corporate system will connect to the interconnected system as soon as there is a network connection and retrieving a live video stream from the remote site, using bandwidth unnecessarily

- Disable the built-in motion detection in the central XProtect Corporate system to reduce CPU load
- Recording retention on the interconnected cameras in the central XProtect Corporate system must be set long enough to allow for play back or investigation to be done. If there are concerns about disk usage or if there is a wish to keep the transferred recordings as long as possible the recording storage container can be set to 365 days (or more) and a set size limit – e.g. 200 GB. In this way the system will automatically delete the oldest recordings once the 200 GB limit is reached
- Recording retention and disk space on the remote interconnected system must be large enough to allow the recordings to be requested and transferred to the central XProtect Corporate system before they are delete from the remote system. For example, if the remote system only can store the recordings for one day there is a risk that they are deleted before they have a change to be transferred to the central XProtect Corporate system
- There should be calculated and allocated enough time and bandwidth on the network hotspots to allow the requested recordings to be transferred from the different vehicles to the central XProtect Corporate system. If there is not enough time and bandwidth to transfer the recordings from the remote site, the retrieval jobs will simply queue up and the system will ultimately delete the recordings before they get a change to be transferred

Following the above recommendation the recording server requirements can be kept low requiring only enough CPU and network bandwidth to retrieve recordings from the interconnected system.

As the recordings from the remote site are transferred one camera at a time (per interconnected site) the disk system can also be any standard disk system consisting of single disks or a disk array configured with any type of RAID configuration.

Play back recordings directly from interconnected remote sites
(For example the city surveillance scenarios on page 12)

The challenge with this configuration is to:

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

In order to address these concerns the following is recommended:

- Disable the built-in motion detection in the central XProtect Corporate system to reduce CPU load

- Ensure there is enough downstream bandwidth available in the central XProtect Corporate site for live viewing and playing back the required amount of remote interconnected cameras
- Ensure there is enough upstream bandwidth available on the interconnected site for live viewing and playing back the required amount of interconnected cameras from this site
- Consider connecting to remote sites via multiple XProtect Corporate recording servers to distribute the network and CPU load
- As the remote interconnected cameras are recorded on and played back directly from the remote system 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 there will not be anything recorded on it

Following the above recommendations, the recording server requirements can be kept to a bare minimum requiring only enough CPU and network bandwidth to act as a gateway for live viewing and play back recordings from the interconnected system.

As the central XProtect Corporate system does not record at all there are no disk requirements other than a disk for the Windows OS.

Recording interconnected cameras in the central XProtect Corporate system

If the system is configured to record all interconnected cameras in the central XProtect Corporate system, the same recording server requirements and configuration guidelines apply as for recording standard cameras.

Supported products

Milestone XProtect Corporate 2013 supports the following products in the initial release:

- XProtect® Enterprise 8, or later
- XProtect® Professional 8, or later
- XProtect® Express 1, or later
- XProtect® NVR 1, or later
- XProtect® Essential 2, or later

Later releases or service packs may add support for additional products.

The current list of supported products, versions and product features can be seen here: http://get.milestonesys.com/?id=38

Licensing

XProtect Corporate requires a dedicated Milestone Interconnect device license per interconnected and enabled camera similar to the regular device license per connected and enabled camera or video encoder.

