MAKE THE
WORLD SEE

Milestone Systems

XProtect® Smart Client 2023 R1

User manual

milestone

Contents

Copyright, trademarks, and disclaimer

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file 3rd_party_software_terms_and_conditions.txt located in your Milestone system installation folder.

Supported VMS products and versions

This manual describes features supported by the following XProtect VMS products:

- XProtect Corporate
- XProtect Expert
- XProtect Professional+
- XProtect Express+
- XProtect Essential+

Milestone tests the features described in this manual with the above-mentioned XProtect VMS products in the current release version and the two previous release versions.

If new features are only supported by the current release version and not any previous release versions, you can find information about this in the feature descriptions.

You can find the documentation for XProtect clients and add-ons supported by the retired XProtect VMS products mentioned below on the Milestone download page (https://www.milestonesys.com/downloads/).

- XProtect Enterprise
- XProtect Professional
- XProtect Express
- XProtect Essential

Overview

This documentation and eLearning courses

This user manual is mainly for XProtect Smart Client operators, but also for system administrators and integrators responsible for configuring, maintaining, and troubleshooting XProtect Smart Client. Most of the configuration, however, takes place in XProtect Management Client. For more information, see the administrator manual for XProtect VMS.

In this manual, references made to the positioning of user interface elements presume that you are using a visual left-to-right interface. See also Right-to-left languages (explained) on page 54.

If this manual does not provide the information you need, please contact Milestone Technical Support.

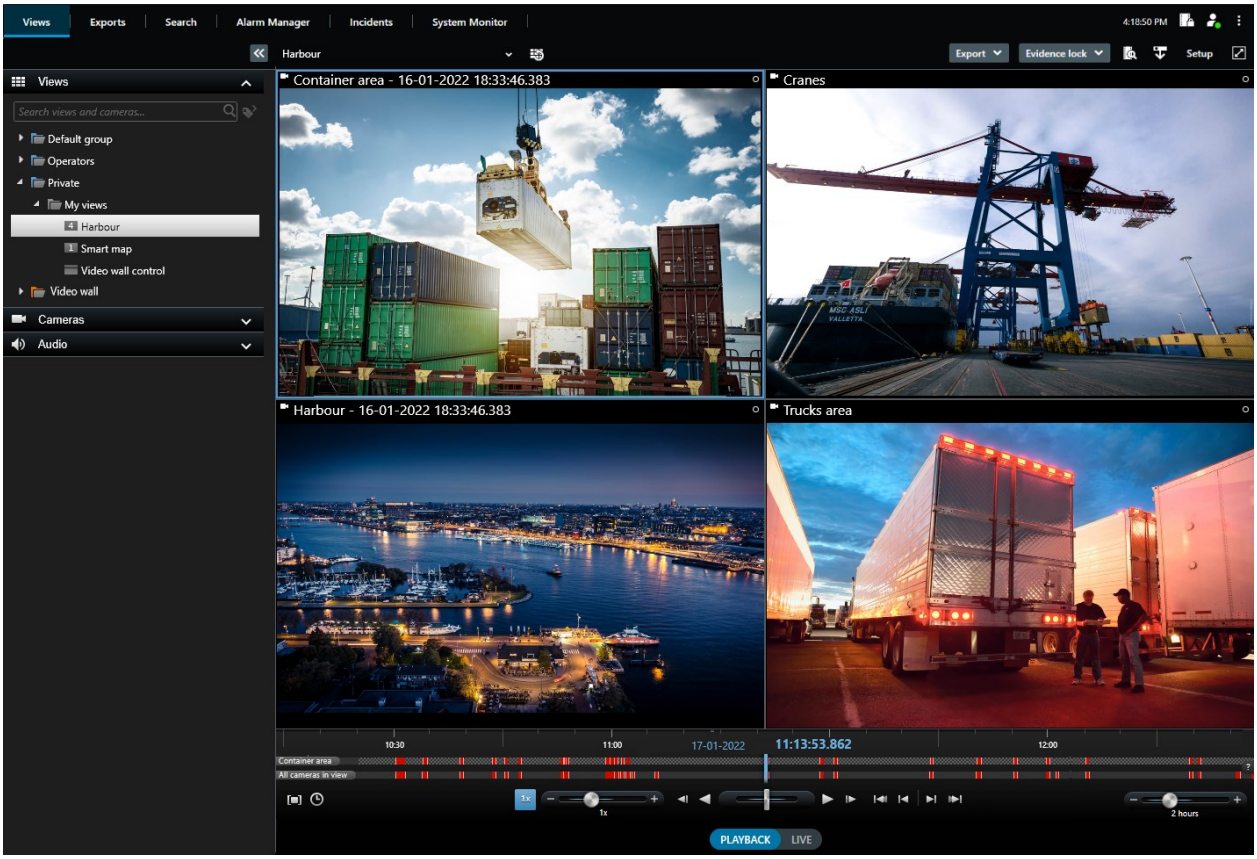
Milestone offers eLearning courses for all XProtect products. Visit the Milestone Learning Portal at https://go.bluevolt.com/Milestone/Home/.

To find the XProtect Smart Client courses, search for **smart client**.

XProtect Smart Client (explained)

XProtect Smart Client is a desktop application designed to help you manage and view video from the cameras that are connected to your XProtect VMS system. It gives you access to live and recorded video, instant control of cameras and connected security devices, and allows you to perform advanced searches to find video data and metadata - if any - that is stored on the server.

Available in multiple local languages, XProtect Smart Client has an adaptable user interface that can be optimized for individual operators' tasks and adjusted according to specific skills and authority levels.



Additional functionality

Depending on the XProtect add-ons installed on your XProtect VMS system, you can:

- combine video with integrated access control systems, including restricting or allowing access to buildings
- read license plate information from vehicles and view the live or recorded video that shows the vehicles
- view and investigate transactional data from PoS systems in combination with video from cameras that monitor the PoS systems

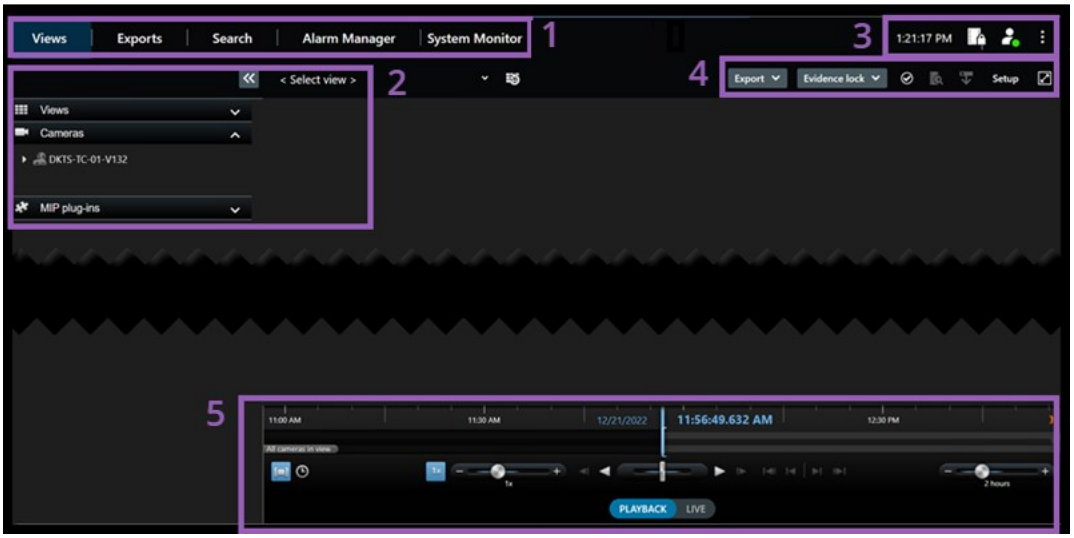
By using the MIP SDK, users can integrate various types of security and business systems, and video analytics applications, which you manage through XProtect Smart Client.

Getting started with XProtect Smart Client

User interface overview

From the XProtect Smart Client desktop app, you have access to workspaces and features such as:

1. Standard tabs like **Views**, **Exports**, **Search**, **Alarm Manager**, and **System Monitor**, located in the upper-left corner of the XProtect Smart Client. See Tabs on page 21
2. Standard panes for setting up views and cameras, located just below the standard tabs. See Viewing live video on page 164
3. Global toolbar with access to **Evidence lock list**, **User profile**, and **Settings and more**, located in the upper-right corner. See Global toolbar on page 305
4. Workspace toolbar with access to **Export**, **Evidence lock**, and **Setup**, located just below the global toolbar. See Buttons on page 24
5. **Playback/live** tabs with timeline, located at the bottom of the application. See Tabs on page 21



Tabs

XProtect Smart Client comes with a set of standard tabs allowing you to perform your daily surveillance tasks.

Some of the XProtect add-ons have tabs that are specific to the functionality of the add-ons. See Add-on products on page 28.

Finally, some tabs may be custom-made through the MIP SDK and specific to your XProtect VMS system. Functionality that depends on MIP SDK is not documented in the current manual.

Standard tabs

If you can't see some of the standard tabs, it is because you do not have the permissions required to access the tabs.

The Views tab for viewing video in live and playback mode

When in live mode, you can view live video feeds, and work with audio, carousels, hotspots, Matrix, smart map, pan-tilt-zoom (PTZ) control, digital zoom, independent playback, and more.

When in playback mode, you can investigate recorded video by playing it back, start search from any camera or view, and then document what you find by exporting evidence. To protect the evidence from being deleted from the database, you can also add evidence locks to recorded video.

In playback mode, the timeline gives you advanced features for browsing recorded video and jumping to a specific date and time.

You can also:

- Listen to audio when connected to selected Milestone surveillance systems
- If your XProtect VMS supports smart map, you can get access to the cameras in your system in a geographical interface, which is easy to navigate
- Use hotspots, digital zoom, or carousels, navigate fisheye lens images, print images, and more

When in live or playback mode you can enter into setup mode, where you can set up views for your cameras and other types of content.

The Exports tab for exporting video data

First, when you want to export video data, you add the sequences that you want to export to the **Export list**. Next, for each item on the **Export list**, you can change the time span by clicking the **Start time** and the **End time**. See also Export video, audio, and still images on page 179.

You can choose which formats to use for the export, and for each format, you can change the **Export settings**.

After you click the **Export** button, you specify an **Export name** and an **Export destination**. Then, you can create the export.

The exports that you create are stored in the folder that you specified in the **Create export** window > **Export destination** field.See also View exported video on page 184.

The Search tab for making advanced searches for video and metadata

On the **Search** tab, you can search across the different types of data available in your VMS system. This includes:

- Video recordings in general
- Recordings with motion
- Recordings with motion in selected areas
- Bookmarks
- People
- Vehicles
- Video recordings with alarms
- Video recordings with events

For each search category, you can apply filters to refine your search.

From the search results, multiple actions are available. For more information, see Actions available from search results (overview) on page 213.

The Alarm Manager tab for investigating and managing alarms

On the **Alarm Manager** tab, you can view and respond to incidents or technical problems that have triggered an alarm. The tab displays an alarm list, an alarm preview, and a smart map or map if one is available.

The System Monitor tab for viewing system information

On the **System Monitor** tab, you can get a visual overview of the current state of your system servers, cameras, other devices, and the computer running XProtect Smart Client.

By default, the tiles represent **Recording servers**, **All servers**, **Failover servers**, and **All cameras**. Your system administrator specifies the tiles and the threshold value for each state.

Here is a description of the colors used:

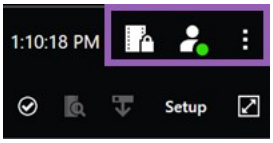
- Green: **Normal** state. Everything is running normally
- Yellow: **Warning** state. At least one monitoring parameter is above the defined value for the **Normal** state
- Red: **Critical** state. At least one monitoring parameter is above the defined value for the **Normal** and **Warning** state

If a tile changes color and you want to identify the server or parameter that caused the change, click the tile. This opens an overview in the bottom of the screen. Click the **Details** button for information about why the state changed.

> If a tile displays a warning sign, a data collector for one of your monitored servers or cameras may not be running. If you place your mouse above the tile, the system shows you when it last collected data for the relevant tile.

Global toolbar

From the Global toolbar, in the upper-right corner of the XProtect Smart Client, you have access to:



- Evidence lock list
  The **Evidence lock list** shows evidence locks with devices that you have permissions to access. You can sort, filter, and search the evidence locks list and see detailed information about the evidence locks. For more information, see View evidence locks on page 196.

- User menu
  From your **User menu**, you can see your **Login information**, and you can log out from the XProtect Smart Client. See Log out on page 150. **Login information** contains information about the status of the XProtect VMS servers that your XProtect Smart Client is connected to. This is useful if you are connected to an XProtect VMS system that is configured to use Milestone Federated Architecture. Milestone Federated Architecture enables organizations to connect related but physically separate XProtect VMS systems. For example, such a setup can be relevant for chains of shops.

  > A red circle on the **User menu**  indicates that one or more servers are unavailable.

  Select **Login information** to view the server status.

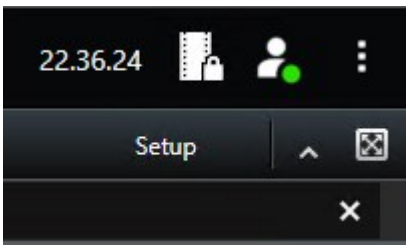
  - Available servers are displayed in green.
  - Unavailable servers are displayed in red.
    If servers are not available at the time you log in, you cannot use cameras or features belonging to those servers. When you have viewed the status, the red button will stop flashing even if the server is still unavailable.

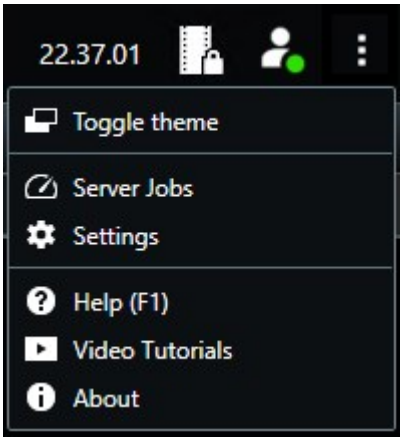
  The number of servers you see reflects the number of servers retrievable from the XProtect VMS system at the time you logged in. Particularly if you connect to large hierarchies of servers, occasionally, more servers may become available after you log in. The server list is a static representation of server status. If a server is unavailable, it will display a reason in the **Status** field when you click it. To connect to the server, click the **Load Server** button. The server status for that server will then be updated. If a server continues to be unavailable for longer periods of time, contact your system administrator for advice.

- Settings and more
  The **Settings and more** window covers **Toggle theme**, **Server jobs**, XProtect Smart Client **Settings**, **Help**, **Video tutorials**, and the **About** button. See also Buttons on page 24.

Buttons

XProtect Smart Client has multiple buttons that allow you to perform different actions. The buttons are located in the in the upper-right corner.





The buttons available vary depending on the tab you are standing on. For example, **Setup** is not available on all tabs.

Button	Description
Time zone	Set up time zone. See Timeline settings on page 42.
Evidence lock list	View evidence lock. See also View evidence locks on page 196.
User menu - Login information	The status of your XProtect VMS servers that your XProtect Smart Client is connected to through Milestone Federated Architecture. See also Check the status of your server connection on page 305.
Log out	Log out of XProtect Smart Client. See also Log out on page 150.
Toggle theme	Switch the XProtect Smart Client theme to dark or light.
Server jobs	Depending on your user permissions to retrieve data from interconnected hardware devices or cameras that support edge storage, you can view the server jobs created for each data retrieval request for these devices. See View all edge retrieval jobs on page 285.
Settings	Configure XProtect Smart Client settings and behavior, joysticks, keyboard shortcuts, language, and more. See also Settings in XProtect Smart Client on page 37.
Help	Access the help system, play online video tutorials, or view version number and plug-in

Button	Description
	information.
Video tutorials	Opens the Milestone Learning Portal.
About	Information about the latest XProtect Smart Client plug-ins and versions.
Setup	Enter setup mode. See also Setup mode (overview) on page 35.
Toggle full screen mode 	Toggle between full screen and a smaller window that you can adjust to the size you want.
Export	Export video evidence. See also Export video, audio, and still images on page 179.
Evidence lock	Create an evidence lock to prevent evidence from being deleted. See also Create evidence locks on page 193.
Retrieve	Retrieve recordings from interconnected hardware devices or cameras that support edge storage.
Lift privacy masks	Users with sufficient user permissions can temporarily lift privacy masks. See also Lift and apply privacy masks on page 247.

What's new?

In XProtect Smart Client 2023 R1

A new **Views** tab replaces the **Live** and **Playback** tabs:

- On the **Views** tab, you can select to view video in live or playback mode with a new toggle switch.
- When in playback mode, the same features and functionalities are available as they were on the **Playback** tab.
- When in live mode, the same features and functionalities are available as they were on the **Live** tab.

The buttons for respectively **Export**, **Evidence lock**, and **Media restrictions** have been moved from the lower-right corner of the XProtect Smart Client to the workspace toolbar in the upper-right corner.

XProtect Incident Manager:

- To comply with GDPR or other applicable laws concerning personal data, administrators of XProtect Management Client can now define a retention time for incident projects.

In XProtect Smart Client 2022 R3

XProtect Incident Manager:

- The XProtect Incident Manager add-on is now also compatible with XProtect Expert, XProtect Professional+, and XProtect Express+ version 2022 R3 or later.
- XProtect Incident Manager can now show more than 10,000 incident projects.

In XProtect Smart Client 2022 R2

XProtect Incident Manager:

- The first release of this add-on
- The XProtect Incident Manager add-on is compatible with XProtect Corporate version 2022 R2 and later and with XProtect Smart Client version 2022 R2 and later.

XProtect LPR:

- On the **LPR** tab, you can now see the license plate style associated with an **LPR** event. See License plate styles on page 293

Bookmarks:

- When you enter a keyword to filter your search results for bookmarks, you can now decide where the system should search for the keyword: in all bookmark fields, in the **Headline** only, or in the **Description** only. See Search for bookmarks on page 208

In XProtect Smart Client 2022 R1

Export:

- Everything related to exporting video data now lives on a dedicated tab called **Exports**. See also The Exports tab for exporting video data on page 22.

In XProtect Smart Client 2021 R2

Export:

- To increase security, the XProtect format is the default export format. To enable other export formats, please contact your system administrator

New camera icons:

- New camera icons allow you to distinguish between fixed cameras and PTZ cameras

Vertical scrolling of views and cameras:

- Use **Shift** in combination with the scroll-wheel to move the navigation area to the left or right

Removed features:

- Camera navigator
- Simplified mode. This feature has also been removed in XProtect Smart Client – Player which is used to view video exports

In XProtect Smart Client 2021 R1

Searching:

- Sort your search results by **Relevance**. See also Sorting options on page 219
- Administrators can control the number of cameras that are allowed in one search

Smart map:

- Use Milestone Map Service as the geographic background of your smart map. After you enable Milestone Map Service, there is no further setup you need to do. See Enable Milestone Map Service
- Get an overview of grouped devices. When you are zoomed out, click a cluster to see the types and number of devices within a specific area. See also Get overview of grouped devices on page 265
- Add different types of devices to your smart map. In addition to cameras, you can also use input devices, microphones, and elements added through the MIP SDK. See also Adding, deleting, or editing devices on smart map on page 95
- Improved zoom capability. Double-click a cluster to zoom in on grouped devices. See also Zoom in and out on page 265

Security:

- Basic users can change their password, either on their own initiative or if an administrator enforces the need for change. See also Change password in XProtect Smart Client on page 150

Add-on products

Milestone has developed add-on products that fully integrate with XProtect to give you extra functionality. Your XProtect license file controls the access to add-on products.

Available functionality depends on the system you are using. See the complete feature list, which is available on the product overview page on the Milestone website (https://www.milestonesys.com/solutions/platform/product-index/).

XProtect Smart Wall (explained)

See also the Smart Wall manual (https://doc.milestonesys.com/2023r1/en-US/portal/htm/chapter-page-smart-wall.htm).

XProtect Smart Wall is an advanced add-on tool that enables organizations to create video walls that meet their specific security demands. XProtect Smart Wall provides an overview of all the video data in the XProtect VMS system and supports any amount or combination of monitors.

XProtect Smart Wall allows operators to view static video walls as defined by their system administrator with a fixed set of cameras and monitor layout. However, the video wall is also operator-driven in the sense that operators can control what is being displayed. This includes:

- Pushing cameras and other types of content to the video wall, for example images, text, alarms, and smart map
- Sending entire views to the monitors
- In the course of certain events, applying alternate presets

Finally, display changes can be controlled by rules that automatically change the presets based on specific events or time schedules.

XProtect Incident Manager (explained)

XProtect Incident Manager is a Milestone add-on that enables organizations to document incidents and combine them with sequence evidence (video and, potentially, audio) from the XProtect VMS.

Users of XProtect Incident Manager can save all the incident information in incident projects. From the incident projects, they can track the status and activities of each incident. In this way, the users can manage incidents effectively and easily share strong incident evidence, both internally with colleagues and externally with authorities.

XProtect Incident Manager helps organizations gain an overview and understanding of the incidents happening in the areas they survey. This knowledge enables the organizations to implement steps to minimize the chance that similar incidents happen in the future.

In XProtect Management Client, the administrators of an organization's XProtect VMS can define the available incident properties in XProtect Incident Manager to the organizations' needs. The operators of XProtect Smart Client start, save, and manage incident projects and add various information to the incident projects. This includes free text, incident properties that the administrators have defined, and sequences from the XProtect VMS. For full traceability, the XProtect VMS logs when administrators define and edit incident properties and when operators create and update the incident projects.

The XProtect Incident Manager add-on is compatible with:

- XProtect Corporate version 2022 R2 and later
- XProtect Expert, XProtect Professional+, and XProtect Express+ version 2022 R3 or later
- XProtect Smart Client version 2022 R2 and later

See also the user manual for XProtect Incident Manager.

XProtect Access (explained)

You can use XProtect Access with access control systems from vendors where a vendor-specific plug-in for XProtect Access exists.

XProtect Access integrates events from one or more access control systems with the features of the XProtect video management software. The incidents from an access control system generates events in the XProtect system.

- In live mode, you can monitor access control events in real time from the cameras associated with a door. In setup mode, you can customize your **Access monitor** view items with overlay buttons. In a map view item you can drag access control units onto the map
- On the **Access control** tab, you can view and investigate events, door states, or cardholders. You can search or filter on events and review any related footage. You can create a report of the events for exporting
- When a person requests access and if your system is configured for it, a separate notification pops up with a list of related information next to the camera feed. You can trigger access control commands, such as locking and unlocking of doors. Available commands depend on your system configuration

XProtect LPR (explained)

On the **LPR** tab, you can investigate LPR events from all your LPR cameras and view the associated video recordings and license plate recognition data. Keep match lists updated and create reports.

The tab includes an LPR event list and an LPR camera preview. In the preview, you can view video associated with LPR event details. Below the preview, information about the license plate appears together with details from the match list and the license plate style that it is associated with.

You can filter the event list according to the period, country module, LPR camera, match list, or license plate style. Use the **Search registration number** field to search for a particular license plate registration number. By default, this list shows LPR events from the last hour. See also LPR event list (explained) on page 292.

You can specify and export a report of relevant events as PDF.

You can make updates to the existing match lists by using the **Match list** function.

XProtect Transact (explained)

XProtect Transact is an add-on to Milestone's IP video surveillance solutions that lets you observe ongoing transactions and investigating transactions in the past. The transactions are linked with the digital surveillance video monitoring the transactions, for example to help you prove fraud or provide evidence against a perpetrator. There is a 1-to-1 relationship between the transaction lines and video images.

The transaction data may originate from different types of transaction sources, typically point of sales (PoS) systems or automated teller machines (ATM). When selecting a transaction line, a video still frame from each of the associated cameras is displayed in a preview area that allows you to review the recordings. Below the preview area, the transaction associated with the selected line is displayed as a receipt.

Licensing

XProtect Smart Client licensing

No license is required for installing and using XProtect Smart Client. Registering and activating licenses is done by your system administrator during installation of the XProtect® VMS system.

Licenses for your add-ons

The XProtect add-ons require additional licenses that must be activated in XProtect Management Client. Most often, this is a task for your system administrator.

Requirements and considerations

Minimum system requirements

For information about the system requirements for the various VMS applications and system components, go to the Milestone website (https://www.milestonesys.com/systemrequirements/).

View information about your system

To view information about your system, for example the operating system and version of DirectX, and the devices and drivers installed:

1. Open the **Start** menu and type **dxdiag**.
2. Click the **dxdiag** text to open the **DirectX Diagnostic Tool** window.

3. On the **System** tab, view the system information.

Surveillance system differences

Most of the features are available in all versions of the XProtect VMS products, but there are exceptions depending on what product you are using.

For more information, see the product comparison chart:
https://www.milestonesys.com/solutions/platform/product-index/

Installation

Install XProtect Smart Client

You must install XProtect Smart Client on your computer before you can use it. You download XProtect Smart Client from the surveillance system server and install it on your computer.

Milestone recommends that you always use the latest version of the XProtect Smart Client to ensure that you have access to all the new features and functions included in your XProtect surveillance system.

1. Open your browser and connect to the management server using the URL or IP address of the server.
2. Enter one of the following:
    - Local server (*http://localhost/installation*)
    - IP address of the remote server (*http://[IP_address]/installation*)
3. On the **Welcome** page, click **Language** and select the language you want to use. The **XProtect Smart Client setup** wizard starts.
4. In the wizard, follow the installation instructions. The wizard suggests an installation path. Normally, you can use the suggested installation path. However, if you have previously used add-on products, this path might not be valid anymore.

Configuration

User permissions (explained)

Your user permissions are specified centrally by your system administrator and these determine your ability to use particular XProtect Smart Client features.

Basically, your system administrator can restrict your user permissions to:

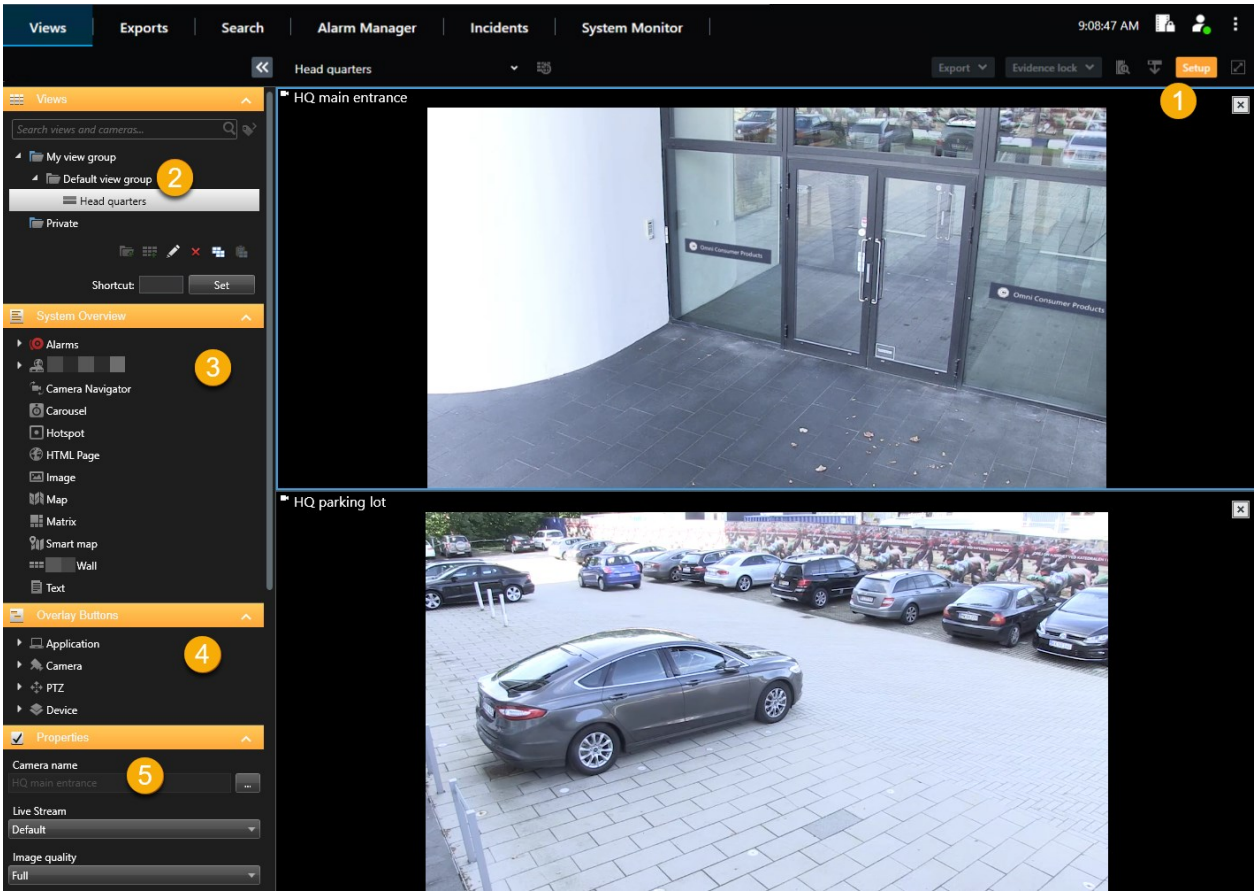
- Access XProtect Smart Client
- Access each of the tabs: **Views**, **Alarm Manager**, and **Search**
- Setup mode
- Use specific features
- Create views that typically contain video from one or more cameras
- View video from specific cameras

The ability to use features of XProtect Smart Client can vary considerably from user to user.

User permissions may even vary depending on the time of day, day of the week, and so on. For example, you may be able to view video from a particular camera during certain hours Monday-Friday, but not outside these hours.

Setup mode (overview)

In setup mode, you can create views for your devices and other types of content, you can add overlay buttons, and set the properties for the cameras and other types of devices.

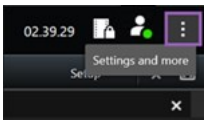


Number	Name	Description
1	**Setup**	When you enter setup mode, parts of the user interface are highlighted.
2	**Views**	Create views and groups for your views. See also Create view groups on page 57 or Create views on page 58.
3	**System overview**	Add cameras and other types of devices and content to your views. See also Add cameras and other elements to views on page 59.
4	**Overlay buttons**	Add overlay buttons to cameras to trigger auxiliary commands. See also Overlay buttons (explained) on page 73.
5	**Properties**	Set the camera properties. See also Camera settings on page 66.

Settings in XProtect Smart Client

The **Settings** window lets you control which features and elements, for example, language selection, joystick setup and keyboard shortcut setup, you want to use on each of the tabs.

Open the **Settings and more** window on the global toolbar and select **Settings**:



Application settings

Application settings let you customize the general behavior and look of your XProtect Smart Client.

If available, the **Follow server** column lets you specify that you want your XProtect Smart Client to follow the recommended settings of the server. Certain settings are server-controlled, in which case, configuration on the server decides whether you can override the settings.

Name	Description
Application maximization	Specify how windows in XProtect Smart Client react when you click the **Maximize** button.  To avoid that the Windows taskbar is covered when you maximize a window, select **Maximize as normal window**.
Camera error messages	Specify how the XProtect Smart Client displays camera-related error messages. These can be displayed as an overlay on top of the camera image or on a black background, or hidden completely. If you **Hide** the camera error messages, there is a risk that the operator overlooks that the connection to a camera has been lost.

Name	Description
Server error messages	Specify how the XProtect Smart Client displays server-related message texts. These can be displayed as an overlay on top of the camera image or on a black background, or hidden completely.
Live video stopped message	Specify if the XProtect Smart Client displays a message when a camera is connected but the camera is not sending live video feed. The message can be displayed as an overlay on top of the camera image or on a black background, or hidden completely.
Default for camera title bar	Select whether to show or hide the camera title bar. The title bar displays the name of the camera and the colored indicators signifying events, detected motion, and video recordings.  You can override this setting on individual cameras by adjusting camera properties for the camera(s) in setup mode.
Show current time in title bar	Specify whether to show or hide the current time and date (of the computer running the XProtect Smart Client) in the title bar.
Show in empty view positions	Specify what to show if there are empty view items in views, for example, you can select a logo or have just a black background displayed.
View grid spacer	Specify the thickness of the border between view items in views.
Default image quality	 Specifying a default quality of video viewed in XProtect Smart Client is only relevant if you are viewing JPEG streams. If you are viewing other codecs like H264 and H265 and reduce the quality, you will increase the bandwith, CPU, and GPU usage when re-coding to JPEG. Note that image quality also affects bandwidth usage. If your XProtect Smart Client is used over the internet, over a slow network connection, or if for other reasons you need to limit bandwidth use, image quality can be reduced on the server by selecting **Low** or **Medium**.

Name	Description
	 You can override this setting on individual cameras by adjusting camera properties for the camera(s) in setup mode.
Default frame rate	Select a default frame rate for video viewed in the XProtect Smart Client.  You can override this setting on individual cameras by adjusting camera properties for the camera(s) in setup mode.
Default video buffer	If you require very smooth display of live video, without any jitter, it is possible to specify a video buffer.  Video buffering can significantly increase memory usage for each camera displayed in a view. If you do need to use video buffering, keep the buffering level as low as possible.
Default PTZ click mode	Specify a default PTZ click mode for your PTZ cameras. Options are click-to-center or virtual joystick. You can override this setting on individual cameras by selecting a different default PTZ click mode for the camera.
Start mode	Specify how the XProtect Smart Client opens after you have logged in. Options are full-screen mode, window mode or your last used mode.
Start view	Specify whether the XProtect Smart Client displays a view immediately after you have logged in. Options are: • The view you last used • No view • You decide after you have logged in
Hide mouse pointer	Lets you specify whether you want the mouse pointer to be hidden after a period of inactivity. You can specify how much time you want to elapse before hiding the mouse pointer. The default option is after 5 seconds. Options are: • Never • After 5 seconds

Name	Description
	• After 10 seconds • After 20 seconds • After 30 seconds If you move the mouse after a period of inactivity, it is enabled immediately.
Snapshot	Specify whether you want the snapshot feature to be available or unavailable. A snapshot is an instant capture of a frame of video from a camera at a given time.
Path to snapshots	Specify the path indicating where you want your snapshots to be saved to.
Help	Specify whether the help should be available or not in XProtect Smart Client. If you disable the help, nothing happens when you press **F1**, and the context-sensitive links are no longer visible. Also, you can't access the help from the **Settings and more** menu.
Video tutorials	Specify whether video tutorials about the XProtect products can be accessed from the **Settings and more** menu.

Panes settings

The **Panes** settings let you specify whether you want a pane to appear on a particular tab.

Some panes may contain functionality which may not be available to you, either because of your user permissions or the surveillance system (see Surveillance system differences on page 33) you are connected to.

The **Mode** column displays where the pane is available, the **Function** column lists the name of the pane, and the **Setting** column lets you specify whether you want the pane to be available or unavailable.

If available, the **Follow server** column lets you specify that you want your XProtect Smart Client to follow the recommended settings of the server. Certain settings may already be server-controlled, in which case configuration on the server decides whether you can override the settings.

Functions settings

The **Functions** settings let you specify the functions (for example, playback in live mode) that you want to display on a particular XProtect Smart Client tab.

The **Mode** column displays where the pane is available, the **Function** column displays the name of the function, and the **Setting** column lets you specify whether or not you want the pane to be available.

If available, the **Follow server** column lets you specify that you want your XProtect Smart Client to follow the recommended settings of the server. Certain settings are server-controlled, in which case configuration on the server decides whether or not you can override the settings.

Name	Description
Live > **Camera playback**	The ability to play back recorded video from individual cameras while in live mode.
Live > **Overlay buttons**	The ability to view and use overlay buttons in live mode for activating speakers, events, output, moving PTZ cameras, clearing indicators from cameras, etc.
Live and **Playback** > **Bookmark**	Select whether you want to add quick or detailed bookmarks from the view item toolbar or through ready-made overlay buttons in live or playback mode. Enabling or disabling this option in playback mode controls whether or not the corresponding button is enabled on the **Search** tab.  Depending on your user permissions, access to adding bookmarks from some cameras may be restricted.
Live and **Playback** > **Print**	The ability to print in live or playback mode. Enabling or disabling this option in playback mode controls whether or not the corresponding button is enabled on the **Search** tab.
Live and **Playback** > **Bounding boxes**	The ability to show bounding boxes on live video in live mode or on recorded video in playback mode on all cameras. Bounding boxes are used for, for example, tracking objects.

Name	Description
	The bounding box feature is only available if connected to certain surveillance systems and to cameras that support metadata. Depending on your user permissions, access to bounding boxes from some cameras may be restricted.
Playback > **Independent playback**	The ability to play back recorded video from individual cameras independently in playback mode, where all cameras in a view otherwise by default display recordings from the same point in time (the playback time).
Setup > **Edit overlay buttons**	The ability to add new or edit existing overlay buttons in setup mode. To add overlay buttons, the **Overlay buttons** list must be set to **Available** (you manage this on the **Panes** tab in the **Settings** window).
Setup > **Edit video buffering**	The ability to edit video buffering is part of the camera properties in setup mode. To edit video buffering, the **Setup** tab's **Properties** pane must also be made available (you manage this on the **Settings** window's **Panes** tab).

Timeline settings

The **Timeline** settings let you specify your general timeline settings.

If available, the **Follow server** column lets you specify that you want your XProtect Smart Client to follow the recommended settings of the server. Certain settings are server-controlled, in which case, configuration on the server decides whether you can override the settings.

Name	Description
Incoming audio	Select to show or hide incoming audio on the timeline
Outgoing audio	Select to show or hide outgoing audio on the timeline.
Additional data	Select to show or hide additional data from other sources.

Name	Description
Additional markers	Select to show or hide additional markers from other sources.
Bookmarks	Select whether to show or hide bookmarks on the timeline.
Motion indication	Select whether to show or hide motion indication on the timeline.
All cameras timeline	Select whether to show or hide the timeline for all cameras.
Playback	Select whether or not to skip gaps during playback.

Export settings

The **Export** settings let you specify general export settings.

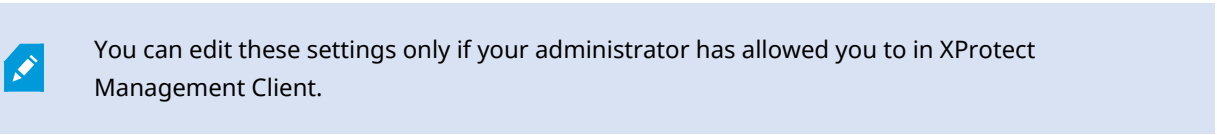
If available, the **Follow server** column lets you specify that you want XProtect Smart Client to follow the recommended settings of the server. Certain settings may already be server-controlled, in which case, configuration on the server decides whether you can override the settings.

Name	Description
Export to	Select the path that you want to export to.
Privacy mask	Select whether you want to cover areas with privacy masks in the exported video. The privacy masks that you add here only apply to the current export and for the selected video. The export may already include video with privacy masks configured by your system administrator. These privacy masks are configured in Management Client > **Devices** > camera > **Privacy masking**.
Media player format	Select whether or not you can export in the media player format.
Media player format - Video texts	Select whether you want video texts to be optional, required or unavailable when you export in the media player format. With video texts, the user can add overlay text on the exported recordings.

Name	Description
Media player format - Video codec properties	Select whether you want codec configuration to be available or not when you export in the media player format. The codec properties depend on the selected codec. Not all codecs support this option.
XProtect format	Select whether or not you can export in the XProtect format.
XProtect format - Project comments	Select whether you want project comments to be optional, required, or unavailable when you export in the XProtect format.
XProtect format - Device comments	Select whether you want device comments to be optional, required, or unavailable when you export in XProtect format.
Still image export	Select whether or not you can export still images.

Smart map settings

Enter the Bing Maps key or Google Maps client ID or key for the Bing Maps API or Google Maps API that you use.



You can edit these settings only if your administrator has allowed you to in XProtect Management Client.

Name	Description
Milestone Map Service	Specify whether Milestone Map Service can be used as a geographic background. If you select **Unavailable**, XProtect Smart Client does not display it as an option.

Name	Description
OpenStreetMap server	To use a different tile server (see Change OpenStreetMap tile server on page 88) than the one specified by your system administrator, enter the server address here.
Create location when layer is added	Specify whether to create a location when a user adds a custom overlay. For more information, see Adding, deleting, or editing custom overlays on page 91.
Bing Maps key	Enter or edit the private cryptographic key that you generated for the Bing Maps API.
Client ID for Google Maps	Enter or edit the client ID that you generated for the Google Static Maps API.
Private key for Google Maps	Enter or edit the private cryptographic key that you generated for the Google Static Maps API.
URL signing secret for Google Maps	Enter the signing secret that you retrieved for the Google Static Maps API.
Remove cached smart map files	If you are using Google Maps as your geographic background, files are not cached. Smart map saves to the cache folder on your local computer so that it can load faster. Use this setting to specify how often you want to remove the cached files.

Search settings

The search settings let you customize the behavior of parts of the search functionality, mainly on the **Search** tab.

Name	Description
Auto-play video clip in preview area	By default, when you select a search result, video in the preview area is paused at the event time. To make it start playing automatically, select **Yes**.
Loop video clip in preview area	By default, when you preview video from a search result, the video clip is played back only once. To make it loop, select **Yes**.

Joystick settings

Even though joystick control is supported for a large number of PTZ cameras, not all PTZ cameras may be joystick-controlled.

When a new joystick is detected by the XProtect Smart Client, a default pan-tilt-zoom (PTZ) configuration for the joystick is added automatically. However, the Joystick settings let you customize the setup for all your XProtect Smart Client joysticks.

Name	Description
Select joystick	Select from the list of available joysticks.
Axis setup: Name	There are three axes: • X-axis (horizontal) • Y-axis (vertical) • Z-axis (the depth or zoom level)
Axis setup: Invert	Select to change the default direction the camera moves in when you move the joystick. For example, select to move a PTZ camera to the left when you move the joystick to the right and move down when you move the joystick towards you.
Axis setup: Absolute	Select to use a fixed rather than a relative positioning scheme (moving the joystick moves the joystick-controlled object based on the object's current position).

Name	Description
Axis setup: Action	Select the function for an axis: • Camera PTZ Pan • Camera PTZ Tilt • Camera PTZ Zoom • No action
Axis setup: Preview	Test the effect of your selections. When you have selected a function for the axis you want to test, move the joystick along the required axis to view the effect, indicated by a movement of the blue bar.
Dead zone setup: Pan/Tilt	Specify the dead zone for the joystick's pan and tilt functions. The further you drag the slider to the right, the larger the dead zone becomes, and the more you will have to move the joystick handle before information is sent to the camera. Dragging the slider to the far left disables the dead zone (only recommended for high-precision joysticks). Use the **Axis setup** preview to test the effect of your dead zone settings.
Dead zone setup: Zoom	Specify dead zone for the joystick's zoom function. The further you drag the slider to the right, the larger the dead zone becomes, and the more you will have to move the joystick handle before information is sent to the camera. Dragging the slider to the far left disables the dead zone (only recommended for high-precision joysticks). Use the **Axis setup** preview to test the effect of your dead zone settings.
Button setup: Name	The name of the button.
Button setup: Action	Select one of the available actions for the required joystick button.
Button setup: Parameter	If relevant, specify a parameter for the command or action. For example, if you want to specify the window and view item for the **Copy the selected camera view item** parameter, enter 2;1 to have the camera copied to the floating window (window 2), in the first view item (view item 1).
Button setup: Preview	Verify that you are configuring the right button, press the corresponding button on the joystick. The relevant button will display in blue in the Preview column.

Keyboard settings

Keyboard settings let you assign your own shortcut key combinations to particular actions in the XProtect Smart Client. The XProtect Smart Client also features a small number of standard keyboard shortcuts (see Keyboard shortcuts (overview) on page 163), immediately ready for use.

Name	Description
Press shortcut key	Enter the key combination you want to use as a shortcut to a particular action.
Use new shortcut in	Select to define how you want to apply the shortcut: • **Global**: On all of the XProtect Smart Client tabs • **Playback mode**: Only on the **Views** tab • **Live mode**: Only on the **Views** tab • **Setup mode**: Only in setup mode
Categories and **Commands**	Select a command category and then select one of the associated commands. If you want all your views listed to allow you to create keyboard shortcuts for individual views, select the **Views.All** category. Some commands only work when the keyboard shortcut is used in certain contexts. For example, a keyboard shortcut with a PTZ-related command will only work when using a PTZ camera.
Parameter	If relevant, specify a parameter for the command or action. For example, if you want to specify the window and view item for the **Copy the selected camera view item** command, enter 2;1 to have the camera copied to the floating window (window 2), in the first view item (view item 1).

Access control settings

Select whether or not you want access request notifications to pop up in XProtect Smart Client.

If the **Follow Server** field is selected, your system administrator controls the setting of **Show access request notifications**.

Alarm Manager settings

Name	Description
Start video playback second (s) before alarm	Start video playback some time before the alarm was triggered. This is useful when, for example, you want to see the moments before a door was opened.
Preview the most recent alarm	When this check box is selected, the selection in the alarms list will change to the most recent list item when a new alarm is triggered. If the check box is not selected, the selection in the alarms list will stay unchanged when a new alarm is triggered.
Play sound notifications for alarms	Specify whether you want alarms to play sound notifications. If the field is grayed out, it is has been locked by your system administrator in XProtect Management Client.
Show desktop notifications for alarms	Specify whether you want desktop notifications for alarms to be displayed. They will only appear when XProtect Smart Client is running. If the field is grayed out, it is has been locked by your system administrator in XProtect Management Client.
Use server settings	Select this check box to use the settings specified by your system administrator in XProtect Management Client.

Advanced settings

The **Advanced** settings let you customize advanced XProtect Smart Client settings. If you are not familiar with the advanced settings and how they work, just keep their default settings. If you connect to some surveillance systems (see Surveillance system differences on page 33), you may see **Follow server** column. You can use this column to make XProtect Smart Client follow the recommended settings of the server as set up in the Smart Client profiles. You may experience that certain settings are already server-controlled, in which case configuration on the server decides whether or not you are able to override those settings.

Name	Description
Multicast	Your system supports multicasting of live streams from recording servers to clients. If multiple XProtect Smart Client users want to view live video from the same camera, multicasting helps saving considerable system resources. Multicasting is particularly useful if you use the Matrix functionality, where multiple clients require live video from the same camera. Multicasting is only possible for live streams, not for recorded video/audio. **Enabled**: is the default setting. In the XProtect Management Client, the recording servers and cameras must also have the functionality enabled to make multicasting from servers to clients available. **Disabled**: multicasting is not available.
Hardware acceleration	Controls if hardware-accelerated decoding is in use. The load on the CPU is high in a view with many cameras. Hardware acceleration moves some of the CPU load to the Graphics Processing Unit (GPU). This improves the decoding capability and performance of the computer. This is useful, mainly if you view multiple H.264/H.265 video streams with a high frame rate and a high resolution. **Auto** is the default setting. It scans the computer for decoding resources and always enables hardware acceleration if available. **Off** disables hardware acceleration. Only the CPU processes the decoding.
Maximum decoding threads	Controls how many decoding threads are used to decode video streams. This option can help you improve performance on multi-core computers in live as well as playback mode. The exact performance improvement depends on the video stream. This setting is mainly relevant if using heavily coded high-resolution video streams like H.264/H.265—for which the performance improvement potential can be significant—and less relevant if using, for example, JPEG or MPEG-4. Note that multi-threaded decoding generally is memory-intensive. The ideal setting depends on the type of computer you use, the number of cameras you need to view, and on their resolution and frame rate. **Normal** means that no matter how many cores your computer has, it will only use one core per view item with a camera. **Auto** is the default setting. Auto means that the computer uses as many threads per view item with cameras as it has cores. However, the maximum number of threads is eight, and the number of threads actually used may be lower, depending on which codec (compression/decompression technology) is used.

Name	Description
	Advanced users can manually select the number of threads used, with a maximum of eight. The number you select represents a maximum; the number of threads actually used may be lower, depending on the codec (compression/decompression technology).  This setting affects all view items with cameras, in all views, in live as well as playback mode. You cannot specify the setting for individual view items with cameras or views. Because this setting may not be equally ideal for all of your view items with cameras and views, we recommend that you monitor the effects and, if required, re-adjust the setting to achieve the optimum balance between performance improvement and memory use.
Adaptive streaming	Controls if adaptive streaming is in use. The load on the CPU and the GPU is high in a view with many cameras. Adaptive streaming enables XProtect Smart Client to automatically select the live video streams with the best match in resolution to the streams requested by the view items. This decreases the load on the CPU and the GPU and thereby improves the decoding capability and performance of the computer. **Disabled** is the default setting. No automatic stream selection is done. **Enabled** scans the XProtect system configuration for available streams and selects the best matching ones for the selected view.  Even though adaptive streaming can be enabled when only one stream is available, you must have at least two streams per camera with different resolutions to take advantage of adaptive streaming.  This setting affects all views in live mode.
Deinterlacing	Interlacing determines how an image is refreshed on a screen. The image is refreshed by first scanning the odd lines in the image, then scanning every even line. This allows a faster refresh rate because less information is processed during each

Name	Description
	scan. However, interlacing may cause flickering, or the changes in half of the image's lines may be noticeable. With Deinterlacing, you convert video into a non-interlaced format. Most cameras do not produce interlaced video, and this option will not impact quality or performance of non-interlaced video. **No filter** is the default setting. No deinterlacing is applied, so the characteristic jagged edges may show up in images if objects are moving. This is because the even and odd lines of the full image are weaved together to compose the full resolution picture. However, these are not captured at the same time by the camera, so objects in motion will not be aligned between the two sets of lines, causing the jagged-edge effect. Performance impact: None. **Vertical stretch top field**: This option only uses the even lines. Each odd line will be "copied" from the previous (even) line. The effect is that jagged edges do not appear, but this is at the expense of reduced vertical resolution. Performance impact: Less expensive than the **No filter** option because only half the number of lines will need post-processing. **Vertical stretch bottom field**: This option only uses the odd lines. Each even line will be "copied" from the following (odd) line. The effect is that jagged edges do not appear, but this is at the expense of reduced vertical resolution. Performance impact: Less expensive than the **No filter** option because only half the number of lines will need post-processing. **Content adaptive**: This option applies a filter to areas of the image where jagged edges would otherwise show up. Where no jagged edges are detected, the image is left untouched. The effect is that jagged edges are removed and full vertical resolution is preserved in the areas of the image where no jagged edges are perceived. Performance impact: More expensive than the **No filter** option because the total CPU cost per decoded and rendered frame is increased by around 10%.
Video diagnostics overlay	View the settings and performance level of the video stream in the selected view. This is helpful when you must verify settings or diagnose a problem. Select between these options: **Hide**: No video diagnostics overlay. Default setting. **Level 1**: Frames per second, video codec, and video resolution. **Level 2**: Frames per second, video codec, video resolution, multicast, and hardware acceleration status. **Level 3**: Debug level. Mainly for system administrators to troubleshoot or optimize

Name	Description
	system performance.
Time zone	Change the time zone, for example if the time that is displayed in the camera title bar does not match your current time. Select a predefined time zone or a custom time zone: • **Local**: The time zone of the computer running the XProtect Smart Client • **Server time zone**: The time zone of the server • **UTC** • **Custom time zone**: If you want a particular time zone, select this option and then select from the list of available time zones in the **Custom time zone** field.
Custom time zone	If you have selected **Custom** in the **Time zone** field, you can select any time zone known by the computer. This is useful if two users in different time zones need to view an incident—having the same time zone makes it easier to identify and establish that they are watching the same incident.
PDF report format	Select A4 or letter format for your PDF reports. You can create reports of events.
PDF report font	Select a font to be used in your PDF reports.
Logging (for technical support)	Enable the logging of application events, for example when alarms are triggered. This is mainly to help technical support troubleshoot issues that may occur in XProtect Smart Client. There are three different log files: • ClientLogger.log • MIPLogger.log • MetadataLogger.log The logs are located here on the machine where XProtect Smart Client is installed: C:\ProgramData\Milestone\XProtect Smart Client\Logs. These logs are different from the **System logs** in XProtect Management Client.

Language settings

Specify the language version of your XProtect Smart Client, including whether you want the user interface elements to be displayed right-to-left. Select from the list of available languages and then restart the XProtect Smart Client for the change to take effect.

Right-to-left languages (explained)

For some of the languages available in XProtect Smart Client, a visual right-to-left user interface is supported. The languages are:

- Arabic
- Farsi
- Hebrew

You can change this setting in the **Settings** window > **Language** tab. If you set the interface to right-to-left, buttons, toolbars, and panes are reversed.

Disable the help

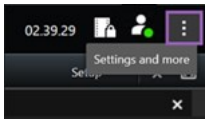
To prevent operators from accessing the help function, you can disable the help. Then nothing happens when you press **F1**, and the context-sensitive links and **Help** buttons are no longer visible. If required, you can enable the help again.

Requirements

The availability of the help can also be controlled server-side by your system administrator. You can only disable or enable the help if the system administrator has not locked this setting.

Steps:

1. On the global toolbar, select **Settings and more** and then **Settings** to open the **Settings** window.



2. From the **Application** tab and in the **Help** list, select **Unavailable**.
3. Close the dialog.
4. To test that the help has been disabled, press **F1**. Nothing should happen.

Views (configuration)

In setup mode, you can create views and specify which cameras or other types of content should be included in each view. To organize your views, you must create at least one view group. This is often done by your system administrator.

Your ability to edit views and groups depends on your user permissions. If you can create the view or group, you can also edit it.

Views and view groups (explained)

The way video is displayed in XProtect Smart Client is called a view. XProtect Smart Client can handle an unrestricted number of views, allowing you to switch between video from various groups of cameras. Views can hold between one and hundred cameras, but can also contain other types of content, for example images and text.

Views must be contained inside view groups that help you organize your views.

Views are available in live and playback mode. Views can be private or shared:

- Private views can only be accessed by the user who created them. To make the view private, create it inside the **Private** folder
- Shared views allow multiple operators to share the same views. Depending on your XProtect VMS system:
  - There may be a default folder for shared views named **Shared** or **Default group**
  - Shared views can be shared by all operators, or access to selected shared views can be given to certain operators. Typically, only a few people in an organization can create and edit shared views, for example the system administrators

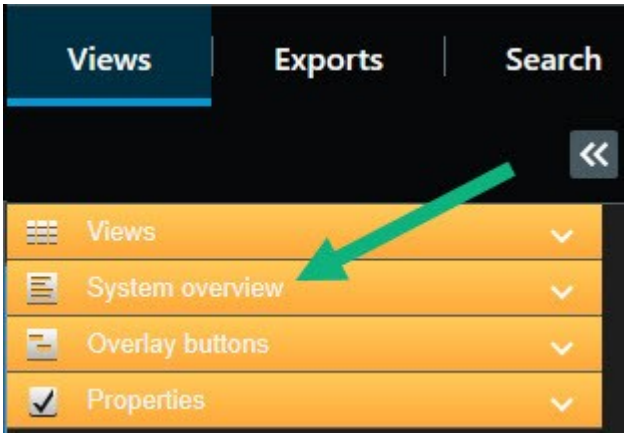
Not all users may have access to all cameras on the XProtect VMS system. Some of the features you include in your shared view may not be supported in earlier versions of XProtect Smart Client. Always make sure that the users you want to share with have the necessary permissions and are running the same XProtect Smart Client version as yourself.

Your user settings, including information about your views, are stored centrally on the XProtect VMS server, so you can use your views on any computer that has XProtect Smart Client installed.

Example of a 2x2 view

What can views contain?

In setup mode in the **System overview** pane, you can see the elements that you can add to your views:



Item	Description
Alarms	Allows you to show a list of alarms or an alarm preview. Both elements are also available on the **Alarm Manager** tab.
Access Monitor	Access monitor - with XProtect® Access installed, you can show access monitors in your views, for example for a specific door.
Cameras	Allows you to show video feed from a live camera or play back video. The cameras appear under the site name, which is defined by your system administrator.
Carousels	Allows you to shift between cameras at a pace that you define.

Item	Description
Hotspots	Allows you to show whatever camera is in focus in a high resolution or frame rate.
HTML pages	Allows you to show a webpage, for example an online news channel.
Images	Allows you to show an image, for example if you want to distribute a picture of a suspect.
LPR	With XProtect® LPR installed, you can add LPR cameras to views.
Maps	Allows you to show a floor plan or a geographical area.
Matrix	Allows you to show a view item with Matrix content. See also Matrix (explained) on page 277.
Smart maps	Allows you to navigate your cameras on a geographical map of the world based on one of these online map services: • Bing Maps • Google Maps • Milestone Map Service • OpenStreetMap
Smart Wall controls	If XProtect Smart Wall has been configured by your system administrator, Smart Wall controls allow you to push cameras and other types of content to your video walls.
Text	Allows you to show text, for example if you want to provide instructions for other operators.
Transact	If XProtect Transact has been installed in your system, you can add point-of-sales systems together with cameras.

Create view groups

Your XProtect Smart Client may be preconfigured to display view groups that you can add your views to. However, you can create your own view groups to help you organize your views.

Example

Imagine that you have cameras installed on ten different levels in a multi-story building. You decide to create a view group for each level and name them accordingly: **Ground floor**, **First floor**, **Second floor**, and so on.

Steps:

1. In setup mode, in the **Views** pane, select the **Private** or **Shared** top-level folder you want to add a group to.
2. Click **Create new group**  .

   A new group is created named **New group**.
3. Select and click the **New group** to overwrite the name.
4. You can now create views within this group.

Create views

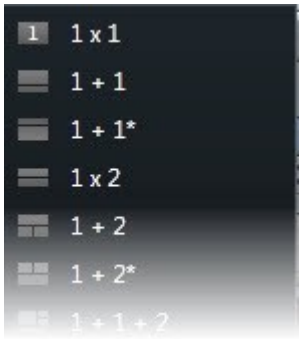
To view or play back video in XProtect Smart Client, first you must create a view, where you add the cameras you need.

Requirements

Before creating the view, you need a group that you can add the view to. See also Create view groups on page 57.

Steps:

1. In the right corner, click **Setup** to enter setup mode.
2. In the **Views** pane, select the group you want to add the view to.
3. Click  to create a new view.
4. Select a layout. The layouts are grouped according to their aspect ratio, and according to whether they are optimized for regular content or content in portrait mode (where the height is greater than the width).

5. Enter a name for the view by overwriting the default **New View** name.
6. Click **Setup** again to exit setup mode. Your changes are saved.

Copy, rename, or delete views or groups

If you have a view and you want to reuse it, you can copy it. You can also copy a group of views or a private view to a shared view.

Steps:

1. In setup mode, in the navigation pane, select the view.
2. Click **Copy**  , or press **CTRL**+**C**.
3. Browse to where you want to paste the view and select **Paste**  , or press **CTRL**+**V**.

   Alternatively, you can select and drag the view to another folder.

4. The copied view is by default named the same as the original followed by (2). To change the name, right-click and select **Rename**  .
5. To delete a view, right-click and select **Delete**  .

Add cameras and other elements to views

You can add different types of elements to your views, for example cameras.

Steps:

1. Open the view that you want to modify.
2. Click **Setup** to enter setup mode.
3. From the **System overview** pane, drag the wanted element into a view item.
4. Fill out any additional information about the element.
5. Click **Setup** again to exit setup mode. Your changes are saved.

For detailed information, see Adding content to views (in detail) on page 60.

Assign shortcut numbers to views

You can assign shortcut numbers to views to let users select views using standard keyboard shortcuts (see Keyboard shortcuts (overview) on page 163).

1. Click **Setup** to enter setup mode.
2. In the **Views** pane, select the view you want to assign a shortcut to.
3. In the **Shortcut** field, specify a shortcut number, and then press ENTER. The shortcut number appears in parentheses in front of the view name.
4. Repeat as necessary for other views.
5. Click **Setup** again to exit setup mode. Your changes are saved.

Adding content to views (in detail)

As described in Add cameras and other elements to views on page 59, you can add cameras and other types of elements to your views. This section provides more detailed how-tos:

Add alarms to views

Add alarms to views on page 81

Add cameras to views

To view video from a camera, first you must add the camera to a view.

1. In setup mode, select the view you want to add a camera to.
2. In the **System overview** pane, expand the required server  to view a list of available cameras from that server.

   If a server is listed with a red icon, it is unavailable, in which case you will not be able to view cameras from that server.

3. Select the camera from the list and drag it to a view item inside the view. An image from the camera appears in the selected view item.

   If areas in the video are blurred or grayed out, it is because your system administrator has covered these areas with privacy masks (see Privacy masking (explained) on page 246).

4. You can specify the camera properties (such as quality, frame rate and more) in the **Properties** pane. For more information, see Camera settings on page 66.
5. For each camera you want to add, repeat the steps above.
6. To add multiple cameras to a view, for example all of the cameras from a camera folder, drag the folder to the view. Make sure a sufficient number of view items are available in the view.

You can easily change which cameras are included in your view by dragging a different camera to the view item.

Add carousels to views

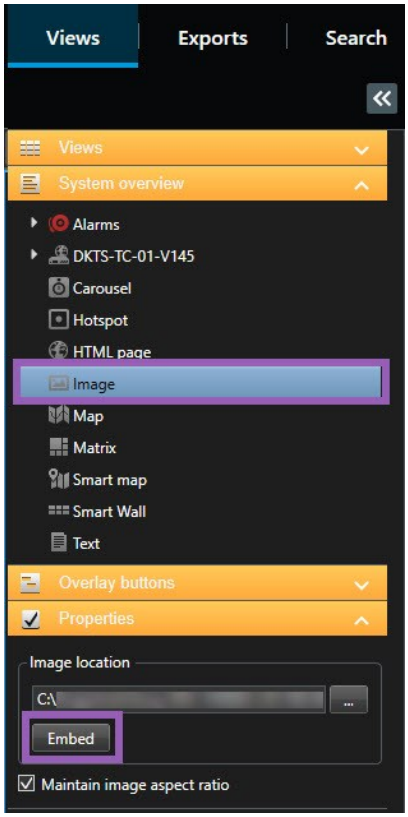
Add carousels to views on page 75

Add images to views

You can display static images in a view. For example, this is useful when you want to share a snapshot of a suspect, or a diagram of emergency exits.

Steps:

1. Click **Setup** to enter setup mode.
2. In the **System overview** pane, drag the **Image** item to a view item. A window appears.



3. Locate and then select the image file that you want to add.
4. Click **Open**. The image now appears inside the view item.
5. To make the image available to others who cannot access the location of the image file, on the

Properties pane, click **Embed**. The file is stored in the system.

6. Click **Setup** again to exit setup mode. Your changes are saved.

Add hotspots to views

Add hotspots to views on page 77

Add maps to views

Add maps to views on page 110

Add smart maps to views

Add smart map to views on page 84

Add text to views

You can add text to one or more a view items inside a view. For example, this is useful when you want to send a message or instructions to operators, or post a work schedule for security personnel. You can use up to 1,000 characters.

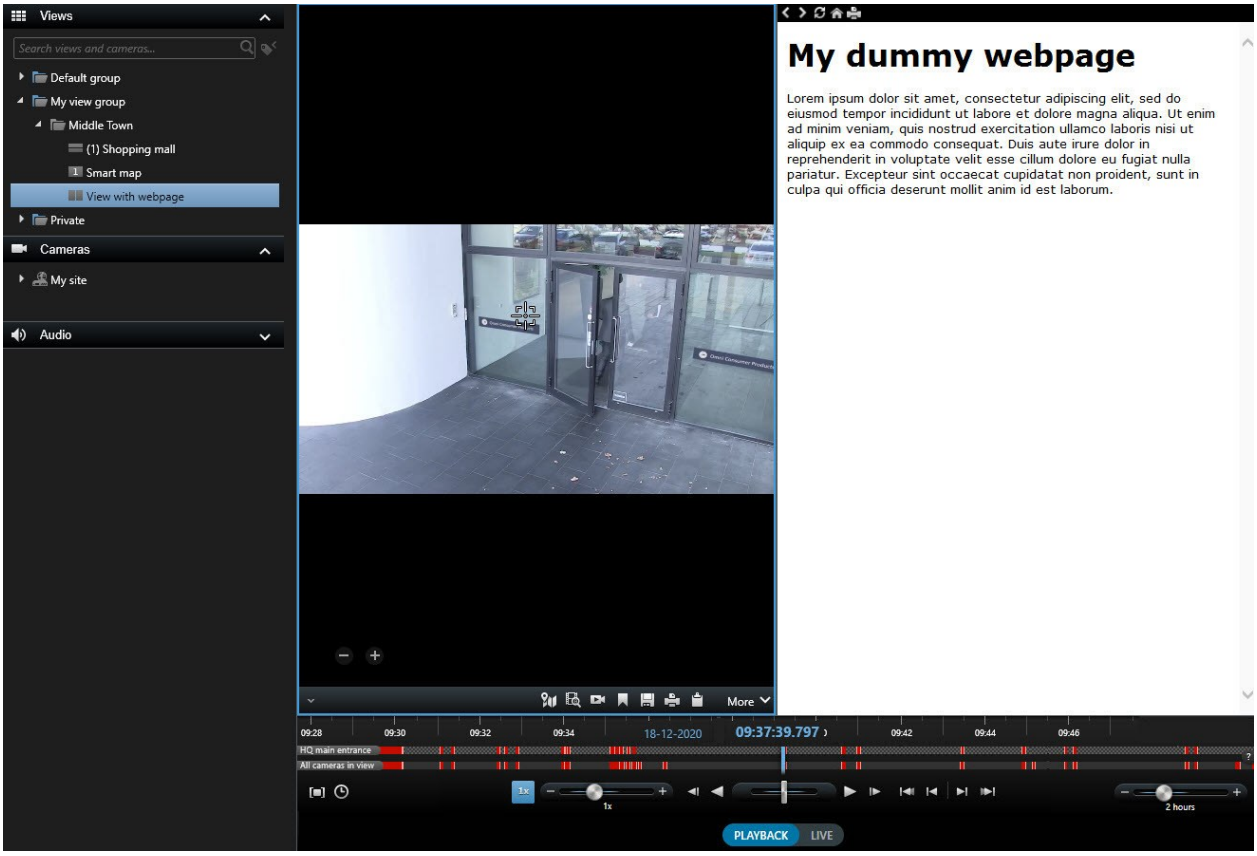
Steps:

1. Click **Setup** to enter setup mode.
2. On the **System overview** pane, drag the **Text** element to the view item, where you want the text to appear. A window appears.
3. Enter the text.
4. Click **Save**.
5. To change your text after you save it, in setup mode, click **Edit text** in the **Properties** pane.

You can insert tables from products such as Microsoft Word and Microsoft Excel, but you cannot make changes to the tables.

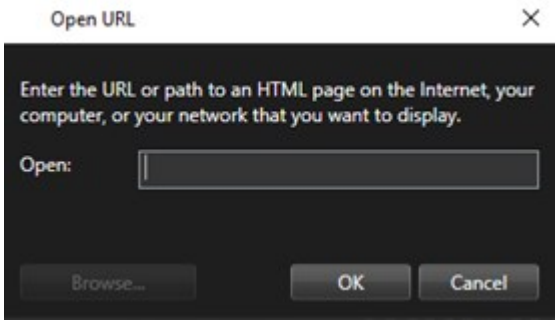
Add web pages to views

You can add web pages to views, for example HTML, PHP, or ASP pages. This is useful, for example, for providing online instructions or showing company web pages in combination with cameras or other types of content.



Steps:

1. Open the view that you want to modify.
2. Click **Setup** to enter setup mode.
3. In the **System overview** pane, click and drag the **HTML page** item to one of the view items. A window appears.



4. In the **Open** field, enter the web address of the web page.

> To use a web page stored on your local computer, network, or on an FTP server, make sure that the display mode is set to **Compatibility** in the properties of the web page. See Web page properties on page 64. Otherwise, you will get an error message. See Web pages (troubleshooting) on page 311.

5. Click **OK**.
6. To set the properties, expand the **Properties** pane.
7. Click **Setup** again to exit setup mode. Your changes are saved.

> You cannot navigate the web page in setup mode.

Web page properties

Name	Description
Edit	Specify a new URL or file location of the web page.

Display mode	Select the browser engine to render the web page. There are two options:
	• **Standard** - this setting uses Microsoft Edge. Choose **Standard** if the web page is located on a web server, and the network protocol used is either HTTP or HTTPS
	• **Compatibility** - this setting uses Internet Explorer. Choose **Compatibility** if the web page:
	  • is stored locally
	  • uses other network protocols than HTTP and HTTPS
	  • contains scripts designed to interact with XProtect Smart Client
	  • uses an older version of HTML

Scaling	Select the scaling of the web page. The optimal scaling

Name	Description
	depends on the content of the imported web page and how you want to display it This setting is only available in **Compatibility** mode.
Hide toolbar	Select the check box to hide the navigation toolbar that gets inserted above each imported web page. 

Add overlay buttons to views

You can activate speakers, events, output, and more through overlay buttons which appear when you move your mouse over individual view items with cameras in live mode.

You can add as many buttons as needed.

1. Click **Setup** to enter setup mode.
2. In the **Overlay buttons** pane, select and drag the action onto the camera view item.
3. When you release the mouse, the overlay button appears. To resize the button, drag the handles that appear.

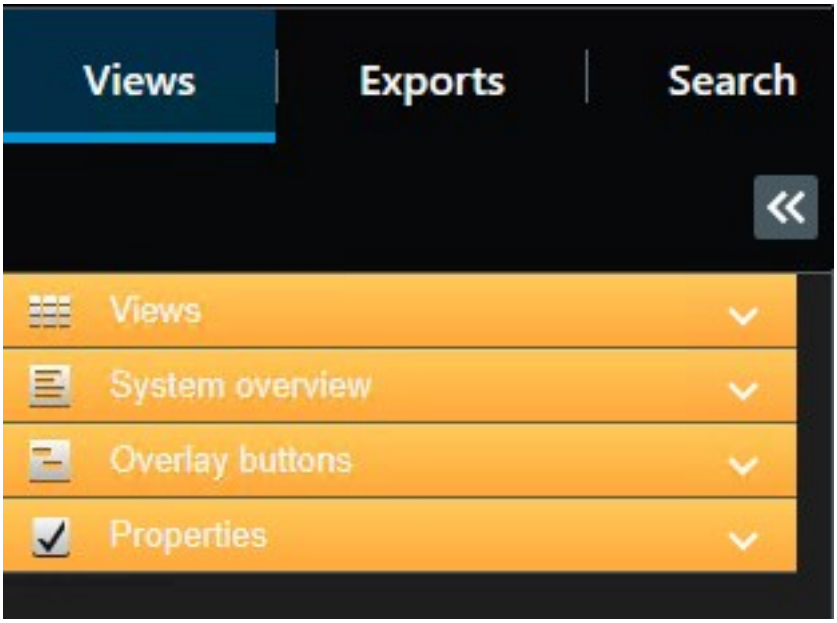
4. To change the text of the overlay button, double-click the text, overwrite it, and then select the check box to save. To undo, click the cancel button. When you save, the text scales to the largest

possible size on the button.

5. Click **Setup** again to exit setup mode. Your changes are saved.

Cameras (configuration)

The settings in this section pertain to the **Overlay buttons** and **Properties** panes. To access these panes, click the **Setup** button and make sure that the navigation pane on the left-hand side is visible.



Camera settings

In **Setup** mode, in the **Properties** pane, you can view and edit properties for the selected camera (the selected camera is indicated by a bold border in the view).

Name	Description
Camera name	Displays the name of the selected camera. To change the camera, click the ellipsis button to open the **Select camera** window and select a different camera. This can be useful if you want to change the camera but keep the settings.
Live stream	If available, select the live stream that you want to display in the view. If multiple

Name	Description
	streams have been set up on the server, you can select either **Default** or one of the available stream options. If you select another option than **Default**, you will not be able to edit **Image quality** or **Frame rate** settings.
Image quality	⚠ Specifying image quality of video viewed in XProtect Smart Client is only relevant if you are viewing JPEG streams. If you are viewing other codecs like H264 and H265 and set the quality to lower than **Full**, you will increase the bandwidth, CPU, and GPU usage when re-encoding to JPEG. Determines the quality of video when viewed, but also affects bandwidth usage. If your XProtect Smart Client is used over the internet, over a slow network connection, or if for other reasons you need to limit bandwidth use, image quality can be reduced on the server side by selecting **Low** or **Medium**. When selecting a reduced image quality, images from the selected camera are re-encoded to a JPEG format on the surveillance system server before being sent to the XProtect Smart Client. Re-encoding takes place along the following lines: **Full**: The default setting, providing the full quality of the original video. **Super high (for megapixel)**: Re-encoding to an output width of 640 pixels (VGA) and a JPEG quality level of 25%. **High**: Re-encoding to an output width of 320 pixels (QVGA) and a JPEG quality level of 25%. **Medium**: Re-encoding to an output width of 200 pixels and a JPEG quality level of 25%. **Low**: Re-encoding to an output width of 160 pixels and a JPEG quality level of 20%. Height will scale according to the width and the aspect ratio of the original video. Your image quality selection will apply for live as well as recorded video, and for JPEG as well as MPEG. For MPEG, however, only keyframes will be re-encoded when viewing live video, whereas all frames will be re-encoded when viewing recorded video. While using a reduced image quality helps limit bandwidth use, it will—due to the need for re-encoding images—use additional resources on the surveillance system server.

Name	Description
	You can quickly reduce the bandwidth usage for all cameras in the view by reducing the image quality for a single camera, then clicking the **Apply To All** button.
Keep when maximized	When you view live or recorded video, you can double-click a particular view item with a camera to maximize it. When you do this, video from the camera is by default displayed in full quality, regardless of your image quality selection. If you want to make sure that the selected image quality also applies when video is enlarged, select the **Keep when maximized** box, located immediately below the **Image quality** setting.
Frame rate	Select a frame rate for the selected camera. Select between **Unrestricted** (default), **Medium**, or **Low**. The combination of the frame rate you select and the way your surveillance system is set up (see Frame rate effect (explained) on page 71) affects the quality of your video.
PTZ click mode	Select a default PTZ click mode for your PTZ cameras. Options are click-to-center or virtual joystick. You can override this setting on individual cameras by selecting a different default PTZ click mode for the camera.
Fisheye split mode	Available only if the selected camera is a fisheye camera. Fisheye technology allows the creation and viewing of 360° panoramic images. The XProtect Smart Client supports up to four different viewpoints from a single fisheye camera. The **Fisheye split mode** list lets you select the required split mode: **No split** lets you view a single viewpoint. **Two by two** lets you view four different viewpoints at a time. When viewed on any of the XProtect Smart Client's tabs, the fisheye camera will appear as specified, with either one or four viewpoints from the same image. When you view different viewpoints from a fisheye camera, you can navigate each viewpoint independently by clicking inside each viewpoint, or by using the **PTZ presets** menu on the camera toolbar.

Name	Description
Maintain Image Aspect Ratio	If selected, video will not be stretched to fit the size of the view item. Rather, video will be displayed with the aspect ratio (height/width relationship) with which it has been recorded. This may result in horizontal or vertical black bars appearing around the images from some cameras. If check box is cleared, video will be stretched to fit the view item in the view; this may lead to slightly distorted video, but you will avoid any black bars appearing around the video.
Update on motion	If selected and in live mode, video from the selected camera will only be updated when motion is detected. Depending on the motion detection sensitivity configured for the camera on the surveillance system server this can help reduce CPU usage significantly. When video is only updated on motion, users will see the message **No motion** together with a still image in the camera's view item until motion is detected. The still image will have a gray overlay, making it easy to identify which cameras have no motion.
Sound on motion detection	When video from the camera is viewed in live mode, it is possible to get a simple sound notification when motion is detected. Sound notifications only work if video from the camera is actually displayed in your XProtect Smart Client. Sound notifications will therefore **not** work if you minimize the window containing the camera in question. Likewise, if you maximize a camera in a view so only that camera is displayed, it will not be possible to hear sound notifications regarding other cameras. **Always off**: Do not use sound notifications on detected motion. **Always on**: Play a sound notification each time motion is detected on the camera.
Sound on event	 This feature is only available in certain XProtect VMS systems. For more information, see the product comparison chart: https://www.milestonesys.com/solutions/platform/product-index/ Being able to use this feature requires that notifications on events have been configured on the surveillance system server. Sound notifications only work if video from the camera is actually displayed in your XProtect Smart Client. Sound notifications will thus not work if you minimize the window

Name	Description
	containing the camera in question. Likewise, if you maximize a camera in a view so only that camera is displayed, it will not be possible to hear sound notifications regarding other cameras. When video from the camera is viewed in live mode, it is possible to get a simple sound alert when events related to the selected camera occur. **Always off**: Do not use sound alerts when events related to the camera occur. **Always on**: Play a sound alert each time an event related to the camera occurs.
Display settings	**Use default display settings**: Use default settings, as defined in the **Settings** window, for showing title bar and video indicator for the selected camera. If you want a non-default behavior for the selected camera, clear the check box and select whether you want title bar and/or video indicator. **Show title bar**: Displays a title bar at the top of each view item. The title bar helps users quickly identify cameras. When displayed in live mode, the title bar displays information about detected motion and events, whether the camera is recording, etc. See Camera indicators (explained) on page 168. If you choose not to display the title bar, you will not be able to see the visual indicators for motion and events. As an alternative, you can use sound notification. **Show bounding box layer**: Displays bounding boxes on individual cameras. Open the **Bounding box providers** (see Bounding box providers (explained) on page 72) dialog box to specify the metadata devices to provide data to the camera.
Video buffering	This part of the **Properties** pane may not be visible. To view it, go to the **Settings** window's (see Settings in XProtect Smart Client on page 37) **Functions** tab, and ensure that **Setup** > **Edit video buffering** is set to **Available**. If you require very smooth display of live video, without any jitter, it is possible to build up a video buffer. If possible, avoid using video buffering. Video buffering can significantly increase memory usage for each camera displayed in a view. If you do need to use video buffering, keep the buffering level as low as possible. When live video is stored in a buffer, it will display smoothly without any jitter, but the

Name	Description
	building up of the buffer will lead to a small delay in the display of live video. Such a delay is often not a problem for the person viewing the video. However, the delay may become very evident if the camera is a pan-tilt-zoom (PTZ) camera, and especially if you use a joystick to operate the camera. Being able to control the amount of video buffering lets you decide whether you want to prioritize smoothly displayed live video (requires buffering and leads to a small delay) or instant PTZ and joystick operation (requires no buffer, but may—due to the lack of a buffer—lead to a slight jitter in live video). To use video buffering, select **Use default video buffer**, then select the required buffer, from **None** to **Maximum 2 seconds**.
Apply to all	The **Apply to all** button lets you quickly apply the camera settings for the selected camera to all cameras in the view.

Frame rate effect (explained)

The effect of the frame rate selection can be illustrated as follows:

Effect	Unrestricted	Medium	Low
JPEG	Send all frames	Send every 4th frame	Send every 20th frame
MPEG/H.264/H.265	Send all frames	Send key frames only	Send key frames only

Example:

If you set the **Frame rate** option to **Low** in your XProtect Smart Client, and your system administrator has configured the camera to feed JPEG images at a frame rate of 20 frames per second, you will experience an average of 1 frame per second when viewing video from the camera. If your system administrator then configures the camera with a feed as low as 4 frames per second, you will experience an average of 0,2 frames per second when viewing video from the camera.

Bounding boxes (explained)

A bounding box is the rectangular border that encloses, for example, an object in a camera image. In the XProtect Smart Client, a bounding box displays as a yellow border in video.

The color may vary depending on how your VMS system is configured.

You can show or hide bounding boxes from individual cameras in **Display settings** in the camera properties.

If bounding boxes are displayed on your screen, they also appear when you:

- Export video in the XProtect format.
- Print still images. See also Printing or creating surveillance reports on page 185.

Bounding box providers (explained)

Requires that **Show bounding box layer** is selected. In the dialog box, enable the metadata devices that you want to provide data for the bounding boxes in videos from this camera. The list of devices is defined by your system administrator.

Overlay buttons (explained)

You can add overlay buttons to view items with cameras to trigger auxiliary commands (commands defined by the camera). The overlay buttons may vary depending on your surveillance system (see Surveillance system differences on page 33). Auxiliary commands differ from camera to camera. For more information, see the documentation for the camera.

Sound notifications (explained)

Your XProtect Smart Client may have been configured to notify you with a sound notification when:

- Motion is detected on one or more specific cameras
- Events (see Events (explained) on page 245) related to one or more specific cameras occur

When you hear a sound notification, special attention may be required. If in doubt about whether or how sound notifications are used in your organization, contact your system administrator.

You can temporarily mute sound notifications for a specific camera: on the camera toolbar, click **More** > **Sound notifications** > **Mute**.

When you minimize the XProtect Smart Client window, sound notification is disabled.

To turn on sound notifications for the camera again, click **More** > **Sound notifications** > **Mute** again.

The ability to mute sound notifications is not available for view items with hotspots, carousels, or Matrix content.

Audio (configuration)

Audio settings

You can listen to recorded audio independently of the views or cameras that you are watching. In playback mode, you select a time for the recorded audio you want to hear.

Name	Description
Microphones	Select the microphone you want to listen to audio from.

Name	Description
	If the **Microphones** list displays **No microphone hardware**, your computer does not have the required hardware for playing audio from the surveillance system. Typically, this occurs because your computer does not have an audio card installed. If the list displays **No microphone sources**, no microphones attached to cameras are available.
Mute	Select to mute either microphones or speakers.
Speakers	Select the speaker you want to talk through. If the **Speakers** list displays **No speaker hardware**, your computer does not have the required hardware for playing audio from the surveillance system. Typically, this occurs because your computer does not have an audio card installed. If the list displays **No speaker sources**, no speakers attached to cameras are available. If your surveillance system has speakers attached to multiple cameras (and you have the necessary user permissions to access them), you can talk through all the speakers simultaneously by selecting **All speakers** from the **Speakers** list.
Talk	Click and hold down the mouse button for as long as you want to talk.
Level meter	The meter indicates the level of your voice. If the level is very low, you may need to move closer to your microphone or adjust your audio settings in Windows. If the **Level meter** shows no level at all, check that the microphone is connected and correctly set up.
Lock to selected audio devices	When you select a camera or view, the corresponding microphone and/or speaker is also selected by default. However, if you want audio for a specific camera regardless of the ones you are viewing, you can select **Lock to selected audio devices**. **Example**: You need to listen and talk to a crime victim through microphones and speakers attached to camera A, but you also urgently need to view cameras X, Y and Z, some of which are displayed in different positions in the view. By selecting **Lock to selected audio devices**, you can communicate with the victim on camera A while viewing the other cameras at the same time.
List only devices from current view	If your surveillance system contains large numbers of microphones and/or speakers, the lists from which you select microphones and speakers in the Audio pane can be very long. To avoid this, you can limit the lists to only contain microphones and speakers relevant to your current view by selecting **List only devices from current view**. In this context, **current view** also includes any views you have open as floating windows and on primary and secondary displays (see Multiple windows or displays (explained) on page 156).

Bookmarks (configuration)

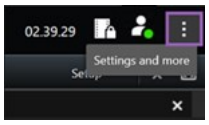
This feature is only available in certain XProtect VMS systems. For more information, see the product comparison chart: https://www.milestonesys.com/solutions/platform/product-index/

Enable detailed bookmarks

To be able to give bookmarks a name and a description and changing the default time span, you must enable details.

Steps:

1. On the global toolbar, select **Settings and more** and then **Settings** to open the **Settings** window.



2. Select the **Functions** tab.
3. To enable detailed bookmarks for live video, switch to live mode and select **Add bookmark details** in the **Bookmark** list.
4. To enable detailed bookmarks for recorded video, switch to playback mode and select **Add bookmark details** in the **Bookmark** list.
5. Click **Close**.

Carousels (configuration)

Before you can use the carousel, you must:

1. Add the carousel to a view.
2. Specify the cameras you want to include in the carousel.

Add carousels to views

Carousels let you constantly browse between the cameras of the carousel at a speed you define.

1. Click **Setup** to enter setup mode.
2. In the **System overview** pane, drag the **Carousel** item to a view item.
3. In the **Carousel setup** window:
    1. Go to the **Cameras** section.
    2. Locate and double-click each camera you want to add to the carousel.
4. To define the sequence the cameras appear in the carousel, in the **Selected cameras** list, move the cameras up or down.
5. Enter the number of seconds each camera appears in the carousel. You can specify a value for all cameras, or for each camera.
6. Click **OK** to close the **Carousel setup** window.
7. Click **Setup** again to exit setup mode. Your changes are saved.
8. (optional) To change settings for the carousel, in the setup mode, go the **Properties** pane and click **Carousel setup**.

Edit the carousel settings

In the carousel settings, you can add or remove cameras from the carousel, change the order of cameras, or change the time settings.

1. Click **Setup** to enter setup mode.
2. Select the view item with the carousel.
3. On the left-hand side, scroll down to the **Properties** pane.
4. Click **Carousel setup**. A window appears.
5. Make the required changes, and click **OK**.
6. Click **Setup** again to exit setup mode. Your changes are saved.

The **Live stream**, **Image Quality**, **Frame Rate**, and **Maintain image aspect ratio** settings in the **Properties** pane apply to all cameras in the carousel.

Hotspots (configuration)

Before you can use the hotspot, you must:

1. Add the hotspot to a view. See Add hotspots to views on page 77.
2. Specify the hotspot settings. See Hotspot settings on page 77.

Add hotspots to views

If your view contains a hotspot, and you click a camera, the video feed from the camera is displayed in a high resolution in the hotspot view item.

Steps:

1. Click **Setup** to enter setup mode.
2. In the **System overview** pane, click and drag the **Hotspot** item to the required view item in the view. The view item displays a hotspot icon: .
3. Click **Setup** again to exit the setup mode.
4. (optional) To set the properties for the hotspot, in setup mode, go to the **Properties** pane.

To save bandwidth, you can specify a low image quality for the other view items in your view and a high quality for the hotspot.

Hotspot settings

In the **Properties** (see Camera settings on page 66) pane, you can specify the settings for the hotspot. The **Live stream**, **Image Quality**, **Frame Rate**, and **Maintain Image Aspect Ratio** settings apply to all cameras in the hotspot.

To make the properties appear, you must select the view item and then click **Setup**.

PTZ presets (configuration)

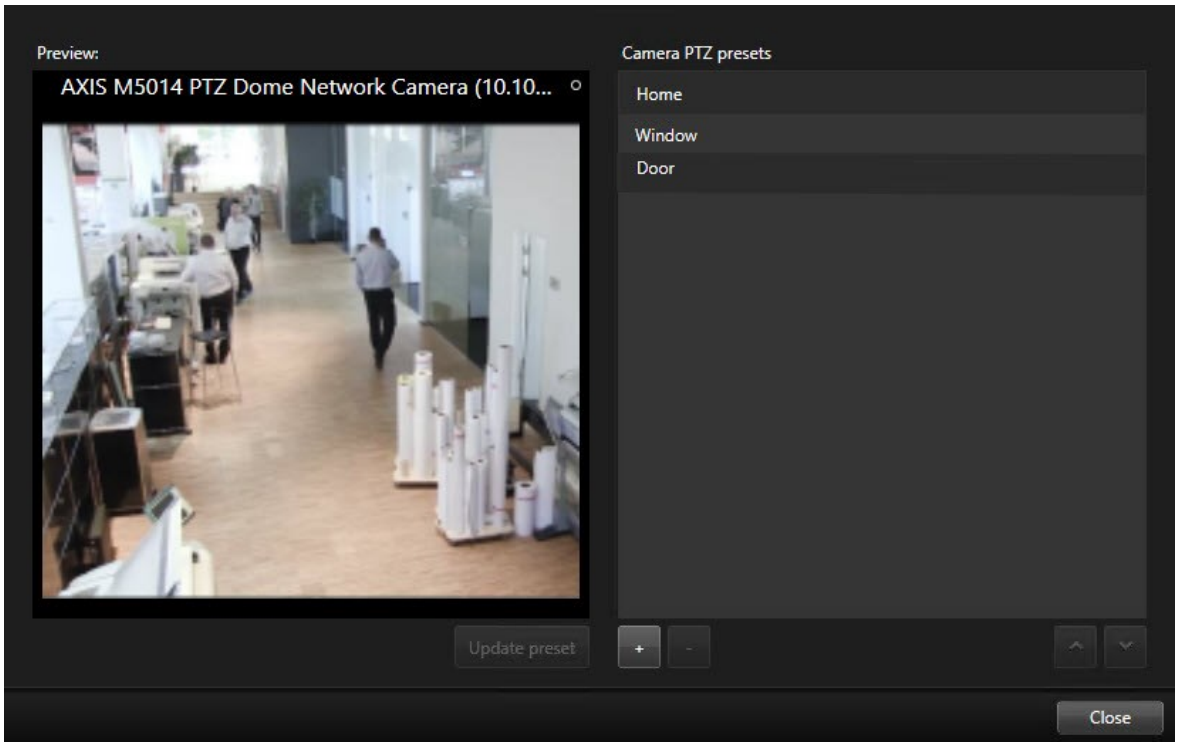
Depending on your surveillance system (see Surveillance system differences on page 33), you can create, edit, and delete PTZ presets.

You define a camera's Home preset position on the camera's homepage. The PTZ capabilities available on the homepage depend on the camera.

Add PTZ presets

You can define additional PTZ presets:

1. In the view, select the relevant PTZ camera that you want to give a new PTZ preset.
2. On the camera toolbar, click the PTZ icon to open the PTZ menu.
3. Click **Manage PTZ presets** to open the window.



4. Click + to add a new preset entry.
5. Select the PTZ preset entry and enter a new name for the PTZ preset.
6. Use the PTZ buttons to navigate to the relevant position and click **Update preset** to save.
7. Use the arrows to move a PTZ preset up or down in the list. This can be useful if your list contains many presets.

Edit PTZ presets

You can make changes to existing PTZ presets, such as renaming or changing the preset position:

1. In the view, select the PTZ camera with the PTZ preset you want to modify.
2. On the camera toolbar, click the PTZ icon to open the PTZ menu.
3. Click **Manage PTZ presets** and in the dialog box, select the PTZ preset.

4. To edit the name of the preset, ensure the name of the PTZ preset is highlighted. Click the text and overwrite the existing name.
5. If the camera is not in the correct position, use the PTZ buttons to navigate to the required position and then click **Update preset** to save.
6. Use the up or down arrows to arrange the PTZ presets on the list.
7. Click **Close**.

Delete PTZ presets

To delete an existing preset, select it and click  .

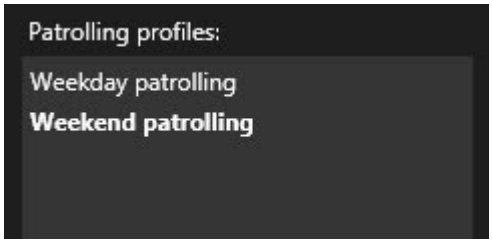
Patrolling profiles (configuration)

Depending on your surveillance system (see Surveillance system differences on page 33), you can create, edit, and delete patrolling profiles.

Add patrolling profile

When you add a patrolling profile, you and other users can see the new patrolling profile in the PTZ menu.

1. In the view, select the relevant PTZ camera where you want to add a new patrolling profile.
2. On the camera toolbar, click the PTZ icon  to open the PTZ menu.
3. Click **Manage patrolling profiles** to open the dialog box.
4. Follow the steps below and click **OK** to close the **Manage patrolling profiles** window.
5. Click  below the **Patrolling profiles** list to add a new patrolling profile.
6. Enter a name for the profile and press **Enter**. You can always rename it later.



The new patrolling profile is added to the **Patrolling profiles** list. You can now specify the positions and other settings for the patrolling profile.

Delete patrolling profile

To delete an existing profile, select the profile and click  .

Edit patrolling profile

Specify positions in a patrolling profile

1. Select the patrolling profile:

2. Click  below the **Positions** list to add a PTZ preset.

   PTZ presets are defined by your system administrator. Depending on your user permissions, you can define PTZ presets by selecting **Manage PTZ presets** (see PTZ presets (configuration) on page 77).

3. In the list, select a PTZ preset.

4. Repeat adding presets until you have selected all necessary positions in the patrolling profile:

5. Use the up or down arrows to move a PTZ preset in the list.

   The camera uses the PTZ preset at the top of the list as the first stop when it patrols according to the patrolling profile. The PTZ preset in the second position from the top is the second stop, and so forth.

Specify the time on each position

When patrolling, the PTZ camera by default remains for five seconds on each position specified in the patrolling profile.

To change the number of seconds:

1. Select the patrolling profile in the **Patrolling profiles** list.
2. Select the PTZ preset that you want to change the time for in the **Positions** list:

3. Specify the time in the **Time on position (sec)** field.
4. If required, repeat for other presets.

Specify an end position

You can specify that the camera should move to a specific position when patrolling ends. You do that by selecting an end position on the patrolling profile.

1. Select the patrolling profile in the **Patrolling profile** list.
2. Below **On finish, go to**, select one of the presets from the drop-down list as the end position.

> You can select any of the camera's PTZ presets as the end position, you are not limited to the presets used in the patrolling profile. You can also choose not to specify an end position at all, but to keep the default setting: **No end position**.

Alarms and events (configuration)

Add alarms to views

By adding the following items to your views, you can share a list of prioritized alarms allowing operators to put focus on and respond to alarm-related incidents. Typically, you would add both of the following to the same view:

- The **Alarm List** shows a prioritized list of alarms and has multiple filtering options
- The **Alarm Preview** lets you preview video from the alarm that is selected in the **Alarm List**

> To perform the following steps, you need a view layout with at least two view items.

Steps:

1. On the **Views** pane, select the view where you want to add the **Alarm List** and the **Alarm Preview**.
2. Click **Setup** to enter setup mode.
3. On the **System overview** pane, expand **Alarms** and drag the **Alarm List** to a view item.
4. Drag the **Alarm Preview** to a different view item.
5. Click **Setup** again to exit setup mode. Your changes are saved.

Alarm list settings

In setup mode, you can select whether or not you want to see the alarms or events grouped by servers in a navigation tree and how many alarms or events you want the list to display at a time. This is also where you specify whether you want the alarm list to display alarms or events.

Name	Description
Show navigation tree	Select to display the navigation tree on the left of the alarm list. The navigation tree lets you view alarms or events grouped by server and filter for alarms with different states.
Max. rows to fetch	Controls the maximum number of lines to fetch and display in the alarm list. By default, the alarm list displays up to 100 alarms or events at a time. This provides a good response time because retrieving and displaying larger numbers of alarms or events can take time. If there are more than 100 alarms or events, click the following button to view and retrieve the next 100 alarms:  In the field, you can set the maximum numbers of rows from 1 to 999.
Data Source	Select whether you want to display a list of alarms or events in the **Alarm List**. The event list does not display system or user-generated events, such as motion detection or archive failure.

Alarm preview settings

If alarms or events have video associated with them, when you select a particular alarm in the **Alarm List**, the alarm preview displays the recorded video from the selected alarm or event. If there are many cameras associated with an alarm, or if you have selected more than one alarm, the preview displays several previews.

If there is no video associated, the alarm preview will be gray. You can change the alarm preview's properties in setup mode.

Name	Description
Show duplicate cameras	Select to display video from duplicate cameras several times in the alarm preview. The alarm preview reflects what is selected in the alarm list. Because you can select multiple alarms or events, video from the same camera may appear several times in the alarm preview if some of the selected alarms or events relate to the same camera.
Show event source cameras	Select to display video (if any) from the camera for which the alarm or event has been set up on the surveillance system server.  We do not recommend clearing this field.
Show related cameras	Select to display video from related cameras in the alarm preview. You can display associated video from up to 16 related cameras for a single alarm or event. You cannot determine the number of related cameras in the XProtect Smart Client; the number may vary from alarm to alarm, and is specified as part of the surveillance system configuration.
Show overlay	Only relevant if using the alarm preview together with a plug-in capable of displaying overlay information, such as lines tracking the paths of moving objects, or similar. This is not standard functionality in the XProtect Smart Client.