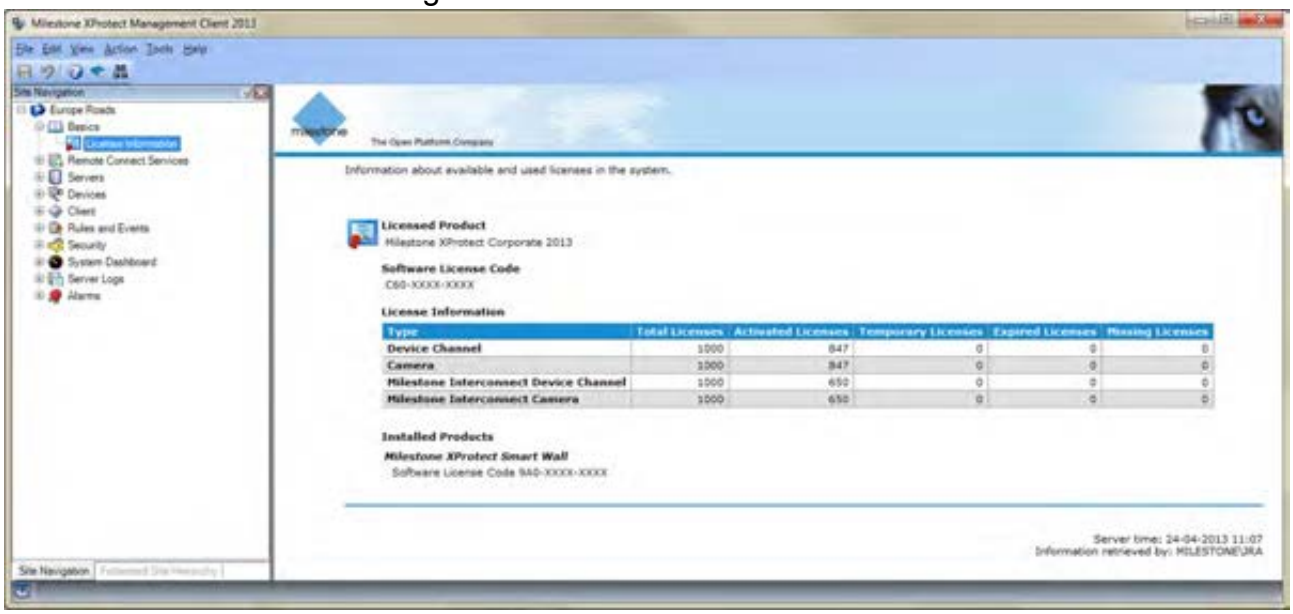
The Milestone Interconnect camera licenses are purchased the same way as regular camera licenses and are included in the standard license file used for the XProtect Corporate system.

Interconnected remote systems do not require additional licenses. Milestone Interconnect support is included in the standard license, this also includes products purchased before Milestone Interconnect was introduced.

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

As for regular cameras, only enabled Milestone Interconnect cameras will use a camera license, which means the system does not necessarily need licenses for all cameras present on the interconnected remote systems. It only requires license for the cameras that are enabled in the central XProtect Corporate site.

License overview in the Management Client



Benefits and summary

Milestone Interconnect is a unique system concept that allows most Milestone video management software (VMS) to be interconnected with Milestone's premium software XProtect Corporate. It provides the possibility to deploy central surveillance across geographically dispersed sites in a flexible way, by combining cost-efficient remote Milestone VMS solutions with the advanced surveillance functions of XProtect Corporate in one cohesive and powerful security solution.

Milestone Interconnect complements the Milestone Federated Architecture concept and both concepts are modeled to excel in their respective application 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 most Milestone video management software (VMS)**
  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**
  Made possible with the easy to install XProtect VMS products and the ability to clone and reuse standard system configurations across multiple sites. Furthermore, Milestone Interconnect does not require common or trusted domains between the central system and its remote sites
- **Intelligent video storage management**
  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 allowed bandwidth usage and by scheduling the retrieval to preserve bandwidth for critical business systems
- **Remote management of interconnected systems**
  Reduces the need for costly onsite visits by technicians and service personnel
- **Proactive system monitoring**
  The central system receives notifications when there are issues in any of the connected systems. This way, system 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 system enabling cost-efficient 24/7 monitoring and centralized evidence management
- **Transportation** – where remote systems are installed onboard vehicles enabling continuous fleet monitoring, efficient evidence handling and seamlessly correlated surveillance with stationary surveillance installations at stations, writing 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 surveillance system

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

Milestone Systems Headquarters, DK

Tel: +45 88 300 300

Milestone Systems US

Tel: +1 503 350 1100