Smart map (configuration)

Before you can take advantage of the smart map features, you must go through certain configuration tasks in XProtect Smart Client.

You can only view your smart map if it has been added to a view. See also Add smart map to views on page 84.

 For more information, see Smart map (explained) on page 260.

Differences between maps and smart maps (explained)

XProtect Smart Client offers map features that can help you visualize your surveillance system and quickly respond to incidents.

- **Maps** - these maps are based on still images that do not contain geographical references. You can add devices such as cameras, microphones, and recording servers. You can also add alarms, events, and access controls that let you interact with your surveillance system directly from the map. You must manually position device and feature elements on the map. For more information, see Maps (explained) on page 271
- **Smart map** - this type of map uses a geographic information system to accurately reflect geography in the real world. This can give you a more exact overview of your cameras in multiple locations. You can also:
  - Use the Bing Maps and the Google Maps services
  - Use the Milestone Map Service as geographic backgrounds
  - Use the OpenStreetMap map project as geographic backgrounds
  - Add computer-aided design (CAD) drawings, shapefiles, and images as overlays

  For more information, see Smart map (explained) on page 260

Maps and smart maps are not interchangeable. If you are using maps, you can use the image file as a smart map, but you must add the devices again. You cannot transfer maps with devices to a smart map. You can, however, link a smart map to maps. For more information, see Adding, deleting, or editing links on smart map on page 100.

Add smart map to views

Start using a smart map by adding it to a view. By default, the basic world map is displayed. After you add the smart map, you can change the geographical background.

Steps:

1. In live or playback mode, select the view that you want to add to the smart map.
2. Click **Setup** to enter setup mode.
3. Expand the **System overview** pane, and then drag the **Smart map** item to the relevant position within the view.
4. Click **Setup** again to exit setup mode. Your changes are saved.
5. Now you can change the geographic background.

Change geographic backgrounds on smart maps

By default, the basic world map displays when you add a smart map to a view. After you have added the smart map to a view, you can select a different geographic background. Every user who uses the smart map sees the new background the next time that they display this view.

Requirements

The Bing Maps and Google Maps geographic backgrounds are available only if your system administrator has made them available in XProtect Management Client.

Steps:

1. Select the view that contains the smart map.
2. In the toolbar, click **Show or hide layers and custom overlays**.
3. Under **Geographic backgrounds**, select the background and the type of detail that you want to display. For example, if you want to see topographical information, select **Terrain**. If you want to see roads, select **Road**.

Geographic backgrounds (explained)

You can use the following services as the geographic backgrounds of your smart map:

- Bing Maps
- Google Maps
- Milestone Map Service
- OpenStreetMap

After you have selected the geographic background, you add the devices, for example cameras, and custom overlays, for example shapefiles. For more information, see Custom overlays (explained) on page 91.

Types of geographic backgrounds (explained)

After you have added a smart map to a view, you can use one of the following geographic backgrounds:

- **Basic world map** - use the standard geographic background provided in XProtect Smart Client. This map is intended for use as a general reference, and it does not contain features such as country boundaries, cities, or other details. However, like the other geographic backgrounds, it does contain geo-reference data
- **Bing Maps** - connect to Bing Maps
- **Google Maps** - connect to Google Maps

  > The Bing Maps and Google Maps options require access to the internet, and you must purchase a key from Microsoft or Google.

- **Milestone Map Service** - connect to a free map provider. After you enable Milestone Map Service, no further setup is needed.

See Enable Milestone Map Service

- **OpenStreetMap** - connect to:
  - A commercial tile server of your own choice
  - Your own, online or local tile server

  See Change OpenStreetMap tile servers

- **None** - this option hides the geographic background. Note that the geo-reference data remains there. See also Layers on smart map (explained) on page 89

By default, Bing Maps and Google Maps display satellite imagery. You can change the imagery, for example to aerial or terrain, to see different details.

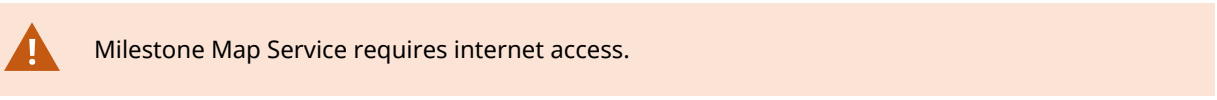
Enable Milestone Map Service

Milestone Map Service is an online service with which you can connect to a tile server of Milestone Systems. This tile server uses a free, commercially available map service.

After you enable Milestone Map Service on your smart map, the smart map uses Milestone Map Service as its geographic background.

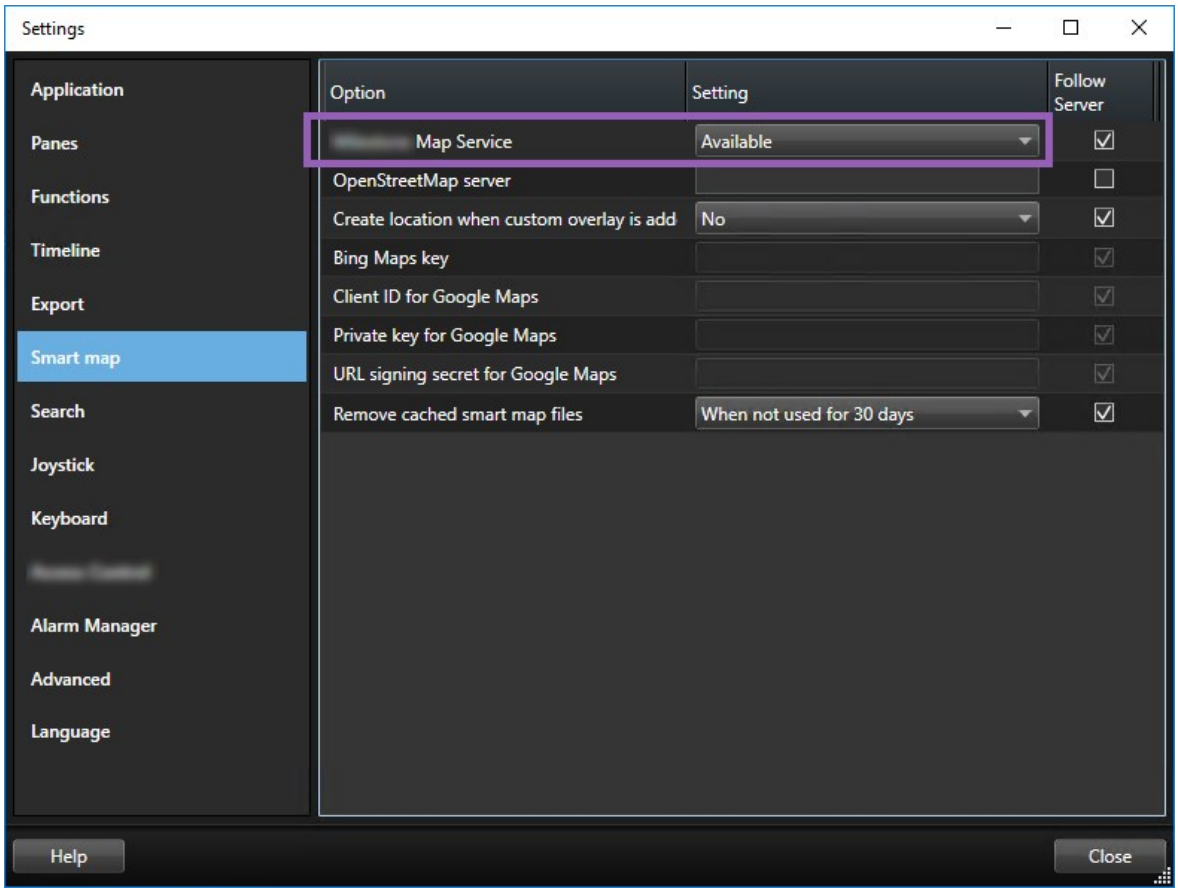
Requirements

If the Milestone Map Service field is grayed out, you don't have the necessary user permissions to enable or disable the service. Contact your system administrator to help you enable the feature in XProtect Management Client.



Steps:

1. On the global toolbar, select **Settings and more** and then **Settings** to open the **Settings** window.



2. In the left section, click **Smart map**.
3. In the **Milestone Map Service** field, select **Available**.
4. Click **Close**. Next time you load your smart map, it uses Milestone Map Service as the geographic background.

OpenStreetMap tile server (explained)

If you use OpenStreetMap as the geographic background for your smart map, you need to specify a tile server. You can specify a local tile server, for example if your organization has its own maps for areas such as airports or harbors, or you can use a commercial tile server.

To use a local tile server, you do not need internet access.

The tile server address can be specified in two ways:

- In XProtect Management Client - you set the tile server address on the Smart Client profiles. The server address applies to all XProtect Smart Client users assigned to the Smart Client profiles
- In XProtect Smart Client - you set the tile server address in the **Settings** dialog. The server address applies only to that installation

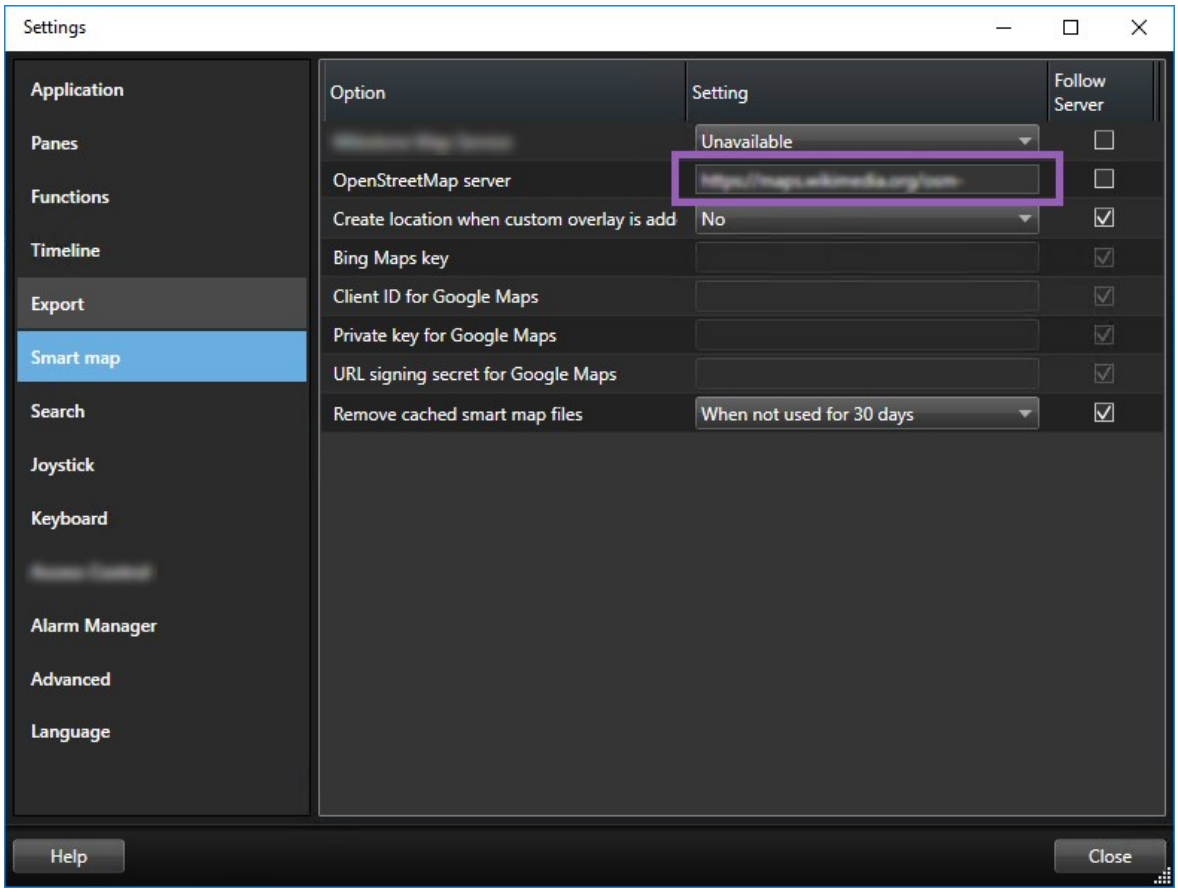
Change OpenStreetMap tile server

Requirements

If the tile server specified server-side has been locked for editing, the field is grayed out and you cannot change the server address. Please contact your system administrator to help you enable the feature in XProtect Management Client.

Steps:

1. On the global toolbar, select **Settings and more** and then **Settings** to open the **Settings** window.



2. In the left section, click **Smart map**.

3. In the **OpenStreetMap server** field, do one of the following:
    - Enter the server address. If the field is grayed out, it has been locked server-side
    - To use the server specified server-side, if any, select the **Follow server** check box
4. Click **Close**. Next time you load your smart map, it will use the OpenStreetMap server that you have specified.

If no server address is specified, or the server address is invalid, then OpenStreetMap is not available as a geographic background.

Showing or hiding layers on smart map

You can turn layers on and off on your smart map depending on what you want to see.

Layers on smart map (explained)

Use layers to filter the information that the smart map displays. There are three types of layers on a smart map:

- **System elements** - include cameras, links, and locations
- **Custom overlays** - bitmap images, CAD drawings, and shapefiles
- **Geographic backgrounds** - the basic world map or one of the following services:
    - Bing Maps
    - Google Maps
    - Milestone Map Service
    - OpenStreetMap

Bing Maps and Google Maps are available as geographic backgrounds only if your system administrator has enabled them in XProtect Management Client. For more information, see Geographic backgrounds (explained) on page 85.

Order of layers (explained)

All system elements of each type are on the same layer. For example, all cameras are on the same layer. If you hide the camera layer, all cameras are hidden. From top to bottom, layers for system elements are arranged in the following order: locations, cameras, links, and geographic background. You cannot change this order.

The geographic background is always the lowest layer on a smart map. You can switch between geographic backgrounds, but you can select only one geographic background at a time.

Custom overlays are added as separate layers, and are stacked in the order in which they were added to the smart map. You rearrange the order by configuring default settings for the map.

Example

A city planner has a shapefile that shows the city boundaries, and a shapefile that includes all major roads within the city. The planner can arrange the order of layers so that the roads display on top of the city boundaries. This gives a general view of where cameras are in the city, and the ability to zoom in to see the name of the street that a particular camera is on.

Show or hide layers on smart map

You can show or hide layers on your smart map, including the geographical background. For example, this is useful when you want to focus on a particular element, or just simplify the content that the smart map is displaying.

Steps:

1. On the toolbar, click **Show or hide layers and custom overlays**.
2. To show or hide system elements and custom overlays, select or clear the check boxes.
3. To hide the geographic background, select **None**.

Selecting **None** hides the geographic background, but the geo-references still apply to the smart map. For example, if you add a new shapefile that contains spatial reference, the system still uses the spatial reference to place the file on the map.

Hiding microphones will mute the currently unmuted microphone until you show microphones again.

Specify default settings for smart map

After adding a smart map to a view, and you have added the overlays, cameras, and links, you can specify the default settings for the custom overlays. You can also delete custom overlays to clean up.

Steps:

1. Click **Setup**.
2. Click **Manage default settings**.
3. Do any of the following:
   - To show or hide an overlay, select or clear the check box
   - To rearrange the order, use the drag handle in front of the overlay to drag it to a new position in the list. Layers are ordered from top to bottom in the list
   - To delete an overlay, hover the pointer over the overlay, and then click **Delete**
4. Click **Save**.

Adding, deleting, or editing custom overlays

Custom overlays (explained)

You can add the following types of files as custom overlays on a smart map in XProtect Smart Client:

- **Shapefile** - can contain geo-spatial vector data, such as points, lines, polygons, and attributes that represent objects on a map, such as walls, roads, or geographical features like rivers or lakes. For example, city planning and administration offices often use shapefiles because they scale well when you zoom in and out, and their file size is often smaller than CAD drawings or bitmap images
- **CAD** - a computer-aided design (CAD) drawing is useful as an overlay because, like shapefiles, CAD data can use a coordinate system and spatial reference to provide accurate geographical context. For example, you can use a detailed ariel map or a road map of a location
- **Image** - if you have an image file, such as the floor plan of a building, you can add it as an overlay on the smart map. You can use the following types of image files: PNG, BMP, GIF, JPG, JPEG, PHG, TIF, and TIFF

To put custom overlays into focus, you can temporarily hide other types of layers. See Layers on smart map (explained) on page 89.

Custom overlays and locations (explained)

You can quickly jump to custom overlays that you have added to your smart map as described in Jump to custom overlays on smart map on page 270. However, in the settings, you can establish a connection between custom overlays and locations. This means that whenever you add a new custom overlay, XProtect Smart Client creates a location with the same name as the overlay on the exact same spot on the map. The location of the custom overlay now becomes available in the **Select a location** list.

The overlay and location are not linked. For example, you can delete or rename the location without changing the overlay, and vice versa.

To turn on this feature, see Add locations to custom overlays (smart map) on page 93.

Add custom overlay on smart map

Increase the level of detail on your smart map by adding custom overlays. When you add a custom overlay, XProtect Smart Client creates a location with the same name as the overlay.

Steps:

1. Select the view that contains the smart map, and then click **Setup**.
2. Click **Add a custom overlay**:
   - If the overlay is geo-referenced, click anywhere on the smart map. XProtect Smart Client uses the geo-reference information to place the overlay in the correct geographic location. Additionally, the smart map will center on the overlay at a default zoom level
   - If the overlay is not geo-referenced, go to the point on the map where you want to add the element, and then click the point on the smart map

     Before you add an overlay, it's a good idea to zoom in to the place on the map where you want to put it. This makes it easier to accurately position the overlay.
3. Enter a name for the overlay.

4. Depending on the file type you select:
   - **Image** - select the image file, and then click **OK**
   - **Shapefile** - select the SHP file. If you have a PRJ file, XProtect Smart Client will find it, and you can just click **OK**. If you do not have a PRJ file, you can reposition the overlay manually after you add it. You can also apply a color. For example, adding a color can make the shapefile stand out more on the smart map
   - **CAD** - select the DWG file. If you have a PRJ file, click **OK**. If you do not have a PRJ file, and you want to use geo-referencing to position the file on the smart map, enter the spatial reference identifier (SRID), and then click **OK**. If you do not have a PRJ file or an SRID, you can reposition the overlay manually after you add it

     For more information about the types of overlays, see Custom overlays (explained) on page 91.

Add locations to custom overlays (smart map)

You can configure XProtect Smart Client to automatically add locations to custom overlays on your smart map. This allows you to jump to the custom overlays through the **Select a location** list.

Steps:

1. On the global toolbar, select **Settings and more** and then **Settings** to open the **Settings** window.
2. Go to the **Smart map** tab.
3. In the **Create location when layer is added** list, select **Yes**.
4. Close the dialog to save the changes.

For more information, see Custom overlays and locations (explained) on page 91.

Delete custom overlay on smart map

1. Select the view that contains the smart map, and then click **Setup**.
2. In the toolbar, click **Manage default settings**.
3. Hover the pointer over the custom overlay, and then click **Delete**.
4. Click **Save** to delete the custom overlay.
5. Optional: If a location was created for the custom overlay, you might want to delete that as well. For more information, see Adding, deleting, or editing locations on smart map on page 101.

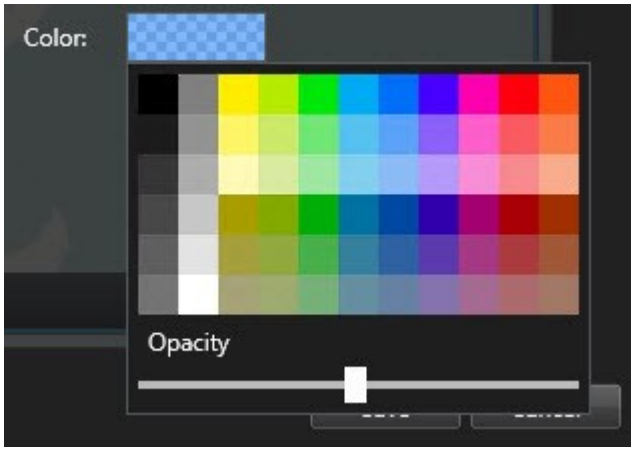
Make areas in shapefiles more visible (smart map)

This topic is relevant only if you are using shapefiles with polygons.

If you want to use a shapefile on your smart map that consists of polygons in close proximity, you may need to distinguish the individual polygons from each other. You do that by decreasing the opacity of the color you pick for the shapefile. The borders of the polygons will stand out.

Steps:

1. Follow the steps described in Add custom overlay on smart map on page 92.
2. When selecting the color, drag the **Opacity** slider to the left until you are ok with the level of transparency.



3. Click **Save**.

Adjust position, size, or alignment of custom overlay

You can move an overlay to a different place on the map, make it larger or smaller, and rotate it. For example, this is useful if your overlay is not geo-referenced, or the overlay is geo-referenced but for some reason does not align exactly with the geographic background.

Steps:

1. Select the view that contains the smart map, and then click **Setup**.
2. Right-click the overlay, and select **Edit position**.
3. To resize or rotate the overlay:
   - Click and drag a corner handle
   - To rotate the overlay around a specific point, move the pivot point to that place on the map. Then click and drag a corner handle

4. To move the overlay on the map, click and drag the overlay.
5. To save the change, click **Save**.

Adding, deleting, or editing devices on smart map

You can add devices to a smart map in their actual positions in your environment. This gives you a good overview of your surveillance system, and can help you respond to a situation. For example, if you want to follow a suspect during an ongoing incident, you can click the cameras on the map to view their footage.

After you add a camera to a smart map, you can adjust the field of view for the camera icon so that it reflects the field of view of the actual camera. This makes it easy to find the camera that is covering a particular area. Additionally, you can select an icon to represent the camera on the map, which can help you identify the type of camera on the map.

You can work with the following device types on smart maps:

- Cameras
- Input devices
- Microphones

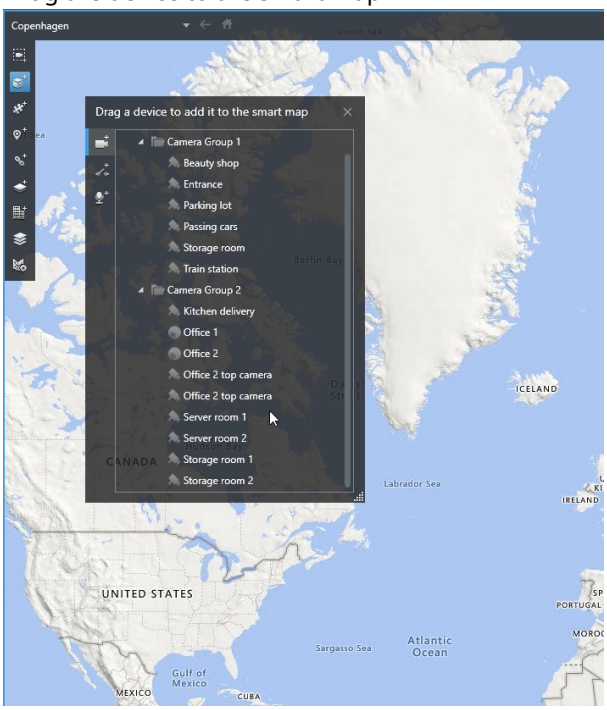
Add devices to smart map

If the geo coordinates of the device have been specified in XProtect Management Client by your system administrator, the device will automatically be positioned on the smart map when you add it. If not, you must position the device yourself in its exact geographic location.

1. Select the view that contains the smart map, and then click **Setup**.
2. To add a device or a group of devices:

   > Before you add the device, it's a good idea to zoom in to the location on the map. This makes it easier to accurately position the device.

   - Expand the **System overview** pane, find the device or device group, and then drag it to the point on the smart map where you want to display it. You can drag devices afterward to reposition them
   - On the smart map toolbar, select  **Add a device** > select the device type.
     - Example: In the case of a camera, select  **Add a camera**, and then select the camera.
   - Drag the device to the smart map



3. To save the change, click **Setup** to exit setup mode.

Change field of view and direction of camera

Once the camera has been added to the smart map, you can change field of view and direction by adjusting the camera icon.

> If you are zoomed out on the map, you may have to zoom in until the field of view is displayed.

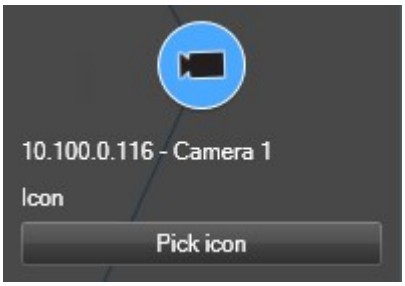
1. Select the view that contains the smart map that you want to work with.
2. Click **Setup** to edit the camera icon.
3. Click the camera icon.

4. Use the rotate handle to point the camera in the right direction.
5. To adjust the width, length, and angle of the field of view, click and drag the handles at the front edge of the field of view.
6. To save your changes, click **Setup** to exit setup mode.

Select or change device icon

You can choose a device icon that matches the type of device that you are using.

1. Select the view that contains the smart map that you want to work with.
2. Click **Setup**, and then double-click the device icon on the map.



3. Click **Pick icon**, and then select the icon for the device.
4. Click **Setup** again to save the change.

Show or hide device information

You can show or hide information about devices on a smart map. This is useful, for example, when you want to increase or reduce the amount of content on your smart map.

1. Select the view that contains the smart map that you want to work with.
2. Click  **Show or hide layers and custom overlays**.
3. Select or clear the check boxes for the information to show or hide.

Listen to audio from microphone on smart map

After you add microphones to a smart map, you can listen to audio from one microphone at a time in live mode.

Steps:

1. In live mode, navigate to the place on the smart map where the microphone is placed.
2. Double-click the microphone to mute or unmute it.

> Alternatively, right-click the microphone and select **Mute microphone** or **Unmute**.

Remove devices from smart map

You can remove devices, for example if devices have been physically removed or were added by mistake. By removing a device, the positioning information of the device, for example the geo coordinates, are removed from your VMS system.

Requirements

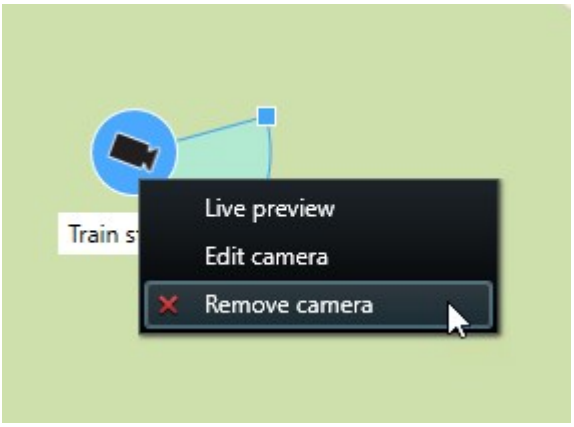
These user permissions must be enabled in XProtect Management Client:

- Editing of smart maps
- Editing of devices

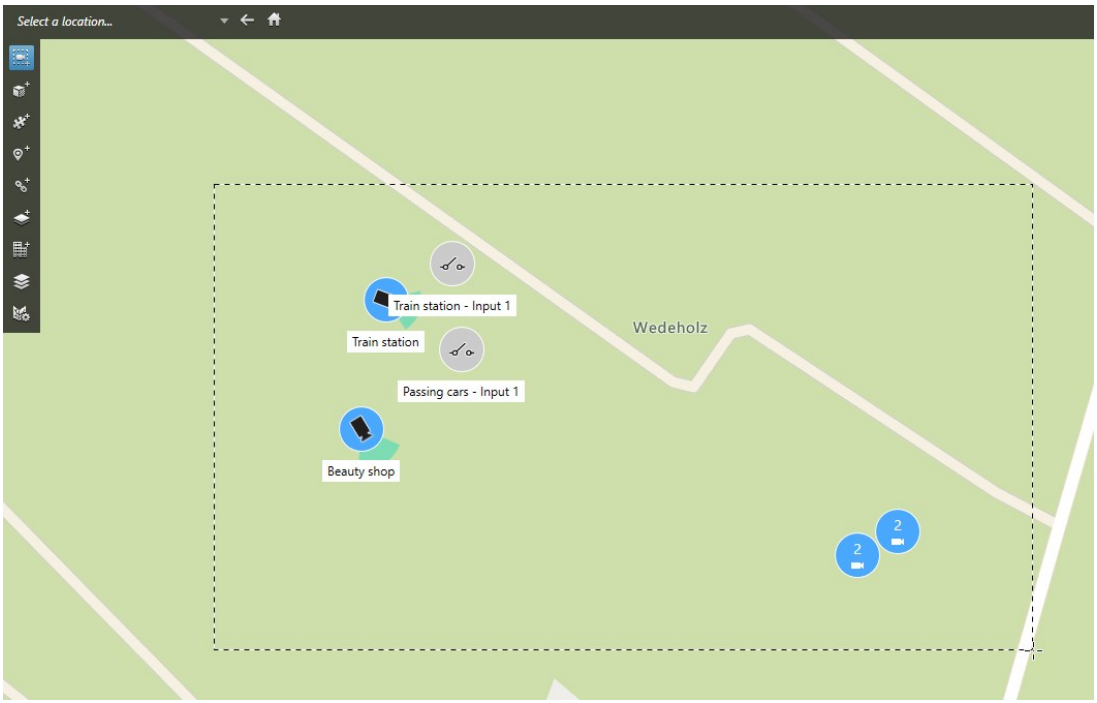
Steps:

1. Navigate to the device that you want to remove.
2. Click **Setup** to enter setup mode.
3. To remove a single device, right-click the device and click **Remove**.

   Example: In the case of a camera, click **Remove camera**.



4. To remove several cameras:
   1. On the smart map toolbar, click **Select multiple cameras**.



   2. Click and drag to select multiple cameras. Other types of devices, for example input devices, are not included in the selection.
   3. Right-click and select **Remove cameras**.

5. To remove several devices that are not cameras:
    1. On the smart map, press and hold Ctrl.
    2. While holding down Ctrl, click the devices that you want to remove.
    3. Right-click one of the selected devices and select Remove.
6. Click **Setup** again to exit setup mode. Your changes are saved.

You can also delete a single device by selecting it and then pressing **DELETE** on your keyboard.

Adding, deleting, or editing links on smart map

Links on smart map (explained)

You can add links that go to locations on your smart map, or go to the static maps in XProtect Smart Client. This lets you quickly visit locations, or display another type of map without changing to another view. You cannot link to another smart map. For more information, see Differences between maps and smart maps (explained) on page 83.

Links display locations and maps as follows:

- A link to a location displays the location in the current view. To return to a location that you previously viewed, click **Back** on the smart map toolbar
- A link to a map displays the map in a floating window. This lets you access both types of maps at the same time. You can view and interact with the map but you cannot make changes in the floating window, such as adding cameras

If you color code links, or want to make them more visible on the map, you can specify a color for the link. By default, links to smart map locations are blue, and links to legacy maps are red. If you use a different color, it is a good idea to use the same color for each type of link. For example, this can make it easier to distinguish between links when you use layers to filter items on the map.

Add link to smart map location or map

Adding links to your smart map lets you quickly visit locations, or display another type of map without changing to another view.

Steps:

1. Select the view that contains the smart map, and then click **Setup**.
2. Go to the point on the map where you want to add the link.
3. In the map toolbar, click **Add a link**, and then click the point on the map where you want the link to be.
4. Specify whether you want to link to a smart map location, or a map, and then click **Add**.
5. Enter a name for the link.

   You can display the title of the link on the smart map if you select **Icon and text** as the display style. Typically, names indicate where the link takes you.

6. In the **Destination** field, select the map or location that the link goes to.
7. In the **Display style** field, specify whether to display the name and link icon, or only the link icon on the map.
8. Optional: Click **Color** to specify a color for your link.

Edit or delete link on smart map

Once you have added a link on your smart map, you can edit or delete it.

Steps:

1. Click **Setup** to enter setup mode.
2. To edit the link, right-click the link and select **Edit link**.
3. To delete the link, do one of the following:
   - Right-click the link and select **Delete link**
   - Select the link and press **DELETE** on your keyboard

Adding, deleting, or editing locations on smart map

Locations on smart map (explained)

You can create locations at the points on the smart map that are of interest to you. For example, you can create locations for your home office, and satellite offices. Not only do locations give you a full picture of your environment, they are also useful for navigating the smart map.

Depending on your configuration, when you add a custom overlay, XProtect Smart Client may add a location with the same name as the overlay. For example, this makes it easier to go to the overlay on the smart map when you are zoomed out. The overlay and location are not, however, linked. For example, you can delete or rename the location without changing the overlay, and vice versa. For more information, see Adding, deleting, or editing custom overlays on page 91.

Home locations for smart map (explained)

Home locations are specific to the view item they are set in. You can have different home locations in different view items. If a home location is not specified for a view item, the view item displays the whole world, regardless of the type of background you are using. This is also the case if you delete the home location.

While you are working with the smart map, you can click **Home** to return to the home location. This is similar to resetting the smart map in the view. You return to the default settings for the view item, and the system deletes the history of the locations you visited.

Selecting a new home location affects everyone who uses the view item. If someone else had set another location as home, you are changing their setting.

Add location to smart map

To keep track of the places that are of interest to you, you can add locations that allow you to quickly navigate to those places on the smart map.

Steps:

1. Select the view that contains the smart map, and click **Setup**.
2. If needed, pan and zoom in to the point on the smart map where you want to add the location.
3. In the toolbar, click **Add a location**, and then click the point on the smart map.
4. Give the location a name, and then add the following optional details:
   - Specify a zoom level to apply when someone goes to the location on the smart map
   - Select a color for the location icon. Color-coding locations is useful, for example, for distinguishing between types of locations. This could be based on the function of the location or its type, or indicate the location's priority
   - Optional: Make the location your home location. The smart map centers on this location, and applies the default zoom level setting for it, when you click **Home**

Edit or delete location on smart map

Once you have added locations on your smart map, you can delete them or edit the settings, for example deleting the home location.

Steps:

1. Click **Setup** to enter setup mode.
2. To edit a location, right-click the location and select **Edit location**.
3. To delete a location, do one of the following:
    - Right-click the location and select **Delete location**
    - Select the location and press **DELETE** on your keyboard

Linking between locations (explained)

For example, you can create a patrol route by creating a series of links between locations. Create a link at location A that goes to location B, and a link at location B that goes to location C, and so on. For more information, see Adding, deleting, or editing links on smart map on page 100.

Adding, deleting, or editing buildings on smart map

Buildings on smart map (explained)

Buildings on the smart map are depicted as polygons with four edges. Once added, you can adjust the dimensions, angles, and size to match the actual shape and position of the building.

If the building is a multistory building, you can start adding levels and add cameras to the individual levels. This allows you to navigate the cameras inside the building, level by level.

To help you illustrate the interior of a level, you can add custom overlays to levels, for example an image illustrating a floor plan. For more information, see Add floor plans to levels (smart map) on page 108.

Buildings are automatically given a name, for example **Building 4**. Milestone recommends that you change the name. This makes it easier for you to distinguish buildings from one another.

Add buildings to smart map

Instead of using images or shapefiles to illustrate buildings, you can add an outline of a building. Afterwards, you can change the dimensions, angles, and size to match the shape and position of the actual building.

Requirements

Smart map editing has been enabled on your Smart Client profile in XProtect Management Client.

Steps:

1. Click **Setup** to enter setup mode.
2. Navigate to the place on the smart map, where you want to position the building.
3. Click  and place the cursor in the relevant position on the smart map.
4. Click again. A rectangle is added to the smart map. If zoomed out, the zoom level automatically increases.
5. If necessary, use the corner handles to adjust the shape and position of the actual building.
6. Click **Setup** again to exit setup mode. Your changes are saved.

Edit buildings on smart map

Once a building has been added to the smart map, you can change the name of the building, and adjust the position, the size, dimensions, and angles. You can also add, remove, or reorder levels.

Requirements

Smart map editing has been enabled on your Smart Client profile in XProtect Management Client.

Steps:

1. Navigate to the building on your smart map. If necessary, zoom in.
2. Click **Setup** to enter setup mode.
3. Click anywhere inside the building. A blue-ridged border indicates that you can edit the building.

4. To rename the building, go to the top of the right-side pane and click  . Change the name and click  . To cancel, press **Esc**.
5. To adjust the corners, click and drag them to a new position.
6. To add or remove levels, see Add or remove levels from buildings (smart map) on page 106.
7. Click **Setup** again to exit setup mode. Your changes are saved.

Delete buildings on smart map

If a building is no longer needed, you can delete it. Next time someone logs into XProtect Smart Client or reloads, the building is gone.

Requirements

Smart map editing has been enabled on your Smart Client profile in XProtect Management Client.

Steps:

1. Open the smart map.
2. Click **Setup** to enter setup mode.
3. Do one of the following:
   - Right-click the building and select **Delete**
   - Select the building, and press **DELETE** on your keyboard

An alternate way of deleting a building: In the  **Manage default settings**, scroll down to the **Buildings** section, hover on the building, click **Delete** and then **Save**.

Managing levels and devices in buildings (smart map)

Devices and levels in buildings (explained)

When you add a device to a building, by default, the device is associated with the default level if one has been specified. Otherwise, the device is assigned to the first level. However, you can change this and associate the device with any other level, or several levels at the same time.

More facts:

- If no levels are selected, the device is visible on all levels
- If you add a building on top of a device that is already positioned, by default, the device is associated with all levels
- If you expand the boundaries of a building so that it covers a device that is already positioned, the device is associated only with the level that is selected

If you readjust the boundaries of the building so that it no longer covers the device, the device is no longer associated with the building.

Floor plans and devices in buildings (explained)

To help you visualize the interior of the levels in a building, you can add floor plans as custom overlays. With a floor plan in place, it is easier to precisely position the device. For more information, see Add floor plans to levels (smart map) on page 108.

The devices that you position are associated with levels, not custom overlays. If you delete a level inside a building with devices and a custom overlay, the devices stay in their geographical position, but are no longer associated with the level. However, the custom overlay is deleted together with the level.

If you reorder a level, both the devices and the custom overlay stay with the level. The devices maintain their geographical position.

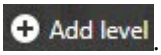
Add or remove levels from buildings (smart map)

After adding a building to your smart map, you can add any number of levels. The first level is assigned the number **1**, the next **2**, and so forth. Afterwards, you can rename and reorder the individual levels.

Requirements

Smart map editing has been enabled on your Smart Client profile in XProtect Management Client.

Steps:

1. Navigate to the building on your smart map. If necessary, zoom in.
2. Select the building. A pane appears on the right-hand side.
3. Click the **Setup** button to enter setup mode.
4. Click **Add level** 

.
5. To edit the level name:
    1. Click the dots 

and select **Rename**.
    2. Enter a new name.
6. To delete a level, click the dots 

and select **Delete**. Devices on this level stay in their geographical position, but they are no longer associated with the level.
7. Click **Setup** to exit setup mode.

Change order of levels in buildings (smart map)

Requirements

Smart map editing has been enabled on your Smart Client profile in XProtect Management Client.

Steps:

1. Navigate to the building on your smart map. If necessary, zoom in.
2. Select the building. A pane appears on the right-hand side showing you the levels of the building.
3. Click **Setup** to enter setup mode.
4. Click and drag the dotted area 

to the correct position. Any associated devices and custom overlays stay with the level.
5. Click **Setup** again to exit setup mode. Your changes are saved.

Set default level for buildings (smart map)

If a particular level in a building is more relevant than others, for example the ground floor, you can set that level as the default level. When you open your smart map and go to the building, automatically the default level is selected.

If you navigate away from the building and back, XProtect Smart Client brings you to the level where you left off.

Requirements

Smart map editing has been enabled on your Smart Client profile in XProtect Management Client.

Steps:

1. Navigate to the building on your smart map. If necessary, zoom in.
2. Select the building. A pane appears on the right-hand side showing you the levels of the building. The default level is highlighted.
3. Click **Setup** to enter setup mode. Notice the asterisk 

. It indicates where the current default level is.
4. On the level you want to set as the default level, click the dots 

.
5. Select **Set as default**.
6. Click **Setup** again to exit setup mode. Your changes are saved.

Add floor plans to levels (smart map)

You can add custom overlays, for example floor plan images, to the levels in your building to help you illustrate the interior of a level inside a building. As you navigate the levels, automatically the associated floor plans are displayed.

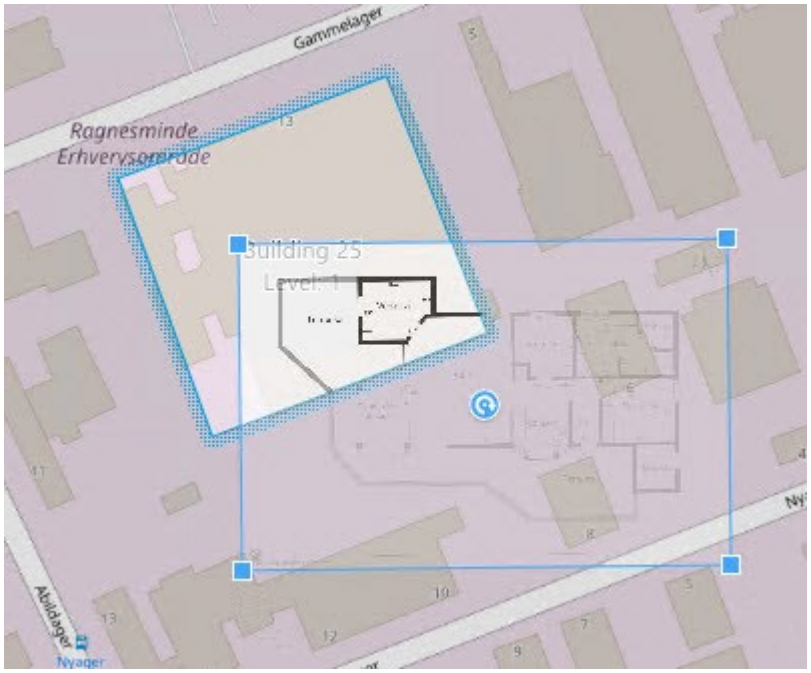
Requirements

Smart map editing has been enabled on your Smart Client profile in XProtect Management Client.

Steps:

1. Navigate to the building on your smart map. If necessary, zoom in.
2. Select the building. A pane appears on the right-hand side showing you the levels of the building.
3. Click **Setup** to enter setup mode.
4. Select the level where you want to add the custom overlay.
5. In the upper left corner, click **Add a custom overlay**, and then click anywhere inside the building outline. A window appears.
6. Select the type of custom overlay. For more information, see Custom overlays (explained) on page 91.

7. Select the location on your computer where the file is stored and click **Continue**. The custom overlay is displayed as a blue outline.



8. Drag it onto the outline of the building and use the pivot point and corner handles to rotate and reposition the custom overlay.
9. In the bar at the top, click **Save**.
10. Click **Setup** again to exit setup mode. Your changes are saved.

Delete floor plans on levels (smart map)

If a floor plan on a level inside a building has changed, you may need to replace the custom overlay illustrating the floor plan. Milestone recommends that you delete the old floor plan, before adding a new one.

Requirements

Smart map editing has been enabled on your Smart Client profile in XProtect Management Client.

Steps:

1. Navigate to the building on your smart map. If necessary, zoom in.
2. Select the building. A pane appears on the right-hand side showing you the levels of the building.
3. Click **Setup** to enter setup mode.
4. Select the level where the custom overlay is.
5. Right-click anywhere on the custom overlay and select **Delete custom overlay**.
6. Click **Setup** again to exit setup mode. Your changes are saved.

To edit the position or size of the floor plan, right-click the custom overlay and select **Edit position**. Now you can move, rotate, and change the size of the custom overlay.

Add devices to buildings (smart map)

After creating a building and adding levels, you can add devices to the building. If a default level has been specified, the devices are associated with it. Otherwise, the devices are associated with the first level. You can change this and associate the device with any of the levels in the building.

Requirements

Smart map editing has been enabled on your Smart Client profile in XProtect Management Client.

Steps:

1. Navigate to the building on your smart map. If necessary, zoom in.
2. Click **Setup** to enter setup mode.
3. To add a device, click its icon.

   Example: In the case of a camera, click  **Add a camera**.
4. Click again on the location where you want to position the device. A dialog appears.
5. Select the device and click **OK**. For each device that you want to add, repeat steps 3-5.
6. To associate a device with one or more levels, right-click the device and select the required levels.
7. Click **Setup** again to exit setup mode. Your changes are saved.

If no levels are selected, the device is visible on all levels.

Maps (configuration)

Add maps to views

You can add existing maps to views or create new ones.

1. Click **Setup** to enter setup mode.
2. In the **System overview** pane, drag the **Map** item to a position in the view. A window appears.
3. Select either **Create new map** or **Use existing map**. A triangle next to a map name indicates that the map might have one or more sub-maps. Sub-maps and the elements they contain are also added.

4. In the **Name** field, enter a name for the map. The name will be displayed in the title bar of the position.

   If you leave the **Name** field blank and click **Browse**, the **Name** field displays the name of the image file you select.

5. Click **Browse** to browse for the image file to use as a map.
6. Click **Open** to select image file.
7. Click **OK**.
8. Click **Setup** again to exit setup mode. Your changes are saved.

Map settings

In setup mode, you can use the **Properties** pane to adjust a number of settings for individual maps.

Name	Description
Home map	Displays the map that forms the basis of the particular map view. The field is read-only, but you can change the map by clicking the selection button  to open the **Set up map** window.
Rename map	Edit the name of your map.
Change background	Change the map, but keep the elements on the map in their relative positions to each other.
Icon size	The **Icon size** drop-down list lets you select the size of new elements added to the map, ranging from **Tiny** to **Very large**. You can re-size icons on the map by pulling the sizing handles in the corners of the icons.
Show name	The **Name** check box lets you enable/disable whether names of elements are displayed when adding new elements.

Name	Description
	If you have added an element to the map and the element name is not displayed on the map, right-click the required element and select **Name**. If you do not want the element name displayed, right-click the name and select **Delete text**. **Icon size** drop-down list lets you select the size of new elements added to the map, ranging from **Tiny** to **Very large**. You can re-size icons on the map by pulling the sizing handles in the corners of the icons.
Allow pan & zoom	Select to allow pan and zoom on the map in live mode.
Auto maximize map	Select to automatically maximize the map to full screen in Live mode when the XProtect Smart Client has not been used for the number of seconds defined in **Timeout**. The maximum number of timeout seconds is 99999.
On mouse over	Select to display a live video preview when you move the mouse over a camera.
Use default display settings	Select to define that the preview window looks the same as your other views. Clearing this check box lets you define the **Title bar** and **Live indicator** settings for previews. **Title bar**: select to display a title bar with the name of the camera. **Live indicator**: select to display the indicator for live video (see Camera indicators (explained) on page 168), which flashes green when the image is updated. You can only select **Live indicator** if you have also selected **Title bar**.
Status visualization	Select to graphically display the status of the elements (see Maps (explained) on page 271) added to a map.
Enable status details support	When selected, you can see status details on cameras and servers in live and playback mode.
Automatically change map on alarm	Select to automatically change the map in the preview when you select an alarm to display the map for the camera that the alarm relates to.

Name	Description
Only show on hover	Select to only show camera view zones and PTZ presets when you move your mouse over the camera, view zone or preset. This setting is useful if you have several cameras on a map with overlapping view zones or several presets. The default value is to show view zones and presets.

Map toolbox (explained)

The map toolbox consists of a number of tools for configuring the map. Selecting either **Camera**, **Server**, **Microphone**, **Speaker**, **Event**, or **Output** opens the **Element selector** with a list of cameras, servers, microphones, speakers, events, and output, allowing you to place these elements on the map.

Maps - the right-click menu (explained)

By right-clicking maps or map elements on the **Setup** tab, you get access to a shortcut menu.

Change the background of a map

If you need to update the map but want to keep all the information on it, you can just replace the map background (if you have the necessary map edit user permissions). This allows you to keep all your cameras, and other elements in their relative positions on a new map. Select **Change map background**, by right-clicking the map or in the **Properties** pane.

Remove the map

Right-click the map in the view, and select **Remove Map**. This will remove the entire map, including added elements representing cameras, microphones, speakers, etc. The map is only removed from the view. The image file will still exist on the surveillance system, and can thus be used for creating a new map.

You can also remove a map through the **Map overview**.

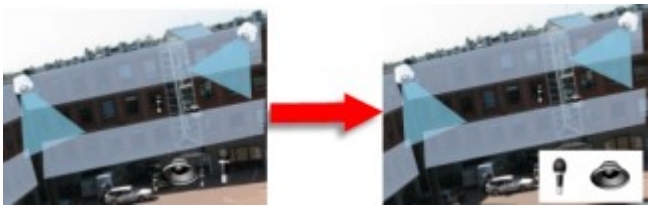
Add and remove elements from maps

1. In setup mode, right-click the map and select **Toolbox**.
2. In the toolbox, click the required element icon to open the **Element selector** window.
3. You can use the filter to quickly find a required element: enter a search criterion to narrow down the list of displayed elements to fit your search criterion.
4. Select the element and drag it onto the map.

5. To remove an element, right-click the unwanted element (camera, hot zone, server, event, output, microphone, or speaker) and select **Remove [element]**.
6. To move an element, click and drag it to a new position on the map.
7. To change the orientation of an element, select it and place your mouse over one of the element's sizing handles. When the mouse pointer changes appearance to a curved arrow, click and drag the element to rotate it.

You can use the selector tool from the toolbox to select and move elements on a map, or to pan the map.

If your map has a color that makes it difficult to see the elements on the map, try creating a text box and fill it with a color that makes it stand out from the map. Add the required elements to the map, then drag them into the text box.



Add a hot zone to a map

1. In setup mode, right-click the map and select **Toolbox** (see Map toolbox (explained) on page 113).
2. In the toolbox, select the **Hot zone** tool:

3. Move the mouse pointer onto the map. The mouse pointer now displays the hot zone icon and a small white cross to indicate that hot zone drawing is enabled.

   To draw the hot zone, click the map where you want to start drawing the hot zone. The starting point is now indicated by a large blue dot—also known as an anchor—on the map:

   The hot zone drawing tool makes straight lines only; if you want a rounded hot zone border, you must use several small straight lines.

4. Click the hot zone starting point to complete drawing the hot zone. The hot zone is now outlined with a dotted line, indicating that no sub-map has been attached to the hot zone.

   > You can alter the outline of a hot zone by pulling the hot zone anchors.

5. To attach a sub-map to the hot zone, double-click the dotted hot zone to open the **Map Setup** window.

You can change the color of the hot zone using the color tool. Using different colors for hot zones helps users differentiate between adjacent hot zones.

> If you are connected to a surveillance system that supports Milestone Federated Architecture (see Surveillance system differences on page 33), a maximum of 20 hot zones on a single map can point to maps from other surveillance system servers. There is no such limit for hot zones pointing to maps belonging on the server to which you are logged in.

Change the appearance of map elements

You can change the color of texts, backgrounds, hot zones, etc. on maps to differentiate map elements from each other.

1. In **setup** mode, right-click the map and select **Toolbox**.
2. Select the element that you want to change.
3. In the toolbox, select the color fill tool  . This will open the **Color selection** window.

   Use the color picker tool  to use an existing color from the map.

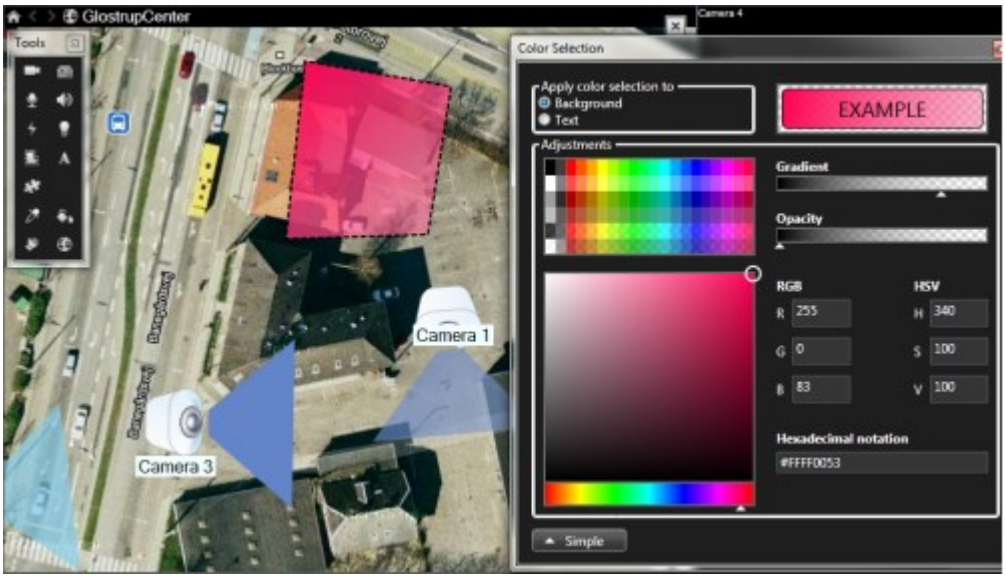
4. Only relevant for text elements: Select whether you want the color change to apply to text or background.
5. Select the color from the color palette—you can see a preview of the selected color in the EXAMPLE box.
6. Click the map element to fill it with the new color.

Adjusting Gradient

Use the **Gradient** slider to adjust how the element color fades from left to right.

Dragging the slider to the far right will make the element color fade instantly. Dragging the slider to the far left will make the element color almost not fade at all.

Drag the **Gradient** slider to the required level, then click the map element to apply color and gradient.

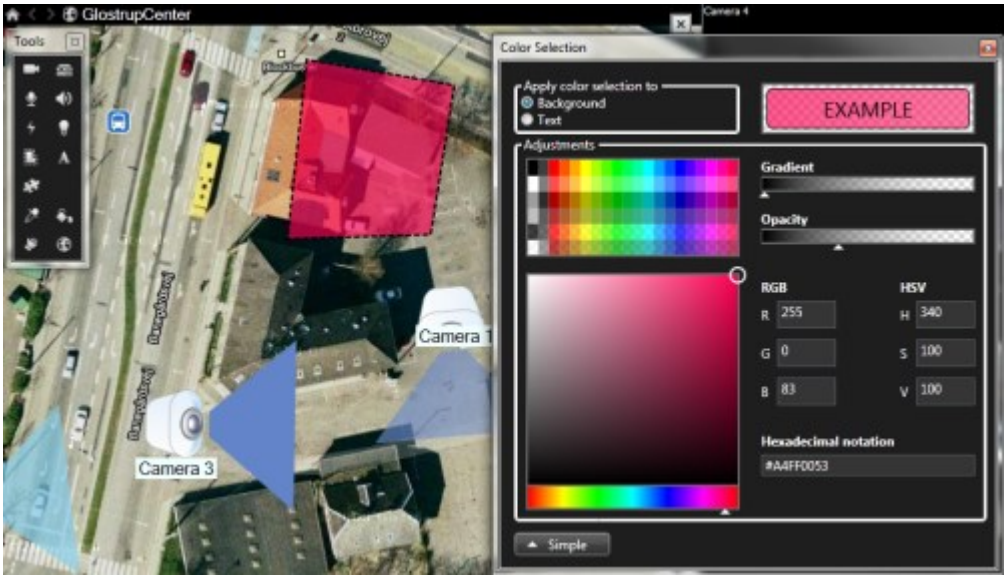


Adjusting Opacity

Use the **Opacity** slider to adjust the transparency of the color fill.

Dragging the **Opacity** slider to the far right will make the color completely transparent, while dragging the **Opacity** slider to the far left makes the color completely solid.

Drag the **Opacity** slider to the required level, then click the map element to apply color and opacity.



Advanced Color Change

You can fill map elements with any color you like. Click the **Color selection** window's **Advanced** button to access the advanced color selection options. Do one of the following:

- Use the color slider to select the main color shade, then drag the color circle to select the required tone.
- Enter the hexadecimal color code in the **Hexadecimal notation** field.

Edit and rotate labels on a map

All elements on a map have a label, making it easy to identify them.

If you have a great number of elements on a map, it can be difficult to have enough room for all the labels. You can edit the name of the devices, by selecting the label and then entering a new (shorter) name for the device.

> When you rename a label, you are only changing the label on the map, not the name of the camera or element in the system.

You can also make sure your labels don't overlap by rotating them. To rotate a label on a map:

- Select the label and place your mouse over one of the sizing handles. When the mouse pointer changes appearance to a curved arrow, click and drag the label to rotate it

> Another way to save space on a map is to select only to show view zones and PTZ presets on hover (see Map settings on page 111).

Add/edit text on a map

You can insert text anywhere on the map, for example, to inform users of maintenance situations.

1. In setup mode, right-click the map and select **Toolbox**.
2. In the toolbox, select the text tool:

3. In the **Font selection** window, edit your text settings.

   You can always edit your text settings; click the required text box and select the text tool from the toolbox, then change the text settings for the selected text box.

4. On the map, click where you want to place the text.
5. Enter your text. Press **ENTER** on your keyboard to make the text box expand downwards.

You can use the color fill tool to change the text color and background.

You can move the text box around; select the selector tool, grab the text box on the map, and move the text box.

Matrix (configuration)

Add Matrix to views

To be able to send live video to a Matrix-recipient, first you must add the Matrix item to a view. Only from within the view, can the operator send the video to a Matrix-recipient.

1. In setup mode, in the **System overview** pane, drag the **Matrix** element to the view item where you want to add Matrix content. A blue border appears indicating that the view item has Matrix content.
2. When you select a view item with Matrix content, you can specify its properties in the **Properties** pane.

   When viewing live or recorded video, you can double-click a view item with Matrix content (or any view item with a camera) to maximize it. When maximized, video from cameras in the view item with Matrix content is displayed in full quality by default, regardless of your image quality selection. If you want to make sure that the selected image quality also applies when maximized, select **Keep when maximized**.

3. Repeat for each view item with Matrix content you want to add.

Matrix settings

In setup mode, in the **Properties** (see Camera settings on page 66) pane, you can specify the settings for view items with Matrix content.

Name	Description
Window index	Change the ranking of the view item with Matrix content by choosing a different number. You can only choose a number in the range that corresponds to the number of Matrix view items in your view. **1** is the primary view item in which video from the newest event is always shown, **2** displays video from the previously detected event, **3** displays video from the event detected before the event in view item **2**, and so on.
Connection settings	Lets you specify the **TCP port** and **Password** for transferring Matrix-triggered video from XProtect VMS server to the XProtect Smart Client view. This is only available when Matrix view item **1** is selected; other Matrix view items inherit the connection settings specified for view item **1**. By default, the TCP port used for Matrix is 12345. Contact your system administrator about which port number or password to use.

XProtect Smart Client – Player (configuration)

Managing views in XProtect Smart Client – Player

You create and manage views by clicking **Setup** on the XProtect Smart Client – Player toolbar. The panes on the left-hand side turn yellow.

Project pane (explained)

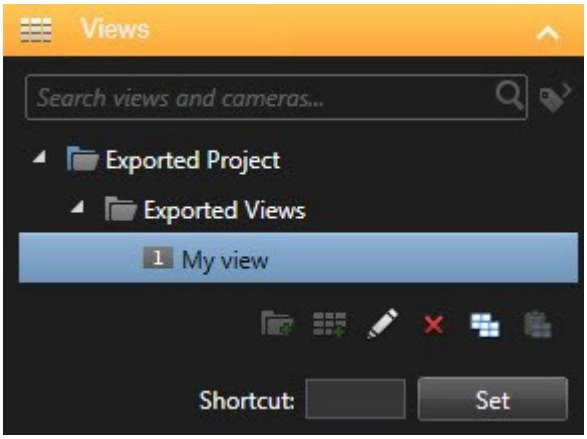
A project in XProtect Smart Client – Player is a collection of files that are created when video is exported in database format from XProtect Smart Client. Your user settings, including information about your views, are stored as part of a project.

The **Project** pane appears when you click **Setup**. In setup mode, you can:

- Change the name of the project.
- Create or open a project
- Assign passwords to projects - only people with permission can view a video. You can also assign passwords to devices when you export them. To avoid having to keep track of several database passwords, you can assign a single password to the overall project. If you do not assign an overall password and you have databases with passwords added to your project, you will be asked to enter a password for each database when you open the project. If you assign a password to a project, you cannot delete it. However, you can change the password or create a new identical project in the **Project** pane.

Views pane (explained)

In the **Views** pane in XProtect Smart Client – Player, you can add, edit, and delete views. You can also search for views and cameras.



Overview pane (explained)

The **Overview** pane in XProtect Smart Client – Player displays the cameras, microphones, speakers, webpages, images, and plug-ins assigned to the project. When you have selected a device, you can delete it and rename it. You can link speakers and microphones to cameras. Then associated audio is automatically selected when you view recorded video for a particular camera.

To open a database from an archive or previously exported material, click the  button. The **Open database** wizard appears.

When you delete a device, this does not delete the actual database files associated with the device, it just removes them from the project.

Digital signatures (explained)

This feature is only available in certain XProtect VMS systems. For more information, see the product comparison chart: https://www.milestonesys.com/solutions/platform/product-index/

You can use digital signatures to verify the authenticity of your recorded video. This is useful, for example if you want to demonstrate that the video has not been tampered with.

There are two stages of verification. You can verify:

- whether the video has been modified after it was recorded. The recording server creates a digital signature for the recording. Later when you view exported video in XProtect Smart Client – Player, you can compare the recording signature with the one that was originally created by the recording server.
- whether video that you export in XProtect Smart Client has been modified after it was exported. During the export process, XProtect Smart Client creates a signature for the export file. Later when you review the exported evidence in XProtect Smart Client – Player, you can compare the export signature with the one that was created during the export.

If you find that there is a discrepancy, there is reason to question the reliability of the video evidence.

The original digital signatures are contained in the **PublicKey.xml** and **Public Key Certificate.xml** files in these locations:

- XProtect Smart Client - **<export destination folder>\<export name>\Client Files\Data\Mediadata\<camera name>\<camera name>\Export signatures**
- XProtect Management Client - **C:\Program Files\Milestone\Management Server\Tools\CertificateIssuer**

There are two scenarios where digital signatures are excluded during the export process:

- If there are areas with privacy masks, digital signatures for the recording server will be removed in the export.
- If the data you are exporting is very close to the current date and time, the digital signature for the recording server might not be included for the whole sequence. In this case, only part of the export will have digital signatures added.

The export process will complete, but when you verify the signatures, you will see that the digital signatures for the recording server were removed or partially OK.

XProtect Access (configuration)

Add access monitors to views

You start by defining a view item for access control:

1. In setup mode, select the view you want to use for access monitoring.
2. In the **System overview** pane, click **Access monitor** and drag it to a view item.
3. In the **Access monitor settings** (see Access monitor settings on page 122) dialog box that appears, specify the settings. Once you have selected a door, you can keep the default settings or change them if needed.
4. Click **OK** and the access monitor is added to the view.

   When an access control incident occurs that triggers an event, it appears in the right side of the view item.

Access monitor settings

Specify the following settings for access monitors:

Name	Description
Door	Select the door you want to view access control events from. When you select a door, the remaining settings in the dialog box appear with their current values.
Sources	Select the type of access control sources that you want to receive events from. The list can contain, for example, doors or specific access points for a door. An access point is a point of entry, including its associated physical devices such as card readers, keypads, sensors, or buttons. A door has typically two access points that control entry and exit through the door respectively. The list of sources is configured by your system administrator.
Camera	Select the camera from which you want to show video related to this door. By default, the system lists the cameras that your system administrator has associated with the selected door, but you can also select another camera in your system.
Events	Select the type of events you want to receive. You can select events from the event categories defined by your XProtect system administrator or from the list of events defined in your access control system.

Name	Description
Commands	Select the command buttons that you want to have available in the access monitor, for example, lock and unlock doors. The list of commands depends on your system configuration.
Order	Select if you want new events to appear in the top or at the bottom of the event list.

Modify access monitor settings

In live mode, you can change the settings of your access monitor:

1. Click **Setup** and select the view item you want to modify.
2. In the **Properties** pane, click the **Access monitor settings** button.
3. In the **Access monitor settings** (see Access monitor settings on page 122) dialog box that appears, specify the settings.
4. Click **OK** to close the dialog box and then **Setup** to return to live viewing.

Customize your view

With overlay buttons you can customize your interface. You can add overlay command buttons for access control to a view item from a list of commands configured for the doors or access points.

Examples of usage:

- Have direct access to command buttons in view items other than access monitors
- Place the command buttons directly by a door in the view item
- Add other command buttons than those specified in Access monitor settings on page 122

Steps:

1. In live mode, select **Setup** and select the view item you want to modify.
2. In the **Overlay buttons** pane, click **Access control**.
3. Locate the command you want to add and drag it to your view item.
4. Click **Setup** to return to live viewing.

   The overlay button appears when you drag the mouse over the view item.

Manage cardholder information

If your access control system is set up for it, you can go directly to a web page representation of a cardholder record and do, for example, user administration or get further information about the cardholder.

Provided that the plug-in supports deep link, the following prerequisites exist for the access control system:

- Must include a web client
- Must support deep links

To manage cardholder information:

1. On the **Access control** tab, select **Cardholders** list.
2. Search for a cardholder and select the person from the list.
3. On the right-hand side, below the cardholder information, you can click a link to, for example, a webpage. Depending on the plug-in, more links may be supported and you may be asked for additional login credentials.
4. You can edit several functionalities, including cardholder information and access permissions.
5. Close, in this example, the webpage and return to XProtect Smart Client.

Turn access request notifications on or off

You can turn off access request handling, for example in cases where only one person should handle access requests.

1. On the global toolbar, select **Settings and more** and then **Settings** to open the **Settings** window.
2. Select **Access control** and turn off access request notifications.

If you later need to handle access requests again, turn on access request notifications. You can also change the options for access control, by clicking the **Settings** icon from within an access request notification.

If the **Follow Server** field is selected, your system administrator controls the setting of **Show access request notifications**.

XProtect LPR (configuration)

Add LPR cameras to views

1. In **Setup** mode, select the view you want to add an LPR camera to.
2. In the **System overview** pane, click **LPR** and drag it to the relevant view item.
3. In the **Select LPR camera** dialog box, expand the required server to view a list of available LPR cameras from that server.

You can specify how you want to display LPR camera events in live mode in the **Properties** pane (see Adjust LPR view settings on page 125).

Adjust LPR view settings

1. In live mode, click **Setup**.
2. In **Properties**, next to **LPR camera**, click the **Browse** button to open the **Select LPR camera** dialog box and select another LPR camera.
3. Choose the order of LPR events in your lists on the right-hand side of the preview:
   - **Newest on top**: Display the newest LPR events at the top of the list
   - **Newest on bottom**: Display the newest LPR events at the bottom of the list
4. If you want to display the list of license plates from one camera but want to view video from another, select a different camera in the **Camera name** field.

Enable LPR server status on maps

It is possible to visualize LPR servers on maps and have their current status shown on the maps. To enable the LPR server status on maps:

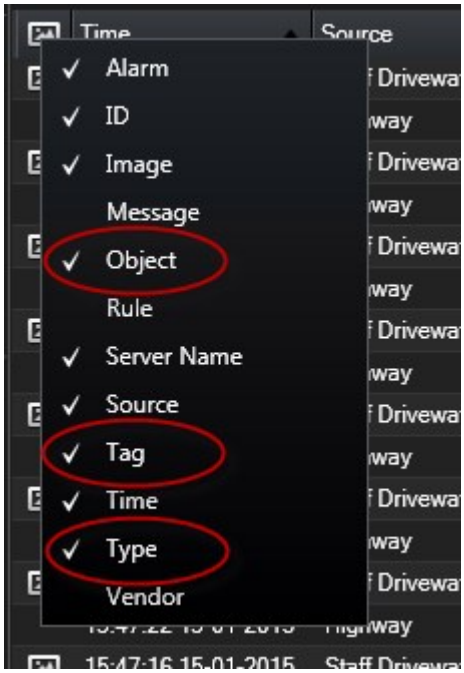
1. In live mode, click **Setup**.
2. In **Views**, select the relevant map.
3. Right-click the map and select **Toolbox**.
4. In the toolbox, click the  **Add plug-in element** icon to open the **Element selector** window.
5. Select the relevant LPR server and drag it onto the map.
6. On the map, right-click the LPR server icon and select **Status details** to get live status on the LPR server and the LPR cameras related to the server.

You can associate the LPR specific map with your **Alarm list** by adding the map on the **Alarm Manager** tab.

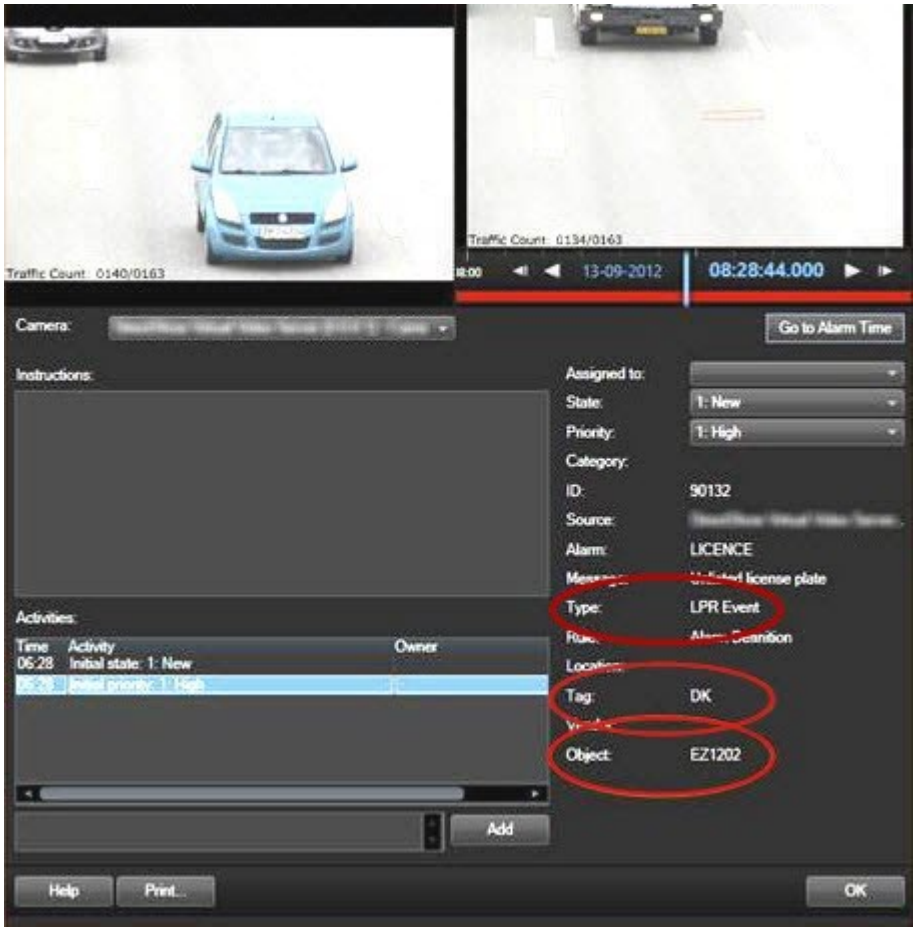
Enable LPR-specific elements

To be able to see all relevant information regarding LPR recognitions in your XProtect Smart Client, on the **Alarm Manager** tab, do the following:

1. On the **Alarm Manager** tab, in the **Alarms** list, right-click the **Image** icon  next to the **Quick Filters** column. From the menu, select: **Object**, **Tag**, and **Type**.



2. Now **Type** displays all events related to LPR, **Tag** displays their country codes, and **Object** displays license plate numbers of the registered vehicles.



XProtect Transact (configuration)

Getting started with XProtect Transact

Before you start observing and investigating your transactions in XProtect Smart Client, you need to:

1. Verify that your XProtect Transact base license has been activated during installation of the VMS. To do this, open XProtect Smart Client and check that the **Transact** tab is visible. Even if you do not have a base license, you can still use XProtect Transact with a trial license. For more information, see XProtect Transact trial license on page 128.
2. Verify that transactions are displayed correctly. This includes the individual transaction lines and receipts. To do this, click the **Transact** tab and select a transaction source and a time interval. If configured correctly, a list of transaction lines appear, and if you click a line, the corresponding video

still frame is displayed, one for each connected camera.

3. Set up a view for transactions, if you want to observe real time transactions in live mode or investigate transactions in playback mode. For more information, see Set up views for transactions on page 128.

XProtect Transact trial license

With an XProtect Transact trial license, you can try out the XProtect Transact functionality for up to 30 days. All related features are enabled, and you can add one transaction source, for example a cash register. When the 30 days trial period expires, all XProtect Transact features are deactivated, including the **Transact** workspace and transaction view items. By purchasing and activating an XProtect Transact base license and the transaction source licenses you need, you can use XProtect Transact again, and your settings and data are maintained.

You must acquire the trial license from Milestone. The system administrator must activate the trial license in the configuration.

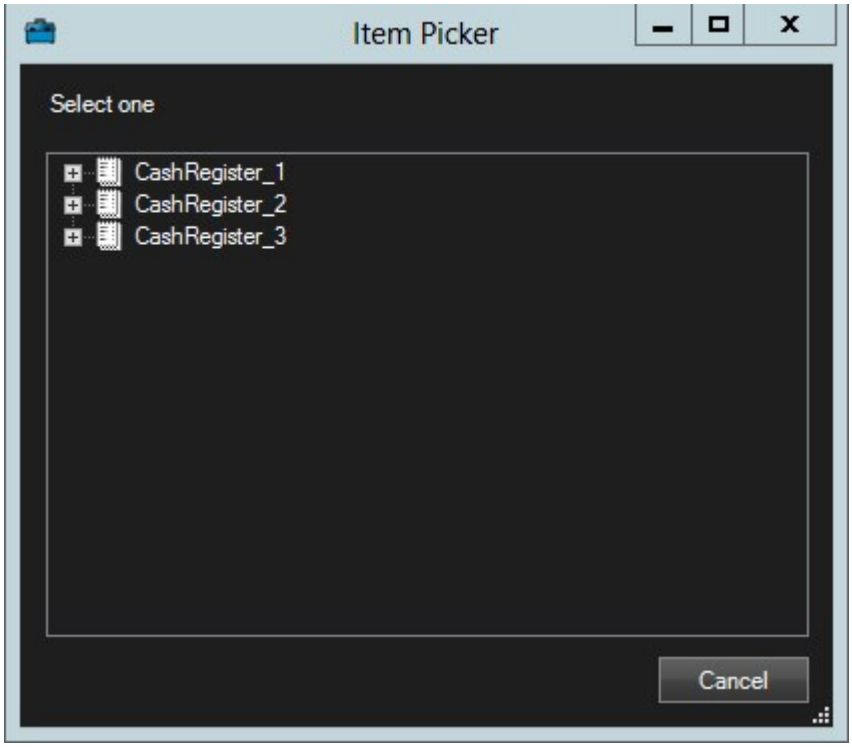
Set up views for transactions

Before viewing transactions in live or playback mode, you need to set up a view where you include a transaction view item for each transaction source. In case of ongoing transactions, the receipts roll over the screen inside the view item when you leave the setup mode.

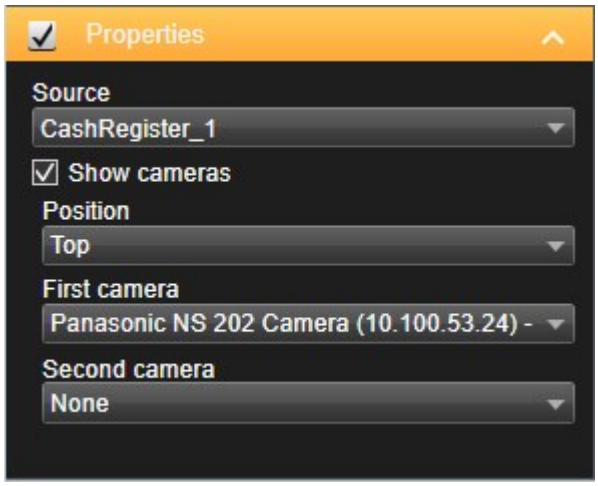
Steps:

1. In live or playback mode, click **Setup** in the upper right corner to enter the setup mode.
2. Create a new view or select an existing one.
3. Expand the **System overview** pane.

4. Drag and drop the **Transact** item into the view item, where you want the transactions and video feed to be displayed. A pop-up window appears.



5. Select a transaction source, for example a cash register, and click **OK**. A receipt preview is displayed inside the view item.
6. Expand **Properties** and select the **Show cameras** check box to add cameras associated with the transaction source. By default, the first camera added to the transaction source in the configuration is selected.



7. Use the **First camera** and **Second camera** drop-down lists to specify which cameras are displayed in the view item. By default, no second camera is selected. If you do not want a second camera, leave it as is.

8. If you want to change the position of the cameras, select a value in the **Position** drop-down list, for example to the left of the receipt.

For each transaction view item you want to add to the view, repeat steps 4-8.

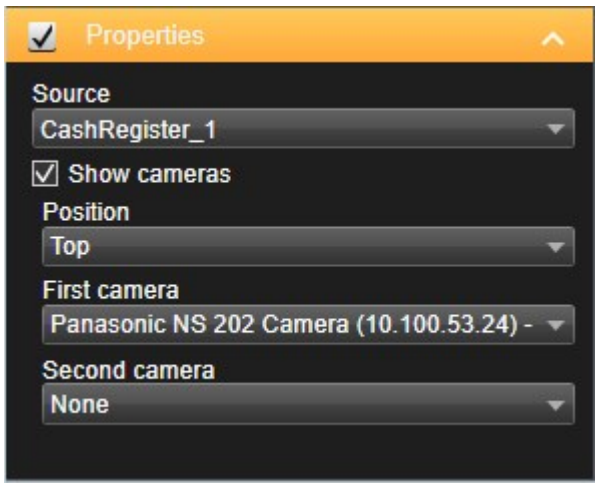
Adjust settings for transaction view items

Once you have created a view that includes one or more transaction view items, you can:

- Change the cameras selected and their display order. You can select maximum two cameras per transaction view item, and only cameras associated with the transaction source
- Change how the cameras are positioned in relation to the receipt
- Add (or remove) transaction view items

Steps:

1. In live or playback mode, click **Setup** in the upper right corner to enter the setup mode.
2. Select the view and then the view item you want to adjust.
3. To modify the cameras selected or their position, expand **Properties** and verify that the **Show cameras** check box has been selected.



4. Use the **Position** drop-down list to specify how the camera or cameras are displayed in relation to the receipt, for example below the receipt.
5. Use the **First camera** and **Second camera** drop-down lists to change which cameras are displayed in the view item.
6. If you want to add a transaction source to the view, follow steps 3-8 in Set up views for transactions on page 128.

Scripting

Scripting for log in (explained)

You can use scripting to control parts or all of the login procedure in XProtect Smart Client.

- If using **Basic authentication** or **Windows authentication**, you can make the XProtect Smart Client login window open with a pre-filled server address and user name fields so users only have to enter a password to log in.
- If using **Windows authentication (current user)**, you can make the XProtect Smart Client connect to the surveillance system automatically, based on the user's current Windows login.

Scripting the login procedure based on **Basic authentication** or **Windows authentication** requires that you add non-encrypted, sensitive information to an SCS file that you store locally with the XProtect Smart Client program files:

- Host name
- Username
- Password

Storing non-encrypted information may compromise the security of your system or GDPR compliance. The information in the SCS file can be read:

- By anyone who can access the file
- In the memory footprint of the XProtect Smart Client application that was started by the SCS file or a command-line that delivers the username and password

Milestone recommends that you use **Windows authentication (current user)**. If you must use **Basic authentication** or **Windows authentication**, you should limit access to the SCS file.

Scripting for log in - parameters

You can use these parameters:

ServerAddress

Refers to the URL of the Management server that XProtect Smart Client connects to.

The following example shows the XProtect Smart Client login window with *http://ourserver* in the **Server address** field:

```
Client.exe -ServerAddress="http://ourserver"
```

The default authentication type is **Windows authentication (current user)**. Unless you change this, using the **AuthenticationType** parameter (described in the following section), the login window automatically displays the current Windows user in the **User name** field.

UserName

Refers to a specific user name.

The following example shows the XProtect Smart Client's login window with *http://ourserver* in the **Server address** field, and **Tommy** in the **User name** field:

```
Client.exe -ServerAddress="http://ourserver" -UserName="Tommy"
```

This parameter is relevant only for **Windows authentication** and **Basic authentication**. You use the **AuthenticationType** parameter to control which authentication method to use.

Password

Refers to a specific password.

The following example shows the XProtect Smart Client's login window with *http://ourserver* in the **Server address** field, **Tommy** in the **User name** field, and **T0mMy5Pa55w0rD** in the **Password** field:

```
Client.exe -ServerAddress="http://ourserver" -UserName="Tommy" -
Password="T0mMy5Pa55w0rD"
```

This parameter is relevant only for **Windows authentication** and **Basic authentication**. You use the **AuthenticationType** parameter to control which authentication method to use.

AuthenticationType

Refers to one of XProtect Smart Client's three possible authentication methods: **Windows authentication (current user)** (called **WindowsDefault** in startup scripts), **Windows authentication** (called **Windows** in startup scripts), or **Basic authentication** (called **Simple** in the startup scripts).

The following example shows the XProtect Smart Client login window with *http://ourserver* in the **Server address** field, **Basic authentication** selected in the **Authentication** field, **Tommy** in the **User name** field, and **T0mMy5Pa55w0rD** (masked by asterisks) in the **Password** field:

```
Client.exe -ServerAddress="http://ourserver" -UserName="Tommy" -
Password="T0mMy5Pa55w0rD" -AuthenticationType="Simple"
```

If you use **Windows authentication**, the example is:

```
Client.exe -ServerAddress="http://ourserver" -UserName="Tommy" -
Password="T0mMy5Pa55w0rD" -AuthenticationType="Windows"
```

If you use **Windows authentication (current user)**, the **UserName** and **Password** parameters would not be necessary, and the example looks like this:

```
Client.exe -ServerAddress="http://ourserver" -
AuthenticationType="WindowsDefault"
```

Script

Refers to a full path to an .scs script (a script type targeted at controlling the XProtect Smart Client).

The following example uses an .scs script to login:

```
Client.exe -Script=c:\startup.scs
```

Example of an .scs script for logging in to *http://ourserver* with the current Windows user:

```
<ScriptEngine>
```

```
 <Login>
```

```
   <ServerAddress>http://ourserver</ServerAddress>
```

```
   <AuthenticationType>WindowsDefault</AuthenticationType>
```

```
 </Login>
```

```
</ScriptEngine>
```

You can use many of the XProtect Smart Client's function calls (see View a list of function calls) to add further functionality to .scs scripts. In the following example, we have added a line so the .scs script from the previous example will also minimize the XProtect Smart Client application:

```
<ScriptEngine>
```

```
<Login>
```

```
  <ServerAddress>http://ourserver</ServerAddress>
```

```
  <AuthenticationType>WindowsDefault</AuthenticationType>
```

```
</Login>
```

```
<Script>SCS. Application.Minimize();</Script>
```

```
</ScriptEngine>
```

Format

Valid parameter formats are:

```
{-,/,--}param{ ,=,:}(('.')value(','))
```

Examples:

```
-UserName Tommy
```

```
--UserName Tommy /UserName:"Tommy" /UserName=Tommy -Password 'Tommy'
```

Scripting HTML page for navigation

You can use scripting to create HTML pages that let you switch between views. HTML pages can be added to your views, so they appear together with video from your cameras.

Example: In an HTML page, you can insert a clickable floor plan of a building that allows operators to simply click a part of the floor plan to instantly switch to a view that displays video from that part of the building.

Requirements

- If your XProtect VMS system supports Smart Client profiles, you must enable HTML scripting on the required Smart Client profiles in XProtect Management Client.
- If your XProtect VMS system does not support Smart Client profiles, you must enable HTML scripting in the **Client.exe.config** file.

In the following, you will see examples of HTML pages for XProtect Smart Client navigation:

- A simple HTML page with buttons
- A more advanced HTML page with a clickable image map
- A check list for system administrators outlining the tasks involved in creating and distributing HTML pages to XProtect Smart Client operators

Example of an HTML page with button navigation

A very quick solution is to create an HTML page with buttons for navigation. You are able to create a wide variety of buttons on the HTML page. In this example, we will just create two types of buttons:

- **Buttons for switching between the XProtect Smart Client's views**

  Required HTML syntax:

  ```
  <input type="button" value=" Buttontext" onclick="SCS. Views.SelectView
  ('Viewstatus.Groupname. Viewname');">
  ```

  Where **Viewstatus** indicates whether the view is shared or private (if the HTML page is to be distributed to several users, the view **must** be shared).

  Example from a real button:

  ```
  <input type="button" value="Go to Shared Group1 View2" onclick="SCS.
  Views.SelectView('Shared.Group1. View2');">
  ```

  This button would allow users to go to a view called **View2** in a shared group called **Group1**.

  Buttons for switching between live and playback mode: Bear in mind that, depending on the users' permissions, some users may not be able to switch to a mode.

  Required HTML syntax:

  Live mode: `<input type="button" value="Buttontext" onclick="SCS. Application.ShowLive();">`

  Playback mode: `<input type="button" value="Buttontext" onclick="SCS. Application.ShowBrowse();">`

> For advanced users it is possible to create many other types of buttons using the approximately 100 different function calls available for the XProtect Smart Client.

In the following we have created two shared groups in the XProtect Smart Client. We have called them **Group1** and **Group2**. Each group contains two views, called **View1** and **View2**.

We have also created an HTML page with buttons allowing users to switch between our four different views as well as between the live and playback modes. When viewed in a browser, our HTML page looks like this:

HTML page with buttons for navigating between views and tabs

We have saved the HTML page locally, in this case on the user's C: drive. When the HTML page is to be used for navigation, saving the HTML page locally is necessary to open it in compatibility mode. See also Web page properties on page 64.

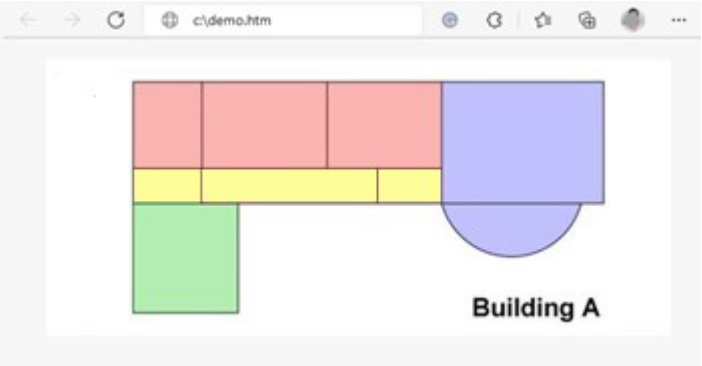
When saving the HTML page locally, save it at a location to which an unambiguous path can be defined, for example in a folder on the user's C: drive (example: C:\ myfolder\file.htm). Saving the HTML page on the user's desktop or in the user's **My Documents** folder will not work properly due to the way Windows constructs the path to such locations.

We then imported the HTML page into the required XProtect Smart Client views.

Example of an HTML page with image map navigation

You can also create an HTML page with more advanced content, for example, an image map allowing users to switch between views.

In the following example we have kept the two groups and two views from the previous example. Instead of using buttons, we have created an HTML page with an image of a floor plan, and created an image map based on the floor plan. Viewed in a browser, our HTML page looks like this:



HTML page with image map for navigating between views

For this example, we divided the floor plan into four colored zones, and defined an image map area for each zone. Users can click a zone to go to the view displaying cameras from that zone.

For instance, the red zone on our image map mirrors the **Go to Shared Group2 View2** button from the previous example. If you click the red zone, you will go to **View2** in **Group2**.

Importing the HTML page

Importing a navigation HTML page into a view is in principle no different from importing any other type of HTML page into a view in the XProtect Smart Client. See Add web pages to views on page 62.

- The HTML page should be stored locally on the operator's computer
- For the navigation to work properly, you may want to import the HTML page into several views

System administrator's check list

To create and distribute navigation HTML pages to XProtect Smart Client operators, do the following:

1. **Create** the required HTML page. The navigation controls in the HTML page must match the views users see in the XProtect Smart Client. For example, in order for a button leading to **View1** to work, a view called **View1** must exist in users' XProtect Smart Client installations. If you intend to distribute the HTML page to a group of users, the views in which the HTML page will be used should be placed in shared groups.
2. **Save** the HTML page locally on each computer on which it will be used. When saving the HTML page locally, save it at a location to which an unambiguous path can be defined, for example in a folder on the user's C: drive (example: C:\ myfolder\file.htm). Saving the HTML page on the user's desktop or in the user's **My Documents** folder will not work properly due to the way Windows constructs the path to such locations.
3. **Import** the HTML page into the required views in XProtect Smart Client. See Add web pages to views on page 62.
4. **Test** that the navigation controls on the imported HTML page work as intended.

For information about troubleshooting, see Web pages (troubleshooting) on page 311.

Optimization

Enabling hardware acceleration

Hardware acceleration (explained)

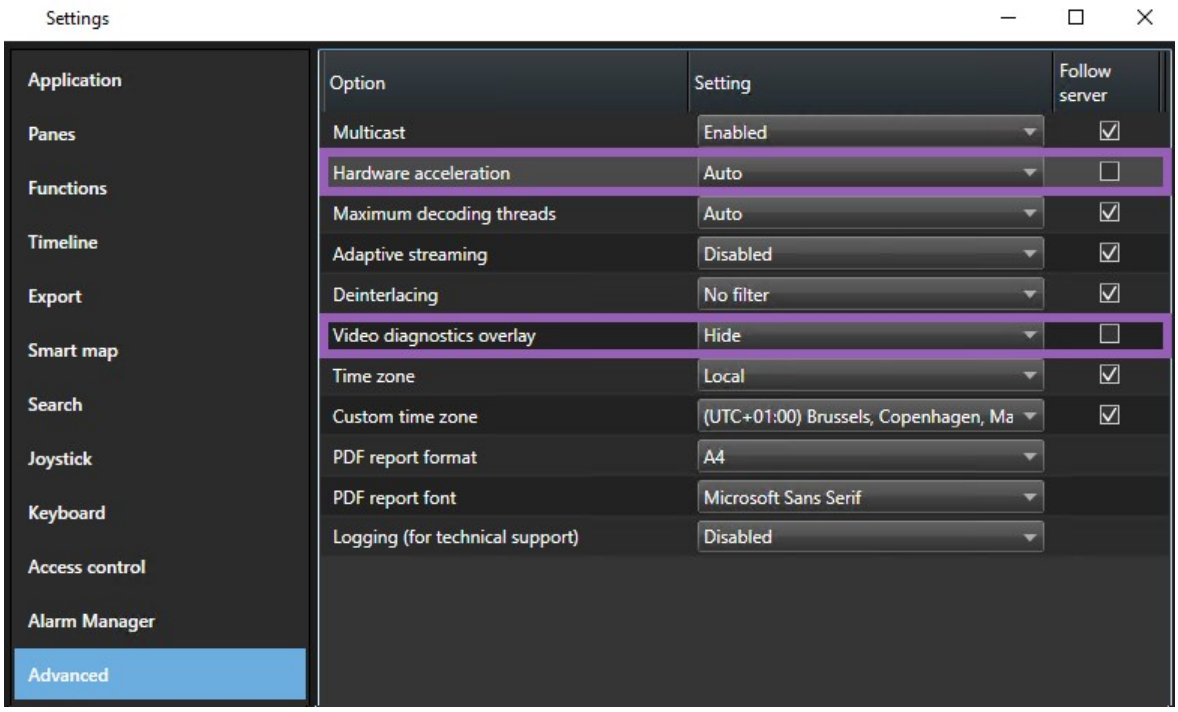
Hardware acceleration improves the decoding capability and performance of the computer running XProtect Smart Client. This is particularly useful when you view multiple video streams with high frame rate and high resolution.

XProtect Smart Client supports hardware accelerated decoding using Intel® and NVIDIA® GPUs. Milestone does not recommend the use of Scalable Link Interface (SLI) configuration of your NVIDIA display adapters.

Check hardware acceleration settings

1. Go to **Settings** > **Advanced** > **Hardware acceleration**.
2. There are two settings for hardware acceleration: **Auto** and **Off**.

   Select the default setting **Auto**.

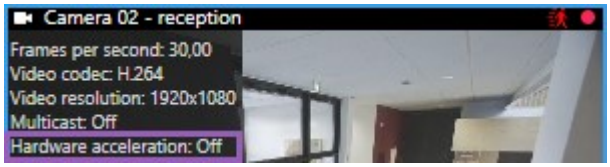


3. Go to **Video diagnostics overlay**.

4. To make the current status of the stream, including the GPU resource used for hardware acceleration visible, select **Level 2**.

   This setting applies to all view items. The default setting is **Hide**.

   The video diagnostics overlay status for **Hardware acceleration** can be: **Intel**, **NVIDIA** or **Off**.

   If the status is **Off**, continue to examine your computer so you can enable hardware acceleration, if possible and make sure that all hardware acceleration resources are utilized.

5. Use the **System Monitor** to check the current XProtect Smart Client decoding performance. See Monitor client resources on page 147.

Verify your operating system

Make sure your operating system is Microsoft® Windows® 10 (build 1809), Windows® Server 2016, or later versions.

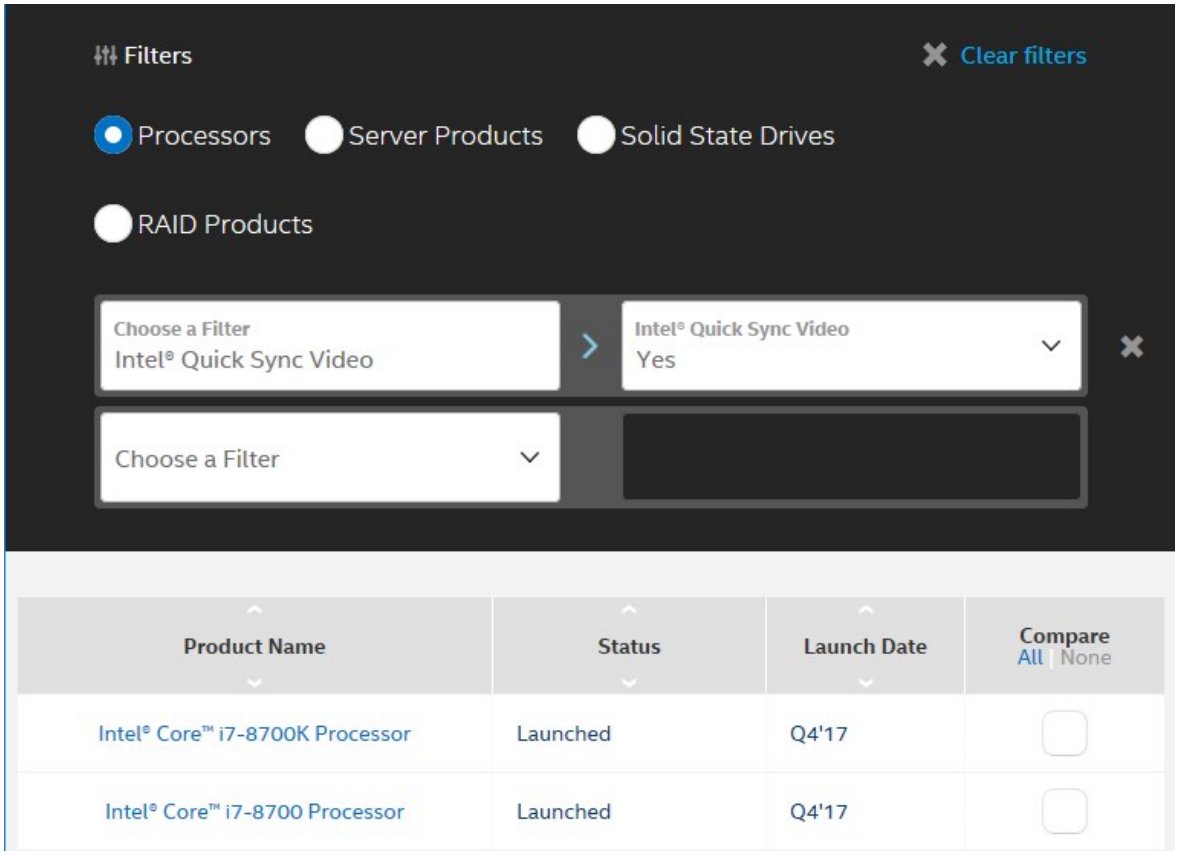
Only non-virtual environments are supported.

Check CPU Quick Sync support

To verify that your processor supports Intel Quick Sync Video:

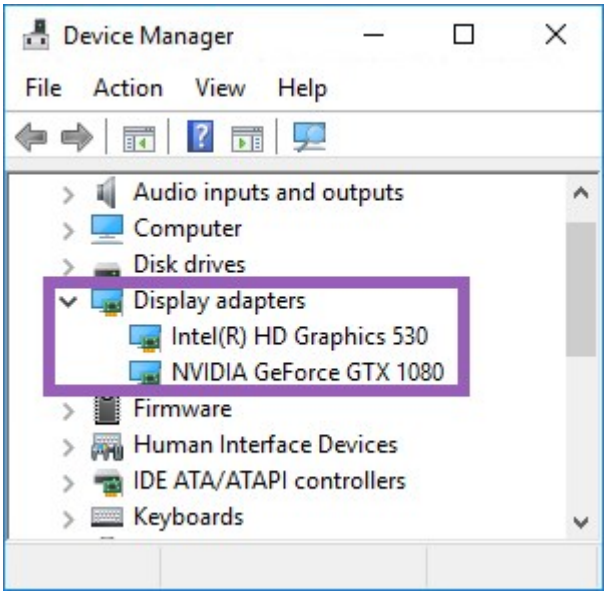
1. Visit the Intel website (https://ark.intel.com/content/www/us/en/ark/search/featurefilter.html?productType=873&0_QuickSyncVideo=True).

2. In the menu, set **Processors** and **Intel Quick Sync Video** filter to **Yes**.
3. Find your CPU in the list.



Examine the Device Manager

Make sure that an Intel or NVIDIA display adapter is present in Windows Device Manager.



You can connect your displays to any display adapter available. If a more powerful display adapter is available in your computer, typically NVIDIA or AMD®, connect your displays to this adapter to use all available GPU resources for hardware accelerated decoding and rendering.

Not all NVIDIA display adapters supports hardware acceleration. See Check NVIDIA hardware acceleration support on page 141.

If the Intel display adapter is not present, enable the Intel display adapter in the BIOS. See Enable the Intel display adapter in the BIOS on page 142.

Check NVIDIA hardware acceleration support

NVIDIA products have different compute capabilities.

Hardware accelerated decoding using NVIDIA GPUs requires compute capability version 6.x (Pascal) or newer.

To find the compute capability version of your NVIDIA product, visit the NVIDIA website (https://developer.nvidia.com/cuda-gpus/).

Enable the Intel display adapter in the BIOS

If another display adapter card, for example NVIDIA or AMD, is available in your computer, the onboard Intel display adapter may be disabled, and you must enable it.

The Intel display adapter is located on the motherboard as a part of the CPU. To enable it, look for graphics, CPU or display settings in the computer BIOS. The vendor's motherboard manual may be helpful to find the relevant settings.

If changing the settings does not enable the onboard Intel display adapter, you can try to move the display adapter card to another slot and then connect the display to the motherboard. In some cases, this can enable the onboard display adapter.

Update the video driver

Make sure that the driver version for all your display adapters are updated to the newest version available from Intel or NVIDIA.

The Intel driver version provided by the PC vendor can be an older version and may not support Intel Quick Sync Video.

There are two ways of updating your video driver. Manual download and install or using a driver update utility.

Intel

Manual download and install:

1. Go to the Intel download website (https://downloadcenter.intel.com/).
2. Enter the name of your integrated display adapter.
3. Manually download and install the driver.

For automatic detection and updates of Intel components and drivers:

1. Download Intel Driver and Support Assistant (https://www.intel.com/p/en_us/support/detect/).
2. Run the assistant to auto search for the drivers.
3. Choose to update the driver for Graphics.

NVIDIA

Option 1: Manually find drivers for my NVIDIA products.

1. Go to the NVIDIA download drivers website (https://www.nvidia.com/Download/index.aspx/).
2. Enter the name of your product and the operating system.
3. Manually download and install the driver.

Option 2: Automatically find drivers for my NVIDIA products.

1. Go to the NVIDIA download drivers website (https://www.nvidia.com/Download/index.aspx/).
2. Click **GRAPHICS DRIVERS**.
3. Your system is scanned.
4. Download and update the driver.

Check memory modules configuration

If your system supports more than one memory channel, you can increase the system performance by making sure that a minimum of two channels have a memory module inserted in the correct DIMM slot. Refer to the motherboard manual to find the correct DIMM slots.

Example:

A system with two memory channels and a total of 8 GB of memory obtains the best performance using a 2 x 4 GB memory module configuration.

If you use a 1 x 8 GB memory module configuration, you only use one of the memory channels.

Enabling adaptive streaming

Adaptive streaming (explained)

Adaptive streaming improves the decoding capability and performance of the computer running XProtect Smart Client. This is useful when you view multiple live video streams in the same view.

To take advantage of adaptive streaming, your cameras must have multiple streams defined with different resolutions. This enables XProtect Smart Client to automatically select the closest match to the resolution requested by the view item. Now XProtect Smart Client does not have to scale down the default streams with an unnecessary high resolution. This reduces the load on the CPU and GPU decoding resources.

To ensure the video quality the closest match is defined as equal or higher than the resolution requested by the view item if possible. This is to avoid the upscaling of the streams. The table below shows the video streams that adaptive streaming selects based on view item requests from XProtect Smart Client.

Resolution requested by a view item	Closest match of available video streams	
636 x 477	Video stream 1	640 x 480 (VGA)
644 x 483	Video stream 2	1280 x 720 (WXGA-H)
1920 x 1080	Video stream 3	1920 x 1080 (FHD)
1920 x 1440	Video stream 4	3840 x 2160 (4K UHD-1)

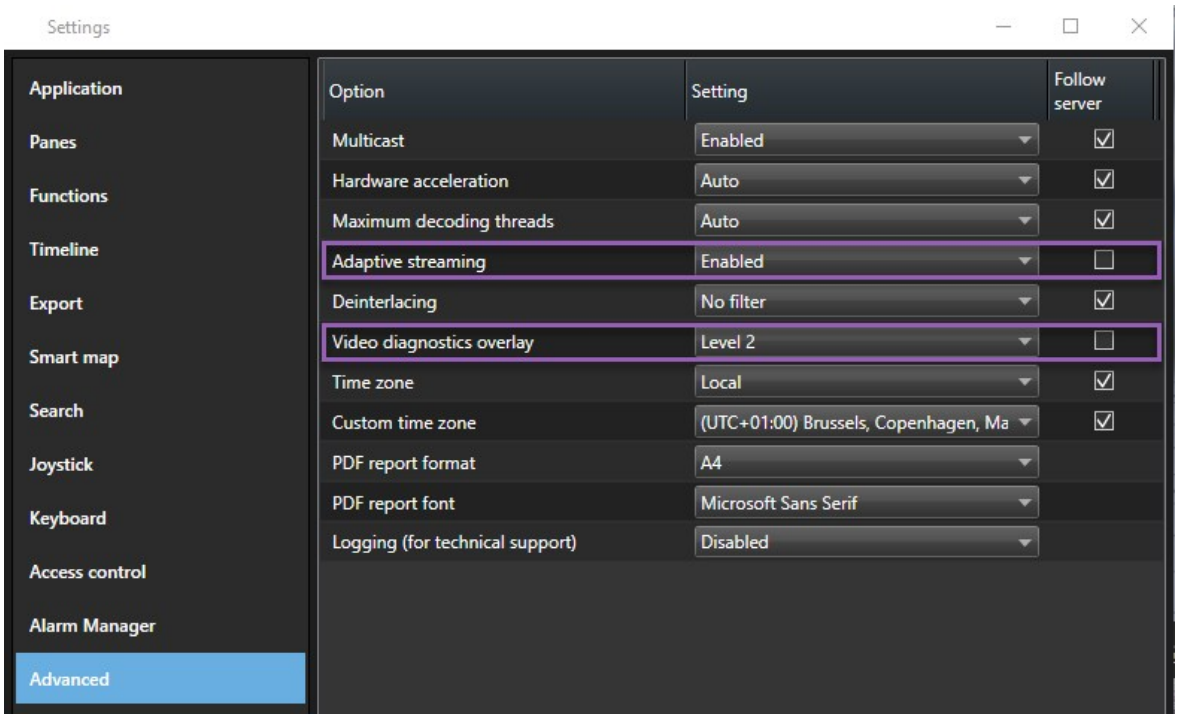
When zooming, the live video stream requested is always the one with the highest resolution.

Bandwidth usage is often reduced when the resolution of the requested streams are reduced. Bandwidth usage also depends on other settings in the configurations of the defined streams.

Check adaptive streaming settings

1. Go to **Settings** > **Advanced** > **Adaptive streaming**.
2. There are two settings for adaptive streaming: **Disabled** and **Enabled**.

   Select **Enabled**.

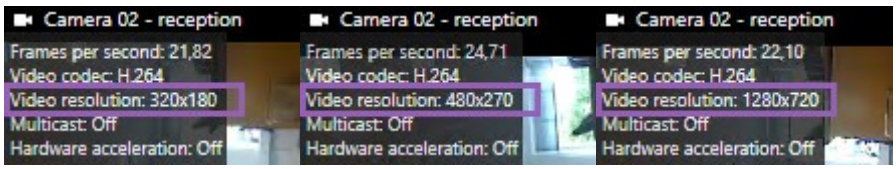


3. Go to **Video diagnostics overlay**.
4. To make the current video resolution of the stream visible, select **Level 2**.

   This setting applies to all view items. The default setting is **Hide**.

5. The video diagnostics overlay should now be **Enabled**.

   Try to resize the view window from small to large, large to small and check if the **Video resolution** value changes.



   If the value doesn't change, continue to examine your available live video streams from your cameras so you can enable adaptive streaming, if possible.

Check available live video streams

To take advantage of adaptive streaming, two or more live video streams with different resolutions must be configured in your camera settings.

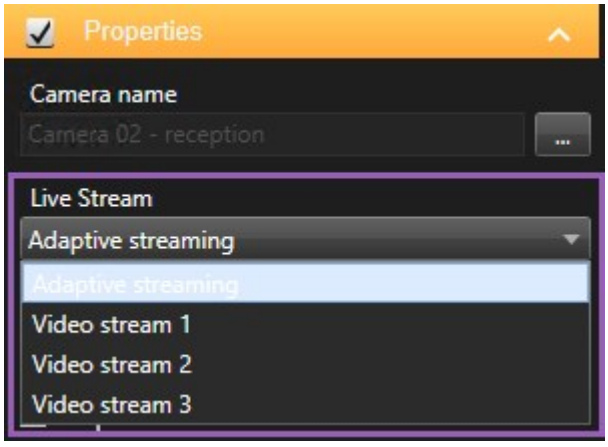
The only supported video resolution format for adaptive streaming is **width x height**. Video resolution formats presented from a camera as 720p, mode2, VGA or a like are not supported.

Not all cameras support multi-streaming.

Multi-streaming allows multiple streams per device to be configured on the server. If multiple streams are configured and adaptive streaming is enabled, you can select **Adaptive streaming** or one of the other available streams.

To make sure that **Adaptive streaming** is configured in a view:

1. Click **Setup** to configure the view.
2. In **Properties**, click the **Live stream** dropdown list, and the list of available live video streams appears.
3. Check if two or more live video streams are available and select **Adaptive streaming**.

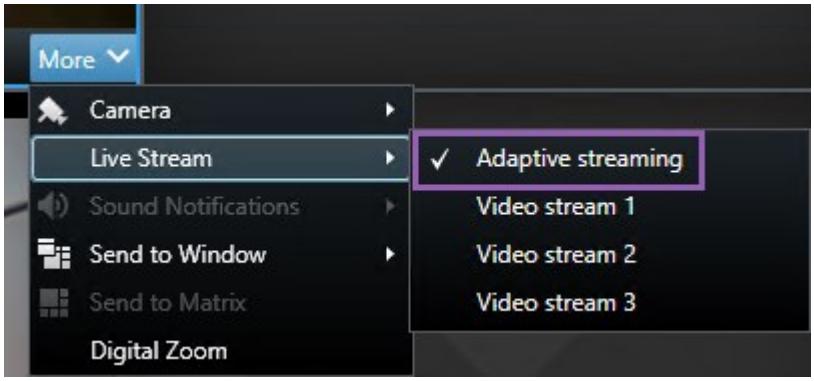


If only one live video stream is available, add more live video streams for the camera in XProtect Management Client.

4. Click **Setup** to close the view configuration.

To make sure that **Adaptive streaming** is selected in a **Live** view item:

1. Click the **More** dropdown list.
2. Select **Live stream**, and the list of available live video streams appears.
3. Check if two or more live video streams are available and select **Adaptive streaming**.



Monitor your system

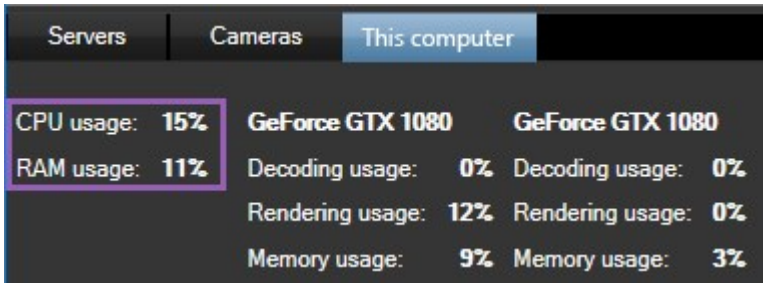
The **System Monitor** tab gives you an overview of the current status of your servers, connected devices, and the computer running XProtect Smart Client.

For more information, see Tabs on page 21.

Monitor client resources

The number of cameras in a view together with the resolution, frame rate, and codec results in a load on your PC running XProtect Smart Client. To observe the current load on **CPU**, **RAM**, and NVIDIA GPU resources:

1. Click and drag the **System Monitor** tab to undock it to a separate window.
2. Select **This computer**.
3. Select a view to monitor the load of the current view.



If your client PC has additional NVIDIA display adapters installed, the load on these GPU's are also visible.

If the load is too high, you can add GPU resources to your PC by installing multiple NVIDIA display adapters. Milestone does not recommend the use of Scalable Link Interface (SLI) configuration of your NVIDIA display adapters.

System Monitor tab with Milestone Federated Architecture (explained)

If you run Milestone Federated Architecture™, the **System Monitor** tab is divided into two parts:

- One pane displays a hierarchical tree-structure representing your federated architecture
- The other pane is a browser-based area with relevant system data for the selected server

Click any server in the site pane to see its system data.

If you move away from the tab or log out of the system and come back, the **System Monitor** tab remembers which server is selected in your federated architecture and continues to display system data from this server.

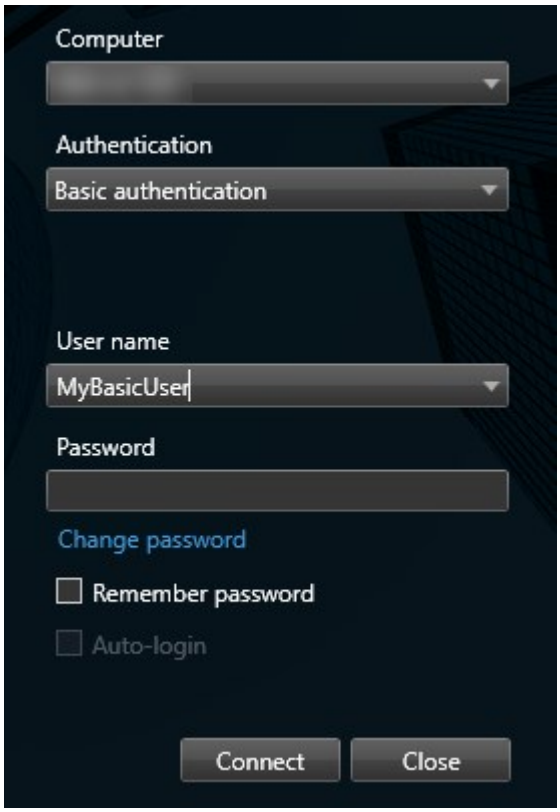
You can drag the **System Monitor** tab to an independent window to monitor multiple servers.

Operation

Logging in and out

Log in

1. Start XProtect Smart Client. The login window appears.



2. Specify the name or address of the server that you want to connect to.
3. Select one of these authentication methods:
   - **Windows authentication (current user)** - select this option to log in with your current Windows user credentials
   - **Windows authentication** - select this option to log in with Windows user credentials that are different from your currently used Windows user credentials
   - **Basic authentication** - select this option to log in as a basic user. Basic users are defined by your system administrator in XProtect Management Client
   - [Name of external IDP] - select this option to log in with an external IDP. .

4. Click **Connect**. If a problem occurs during login, you may receive an error message. See also Logging in (troubleshooting) on page 307.
5. Depending on the configuration, you may be asked to restore the views used in the previous session:
   - **Main view** - this option restores the view that you used last time in the main window
   - **Detached views** - this option restores the view that you used last time in a floating window. Only available when connecting to specific XProtect VMS systems. See also Surveillance system differences on page 33

If you encounter a second dialog during login, you need additional login authorization to get access to XProtect Smart Client.

Log out

1. On the global toolbar, select **User menu**.
2. Select **Log out**.

Smart Client restarts and the login window is shown so you can log in again.

Login authorization (explained)

When you log into the XProtect Smart Client, you may be asked for additional authorization of your login. You need your supervisor, system administrator or someone else who has permission to authorize you to enter their credentials along with yours in the login window. After that, you are good to go.

If you do not know who can authorize you, please ask your system administrator.

Logging into access control systems (explained)

When you log into XProtect Smart Client, you may be asked for additional login credentials for the access control systems, if they are configured to do so.

Your login controls the parts of an access control integration, for example doors, that you can manage and operate.

If you do not know your login credentials for an access control system, please ask your system administrator.

The system remembers your login credentials, so you only need to fill out your credentials the first time you log in or if the login has failed.

Change password in XProtect Smart Client

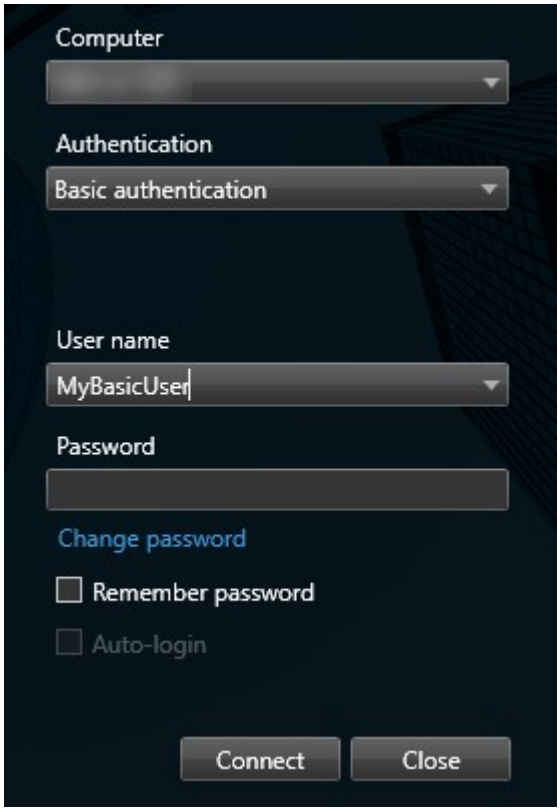
If you log in using as a basic user (**Basic authentication**), you can change your password. If you choose a different authentication method, only your system administrator can change your password. Changing your password often increases the security of your XProtect VMS system.

Requirements

The version of your XProtect VMS system must be version 2021 R1 or later.

Steps:

1. Start XProtect Smart Client. The login window is displayed.
2. Specify your login information. In the **Authentication** list, select **Basic authentication**. A link with the text **Change password** appears.



3. Click the link. A browser window opens.
4. Follow the instructions in the window and save your changes.
5. Log in to XProtect Smart Client using your new password.

Allow connections that use an older security model (HTTP)

If the XProtect VMS server that you are trying to log in to does not have a certificate installed, then you cannot connect with an HTTPS network protocol, the newest available security model in XProtect. In such cases, you are prompted to allow connections with an older security model (HTTP).

If you select the **Remember my choice. Do not show this message again** check box, HTTP connections are always allowed in the future. See also Clear setting that allows connections that use an older security model on page 152.

Clear setting that allows connections that use an older security model

You can clear the setting that allows you to log in to an XProtect VMS server using a network protocol with a connection that use an older security model (HTTP). The next time that you log in, you are then prompted to allow HTTP connections.

> The setting only applies to your user account and the machine that you are currently working on.

Requirements

During the login process, you have allowed HTTP connections and selected the **Remember my choice. Do not show this message again** check box. See also Allow connections that use an older security model (HTTP) on page 151.

Steps:

1. On the global toolbar, select **User menu**, then **Login information**.

   A window appears.

2. Click the **Clear** button.
3. Click **OK** to close the window.

Next time you try to log in, you are prompted to allow HTTP connections.

Managing views

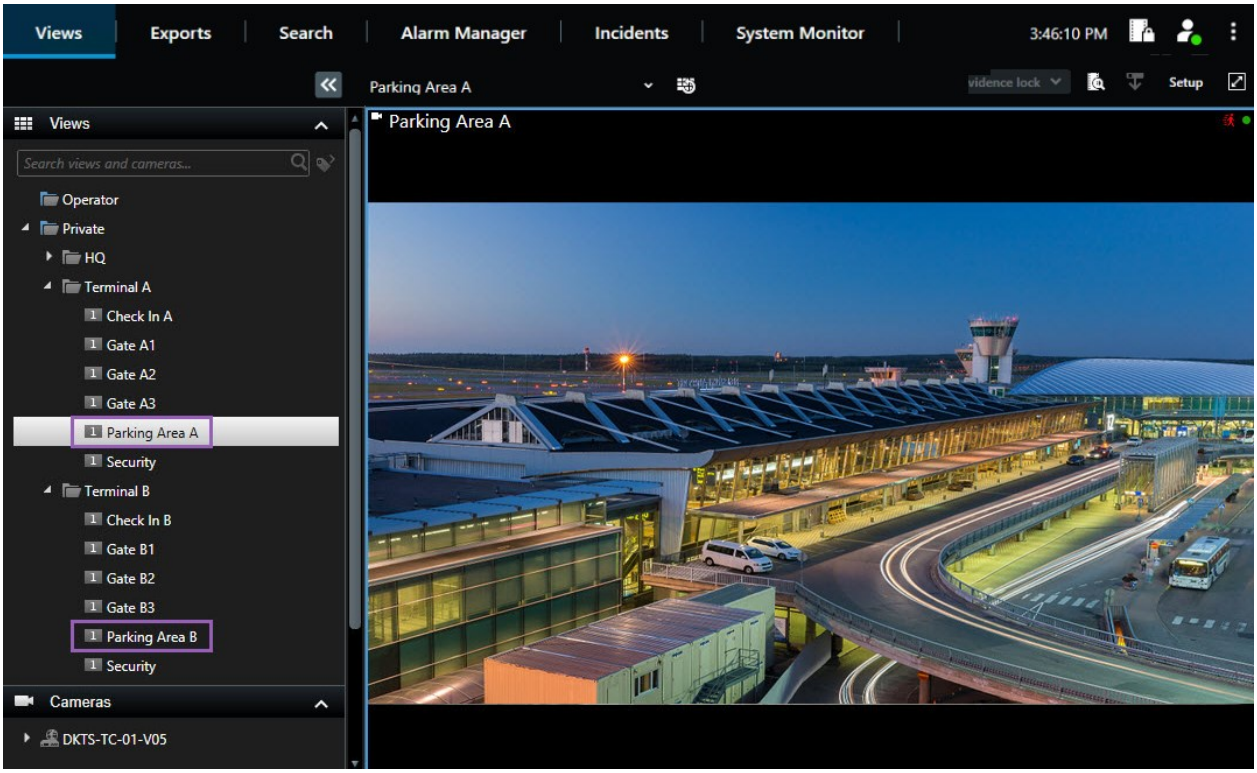
Your views are available in live and playback mode and can contain cameras and other types of content. If views have been assigned shortcut numbers, you can select a view by using keyboard shortcuts. See also Keyboard shortcuts (overview) on page 163.

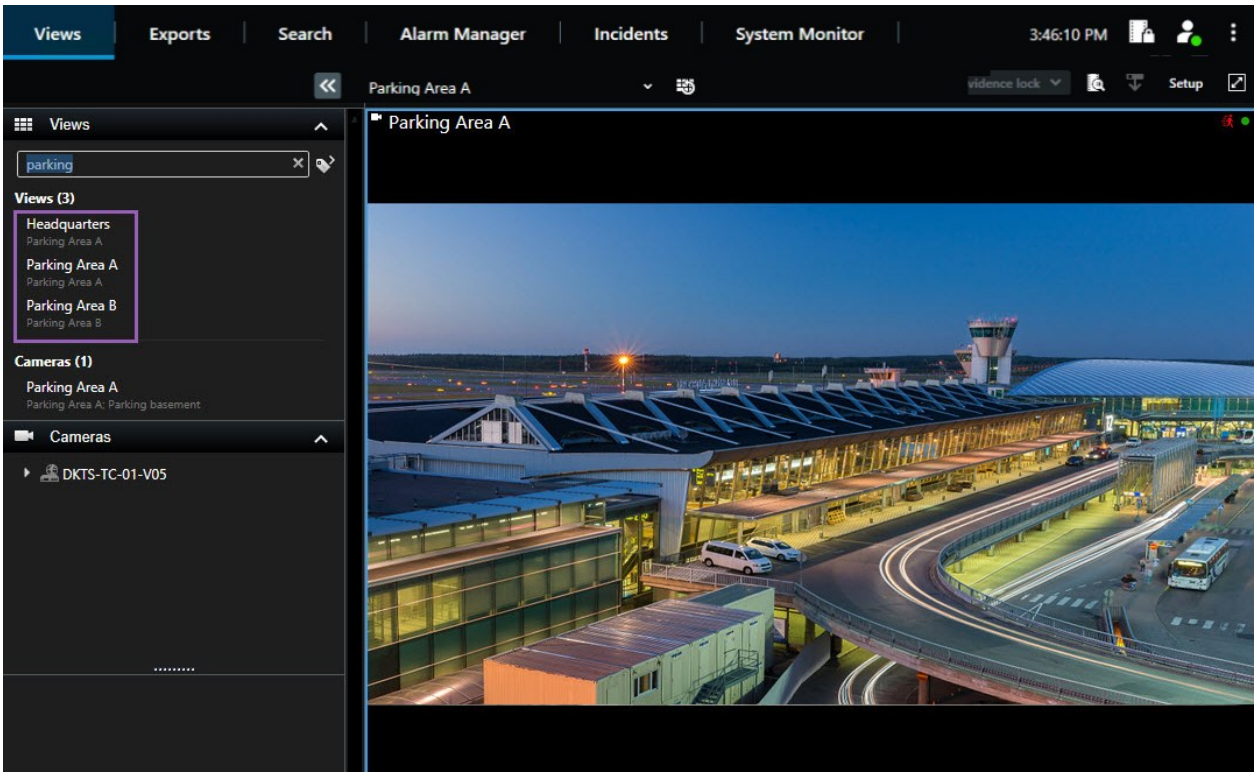
Searching for views and cameras (explained)

If you have a large or complex hierarchy of view groups, the search function makes navigation easier and allows you to search for views, cameras - including camera characteristics (see also Camera characteristics on page 154) - and keywords across the hierarchy. You can find an overview of common keywords if you click  next to the search field.

Example

The following two images show a hierarchy of views and what it looks like when you search for **parking**:


Views
Exports
Search
Alarm Manager
Incidents
System Monitor
3:46:10 PM
Parking Area A
Setup
Views
Search views and cameras...
Operator
Private
HQ
Terminal A
Check In A
Gate A1
Gate A2
Gate A3
Parking Area A
Security
Terminal B
Check In B
Gate B1
Gate B2
Gate B3
Parking Area B
Security
Cameras
DKTS-TC-01-V05
Parking Area A


Views
Exports
Search
Alarm Manager
Incidents
System Monitor
3:46:10 PM
Parking Area A
Setup
Views
parking
Views (3)
Headquarters
Parking Area A
Parking Area A
Parking Area A
Parking Area B
Parking Area B
Cameras (1)
Parking Area A
Parking Area A: Parking basement
Cameras
DKTS-TC-01-V05
Parking Area A

If a top-level folder has a red background  , it is protected. You can still access any views under the protected top-level folder, but you cannot create new views or edit existing views under it.

As you enter the search words, matching results for views and cameras are displayed. When you select one or more of the matching cameras, the cameras appear in a temporary view that is optimized for the number of cameras you select.

To view a single camera in a 1:1 view, click the search result in the **Cameras** section.

To view the first 25 cameras in a view, click the search result in the **Views** section. You can also select cameras manually if you press either **Ctrl** or **Shift** while clicking the cameras. Press **Enter** to view the cameras.

Camera characteristics

- Name
- Description
- Capability:
  - PTZ
  - Audio
  - Input
  - Output
- Views containing a specific camera
- Recording server name or address (shows connected cameras)

Your system administrator can add free text tags in the camera description field on the XProtect VMS server to make it possible to group cameras and search for these tags. An example could be that all outdoor cameras use the tag "Outdoor" in the description field. In that case, you can find all cameras of this type.

Change individual cameras temporarily

You can temporarily change the cameras in a view. However, it does not permanently change the view. If you want to permanently change the content of a view, you must be in setup mode.

Requirements

You can only change the camera if the view item contains a camera.

Steps:

1. Select the relevant item in the view.
2. Do one of the following:
   - In the **Cameras** pane, drag the relevant camera into the wanted view item in the view.
   - On the camera toolbar, click **More** > **Send to window** > **Main window**, and then select a view item in the view.
3. To restore your original view, click  on the workspace toolbar.

In the **Cameras** pane, the list of cameras is grouped by server. If a server is listed with a red icon, it is unavailable, in which case you will not be able to select cameras from that server.

Swap cameras

You can temporarily swap two cameras in a view. The camera in that view item then exchanges places with the one you swap it with. You can only swap cameras with other cameras. This can be useful, for example, if you want to keep all your most important cameras in a certain view item in your view.

Steps:

1. Click the relevant camera title bar and drag it to a new view item.
2. To restore the original view, click  on the workspace toolbar.

If you want to make permanent changes to your view, you must first be in setup mode.

Send video between open views

You can send video from a selected view item with a camera to a single view item with a camera in another open view, including any views you may have in floating windows or on secondary displays.

This feature is not available for view items with hotspots, carousels, or Matrix content.

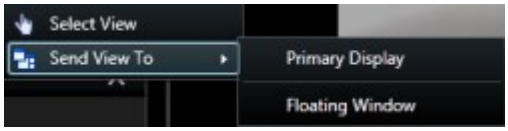
Steps:

1. On the camera toolbar, click **More** > **Send to window**.
2. Select the destination view, and then select the view item in the view where you want the video for that camera to display. If you cannot select some of the view items, they might be unavailable or used for hotspots, carousels, or Matrix content.

Send views between displays

You can send a view to a specific display or a floating window. This is useful, for example, if you have several monitors. Afterwards, you can synchronize the time of the destination display with the time used in the main window.

1. In the **Views** pane, right-click the relevant view.
2. Click **Send view to** and then specify how you want your view to display.



   If more secondary displays are available, they will be numbered.
3. To synchronize the time between the two displays, click **Link window** in the upper-right corner. The timeline is hidden in the destination window, but is still visible in the main window.

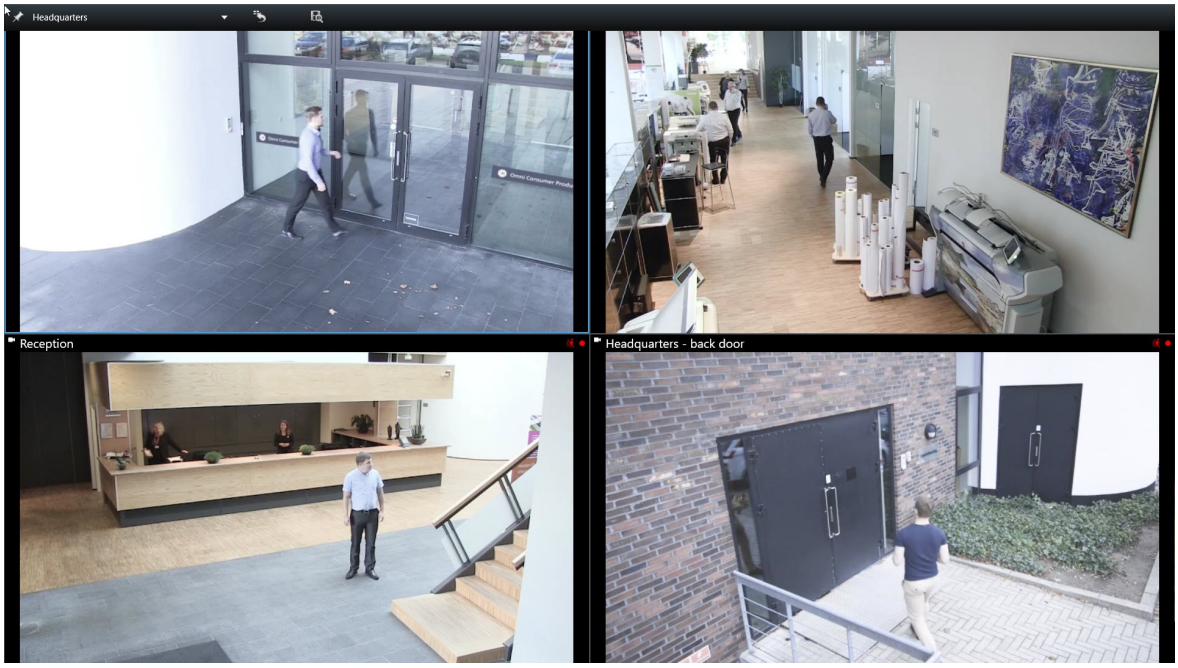
Any view items with hotspots, carousels, Matrix content, still images, or HTML pages included in the view will work as usual in a floating window.

Multiple windows or displays (explained)

You can send individual views to separate windows or displays, while keeping the main window of the XProtect Smart Client in the background, so you can watch several views simultaneously. The selected camera or item is always displayed with a blue border.

You can send any view to:

- A primary display that shows the view in a separate full-screen window on the main display of your computer with the main window hiding behind it

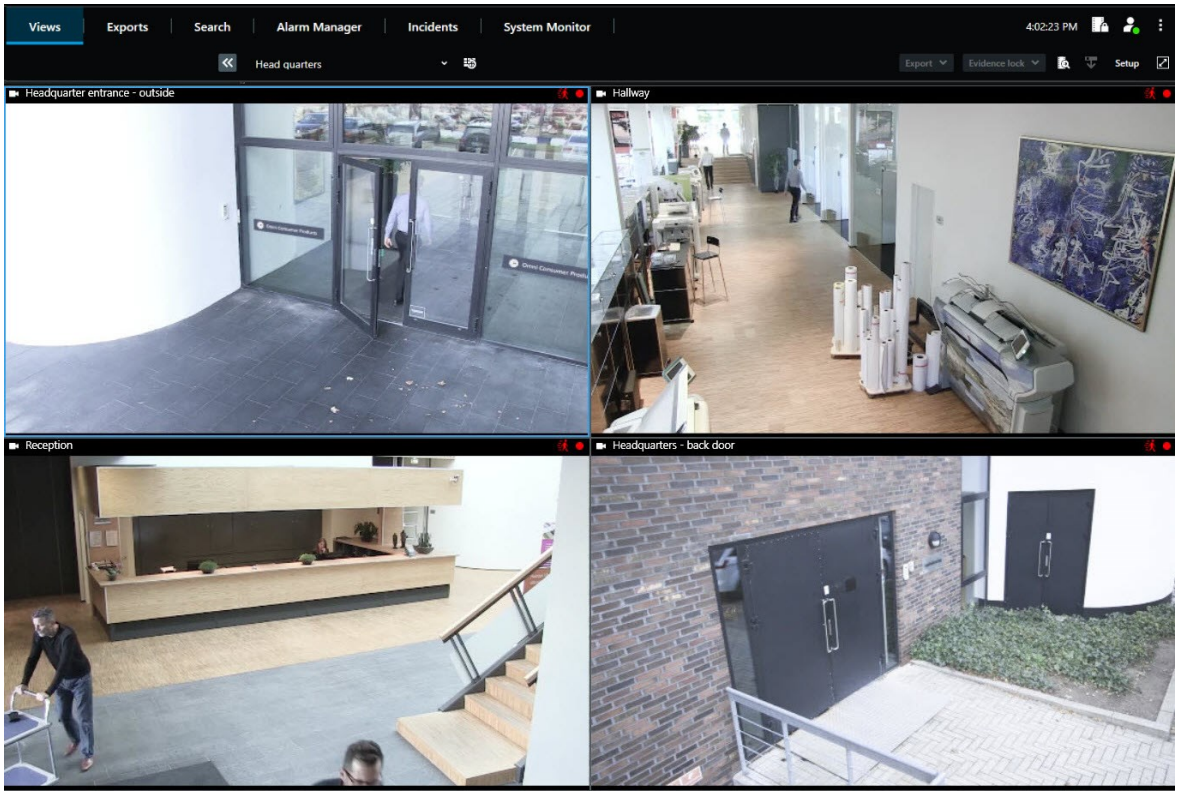


> By default, the tabs and controls are hidden. Press **Esc** to make the tabs and certain controls reappear.

- A secondary display that shows the view in a full-screen window on another monitor (if available). The main window stays visible on the primary monitor

> By default, the tabs and controls are hidden. Press **Esc** to make the tabs and certain controls reappear.

- A floating window that shows the view in a separate window. You can open any number of floating windows and drag them to any monitor that is connected to your computer.



Click **Link window** to synchronize the time in the floating window with the time of the main window.

Your multiple window setup is stored in XProtect Smart Client, so next time you log in, you can reuse it. However, the setup applies only to the computer that you are currently using. To use multiple windows on more than one computer, you must configure your multiple window setup on each computer.

Navigating your cameras and views

Learn about some of the ways of navigating within or between the cameras in XProtect Smart Client.

See also Smart map (explained) on page 260 and Maps (explained) on page 271.

Hotspots (explained)

A hotspot lets you view magnified and higher quality video from a selected camera in a dedicated view item in a view. Hotspots are useful because you can use a low image quality or frame rate for cameras in the regular view items of the view and a high image quality or frame rate for the hotspot. This saves bandwidth on your remote connections.

There are two types of hotspots:

- Global hotspots, which display the selected camera regardless of whether the camera is in the main window or in a secondary display
- Local hotspots, which only display the selected camera of the local display

It is a good idea to have a hotspot in one of the larger view items of a view, for example, the large view item in a **1+7** view.

Use hotspots

- When you click a camera in a view, the hotspot view item updates with video feed of that camera
- The title bar displays the hotspot icon:

When you view live or recorded video, you can double-click a hotspot (or any view items with cameras in a view) to maximize it. When you do this, the video in the hotspot is displayed in full quality, regardless of your image quality selection. If you want to make sure that the selected image quality also applies when maximized, in **Setup** mode, in the **Properties** pane, select **Keep when maximized**.

Carousels (explained)

A carousel is used for displaying video from several cameras, one after the other, in a single view item in a view. You can specify which cameras to include in the carousel as well as the interval between camera changes. Carousels are displayed with the carousel icon on the toolbar: .

Fisheye lens cameras cannot be included in a carousel.

You can maximize a carousel by double-clicking the carousel view item. When you do this, video from cameras included in the carousel is by default displayed in full quality, regardless of your image quality selection. This default cannot be overridden for carousels.

You can use digital zoom and PTZ controls from a carousel if the camera supports this. When you use the PTZ or digital zoom controls that appear, the carousel pauses automatically.

Use carousels

If any of your views contain carousels, this icon will appear in the title bar next to the camera name: .

Requirements

- Carousels must be configured before you can use them. See also Add carousels to views on page 75.
- In the **Settings** window, **Default for camera title bar** must be set to **Show**.

Steps:

1. In live mode, open a view that contains a carousel. When you hover over the view item, this toolbar appears:  .
2. The carousel starts automatically. To pause it, click the **Pause** button.
3. To shift to the next or previous camera in the carousel, click the **Previous camera** or **Next camera** button.
4. Additional actions available in the toolbar:
    - Jump to the place on the smart map, where the camera is located
    - Start search from the camera currently in focus, in a new window
    - Create snapshot
    - Copy to clipboard

You can maximize a carousel by double-clicking the view item with the carousel. Video from cameras included in the carousel is by default displayed in full quality, regardless of your image quality selection.

Digital zoom (explained)

Digital zoom lets you magnify a portion of a given image so you are able to have a closer look at it. It works both in live and playback mode.

Digital zoom is a useful feature for cameras that do not have their own optical zoom capabilities. Using digital zoom will not affect any recording of the video. Recording will still take place in the regular format of the camera.

For non-PTZ cameras, digital zoom is enabled by default. If you enable or disable digital zoom on one camera, all cameras in your view are affected. For PTZ cameras, this setting only applies to one camera at a time.

When you export video data, you can choose to export the regular images or the digitally zoomed images in the AVI or in the JPEG formats. When you export in the XProtect format, this is unavailable because the recipient can use digital zoom on the exported recordings. If you print an image on which you have used digital zoom, the digitally zoomed area of the image will be printed.

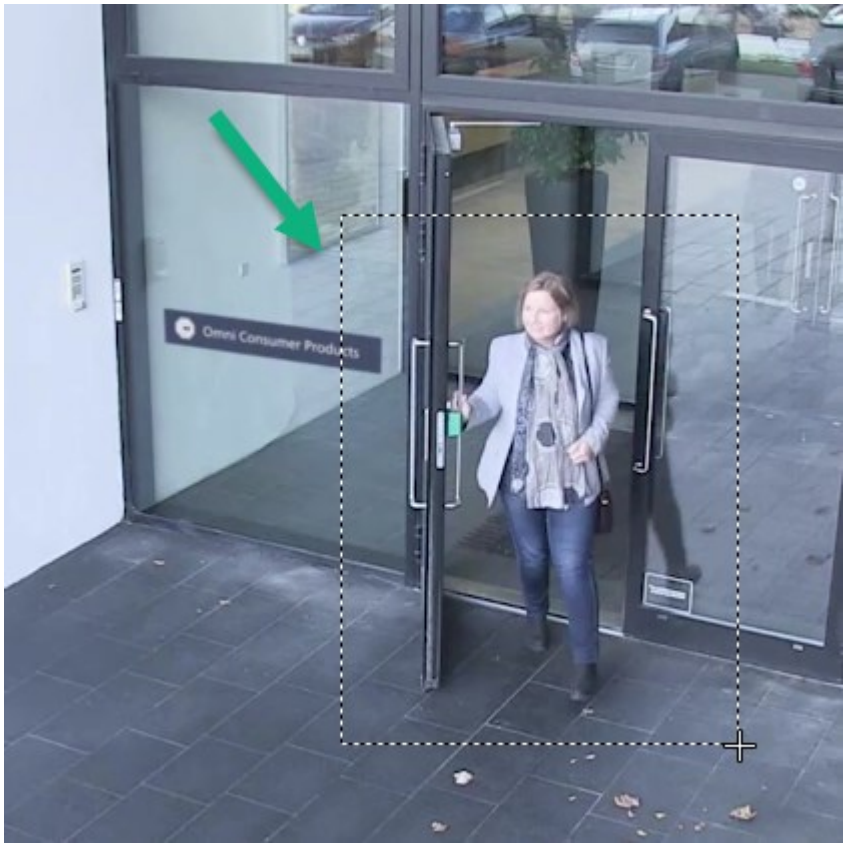
Use digital zoom

Requirements

To enable digital zoom, on the camera toolbar, click **More** and select **Digital zoom**.

Steps:

1. Click and drag inside the image to zoom. The area you select is highlighted by a dotted line. When you release the mouse button, the zoom will take effect.



2. To move to other areas of the image while maintaining your zoom level, in the overview frame, drag the highlighted area to the required position.

3. To adjust the zoom level, click inside the image and use the scroll wheel on your mouse.
4. Click the **Home** icon inside the virtual joystick to return to the normal zoom level.

Virtual joystick and PTZ overlay buttons (explained)

If your views include fisheye cameras or lenses, or PTZ devices, you can navigate the images by using the virtual joystick or the PTZ navigation buttons that may appear inside the image. See also PTZ and fisheye lens images (explained) on page 252.

The virtual joystick:

If you do not want the camera toolbar to pop up when you hover over the view item, press and hold the **CTRL** key while moving the mouse.

Views and shortcuts (explained)

You can use keyboard shortcuts to select views if the views have been assigned numbers. You assign numbers to the views in setup mode. See also Setup mode (overview) on page 35.

Using keyboard shortcuts to select a view only works if you are using a numeric keypad.

Example

If you have assigned the number **1** to a particular view, you select the view by pressing ***** + **1** + **Enter**.

Keyboard shortcuts (overview)

In live or playback mode, a number of keyboard shortcuts allow you to navigate within and between views.

These shortcuts cannot be used for view items with Matrix content or static images.

You can also assign your own custom shortcut key combinations for particular actions in XProtect Smart Client. See also Keyboard settings on page 48.

Press these keys	To do this
Enter	Toggle maximized and regular display of the selected view item in the view.
Alt	Select a specific view item within a view. First, press **Alt**. A number is displayed for each open window. If, for example, you want to select a view item in the second window, press **2**. Multiple numbers now appear, one for each view item that is visible in the second window. Press the number of the view item that you want to select, for example **4**. When a view item is in focus, it is marked with a blue frame. If you are using a PTZ camera or a hotspot, this allows you to control cameras with a joystick or to send the view item directly to the hotspot without using the mouse.

Press these keys	To do this
/+<camera shortcut number>+Enter	Change the camera in the selected view item to the camera with the matching shortcut number. Example: if the required camera has the shortcut number **6**, press **/+ 6+Enter**. Camera shortcut numbers may not necessarily be in use on your XProtect VMS system. They are defined on the server.
/+Enter	Change the camera in the selected view item to the default camera.
/+/+Enter	Change the cameras in all view items to the default cameras.
***+<view shortcut number>+Enter**	Change the selected view to the view with the matching shortcut number. Example: if the required view has the shortcut number **8**, press ***+ 8+Enter**. If view shortcut numbers are used, you can see them in the **Views** pane, where they appear in parentheses before the names of the views.
6 (numeric keypad only)	Move the view item selection one step to the right.
4 (numeric keypad only)	Move the view item selection one step to the left.
8 (numeric keypad only)	Move the view item selection one step up.
2 (numeric keypad only)	Move the view item selection one step down.

Viewing live video

You view live video mainly when in live mode. To view live video, you must find a view that shows video from the cameras that you are interested in. Select the **Views** tab and then the relevant view from the **Views** pane. For each camera that appears in a view, different actions are available, for example taking snapshots or starting manual recording. See also Camera toolbar (overview) on page 166. If something catches your attention, you can zoom in to take a closer look using the virtual joystick.

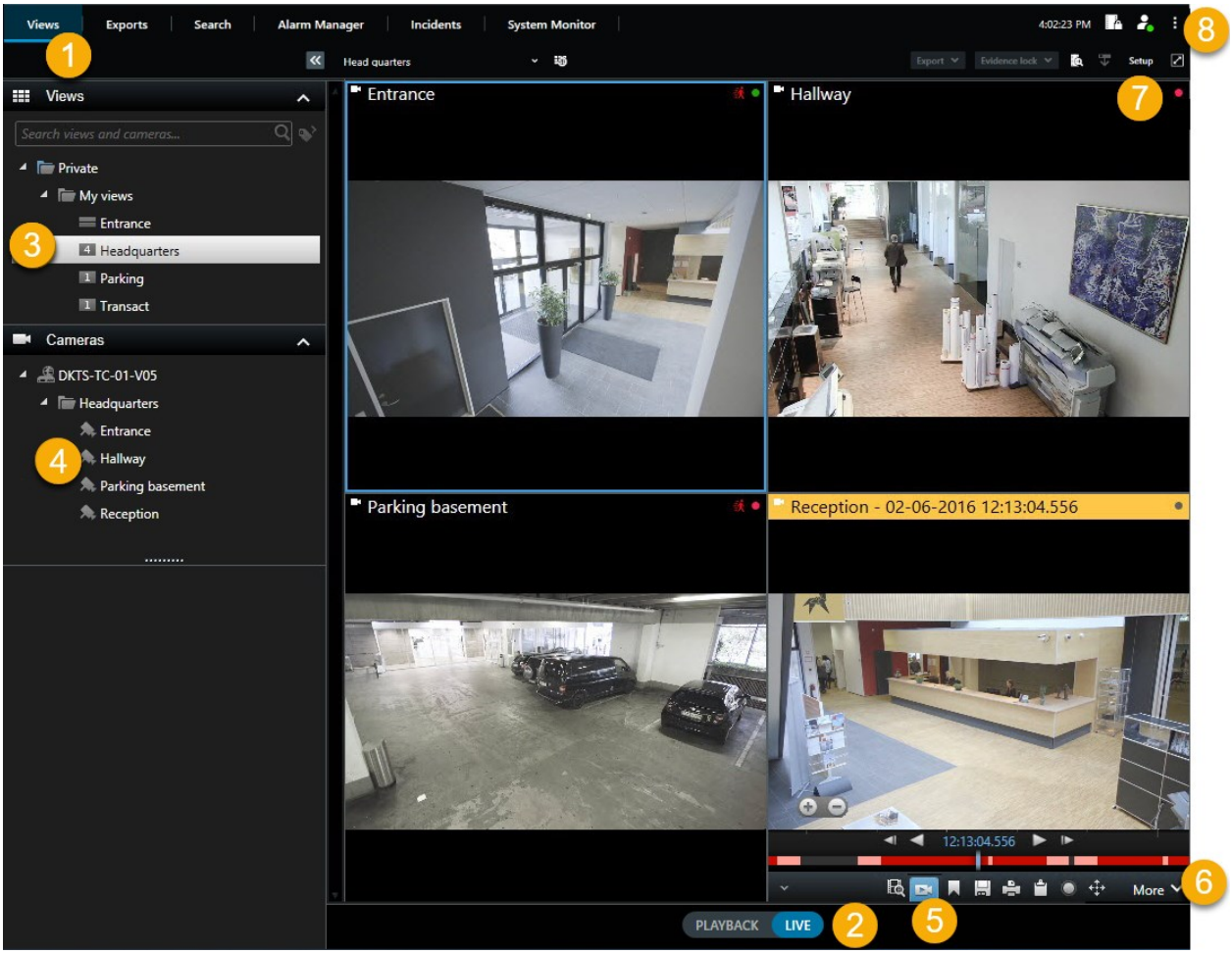
Live video (explained)

The video stream from the camera is not necessarily being recorded. Typically, recording takes place according to a schedule, for example, every morning from 10.00 to 11.30. Or whenever the XProtect VMS system detects special events, for example, motion generated by a person entering a room, a door is opened, or similar.

> If multiple streams have been set up on the server, you can temporarily view a different stream by selecting this from the camera toolbar. On the camera toolbar, click **More** and then select a stream from the available list.

To investigate an incident that was recorded, enter into playback mode. To perform advanced searches, go to the **Search** tab.

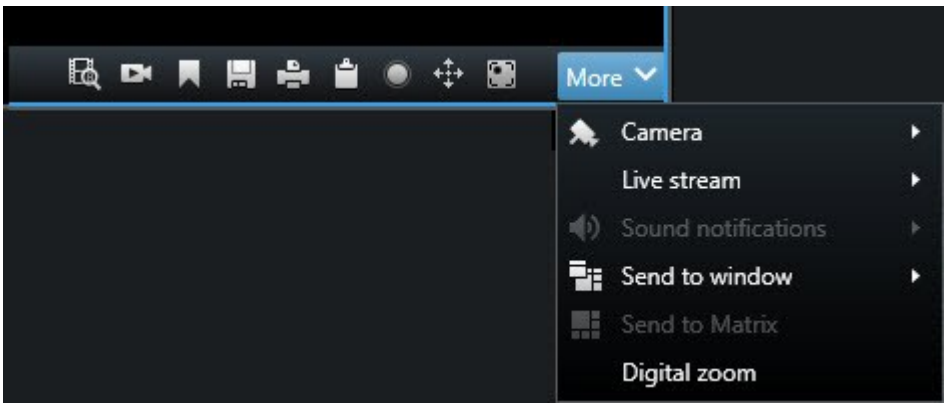
Live mode (overview)



Number	Description
1	The **Views** tab. See also Tabs on page 21.
2	Switch to live mode.
3	Select a view.
4	Change cameras in views temporarily. See also Change individual cameras temporarily on page 154.
5	View recorded video for individual cameras. See also View recorded video independently of timeline on page 177.
6	The camera toolbar. See also Camera toolbar (overview) on page 166.
7	Enter or exit setup mode to add cameras and other types of content to your views.
8	Buttons. See also Buttons on page 24.

Camera toolbar (overview)

The camera toolbar appears whenever the cursor hovers over a camera inside a view. The camera toolbar is available both in live and playback mode.



Icon/menu	Description
	Open a new search window where the camera is preselected. See also Start search from cameras or views on page 216.
	View recorded video independently of the timeline. See also View recorded video independently of timeline on page 177.
	Bookmark the video. See also Add or edit bookmarks on page 235.
	Take simple snapshots of what you are viewing. See also Take single snapshots on page 169.
	Print a surveillance report from a single camera. See also Print report from single cameras on page 185.
	Copy single images to the clipboard. See also Copy images to clipboard on page 187.
	Record video manually from a single camera. See also Record video manually on page 169.
	Work with preset positions for fisheye and PTZ cameras. See also PTZ and fisheye lenses (usage) on page 251.
Digital zoom	Enable digital zoom. See also Use digital zoom on page 161.
Send to window	Change the camera in the view item temporarily. See also Change individual cameras temporarily on page 154.
Camera	Select a camera.

Hide camera toolbar

When you minimize the camera toolbar in a view item, the toolbar remains minimized only to you in the current session. However, you can hide it permanently for a particular view item, for all users with access to the view item.

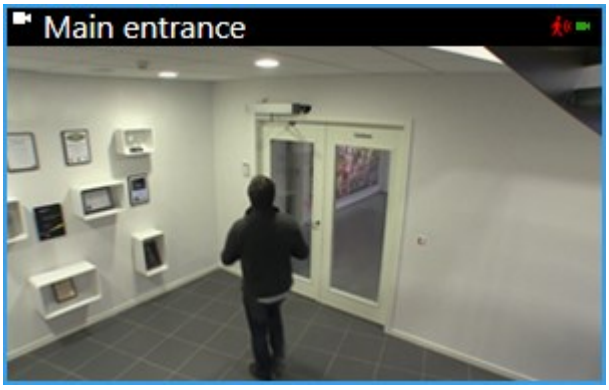
Steps:

1. Click **Setup** to enter setup mode.
2. Find the view item where you want to hide the toolbar.
3. Click  to hide the toolbar.
4. Click **Setup** again to exit setup mode. Your changes are saved.

The setting you make in setup mode is stored on the server, so that the change impacts other XProtect Smart Client operators.

Camera indicators (explained)

The camera indicators show you the status of the video that is displayed in the camera view items. The camera indicators are visible only if the camera title bar is enabled in the **Settings** window on the **Application** tab.



You can turn the camera title bar on and off on individual view items. Click **Setup** and select the **Show title bar** check box in the **Properties** pane.

Indicator	Description
	Motion is detected. Click inside the image to reset the motion indicator.
	The server connection to the camera is lost.
	Video from the camera is being recorded.

Indicator	Description
	A connection to the camera is established. This icon is only relevant for live video.
	Playing back recorded video.
	No new images have been received from the server for more than two seconds.

In the camera properties, you can add sound to notify you when there is motion.

Record video manually

Recording while watching live video is useful if you see something of interest.

Steps:

On the camera toolbar for the view item that you want to record, select one of the following options:

-  Start recording for # Minutes

  Once started, recording will continue for the number of minutes determined by your system administrator. You cannot change this, and you cannot stop recording before the specified number of minutes has passed.

-  Start manual recording

  Once started, recording will continue for the number of minutes determined by your system administrator, or you can click the icon again  to stop manual recording.

  You can start recording the video stream from more than one camera simultaneously, but you must select them one by one.

Take single snapshots

As you are viewing live or recorded video, or searching for video, you can take an instant snapshot that you can share. The path to the folder, where the still image is saved, is specified in the **Settings** window under **Application settings**.

Requirements

In the **Settings** window under **Application**, **Snapshot** must be set to **Available**.

Steps:

1. In live or playback mode:
    1. Hover over a view item that contains a camera, a hotspot, or a carousel.
    2. In the camera toolbar, click  . The icon momentarily turns green.
2. If you are on the **Search** tab, double-click a search result and click  in the camera toolbar. The icon momentarily turns green.
3. To access the snapshots, go to the file location where the snapshots are saved. See Settings in XProtect Smart Client on page 37.

If the image contains a privacy mask, this privacy mask is also applied to the snapshot image.

Investigating incidents

You investigate incidents mainly in playback mode by using the timeline to browse recorded video. To view recorded video, you must find a view that shows video from the cameras that you are interested in. The views are available in the **Views** pane. For each camera that appears in a view, different actions are available, for example taking snapshots or launching search. See also Camera toolbar (overview) on page 166. If something catches your attention, you can zoom in to take a closer look using the virtual joystick.

You can perform advanced searches on the **Search** tab and use the search results as a starting point for further investigation or actions, for example exporting and bookmarking.

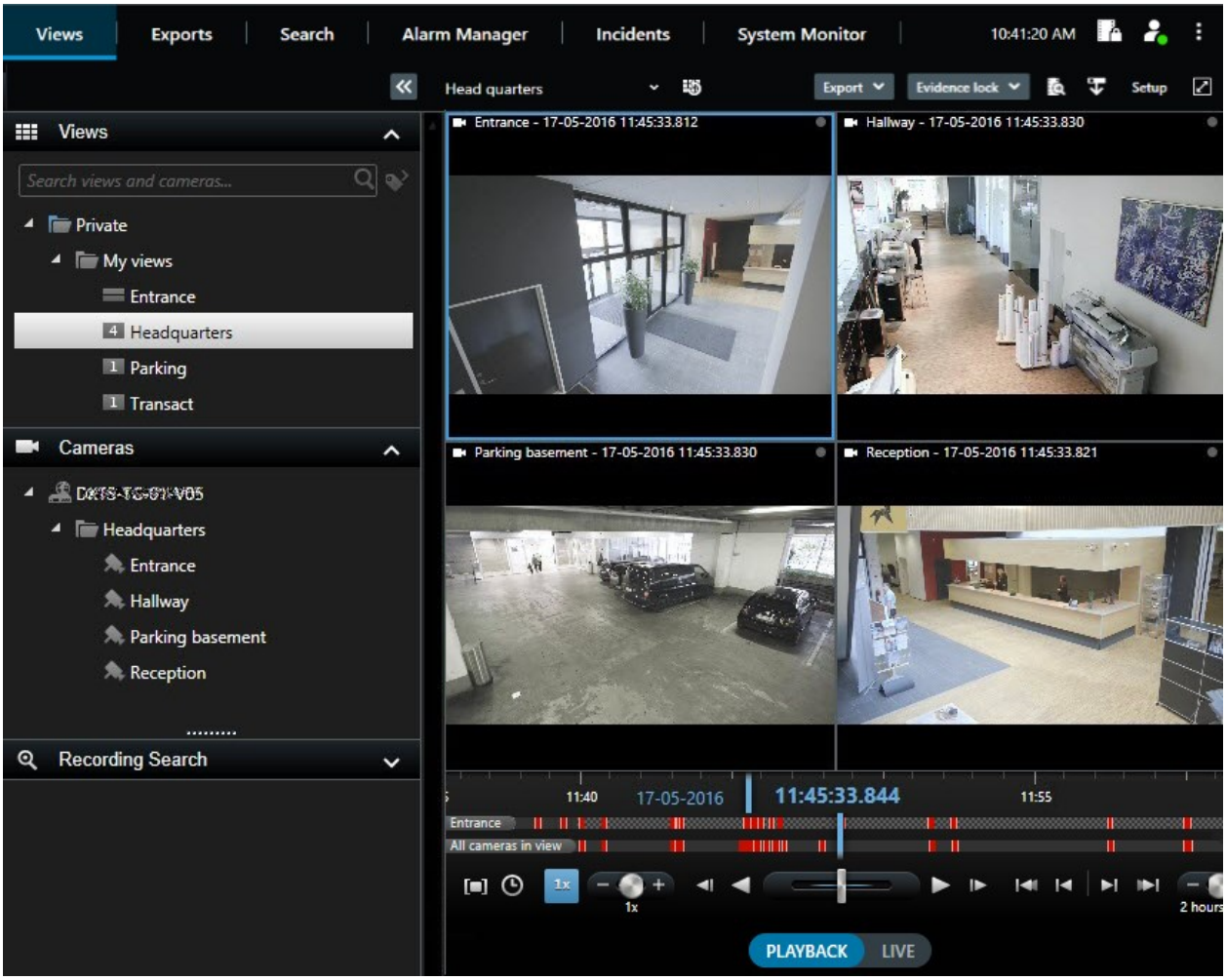
If the incident is associated with an alarm, go to the **Alarm Manager** tab, or select a view where the **Alarm List** has been added.

If you have an **Incidents** tab in Smart Client, you have XProtect® Incident Manager. See XProtect Incident Manager (explained) on page 29. If you do not have XProtect Incident Manager or want to investigate incidents with the built-in Smart Client functionality, you use the features and methods described in this section.

Viewing recorded video (explained)

There are different ways of viewing recorded video:

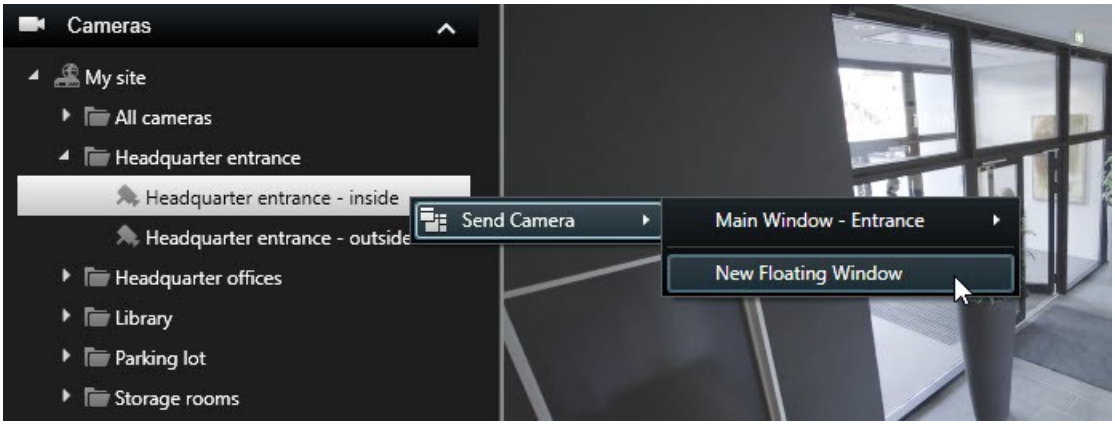
In playback mode



In playback mode, all cameras in a view display recordings from the same point in time, the master time. You can play back or browse recordings by using the timeline. See also Time navigation controls (overview) on page 175.

However, you can also view and navigate recordings from individual cameras independently of the master time. **Independent playback** must be enabled in the **Functions** settings. See also Functions settings on page 41.

If you are accessing your cameras through the tree structure in the **Cameras** pane, you can open individual cameras in a new window when in playback mode.



In live mode

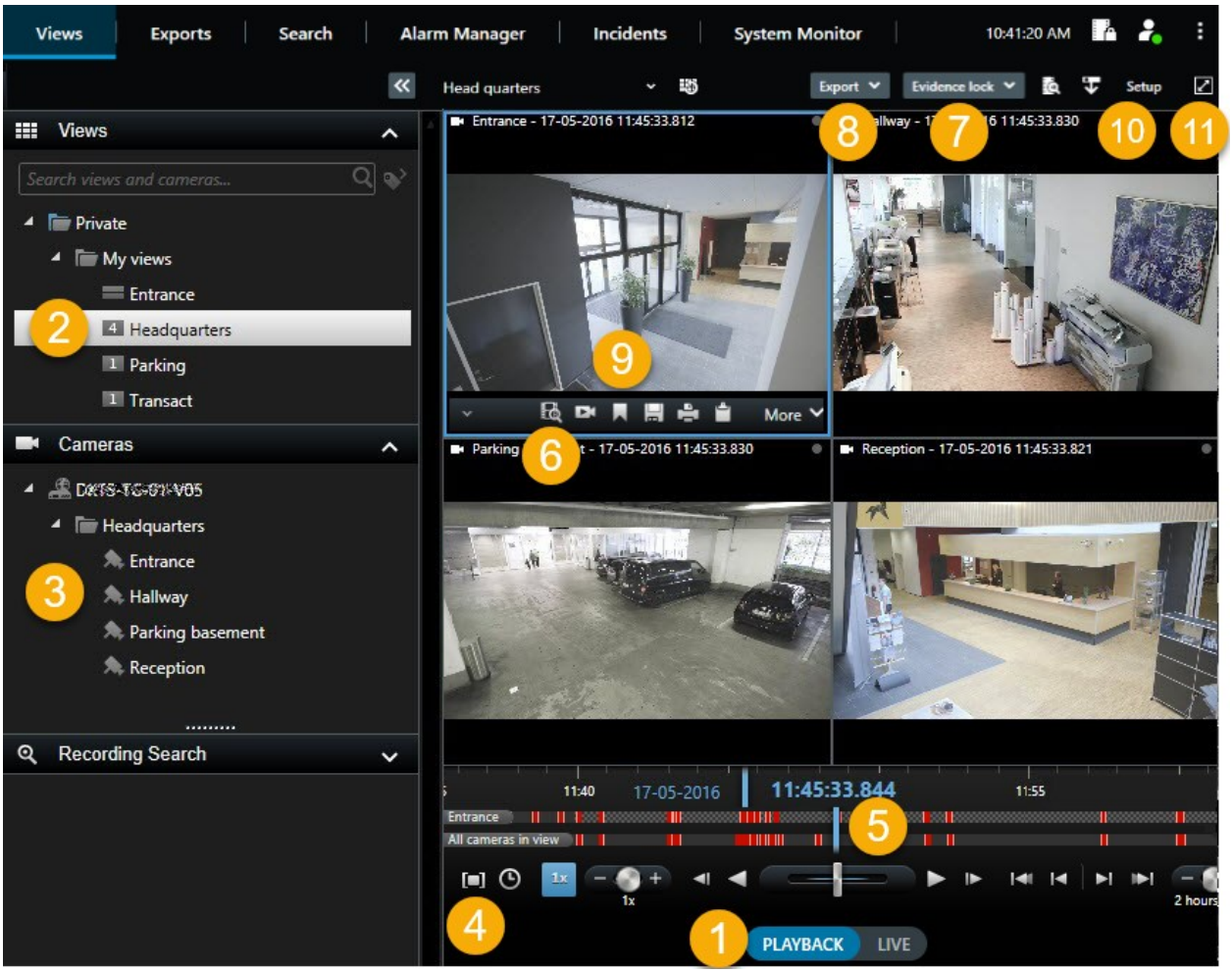
In live mode, you can watch recorded video for individual cameras by clicking the button in the camera toolbar. This will open a new window where you can play back or browse the recordings. **Camera playback** must be enabled. See also Functions settings on page 41.

On the Search tab

The search results are basically video sequences that you can play back:

- Preview the search results. See also Preview video from search results on page 217
- Play back the search results in full screen mode or in a separate window. See also Open search results in separate windows on page 216

Playback mode (overview)



Number	Description
1	View recorded video in playback mode.
2	Select a view in the tree structure or use keyboard shortcuts. See also Keyboard shortcuts (overview) on page 163.
3	Change individual cameras temporarily. See also Change individual cameras temporarily on page 154.

Number	Description
4	Select a time span for exporting video. See also Time navigation controls (overview) on page 175.
5	Browse using the timeline. See also Timeline (explained) on page 174.
6	Open a new search window with the camera preselected. See also Start search from cameras or views on page 216.
7	Create an evidence lock.
8	Export video data. See also Export video, audio, and still images on page 179.
9	Perform various actions on the camera toolbar. See also Camera toolbar (overview) on page 166.
10	Enter or exit setup mode to add cameras and other types of content to your views.
11	Switch to full screen mode.

Timeline (explained)

The timeline displays an overview of periods with recordings from all cameras displayed in your current view. Two timelines are displayed in the timeline area:

- The upper timeline shows the recording periods of the selected camera
- The lower timeline is for all the cameras in the view, including the selected camera. If you have linked floating windows, these will also be included on the lower timeline

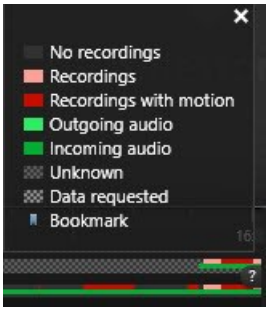
Drag the timeline to the right or left to move in time, or use the scroll wheel of your mouse.

To adjust the range of the timeline, press **CTRL** and use the scroll wheel at the same time.

You will see these colors in the timeline:

- Light-red indicates recordings
- Red indicates motion
- Light green indicates outgoing audio
- Green indicates incoming audio

For a legend of the color codes, to the far right, click the small question mark.



Additional markers and colors

If there are additional sources of data available in your XProtect VMS system, incidents from these sources are shown as markers in other colors. The incidents can appear as pop-ups in the timeline.

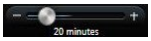
To view markers and colors from additional sources, **Additional data** and **Additional markers** must either be enabled in the timeline settings or server-side by your system administrator.

Bookmarks in the timeline (explained)

Bookmarks in the timeline are indicated with a blue bookmark icon:  . To view the bookmarked video, place your mouse over the icon.

Time navigation controls (overview)

Number or control	Description
1 and 2	The playback date and time is the time to which all the cameras are tied. When you play back recordings, all cameras in the view will show video from the same time. Some cameras, however, may only record if motion is detected. Also, there may be no recorded video from one or more cameras in the view matching the specified point in time. Then, the last image in the database prior to the specified point in time will be dimmed.
3	The time of the timeline is indicated by a blue vertical line.
	Select a period of time by dragging the start and end time indicators on the timeline - typically when you are exporting video. Click again to see the timeline with no time selected.
	Jump to a specific point in time by specifying the date and time.
	The playback speed slider lets you change the current playback speed. Move the slider to the left for slow motion, and to the right for fast motion. Click **1x** for normal speed.
	Move to the image just before the one currently viewed.
	Play backward in time. When selected, it turns into a pause button.
	Adjust the speed. Drag it to the right to increase forward play speed. Drag to the left to increase backward play speed.
	Play forward in time. When selected, it turns into a pause button.
	Move to the image just after the one currently viewed.
	Move to the first image in the database for the selected camera.

Number or control	Description
	Move to the first image in the previous sequence.
	Move to the first image in the following sequence.
	Move to the last image in the database for the selected camera.
	Specify the time span of playback in the timeline.

View recorded video independently of timeline

You can play back video independently for individual cameras. In playback mode, the playback is independent of the selected main timeline. In live mode, the playback is independent of the live video.

You can only use this feature for ordinary view items with a single camera, not for view items with hotspots, carousels, or Matrix content.

Requirements

In the **Settings** window > **Functions** tab, you must set the **Independent playback** option to **Available**.

Steps:

1. Move your cursor to the bottom of the camera from which you want to view recorded video independently. On the toolbar that appears, select **Independent playback**.

   The top bar for the view item with the camera turns yellow, and the independent playback timeline appears:

   In live mode, the video starts by replaying the video from 10 seconds before selecting the **Independent playback** button. In playback mode, what happens depends if the video is played or paused. If playing, the independent playback jumps 10 seconds from the current time on the main timeline in the opposite direction of the current playback direction and plays the video. If you have paused the video when in playback mode and select independent playback, the video remains paused at the current time on the main timeline.

2. Optionally. Drag the timeline to see recorded video from another time.
3. Optionally. To view recorded video from all cameras in your view from the same time as in the view item with independent playback, click the **Use the selected time on the playback timeline** button: .

   This displays all cameras synchronized to the time you initially selected for the independent playback in playback mode.

Investigate your search results

There are different ways of investigating incidents that you have found on the **Search** tab:

- Open the search result in a separate window in playback mode. See also Open search results in separate windows on page 216
- Open the search result in a detailed view. Do one of the following:
  - In the list of search results, double-click the search result to view it in full screen mode. Double-click again to return to the list of search results
  - If you are previewing your search result in the preview area, double-click inside the video image. The search result opens in full screen mode. Double-click again to return to the preview area

Create video evidence

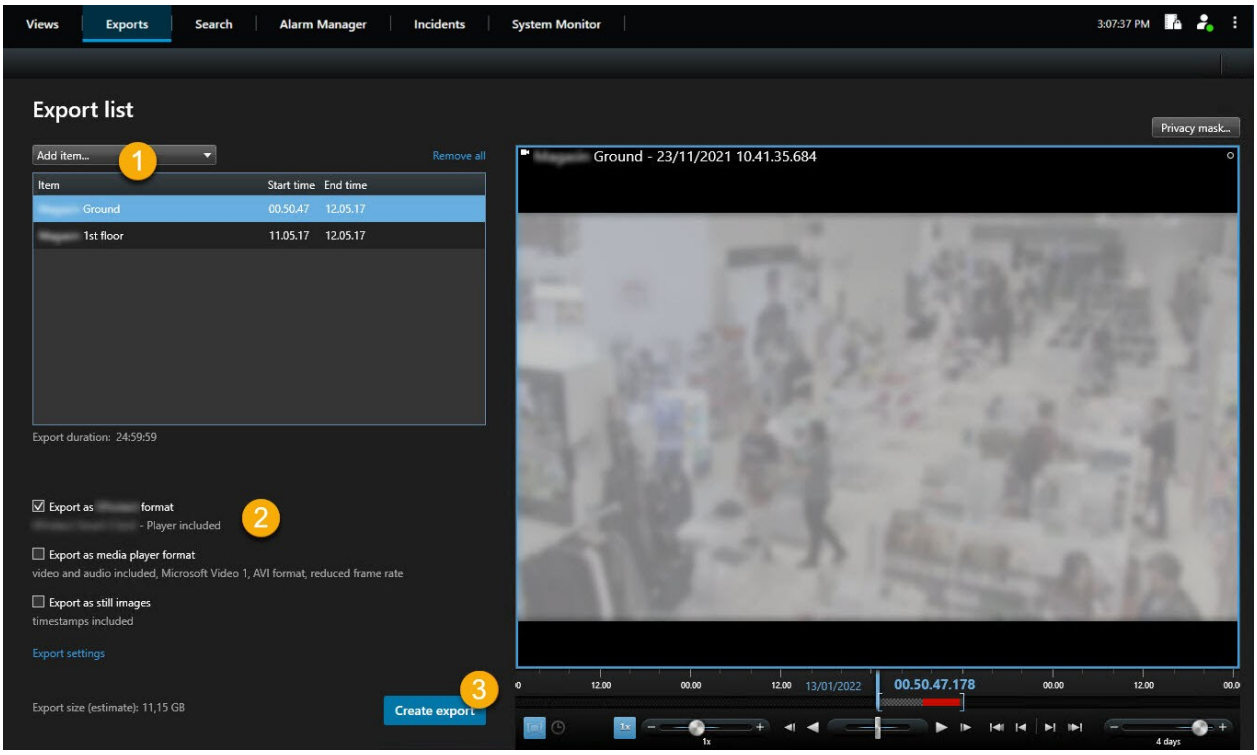
There are several ways of documenting incidents and events in XProtect Smart Client, for example by exporting recordings and creating single still images from the video stream.

You can lock video evidence to prevent it from being deleted, or you can export the locked video.

Export video, audio, and still images

To share video evidence, you can export video and associated audio in different formats. You can also export still images and other types of data that—depending on your XProtect VMS system—may be available.

On the **Exports** tab, you can export video evidence in three steps:



1. Add the video sequences that you want to export to the **Exports** tab > **Export list**. See also Add video sequences to the Export list on page 179.
2. Select at least one export format and adjust the export settings. See also Adjust export settings on page 180.
3. Create the export. See also Create the export on page 182.

Add video sequences to the Export list

You can add video sequences to the **Export list** on the:

Exports tab

In the **Export list**, select **Add item** to add the video sequences that you want to export.

In playback mode

You have two options. Either:

1. In the timeline, select the  button to select the start and end time (see Time navigation controls (overview) on page 175) of the sequence that you want to export.
2. For each item that you want to include in the export, select the associated check box  .
3. Select **Export** > **Export** to add the selected video sequences to the **Export list** and to move to the **Exports** tab.

   OR:

   Select **Export** > **Add to export list** to add the selected video sequences to the **Export list** and to stay in playback mode.

Or alternatively, select **Evidence lock** > **View** > **Evidence lock list**

1. In the **Evidence lock list**, select an existing evidence lock.
2. Select **Add to export list** to add the selected evidence lock to the **Export list** and to stay in playback mode.

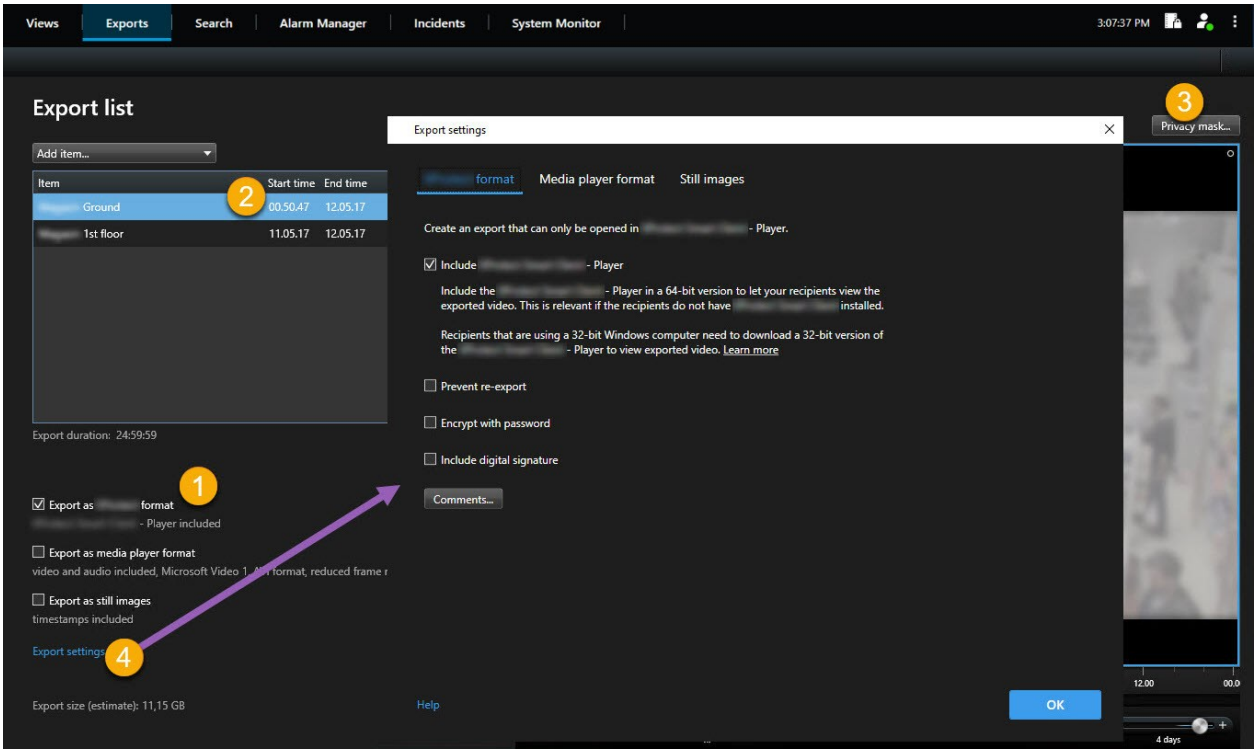
Search tab

1. If you want to export all your search results at one time, select the **Select all** button  on the workspace toolbar in the upper-right corner.
2. For each search result that you want to export, hover over it and select the blue check box  .
3. In the blue action bar, select **Add to export list**  .

Adjust export settings

After you added at least one sequence to the **Exports** tab > **Export list**, you must select at least one export format. Optionally, you can adjust export settings.

Steps:



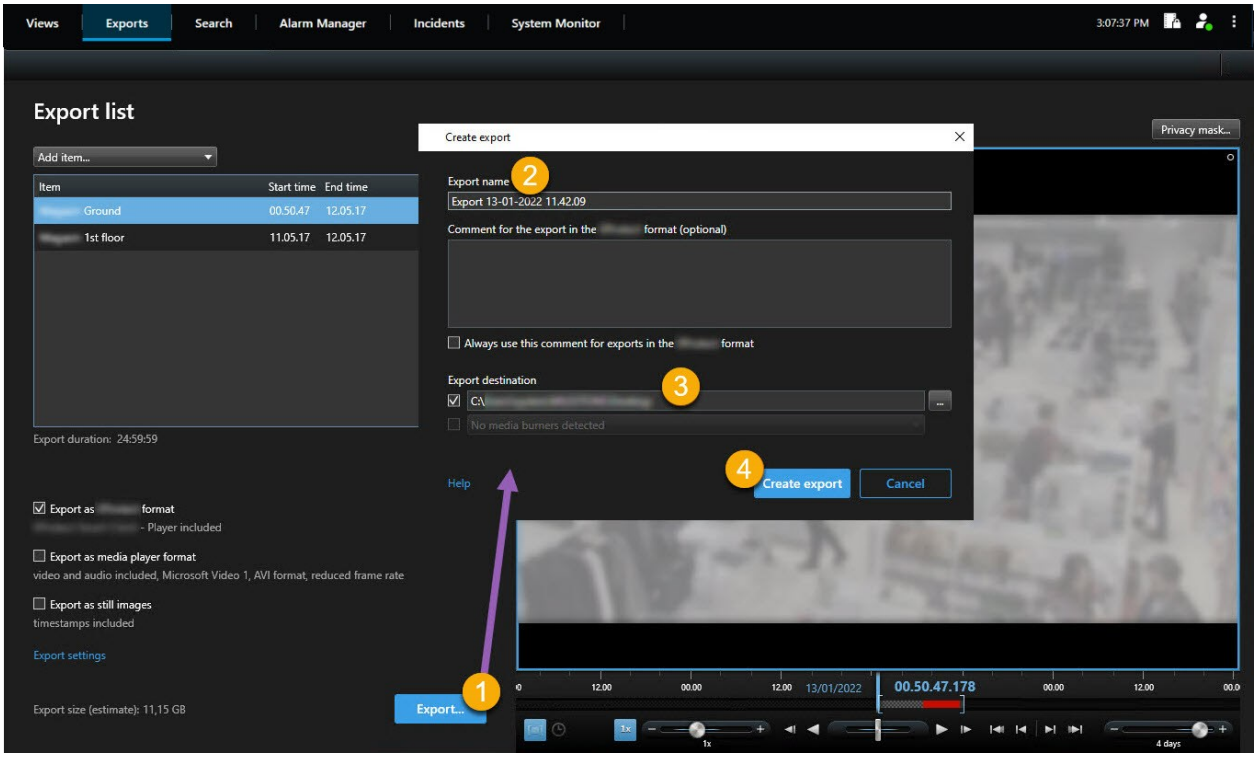
1. Under the **Export list**, select at least one export format.
    - **Export as XProtect format** - use the XProtect format if you want to include the XProtect Smart Client – Player along with the export. Other media players will not work. If you want the recipient to be able to verify that the exported evidence has not been tampered with, select **Export settings** > **XProtect format** > **Include digital signature**. This will enable the **Verify signatures** button in the XProtect Smart Client – Player
    - **Export as media player format** - use a format that most media players can play. This requires that a media player is installed on the computer where the export is to be viewed
    - **Export as still images** - export a still image file for each frame for the selected period
2. Optionally, for each video sequence on the **Export list**, you can change the **Start time** and the **End time**.
3. Optionally, you can add privacy masks to video sequences to cover different video areas. See also Add privacy masks to recordings during export on page 182.
4. Optionally, for each format, you can change the **Export settings**.

The duration of the export and the number of cameras affect how long it takes to complete the export. To reduce the time spent, you may try changing the export format.

Create the export

After you added at least one sequence to the **Exports** tab > **Export list** and selected at least one export format, you can create the export.

Steps:



1. Select the **Export** button. The **Create export** window opens.
2. In the **Export name** field, an export name is automatically created for you. You can change the name.
3. In the **Export destination** field, specify a path for the export. The export you create will be stored in the folder you specify here.
4. Select **Create export** to export the evidence.
5. The export is created and stored in the folder you specified as the **Export destination**. See also View exported video on page 184.

Missing user permissions may prevent you from exporting video data.

Add privacy masks to recordings during export

When you export video, you can add privacy masks to cover selected areas. When someone watches the exported video, the areas with privacy masks appear as solid blocks.

The privacy masks you add here apply to all the video sequences in the current export from the camera you selected in the **Export list**. If you remove a privacy mask from one video sequence, it is also automatically removed from all other video sequences for that camera. The export may also include privacy masks which your system administrator has already defined for certain cameras. See also Privacy masking (explained) on page 246.

Steps:

1. On the **Exports** tab > **Export list**, select the camera you want to add a privacy mask to. If you want to export several video sequences from the same camera, you must divide your camera into several video sequences by clicking the **Divide camera** icon .
2. For each area you want to add a privacy mask to, click the button, and drag the pointer over the area.
3. To remove a part of a privacy mask, click the button, and drag the pointer over the area you want to remove a privacy mask from. Repeat this step for each part you want to remove.

   To temporarily hide privacy masks, click and hold the **Hide privacy mask** button.

4. Click **OK** to return to the **Exports** tab.

The preview image contains an invisible grid with cells. If the area you select includes any portion of a cell, the system adds a privacy mask to the entire cell. The result can be that the system adds a privacy mask to slightly more of the image than you intended.

Storyboards (explained)

The storyboard function helps you paste together video sequences from one camera or from multiple cameras into one cohesive flow. You can use the sequence of events, the storyboard, as proof of evidence in internal investigations or the court of law.

You can skip all sequences that are not relevant and avoid wasting time looking through long sequences of video that you do not need. Also, you avoid wasting storage space on stored sequences that do not contain relevant video.

Export storyboards

You can create a storyboard by pasting together video sequences into one cohesive flow and then export it.

Steps:

1. In playback mode, start by opening a view that contains items that you want to add to your storyboard.
2. In the timeline, click .
3. Select the start time and the end time for the storyboard. See Time navigation controls (overview) on page 175.
4. For each item in the view that you want to add, select the corresponding check box and click **Export** > **Add to export list**.

   Repeat steps 1-4 until you have added all items that you need for your storyboard.
5. Continue with the export process. See Adjust export settings on page 180 and Create the export on page 182.

Export locked video evidence

When you export evidence locks, also the data from devices related to the cameras is included in the export.

Steps:

1. Switch to playback mode.
2. On the workspace toolbar in the upper-right corner, click **Evidence lock** and select **View**.
3. If you want to stay in live mode instead of in playback mode, select **Evidence lock** on the global toolbar.

   A list of existing evidence locks with devices that you have permission to access appears.
4. Select an evidence lock and click **Add to export list**.
5. Continue with the export process. See Adjust export settings on page 180 and Create the export on page 182.

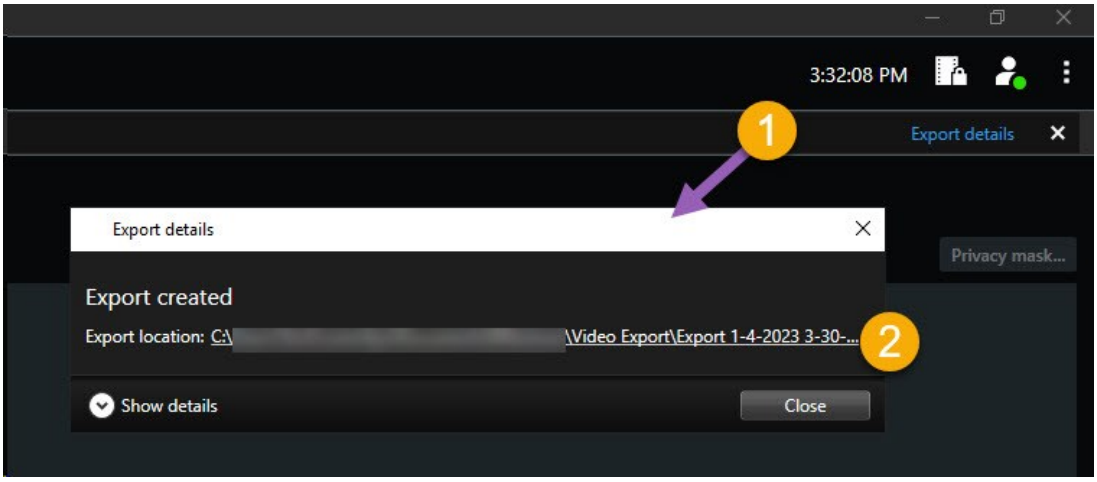
View exported video

The exports that you create are stored in the folder that you specified in the **Create export** window > **Export destination** field.

Steps:

1. To view the exported video immediately after creating it:
    1. In the upper-right corner of XProtect Smart Client, select **Export details**.

       In the **Export details** window > **Export location** field, a link shows the location of the output folder.
    2. Click the link to open the output folder and to access the exported files.



2. If you exported video at a previous point in time:
    1. Go to the folder where you store exports. The default location is *C:\Users\<username>\Documents\Milestone\Video Export*. You can check the folder location in the **Create export** window > **Export destination** field. This works only if you always use the same export destination.
    2. Depending on the output format, open the relevant folder and double-click the video file or still image. If the format is **XProtect format**, double-click the Smart Client – Player file with the .exe extension.

Printing or creating surveillance reports

Depending on your needs, you can either print surveillance reports on the fly based on still images from surveillance cameras, or you can create surveillance reports that you save to your computer.

See also Print alarm reports on page 243 and Get statistics on alarms on page 243.

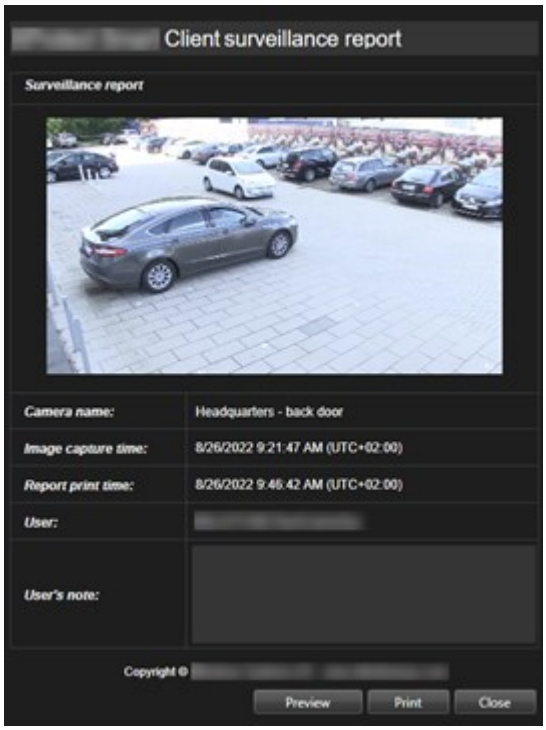
Print report from single cameras

You can print single still images and related information from live cameras or from recorded video. Notes that you add are also printed.

Steps:

1. To print a recorded still image, switch to playback mode.
2. To print a live still image, switch to live mode.
3. Open the view that contains the camera you are interested in.
4. Hover over the view item. The camera toolbar appears.

5. Click the  icon. A window appears.



6. Add notes if required.
7. Click **Print**. The Windows **Print** dialog appears.
8. If necessary, change the print settings and print. Otherwise, just click **Print**.

You can also print information about alarms if your organization uses the alarm handling features. See also Alarms (explained) on page 237.

Create reports from search results

Based on search results, you can create a surveillance report that contains information about the events or incidents, for example still images, event time, information about the cameras, and notes. The report is saved as a PDF file.

Steps:

1. Go to the **Search** tab and run a search.
2. For each search result that you want to include in the report, hover over it and select the blue check box.
3. In the blue action bar, click PDF. A window appears.
4. Change the default report name into something meaningful. In the report, the name is displayed as the page header.
5. To change the folder that the report is saved to, in the **Report destination** section, click ... and select a different folder.
6. Optionally, write a note in the **Report note** field.
7. Click **Create**. A progress bar shows that the report is generated.

8. When the report is generated, select **Details** from the progress bar.
1. Select **Open** to open the report or click the link to open the report's destination folder.

To change the layout of the report, open the **Settings** dialog, click **Advanced**, and then select a different value in the **PDF report format** list.

Copy images to clipboard

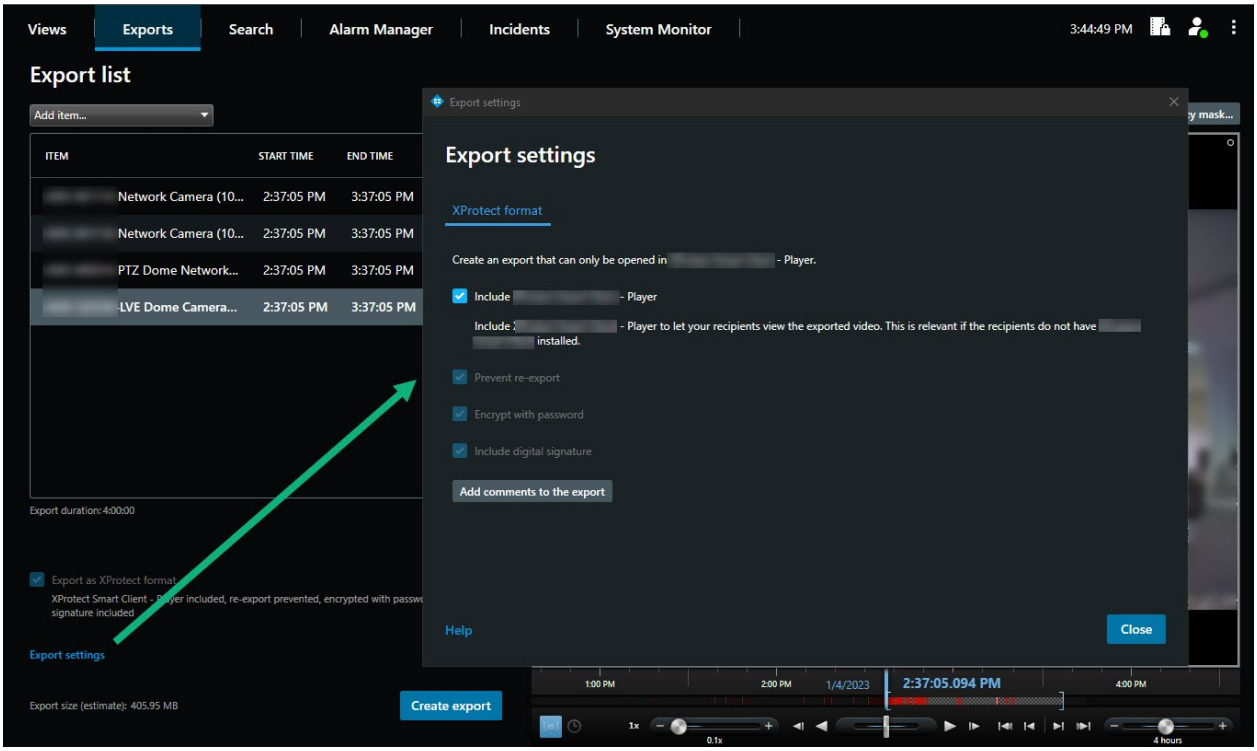
You can copy single still images from selected cameras. Copied images can then be pasted (as bitmap images) into other applications, such as word processors, e-mail clients, etc. You can only copy a single image from one camera at a time.

- On the camera toolbar, click the **Copy to clipboard** button to copy an image

Export settings

On the **Exports** tab, you can choose which formats to use for the export, and for each format, you can change the **Export settings**:

- XProtect format settings on page 189
- Media player format settings on page 190
- Still images settings on page 191



> Your system administrator specifies which formats and which export settings are available to you.
>
> For security reasons, only the XProtect format is available by default. Please contact your system administrator to enable other export formats.

The format and export settings that you choose are stored and displayed the next time you export.

If a setting is grayed out, then it has been locked by your system administrator.

XProtect format settings

Choose the XProtect format to create an export that can only be opened on a Windows computer in XProtect Smart Client – Player.

> To open exports that are created in XProtect version 2020 R1 or later, you must use XProtect Smart Client version 2020 R1 or later.

Name	Description
Include XProtect Smart Client – Player	Include the XProtect Smart Client – Player application with the exported data. The exported data can only be viewed with the XProtect Smart Client – Player.
Prevent re-export	Prevent your recipients from re-exporting the data in any format.
Encrypt with password	Encrypt the export using the encryption standard AES-256. When you select **Export** > **Create export**, you are asked to enter a password that is at least eight characters long. To open and view the exported data, the recipient of the export must enter the password.
Include digital signature	Include a digital signature to your exported database. Depending on your surveillance system settings, the video or audio might already contain a signature. If this is the case, these signatures will be verified during export and if successfully verified, added to the export. If verification fails, the export for the device will also fail. When opening the exported files, the recipients can verify the signature in XProtect Smart Client – Player. See also Verify digital signatures on page 282. > If you do not include a digital signature, neither the signature from the server or the export will be included, and the export will succeed even if the video or audio has been tampered with. Digital signatures can be excluded during the export process in two different situations:

Name	Description
	• If there are areas with privacy masks, digital signatures for the recording server will be removed from the export • If the data you are exporting is very close to the current date and time, the digital signature for the recording server might not be included for the whole sequence. In this case, only part of the export will have digital signatures added The export process will complete, but when you verify the signatures, you will see that the digital signatures for the recording server were removed or partially OK.
Comments	Open the **Add comments to export** window, where you can add comments to individual cameras or to the export project as a whole.

Media player format settings

Choose the media player format to export a standard video clip or audio clip that can be viewed or listened to on computers that have a standard media player installed. The computer must also have the codec installed that you use for the export.

To get the smallest export size possible, select the MKV media player format. If not enabled, please contact your system administrator.

Name	Description
Export content	Export video only, audio only, or both video and audio.
Export format	Export video in the AVI format or in the MKV format.
Codec	Your choice of codec will affect the quality and size of the AVI file. You can change the codec, but we recommend that you keep the default codec settings, unless you have a good reason to change these. The codec that you use must be similar on the computer where you intend to play the exported video.

Name	Description
Include timestamps	Add the date and time from the VMS system to the exported video. The timestamp will be displayed at the top of the exported video.
Reduce frame rate	Reduce the frame rate for the export. Every second image will be included, yet still play back in real-time.
Video texts	Open the **Video texts** window where you can create pre- and post-texts for the AVI file. These texts will be added to all cameras for the export and displayed as still images before (**Pre-slides**) or after (**Post-slides**) the video.

MKV format: If you have not used privacy masking in video recorded in JPEG or MPEG-4/H.264/H.265 formats, no transcoding takes place on recorded video in the export. The recorded video is kept in the original quality. In contrast, if you have used privacy masks or have recorded video using any other codec, recorded video is transcoded into JPEG in the export.

Still images settings

Choose the still image format to export a still image for each frame of each video sequence. The images are in the JPEG format.

Name	Description
Include timestamps	Add the date and time from the VMS system to the exported images. The timestamp will be displayed at the top of the exported images.

Exports tab (overview)

Name	Description
Export list	Lists the items selected for export, for example video sequences. For each item, you can change the time span by clicking the start time or the end time. After selecting a new date and time, click **Go To**. You can also change the time span by dragging the handles underneath the preview area. Click an item to see a preview of the export clip in the preview area. To preview multiple items simultaneously, press and hold down the **Shift** or **Ctrl** buttons while clicking the relevant items. You can delete an item from the **Item** list by clicking the red **x** next to it. The red x appears when you hover over the item with your mouse. If you want to split the item into two, click the **Split** icon in the preview area.
Add item	Use the **Add item** button to select other items that you want to include in the export.
Remove all	Use the **Remove all** button to clear the **Export list**.
Export name	The program automatically fills this in with the local date and time, but you can rename it.
Export destination	**Path** - when you specify a path, the folders you specify do not have to be existing ones. If they do not already exist, they are created automatically. A path may already be suggested in this field. **Media burner** - you can specify a burner that you want to send the export to. In this way, you create the export and make sure it is written directly to an optical media in one go.
Privacy mask	Click to add privacy masks to the video. The privacy masks cover the selected area with a solid, black area. The privacy masks that you add here only apply to the current export and for the selected video. The export may already include video with privacy masks configured by your system administrator. For more information, see Privacy masking (explained) on page 246.

Locking video evidence

You can add, edit, and delete evidence locks, but you can also export them and play back video with evidence locks.

Evidence locks (explained)

With the evidence lock functionality, you can protect video sequences from being deleted, for example while an investigation or trial is ongoing. This protection also covers audio and other data from devices related to the selected cameras.

Once an evidence lock is in place, the system prevents the data from being deleted automatically based on the retention time of the system.

> Depending on your user permissions, you may be able to create, view, edit, and delete evidence locks.

Create evidence locks

You can create an evidence lock to prevent video recordings and related data from being deleted.

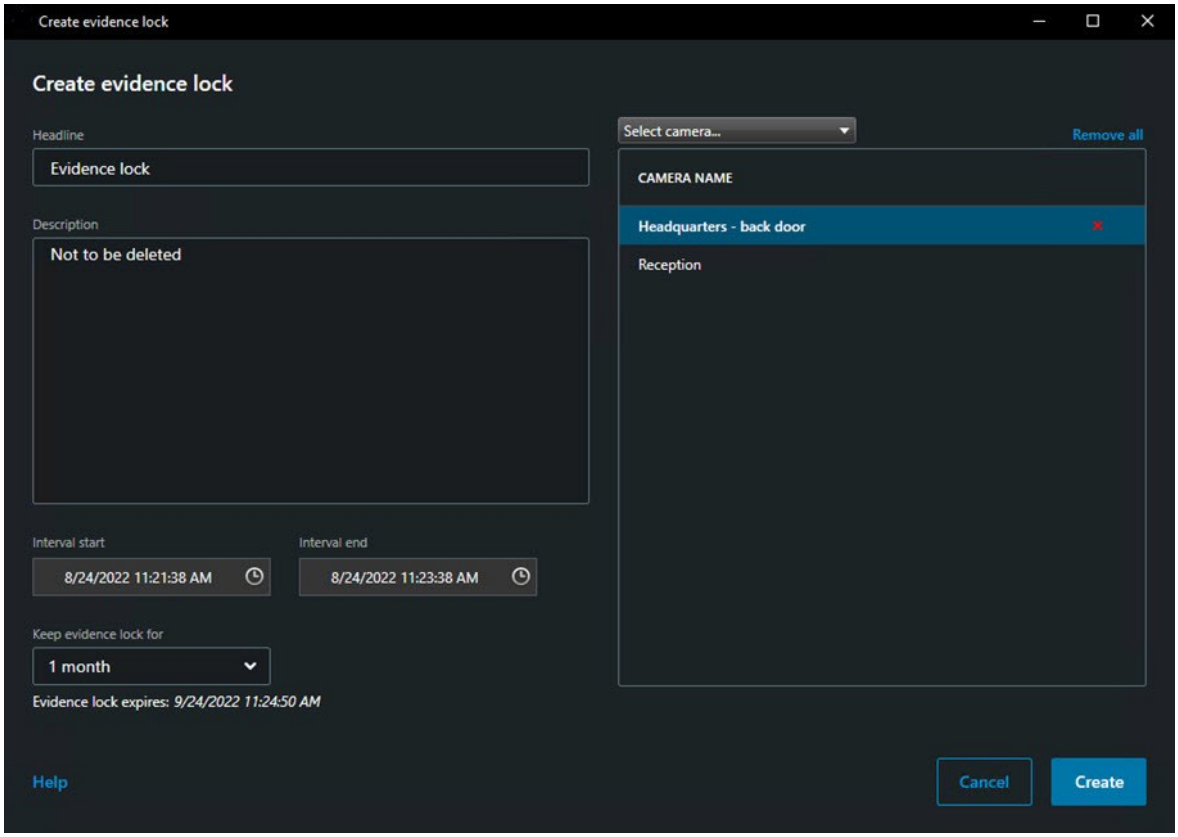
Create evidence locks in playback mode

1. In the timeline, click the **Time selection mode** or the **Set start/end time** button.

2. Select the start and end time for the video sequences you want to protect from deletion.
3. Select the cameras that have video sequences and data from related devices that you want to protect.

4. In the upper right corner, click **Evidence lock** > **Create**. A window appears.

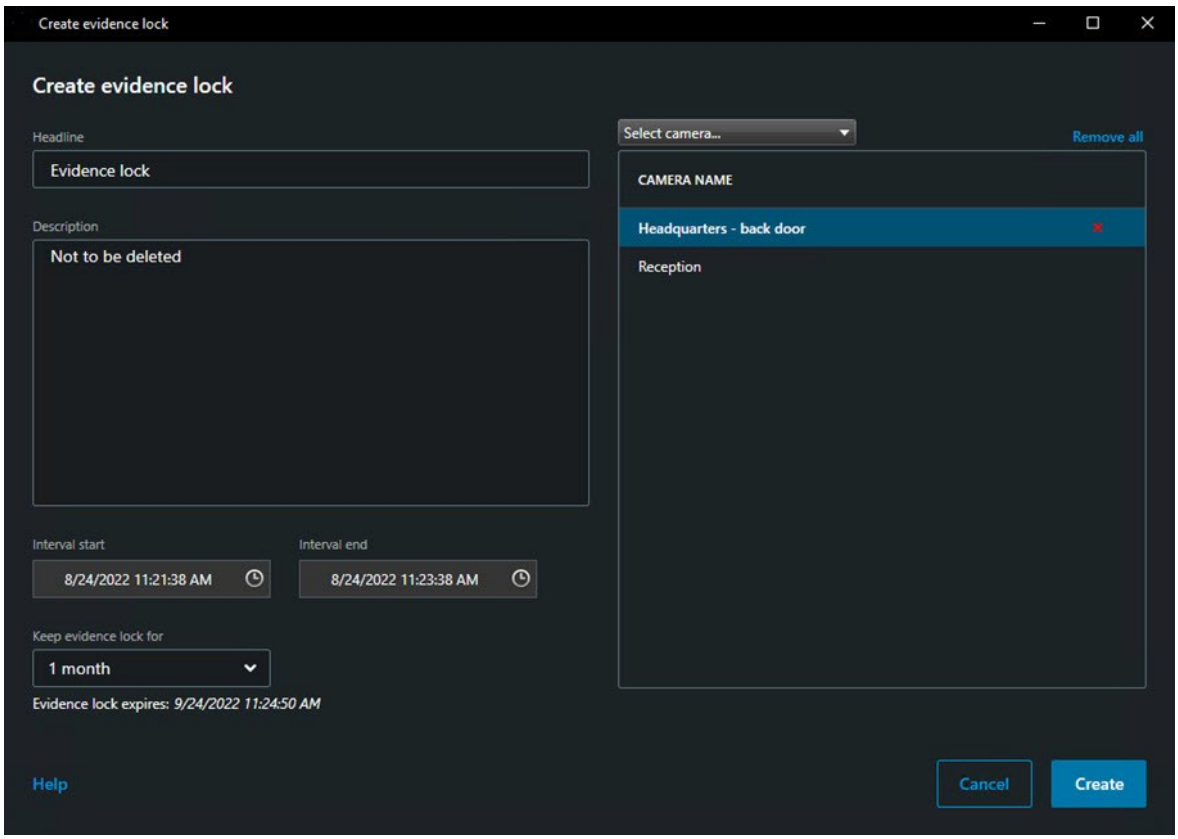


5. Give the evidence lock a headline and, optionally, a description.
6. For information about the remaining fields, see Evidence lock settings on page 198.
7. Click **Create**. If the evidence lock was created successfully, you can click **Details** to see what went well and what did not. See Evidence lock status messages on page 199.

Create evidence locks on the Search tab

1. In the list of search results, select the video sequences that you want to protect from being deleted. The action bar appears. Data from related devices will also be protected.

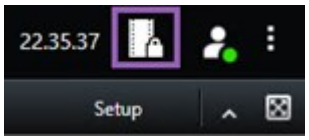
2. Click > **Create evidence lock**. In the window that appears, the cameras associated with the selected search results are listed.



3. Give the evidence lock a headline and, optionally, a description.
4. The time span covers all the selected search results. To change the time span, use the **Interval start** and **Interval end** fields.
5. For information about the remaining fields, see Evidence lock settings on page 198.
6. Click **Create**. A window appears informing you about the progress of the evidence lock. Click **Details** to see what went well and what did not. See Evidence lock status messages on page 199.

View evidence locks

1. Switch to playback mode.
2. On the workspace toolbar in the upper-right corner, click **Evidence lock** and select **View**.
3. If you want to stay in live mode instead of in playback mode, select **Evidence lock** on the global toolbar.



   A list of existing evidence locks with devices that you have permission to access appears.
4. Search for text in the headlines and descriptions, sort the different columns and/or use the filter options to make it easier to find the wanted evidence lock.
5. Select an evidence lock and click **Details** to see the cameras included in the evidence lock and other information.

Edit evidence locks

Depending on your user permissions, you can edit evidence locks, for example time interval, cameras, and how long to keep the evidence lock.

1. Switch to playback mode.
2. In the upper the right corner, click **Evidence lock** and select **View**, or click the **Evidence lock** button on the application toolbar.

3. Select an evidence lock and click **Details**. A window appears.
4. To make the interval of the evidence lock shorter or longer, use the **Evidence lock interval start** and **Evidence lock interval end** fields.
5. To change the time that the evidence lock is valid for, select a value in the **Keep evidence lock for** list.
6. When done, click **Update**.
7. A window shows if the update was successful. Click **Details** to see what went well and what did not. See also Evidence lock status messages on page 199.

Play back video with evidence locks

You can always play back video in playback mode regardless if the video is protected or not. If you want to play back video sequences that are included in a specific evidence lock, do the following:

1. Switch to playback mode.
2. In the upper right corner, click **Evidence lock** and select **View**.
3. If you want to stay in live mode instead of in playback mode, select **Evidence lock** on the global toolbar.

A list of existing evidence locks with devices that you have permission to access appears.

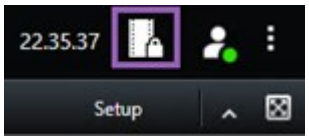
4. Select an evidence lock and click **Play back**. A new window opens and you can see a view with all the cameras in the evidence lock.
5. Use one of the timeline features to go to a specific time or simply click **Play forward**.

Export locked video evidence

When you export evidence locks, also the data from devices related to the cameras is included in the export.

Steps:

1. Switch to playback mode.
2. On the workspace toolbar in the upper-right corner, click **Evidence lock** and select **View**.
3. If you want to stay in live mode instead of in playback mode, select **Evidence lock** on the global toolbar.



A list of existing evidence locks with devices that you have permission to access appears.

4. Select an evidence lock and click **Add to export list**.
5. Continue with the export process. See Adjust export settings on page 180 and Create the export on page 182.

Delete evidence locks

When you delete an evidence lock, you do not delete the video sequences but do only remove the protection of them. If the video sequences are older than the system's default retention time, the system informs you about this and you can keep the evidence lock to prevent that the video sequences are automatically deleted by the system after the removal of the protection.

1. Switch to playback mode.
2. In the upper right corner, click **Evidence lock** and select **View**.
3. If you want to stay in live mode instead of in playback mode, select **Evidence lock** on the global toolbar.

A list of existing evidence locks with devices that you have permission to access appears.

4. Select one or more evidence locks and click **Delete**.
5. A window shows if the deletion was successful. Click **Details** to see what went well and what did not. See also Evidence lock status messages on page 199.

Evidence lock settings

Name	Description
Headline	The headline of the evidence lock.
Description	A description of the evidence lock.
Interval start	Adjust the start date and time for the video sequences you want to protect.
Interval end	Adjust the end date and time for the video sequences you want to protect.
Keep evidence lock for	Specify for how long you want to keep the evidence protected. Depending on your user permissions, you have the following options: hour(s), day (s), week(s), month(s), year(s), indefinite, or user-defined. If you select **User-defined**, click the calendar button to select a date and then adjust the time manually. When done, the date and time for when the evidence lock expires is shown.
Select camera	Click to select more cameras to include in the evidence lock.
Remove/Remove all	Click to remove one selected camera or all cameras from the evidence lock.

Evidence lock filters

Name	Description
Lock interval	Filter your evidence locks based on the start time of the interval they are protected in. Available options are today, yesterday, last 7 days and all.
Created	Filter your evidence locks based on when they were created. Available options are today, yesterday, last 7 days, all and custom interval. If you select custom interval, you select the start and end date in a calendar.
Expiry date	Filter your evidence locks based on when they expire. Available options are today, tomorrow, next 7 days, all and custom interval. If you select custom interval, you select the start and end date in a calendar.
Users	Filter for evidence locks created by all users or just by you.
Cameras	Filter for evidence locks with data from any camera or select one or more cameras that must be included in the evidence locks.

Evidence lock status messages

Message	Description and result	Scenarios and solution
Succeeded	All went well. **Result**: The evidence lock is created/updated/deleted.	
Only partially successful	If the creation, update or deletion of an evidence lock was not entirely successful, an only partially successful message is shown and the progress bar is yellow. Click **Details** to see what went wrong. Result:	**Scenario**: Some of the recording servers with devices included in the evidence lock are offline.

Message	Description and result	Scenarios and solution
	The evidence lock is created/updated/deleted but without including some of the selected cameras and/or their related devices. Additionally, this can be because a recording server is offline, in which case the evidence lock is configured, but not yet applied on the actual video. In this case, the evidence lock will be applied to the video when the recording server becomes available. You can verify that the locks are applied by looking at the size of the lock. An indication of size means that the lock is applied.	**Solution**: Wait for the recording server to come online. **Scenario**: One or more devices have recordings on recording servers that are not upgraded to 2020 R2 or later. **Solution**: Upgrade the recording servers to version 2020 R2 or later. **Scenario**: Your system administrator has changed your evidence lock user permissions after you logged into XProtect Smart Client. **Solution**: Contact your system administrator.
Failed	If the creation, update or deletion of an evidence lock is not successful, a failed message is shown and the progress bar is red. Click **Details** to see what went wrong. Result: The evidence lock is not created/updated/deleted.	**Scenario**: All the recording servers with devices included in the evidence lock are offline. **Solution**: Wait for the recording

Message	Description and result	Scenarios and solution
		servers to come online. **Scenario**: The management server is offline. **Solution**: Wait for the management server to come online. **Scenario**: Only for update and deletion: You do not have user permissions to one or more devices in the evidence lock. **Solution**: Contact your system administrator. **Scenario**: One or more devices have recordings on recording servers that are not upgraded to 2020 R2 or later. **Solution**: Upgrade the recording servers to version 2020 R2 or later.

Searching for video data

The search features are available mainly on the **Search** tab, but they are integrated with viewing video in live and playback mode.

Search for video

The **Search** tab lets you search for video recordings, and - based on the search results - lets you take action, for example by exporting.

What can you search for?

- Video sequences
- Video sequences with motion
- Bookmarked video
- Video sequences with alarms
- Video sequences with events
- Video sequences with people
- Video sequences with vehicles
- Video recorded at a certain location

Requirements

- Searching for people, vehicles, and location is only available if these search categories were enabled by your system administrator
- Searching for vehicles is also available if you have XProtect® LPR installed in your system. For more information, ask your system administrator

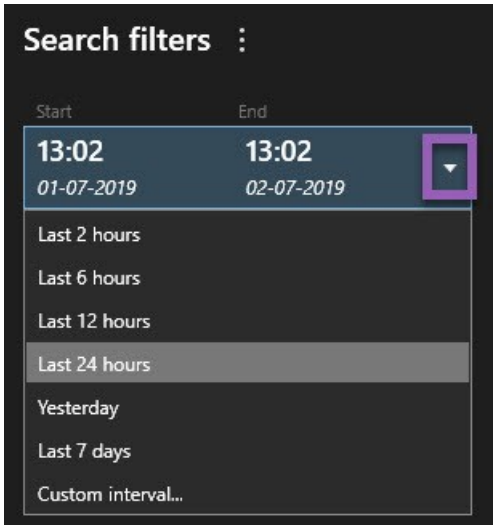
The search categories **Alarms**, **Events**, **People**, **Vehicles**, and **Location** are only available if you are using one of these products:

- XProtect Corporate
- XProtect Expert

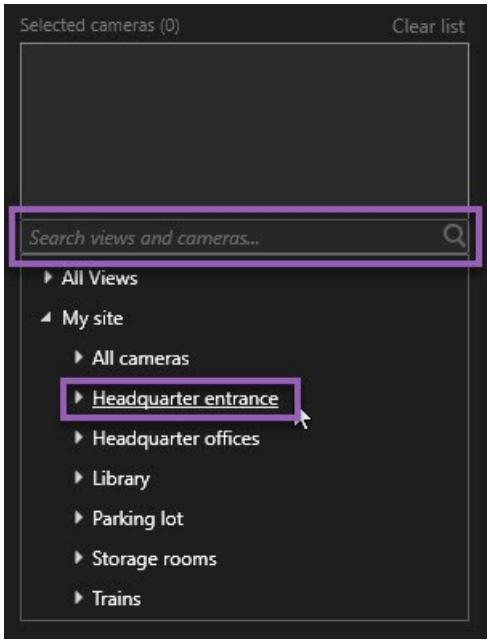
You can only combine search categories if you are using one of the products mentioned above. For information about the features available in your XProtect VMS, see Surveillance system differences on page 33.

Steps:

1. Click the arrow to select a predefined time span, or define your own **Custom interval**.



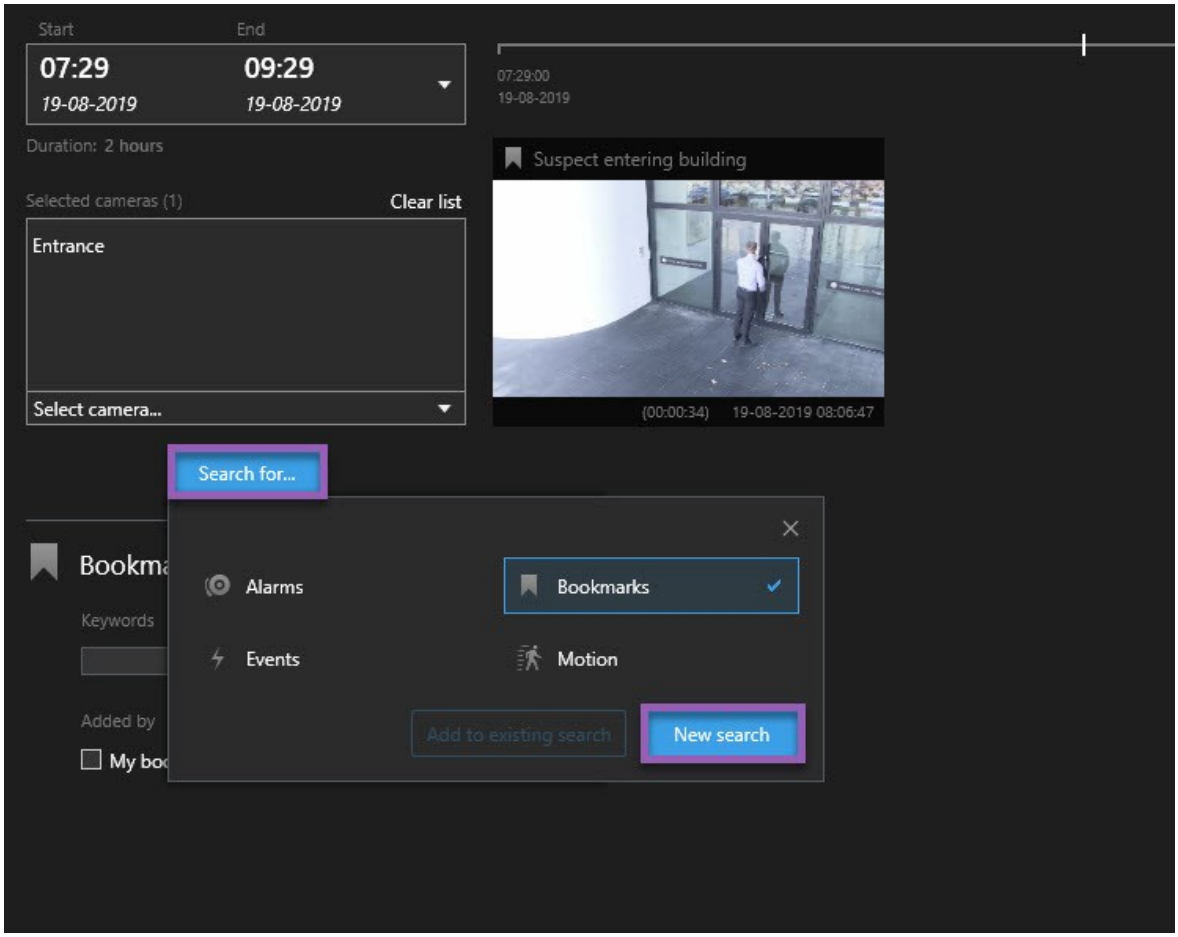
2. In the **Selected cameras** list, do one of the following to add cameras to your search:



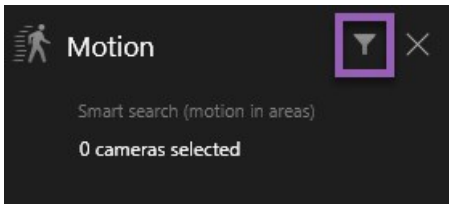
   - Use the search function to find cameras or views
   - Manually select the cameras in the tree structure. To add all cameras within a view, select the name of the view

   As you add cameras, the search is run immediately.

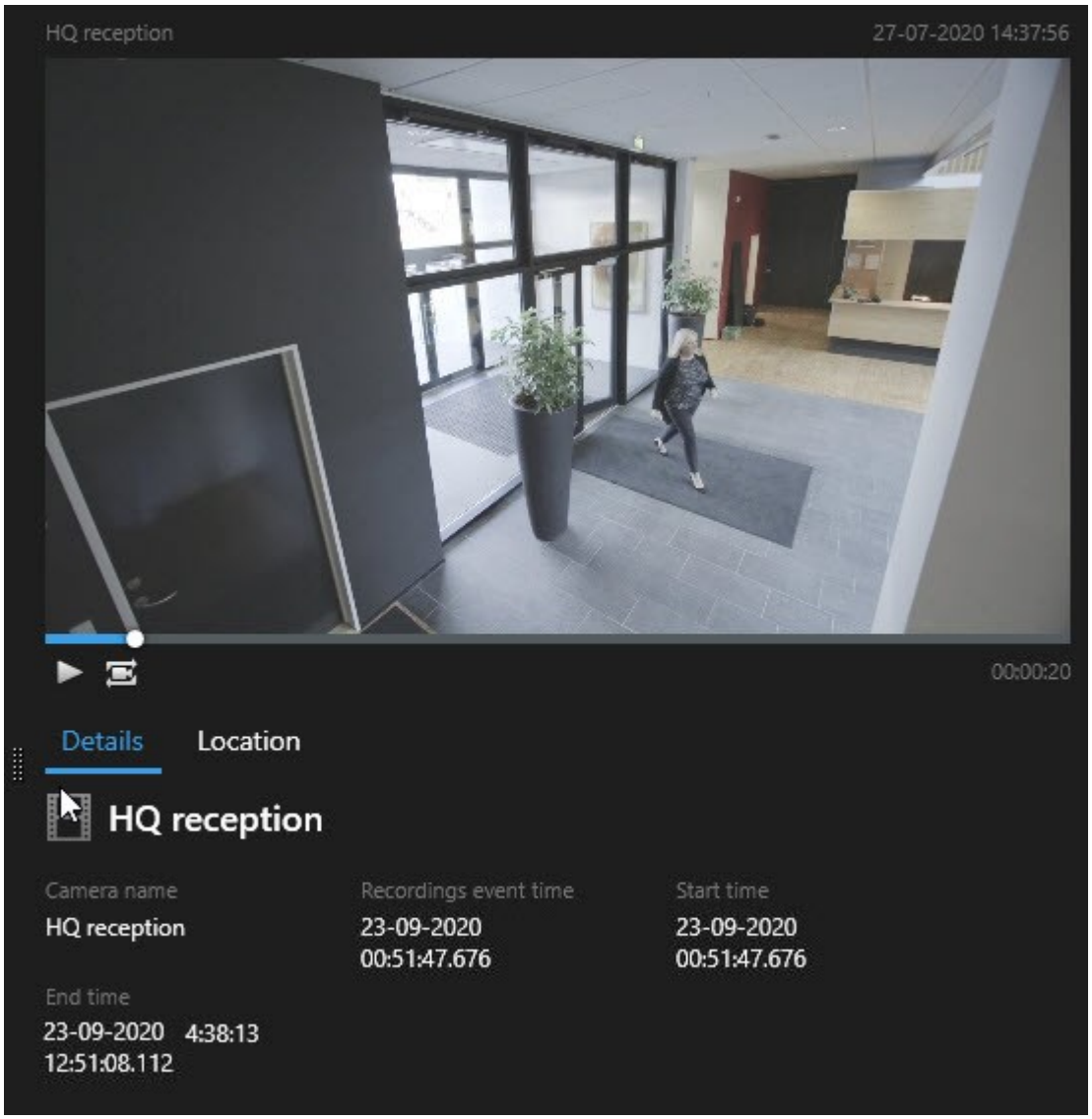
3. Click **Search for** to select the search categories. You can use search categories alone or combined.



4. For each search category that you add, you can refine the search by adding search filters. For more information about search filters, see FAQ: searching on page 319.



5. To preview the video of a search result, select the search result and, in the preview pane, click ▶.



To play back the video sequence in full-screen mode, double-click the search result.

6. To make the action bar appear, hover over the search results, one by one, and select the blue check box that appears.

The blue action bar appears:

Search for motion (smart search)

When you search for video recordings with motion, you can apply smart search filters to show only search results with motion in areas that you define.

Example

Use smart search to find video footage of a person entering through a doorway that is monitored by multiple cameras.

Requirements

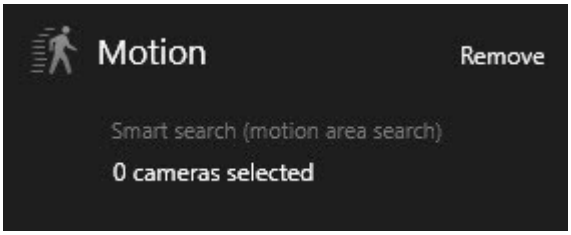
To use smart search filters, smart search must be enabled on your user profile by your system administrator.

Steps:

1. On the **Search** tab, select a time span.
2. Select the cameras that you want to include in your search.
3. Click **Search for** > **Motion** > **New search**. If the database has any recordings with motion within the selected time span and cameras, the recordings appear as thumbnail images in the search results pane.

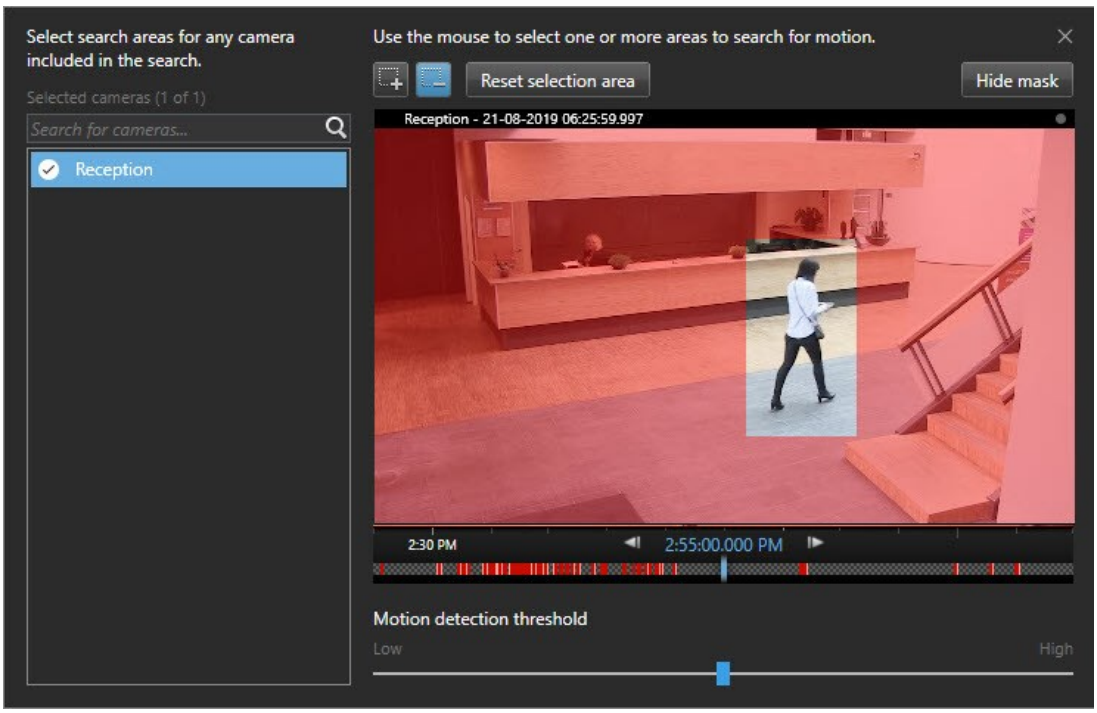
4. To find motion in selected areas only:

    1. Below **Motion**, click **0 cameras selected**.

    A dialog box appears with a list of the cameras that you selected.

    2. Select one camera at a time and, in the red preview area, click and drag to unmask at least one area. The system will look for motion only in that area. You can unmask multiple areas.

    > The sensitivity of the motion detection is defined by your system administrator in Management Client on individual cameras. However, you can use the slider to adjust the sensitivity. For more information, see Motion search threshold (explained) on page 208.

    3. Automatically, the search is run. Click outside the dialog to return to the search results.

4. To perform actions, for example bookmarking search results, hover over the search results and select the check box . The action bar appears.

Motion search threshold (explained)

When you search for motion in selected areas of a camera, you can adjust the motion threshold. The motion threshold determines how sensitive the motion search mechanism is:

- The higher the threshold, the more motion is required to activate motion detection. Likely, this will produce fewer search results
- The lower the threshold, the less motion is required to activate motion detection. Likely, this will produce more search results

Search for bookmarks

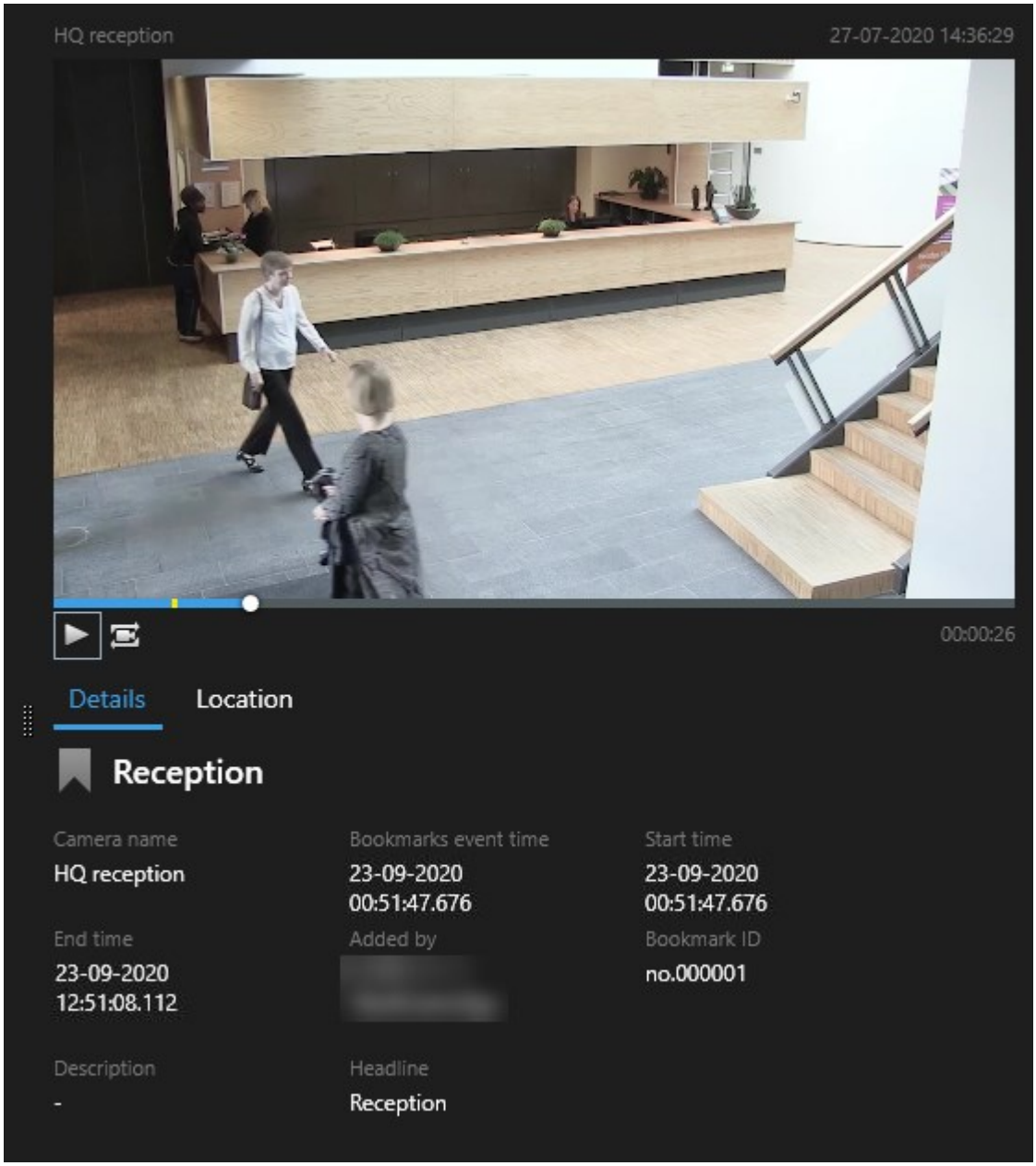
You can find incidents that are bookmarked by you or others for any number of cameras.

Steps:

1. Select the cameras that you want to include in your search.
2. Click **Search for** > **Bookmark** > **New search**. If the database has any bookmarked recordings, they appear as thumbnail images in the search results pane.
3. Optionally, enter a keyword to filter the search results. The keyword can be:
   - The full **Bookmark ID**, for example **no.000004**
   - Who the bookmark was added by, for example **site\user2**
   - Any text that appears in the **Headline** or in the **Description**

> By default, the system will search for the keyword both in the **Headline** and in the **Description**. Use **Search for keyword in** to change that.

4. To preview the video sequence and bookmark details, select a search result and play back the video in the preview pane on the right-hand side.



5. To view the recording in full-screen mode, double-click the search result.
6. To perform other actions, for example editing the bookmark, hover over the search result and select the check box. The action bar is displayed.

Search for alarms

When you search for video recordings associated with alarms, you can apply search filters to show only search results with certain alarms, for example alarms in a certain state that are assigned to a specific operator.

Steps:

1. Select the cameras that you want to include in your search.
2. Click **Search for** > **Alarms** > **New search**.
3. Apply search filters to narrow down search results. You can filter for:
    - **Priority**
    - **State**
    - **ID** - Type the full ID to filter for it
    - **Owner**
    - **Server** - available only if you are using Milestone Federated Architecture™

    If you are using Milestone Federated Architecture™, the **Priority** and **State** filters are applied across all connected sites.

Search for events

When you search for video recordings associated with events, you can apply search filters to show only search results with certain events, for example events that come from a specific source or server.

Steps:

1. Select the cameras that you want to include in your search.
2. Click **Search for** > **Events** > **New search**.
3. Apply search filters to narrow down search results. You can filter for:
    - **Source**
    - **ID** - Type the full ID to filter for it
    - **Server** - available only if you are using Milestone Federated Architecture™

Search for people

This search category and its search filters are only available if they were enabled by your system administrator.

When you search for video recordings that include people, you can apply search filters to show only search results with people that have certain characteristics, for example people of a certain age or height.

1. Select the cameras that you want to include in your search.
2. Click **Search for** > **People** > **New search**.
3. Apply search filters to narrow down search results. You can filter for:
    - **Age** - Filter for people in a certain age range
    - **Gender** - Filter for males or females
    - **Height** - Filter for people in a certain height range
    - **Face** - Select the check box to limit search results to people whose face is visible

Search for vehicles

This search category and its search filters are only available if they were enabled by your system administrator.

Searching for vehicles is also available if you have XProtect® LPR installed in your system.

For more information, ask your system administrator

When you search for video recordings that include vehicles, you can apply search filters to show only search results with certain vehicles, for example a vehicle with a certain license plate that was issued by a certain country.

1. Select the cameras that you want to include in your search.
2. Click **Search for** > **Vehicles** > **New search**.
3. Apply search filters to narrow down search results. You can filter for:
    - **Color** - Filter for vehicles of certain colors
    - **License plate** - Type a part of a license plate number or the full license plate number to filter for it
    - **Country** - Filter for license plates that were issued by certain countries

      This search filter is only available if you have XProtect® LPR installed in your system.

    - **Vehicle type** - Filter for types of vehicles, for example trucks
    - **Vehicle speed** - Filter for vehicles moving at a certain speed

- **Match list** - Filter for license plates that are part of certain match lists

  This search filter is only available if you have XProtect® LPR installed in your system.

Search for video at location

This search category and its search filters are only available if they were enabled by your system administrator.

When you search for video recordings recorded at a certain location, you can apply search filters to show only search results in a specific location.

1. Select the cameras that you want to include in your search.
2. Click **Search for** > **Location** > **New search**.
3. Apply search filters to narrow down search results. You can filter for geographic coordinates by specifying the latitude and longitude coordinates and the radius of the search area.

Search results, settings, and actions

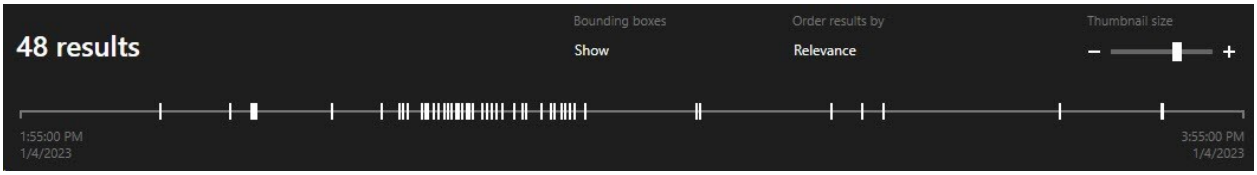
This section describes the search timeline and the different settings and things you can do while searching.

For information about saving and managing searches, see Managing your searches on page 227.

Timeline on Search tab (explained)

The timeline gives you an overview of how the search results are distributed. The timeline also allows you to navigate the search results.

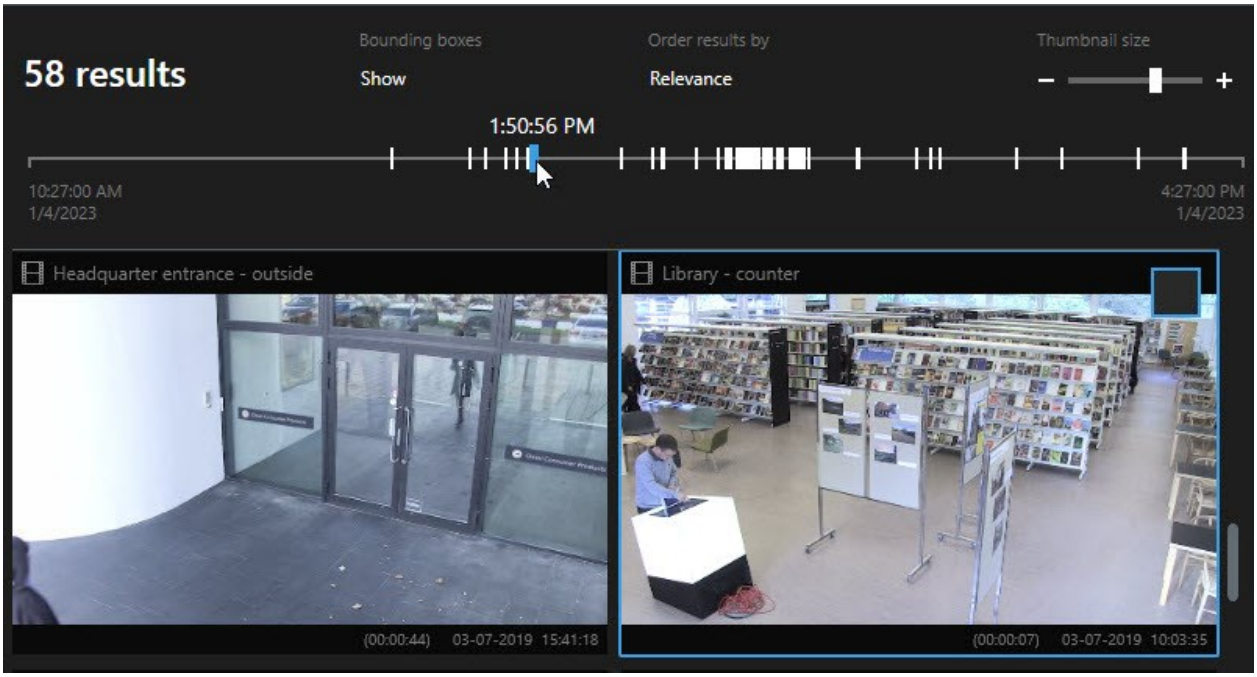
The scope of the timeline changes according to the selected time span, for example **Last 6 hours**.



The white markers indicate where the search results are.

Individual markers may indicate that there are multiple search results. By hovering over the markers, information is displayed about the time and the cameras that recorded the events or incidents.

To navigate the search results, click a marker. The marker turns blue, and the associated search result is marked with a blue border.



If the marker that you select shows more than one search result, the first search result is marked.

If a marker indicates more than 10 search results, a message will inform you about the number of search results and the number of associated cameras.

Actions available from search results (overview)

Based on your search results, there are multiple actions available. Some actions are available in the blue action bar, others in the preview area.

The actions available may differ depending on your user permissions.

Action	Description
	Add the selected sequences to the **Exports** tab > **Export list**. All the sequences that you add to the **Export list** are ready for export on the **Exports** tab. See also Export video, audio, and still images on page 179.

Action	Description
	Create PDF reports with information about the search results, for example still images from the video sequences.
	Bookmark multiple search results at the same time.
	Edit multiple bookmarks at the same time.
	Add evidence locks to protect the video sequences and data from related devices, for example audio, from being deleted.
	Open multiple search results in a separate window, where you can view the video in live or playback mode, export, create evidence locks, and retrieve recordings from devices and cameras belonging to interconnected VMS systems.
	Take multiple snapshots of your search results at the same time.
	When you are previewing video, you can transfer the current time to the playback timeline. This is useful, for example, if you want to look at related cameras in playback mode at the time that an incident took place.

MIP-related actions

There may be additional actions available, related to third-party software. The MIP SDK is used to add these additional actions.

Merged search results (explained)

If you are using multiple search categories, and the search results overlap in time, they are merged into one. In some situations into multiple search results. This happens when different search criteria match video from the same camera within the same time span. Instead of returning different search results that show basically the same video sequences, XProtect Smart Client simply gives you one search result that contains all details, for example the camera name, indications of event time, and search categories.

Examples:

Find vehicle on Memory Lane 15

Suppose you want to find a vehicle of the type truck on Memory Lane 15 within the last two hours. To configure your search:

1. Select 10 cameras placed in the right area.
2. Set **Duration** to **Last 2 hours**.
3. Add the search category **Vehicles** and filter on **Truck**.
4. Add the search category **Location** and filter on the geo coordinates of the address and a search radius.
5. Select the **Match all criteria** check box.

For more information, see Search for vehicles on page 211 or Search for video at location on page 212.

Find bookmarked alarm

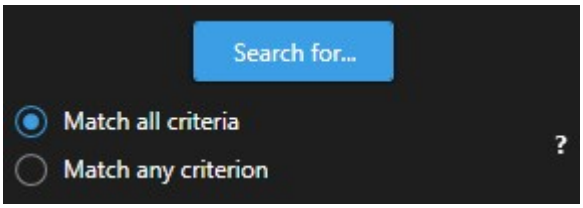
Two days ago an alarm went off in your XProtect VMS system. To make it easy to find the alarm again, you bookmarked it. Now you want to find the bookmark again to make an export. To configure your search:

1. If you remember which camera recorded the incident, select the camera. Otherwise, select a range of possible cameras.
2. Set **Duration** to **Last 24 hours**, or specify a **Custom interval**.
3. Add the search categories **Bookmarks** and **Alarms**.
4. Select the **Match all criteria** check box.

For more information, see Search for bookmarks on page 208 or Search for alarms on page 210.

Match any or all search criteria (explained)

If you are using XProtect Corporate or XProtect Expert, you can use multiple search categories in the same search. While configuring your search, specify whether your search must match any or all the search categories.



Matching all criteria gives you fewer but more accurate search results. In addition, if the search results overlap, they are combined into fewer results. See also Merged search results (explained) on page 214.

Matching any criterion gives you more but less accurate search results.

Actions that are normally available in the action bar may not be available for merged search results. This happens if the action that you are trying to perform cannot be used with one of the search categories. See also After selecting a search result, certain actions may not be available in the blue action bar. on page 320

Start search from cameras or views

If you are looking for something specific in one or more video streams, you can start search from a single camera, or from an entire view. The search workspace opens in a new floating window.

Steps:

1. Switch to live or playback mode.
2. To search a single camera:
    1. Hover over the view item. The camera toolbar appears.
    2. Click  . A new **Search** window opens, and a search for recorded video starts immediately based on the camera in the view item.
3. To search all cameras in a view:
    1. Make sure the correct view is open.
    2. At the top of the view, click  . A new **Search** window opens, and a search for recorded video starts immediately based on the cameras in the view.
    3. Depending on your goal, change the time span, search categories and filters, or similar. For more information, see Searching for video data on page 201.

Open search results in separate windows

You can open a search result in a new window. The window opens in playback mode allowing you to investigate the incident using the full timeline and perform other actions, for example exporting video.

1. Hover over the search result and select the blue check box that appears.

2. The blue action bar appears:

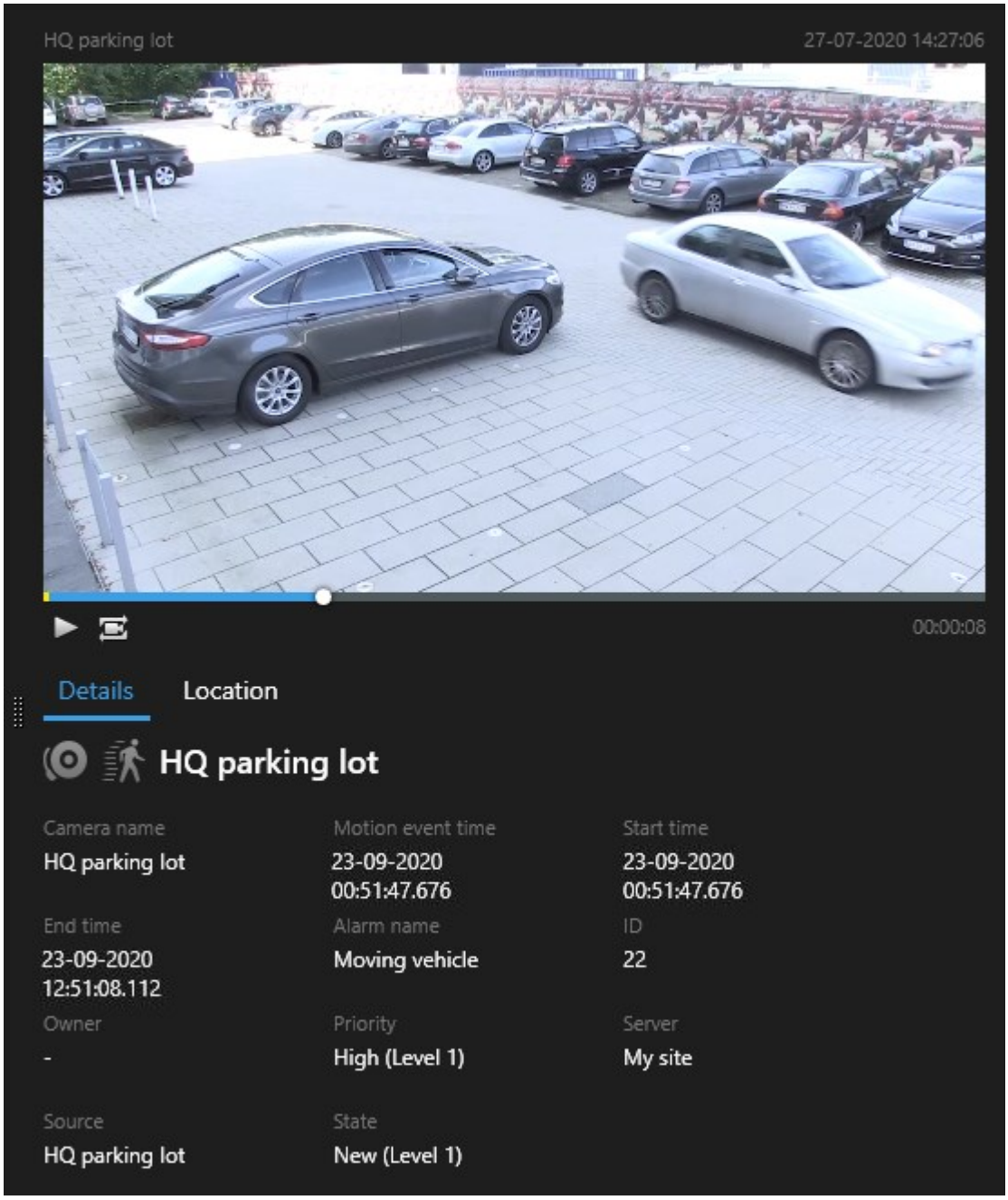
3. Click  to open the search result in a new floating window in playback mode.
4. To move the window to a different monitor, click and drag the window and release when appropriate.

Preview video from search results

To determine whether you have found the video sequence you were looking for, you can do a quick preview.

Steps:

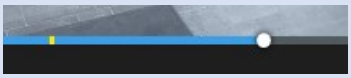
1. When you have run a search on the **Search** tab, select a search result. A still image from the associated video sequence appears in the preview area.



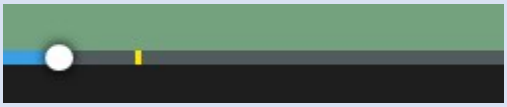
2. Click ▶ to play back the video.
3. To preview the video in full-screen mode, double-click the individual search results. Double-click again to return to the search results.

4. Scroll with your mouse wheel to zoom in or out. You can even click and drag to zoom in on a specific area.

The yellow marker in the timeline indicates the event time. Hover over the marker to view the event time.



Multiple markers appear in the same timeline when search results are combined.



This happens, for example, if you have searched for **Motion** and **Vehicles**, and the search result match both criteria. In this example, one marker would indicate when the motion started. The other marker would indicate when the vehicle was identified as a vehicle.

Show or hide bounding boxes during search

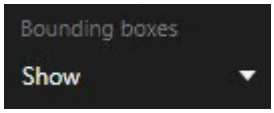
During search, bounding boxes help you identify objects, for example based on motion detection. You can turn the bounding boxes on or off.

The bounding boxes mostly appear in the thumbnail images of your search results. However, if your VMS system is configured to search for metadata, bounding boxes may also appear when you preview video from the search results.

Steps:

1. Go to the **Search** tab and run a search.
2. In the upper-right corner below **Bounding boxes**, do one of the following:

- Select **Show** to make the bounding boxes appear
- Select **Hide** to hide the bounding boxes



Sorting options

You can sort your search results by:

Name	Description
Relevance	This sorting option is only available if you are using one of these products: • XProtect Corporate • XProtect Expert **Relevance** means different things depending on how your search is configured: • None or one search category selected - the search result with the newest event time is displayed first • Multiple search categories selected/**Match any criterion** - the search result with most matching search categories is displayed first. If two search results have the same number of matching search categories, the search result with the newest event time is displayed first • Multiple search categories selected/**Match all criteria** - the search result with most event times is displayed first. If two search results have the same number of event times, the search result with the newest event time appears first
Newest event time	Search results with the most recent event time appear first.
Oldest event time	Search results with the oldest event time appear first.
Newest start time	Search results with the most recent start time appear first.
Oldest start time	Search results with the oldest start time appear first.

Locate cameras while searching

If your VMS system is configured to use smart map , you can view the geographical location of the cameras in a smart map preview while searching for video and related data.

Requirements

- You are using one of these XProtect products:
  - XProtect Corporate
  - XProtect Expert

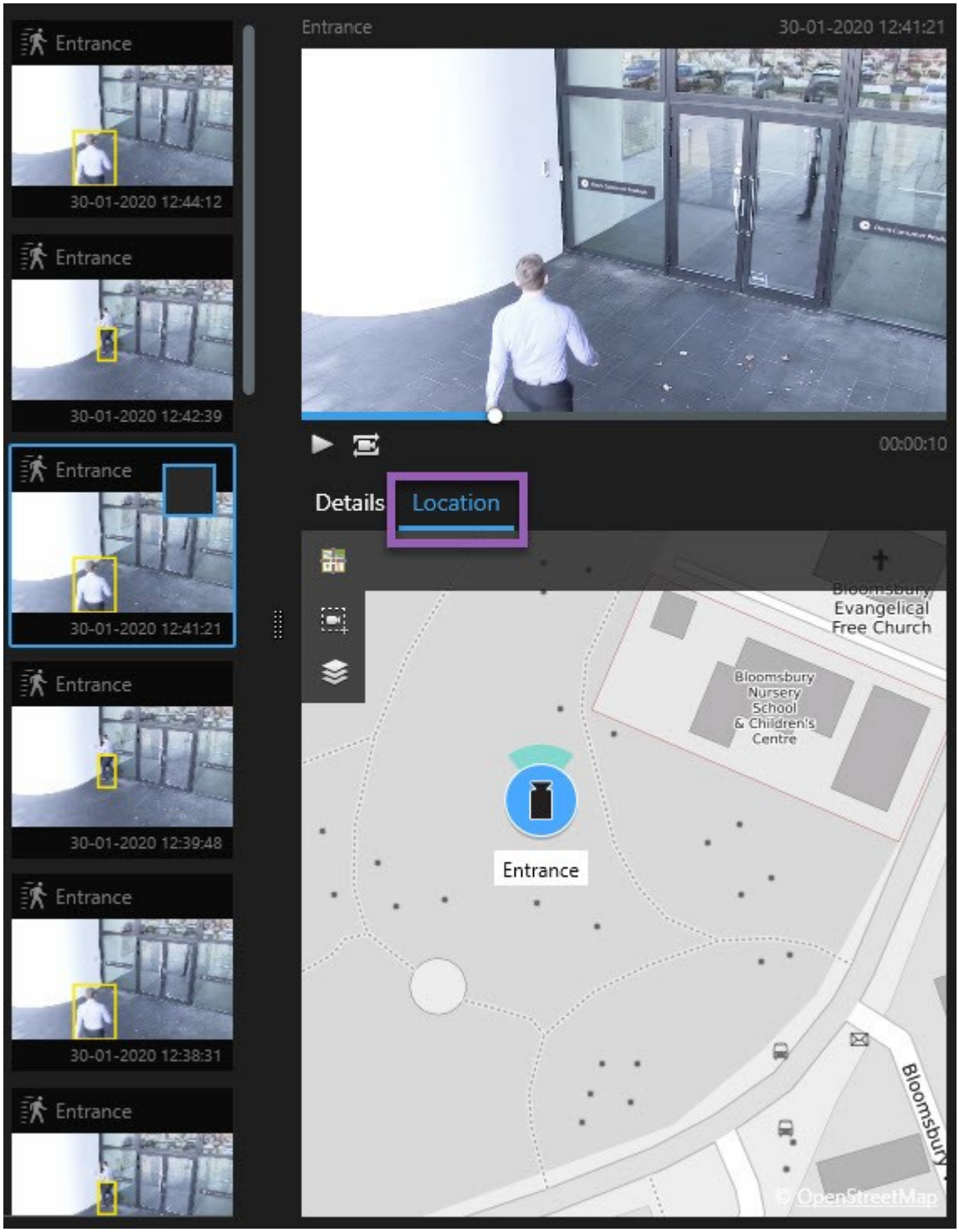
    

    For information about the features available in your XProtect VMS, see Surveillance system differences on page 33.

- Cameras must be geographically positioned. If in doubt, ask your system administrator

Steps:

1. Select the search result that you are interested in.



2. In the preview area, click **Location**. The camera is displayed in its geographic context.

3. To get an overview of the surroundings, use the scroll wheel on your mouse to zoom out, or pan away from the view item.
4. To return to the camera, click **Re-center**.

Camera icons (explained)

Some of the icons described in this topic appear only in the **Location** area on the **Search** tab, whereas icons with red are associated with alarms and also appear in views that contain the smart map. The icons differ depending on the situation.

In the table below:

- Gray background indicates that you have *not* selected the camera
- Blue background indicates that you have selected the camera

Icon	Tabs/modes	Description
	**Search** tab	The camera is not associated with any of the search results.
	**Search** tab	You have selected the search result that the camera is associated with.
	**Live** mode, **Playback** mode, and **Search** tab	This is a source camera: a camera that triggered an alarm.
	**Live** mode, **Playback** mode, and **Search** tab	This is a related camera: a camera associated with the selected source camera, which triggered the alarm. This icon only appears after you select a source camera.
	**Live** mode, **Playback** mode, and **Search** tab	This is both a source camera and a related camera. This camera: • Triggered an alarm, and • Is associated with the selected source camera, which triggered the alarm This icon only appears after you select a source camera.

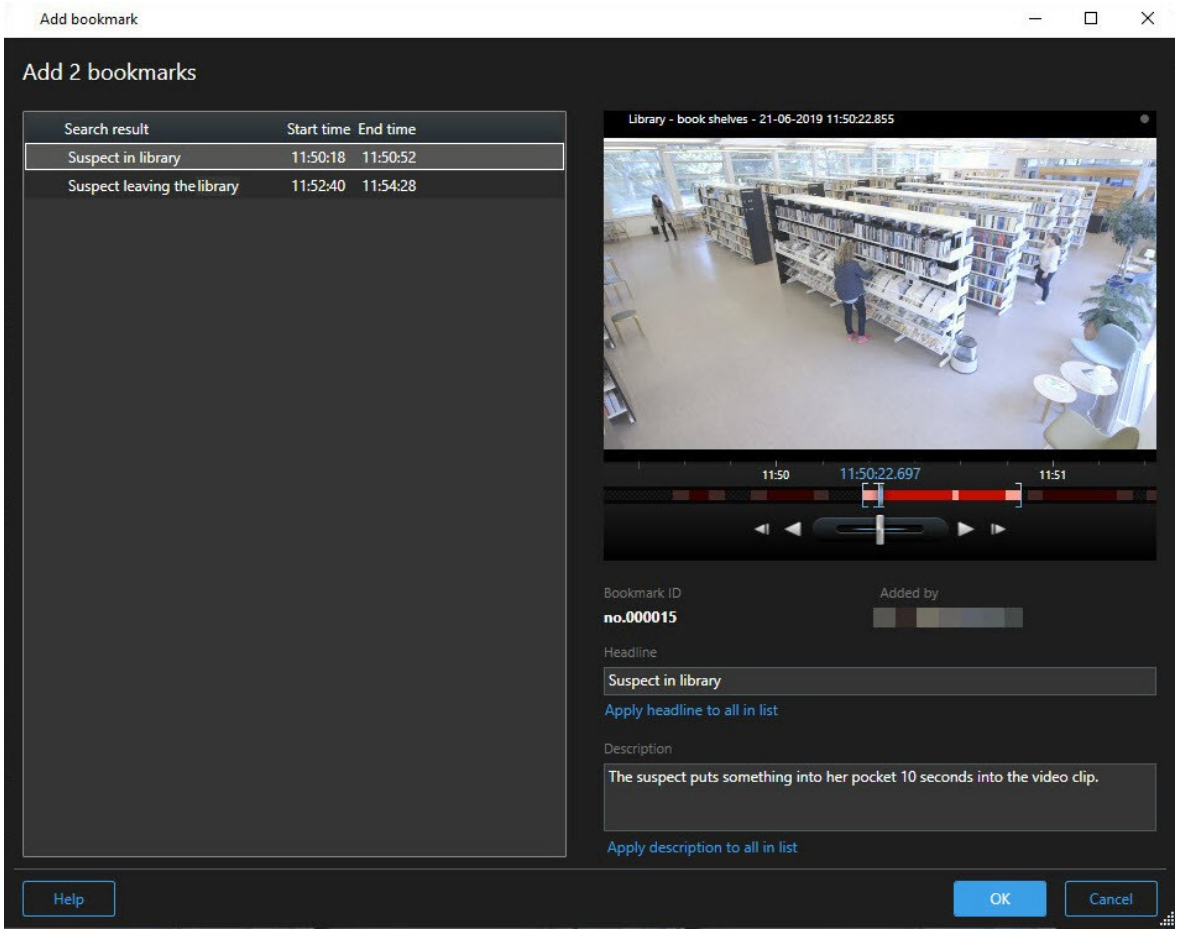
Source cameras and related cameras are defined in XProtect Management Client as part of the alarm definition.

Bookmark search results

To document or share incidents that you have found by searching, you can bookmark multiple search results at the same time. Bookmarking incidents allows you or other operators to find the incidents later.

Steps:

1. For each search result that you want to bookmark, hover over it and select the blue check box .
2. In the blue action bar, click . A window appears. The picture reflects the situation where you have selected two search results.



3. Select the search results one by one to add details to the bookmarks and follow these steps:
    1. To change the default time span, drag the handles in the timeline to a new position.

    2. Enter a headline and possibly also a description of the incident.
    3. If you want the same headline or description to apply to all the bookmarks, click:
        - **Apply headline to all in list**
        - **Apply description to all in list**
4. Click **OK** to save the bookmarks. A progress bar informs you when the bookmarks are created.

If XProtect Smart Wall is set up in your system, click **Display on Smart Wall** to send a bookmark to a monitor in a Smart Wall.

Edit bookmarks from search results

You can edit the details of bookmarks in your system, for example the time span, headline, and description. You can also edit multiple bookmarks at the same time.

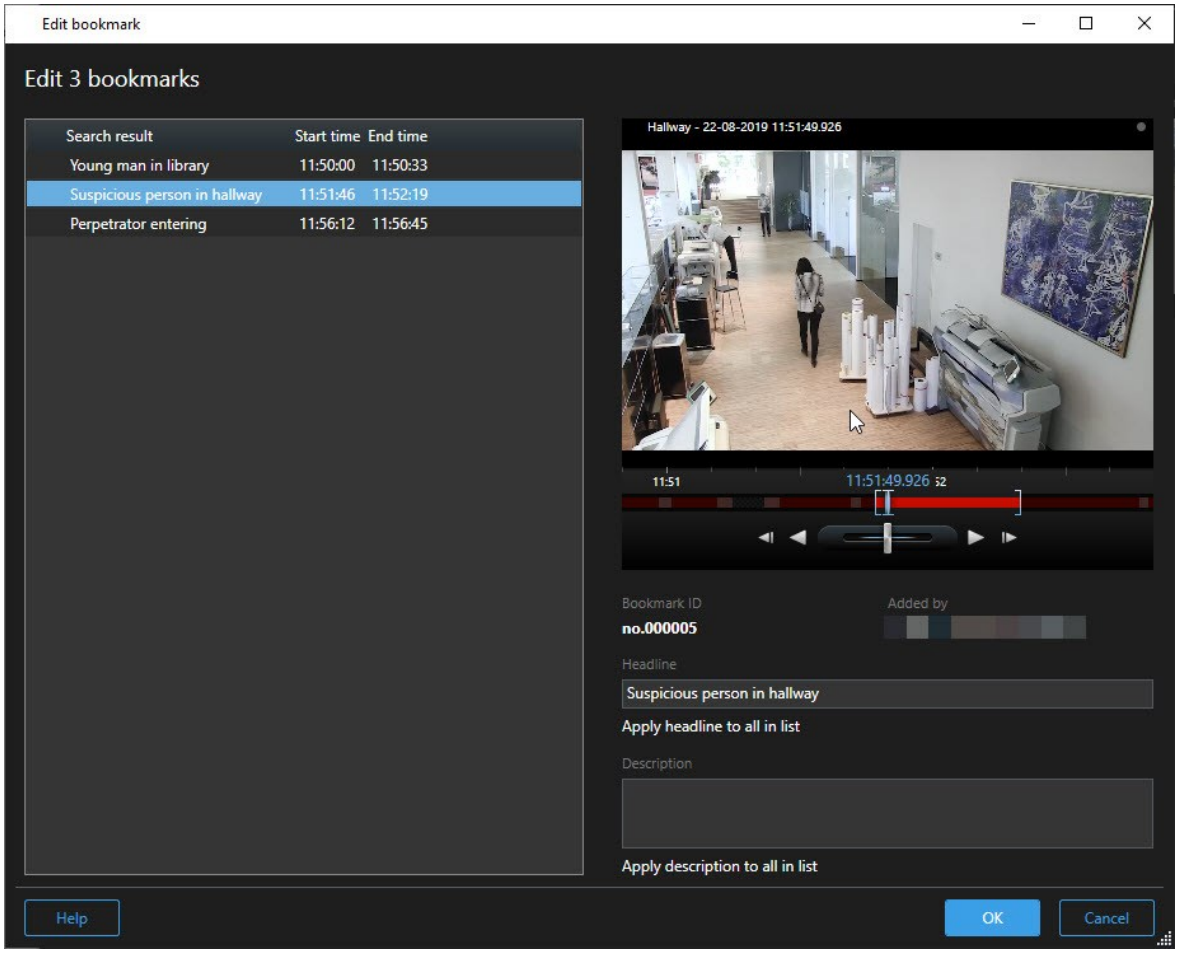
Requirements

You must have the user permissions to edit bookmarks. This is done by your system administrator in Management Client under **Roles** > **Overall Security**.

Steps:

1. On the **Search** tab, find the bookmarks that you want to edit. When you perform the search, make sure that you have selected **Search for** > **Bookmarks**.
2. For each bookmark that you want to edit, hover over it and select the blue check box .

3. In the blue action bar, click . A window appears.



4. Select the search results one by one to edit the details, for example time span, headline, and description.
5. Click **OK** to save your changes. A progress bar informs you when the changes are saved.

If XProtect Smart Wall is set up in your system, click **Display on Smart Wall** to send the bookmarks a video wall.

Take snapshots from search results

To save and share still images from your search results, you can take multiple snapshots at the same time.

Steps:

1. When you have performed your search, hover over the search results, one by one, and select the check box .
2. In the blue action bar, click and select **Create snapshot**. A progress bar informs you when the snapshots are created.
3. To locate the snapshots on your computer, go to the location that is specified in the **Settings** dialog > **Application** > **Path to snapshots**.

Transfer the search time to the playback timeline

When you are previewing a search result on the **Search** tab, you can synchronize the time in playback mode with the time in the preview timeline. This is useful if, for example, you have found an incident, and you want to investigate what happened at that time on other cameras.

1. On the **Search** tab, select a search result.
2. In the preview area, click to transfer the current time to the playback timeline in playback mode. You will stay on the **Search** tab.

3. To check other related cameras, switch to playback mode and select a view that contains the cameras that you are interested in. The timeline is now in sync with the search result.

Managing your searches

This feature is only available in certain XProtect VMS systems. For more information, see the product comparison chart: https://www.milestonesys.com/solutions/platform/product-index/

You can save your searches to reuse them and share them with other operators. Depending on your user permissions, you can also access and use the searches made by others, unless they are private. When a search has been saved, you can:

- Change the name and description, and make the search private or public.
- Modify how the search is configured, for example by adding or removing cameras or by adjusting the search categories.
- Delete the searches as they become obsolete.

Save searches

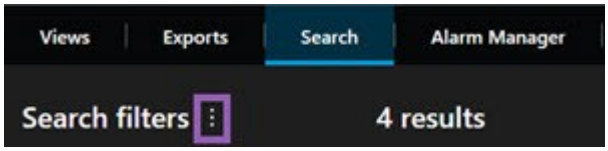
You can save your searches, so you can reuse them later or share them with other operators.

Requirements

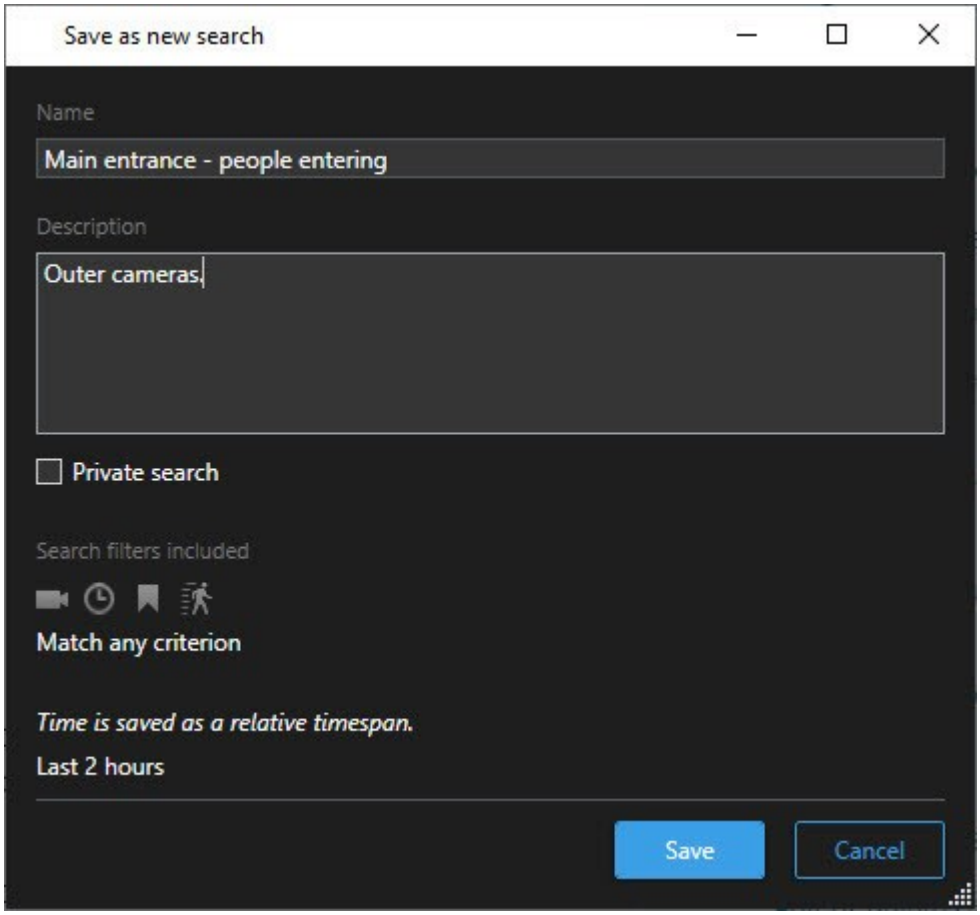
To save new searches that will be available to other users of your VMS system, the **Create public searches** user permission must be enabled on your role in XProtect Management Client.

Steps:

1. On the **Search** tab, configure your search. See Searching for video data on page 201.
2. Click ⋮ to the right of **Search filters**.



3. In the list that appears, click **Save as**. A window appears.



4. Select a name that will make it easy for you to find the search, and possibly also a description. Later, when you use keywords to find the search, the search includes both the **Name** and the **Description** fields.
5. To make the search visible only to you, select the **Private search** check box.
6. Click **Save**. A progress bar informs you when the search is saved.

To get an overview of saved searches, click and then **Open and manage searches**.

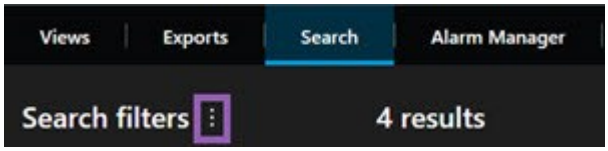
Find and open saved searches

Requirements

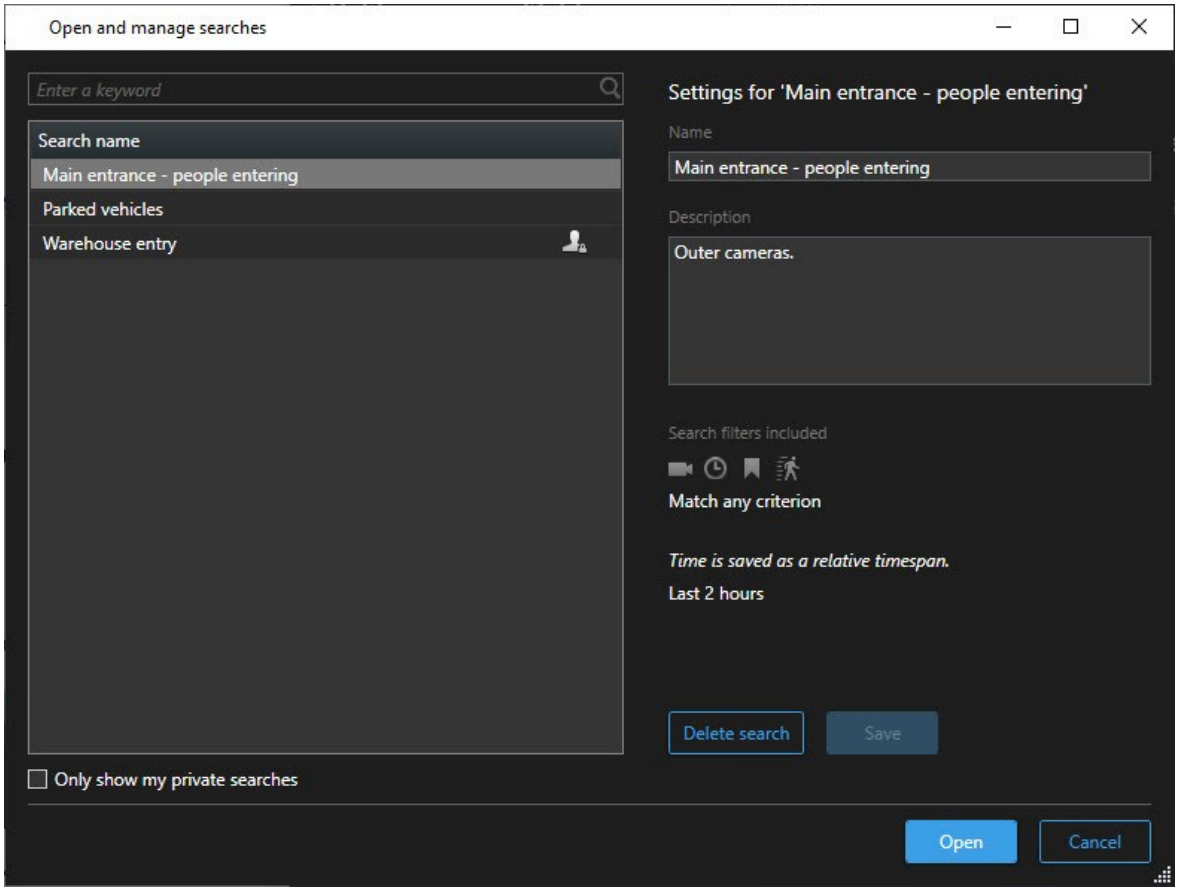
To find and open public searches, the **Read public searches** user permission must be enabled on your role in XProtect Management Client.

Steps:

1. On the **Search** tab, click ⋮ to the right of **Search filters**.



2. In the list that appears, click **Open and manage searches**. A window appears.



3. Find and double-click the search that you want to open, or click **Open**. Immediately, the search is run.

> If many searches are listed, you can use keywords to find the search. The search includes both the **Name** field and the **Description** field.

4. You can modify the search, for example by adding cameras. Click ⋮ > **Save** to save the changes.

Edit or delete saved searches

This feature is only available in certain XProtect VMS systems. For more information, see the product comparison chart: https://www.milestonesys.com/solutions/platform/product-index/

You can change the details of a saved search, or you can change how the search is configured, for example the search categories.

If the searches become obsolete, you can delete them.

Requirements

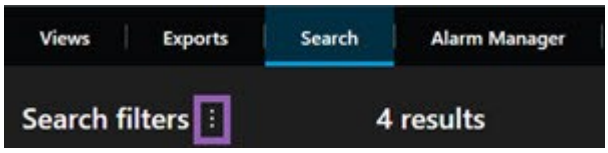
The following user permissions are enabled on your role in XProtect Management Client:

- To find and open public searches, the **Read public searches** user permission must be enabled
- To edit a public search, the **Edit public searches** user permission must be enabled
- To delete a public search, the **Delete public searches** user permission must be enabled

Learn how to:

Edit the details of a saved search

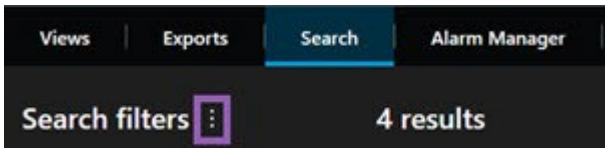
1. On the **Search** tab, click ⋮ to the right of **Search filters**.



2. In the list that appears, click **Open and manage searches**. A window appears.
3. Find and select the search that you want to change.
4. Make your changes, for example by entering a name for the search, and click **Save**.

Change how a search is configured

1. On the **Search** tab, click ⋮ to the right of **Search filters**.



2. In the list that appears, click **Open and manage searches**. A window appears.

3. Find and double-click the search that you want to open, or click **Open**. Immediately, the search is run.

   If many searches are listed, use the search function to find the search.

4. Modify the search, for example by adding cameras, and click  > **Save**.

Delete a saved search

1. Open the **Open and manage searches** window as described above.
2. Find and select the search that you want to delete.
3. Click **Delete search**.

Bookmarks (usage)

This feature is only available in certain XProtect VMS systems. For more information, see the product comparison chart: https://www.milestonesys.com/solutions/platform/product-index/

Bookmarks allow you to quickly find or share relevant video sequences with other users of the system. Detailed bookmarks make it easier to find the bookmarks after creating them. To enable details, see Enable detailed bookmarks on page 75.

Bookmarks (explained)

You can bookmark incidents in live or recorded video. A bookmark is essentially a small video clip. When you bookmark an incident, the program automatically assigns it an ID and the user who created it. Bookmarks are searchable, so operators can easily find them later.

A bookmark video clip typically contains video from a few seconds before and a few seconds after the bookmarked incident (specified by the system administrator) to ensure that the incident is recorded, regardless of any delays.

You can find and edit bookmarked video by using:

- The search functionality on the **Search** tab.
- The timeline in playback mode.

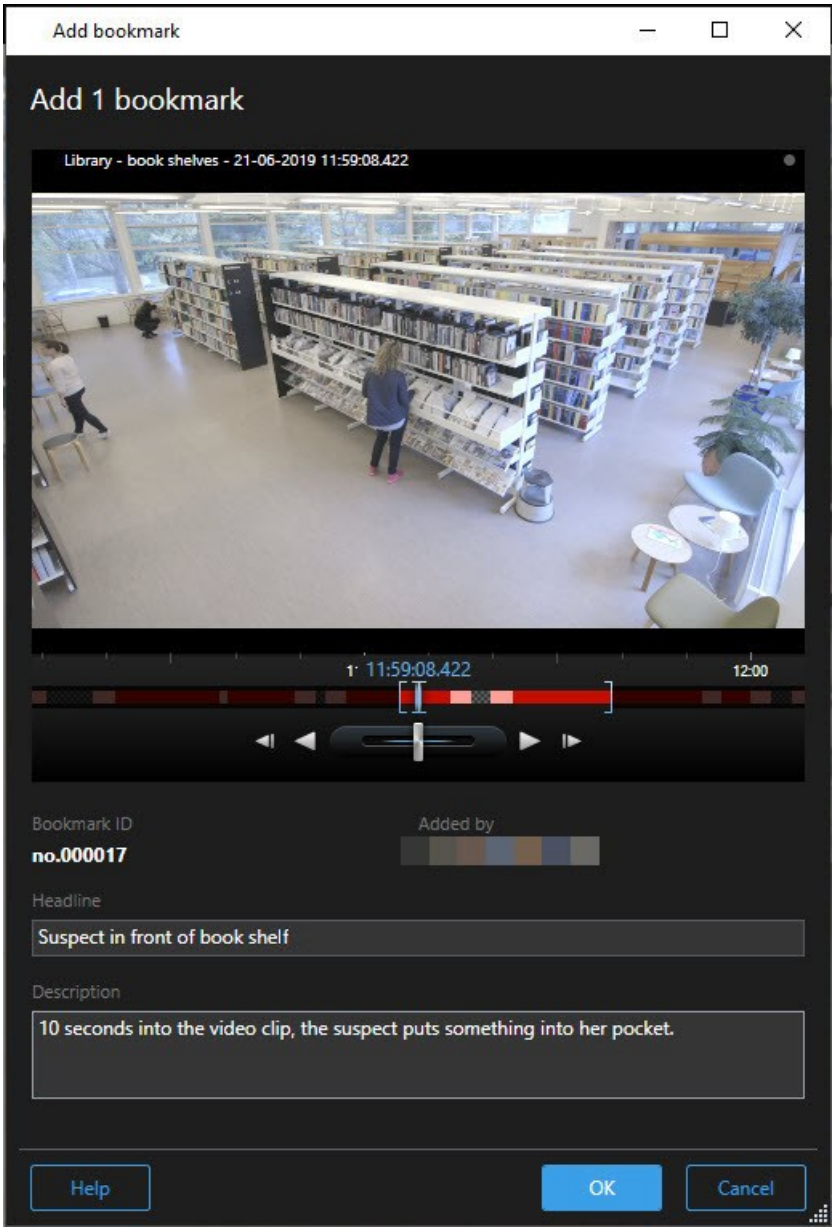
The ability to add bookmarks from a camera depends on your user permissions. Likewise, you may be able to view bookmarks even if you cannot add them, and vice versa.

Bookmark window

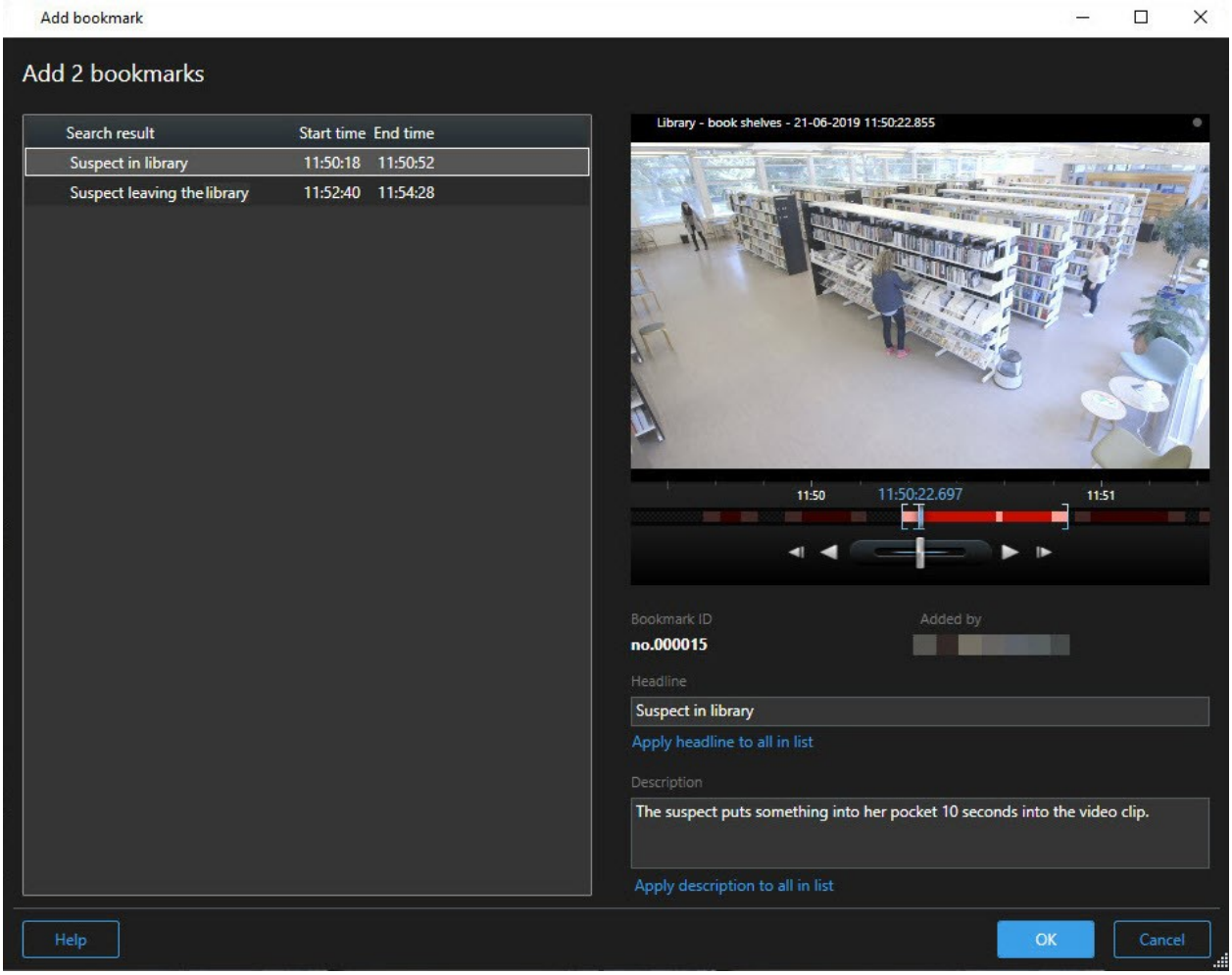
The Bookmark window appears only when you have enabled detailed bookmarks. See Enable detailed bookmarks on page 75.

The layout of the bookmark window changes depending on where you are in XProtect Smart Client, and if you are creating just one or multiple bookmarks. Click below to see images of the window.

Single bookmark



Multiple bookmarks



Fields in the **Bookmark** window.

Name	Description
Bookmark ID	A number that automatically is assigned to the bookmark.
Added by	The person who created the bookmark.
The timeline	Although the bookmark time and the clip start and end time are specified by the system administrator, you can change these settings. To change the time, drag the indicators on the timeline (see Time navigation controls (overview) on page 175) to the required time.

Name	Description
	 **Start time**: The suggested start time of the bookmark clip is a number of seconds before the bookmark time, specified by the system administrator. **Bookmark time**: The time in the video clip that you bookmarked. **End time**: The suggested end time of the bookmark clip is a number of seconds after the bookmark time, specified by the system administrator.
Headline	Lets you specify a headline containing a maximum of 50 characters.
Apply headline to all in list	Only visible if you are creating multiple bookmarks. Click the text to use the same headline for all bookmarks.
Description	Lets you specify a description.
Apply description to all in list	Only visible if you are creating multiple bookmarks. Click the text to use the same description for all bookmarks.

Add or edit bookmarks

You can add bookmarks to live and recorded video. If you have enabled detailed bookmarks, you can give the bookmark a name and a description. You can even adjust the time span. Later, you can find and edit the bookmark details.

Requirements:

Detailed bookmarks must be enabled. For more information, see Enable detailed bookmarks on page 75.

Steps:

1. Select the required camera in the view.
2. Click the bookmark icon  . With details enabled, the **Bookmark** window appears where you can add a detailed description of the incident.
3. Enter a name for the bookmark.
4. The length of a bookmark clip is determined on the surveillance system server, but you can change this by dragging the timeline indicators.
5. (optional) Describe the incident.
6. Click **OK**.

To find and edit the bookmark later, go to the **Search** tab and search for bookmarks. See Search for bookmarks on page 208.

Delete bookmarks

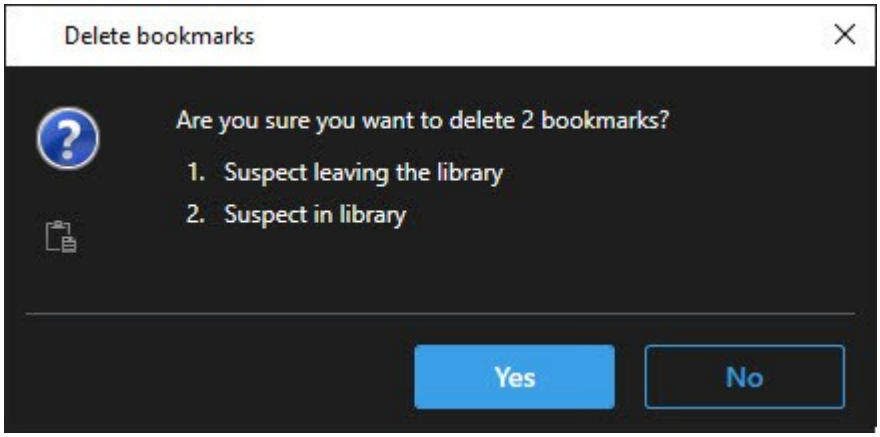
You can delete bookmarks created by yourself or others. If you delete a bookmark, it is removed from the database, and you can no longer find it.

Requirements

You must have the user permission to delete bookmarks. This user permission is controlled by your system administrator.

Steps:

1. On the **Search** tab, find the bookmarks that you want to delete.
2. In the search results, hover over each of these bookmarks and select the blue check box .
3. In the blue action bar, click and select **Delete bookmark**. A window appears.



4. Click **Yes** to delete the bookmarks.

> There may be restrictions in your system preventing you from deleting certain bookmarks. In that case, you will be notified.

Find or export bookmarked video

After creating bookmarks, you can find the bookmarks again on the **Search** tab. Suppose you want to find an incident that you bookmarked within the last six hours on camera 1, then you would set the duration to **Last 6 hours**, select camera 1, and add the **Bookmarks** search criterion. See also Search for bookmarks on page 208.

You can also export the bookmarked video. See also Actions available from search results (overview) on page 213.

Alarms and events (usage)

Alarms (explained)

> This feature is only available in certain XProtect VMS systems. For more information, see the product comparison chart: https://www.milestonesys.com/solutions/platform/product-index/

On the XProtect VMS server, virtually any kind of incident or technical problem - events - can be set up to trigger an alarm. Alarms and events can all be viewed on the **Alarm Manager** tab, which provides a central overview of your VMS incidents, status, and possible technical problems.

You cannot set up alarm triggers in the XProtect Smart Client. Your system administrator does this when configuring the XProtect VMS system.

> The **Alarm Manager** tab is either displayed or hidden depending on the settings defined by your system administrator.

The **Alarm Manager** tab provides a dedicated view for your alarm or event handling. The tab itself displays the number of active alarms. More than nine alarms are shown with a . The **Alarm Manager** tab includes an alarm list, an alarm preview for previewing video associated with individual alarms or events, and possibly also a map that displays the geographical location of the camera associated with the alarm.

Alarm list (explained)

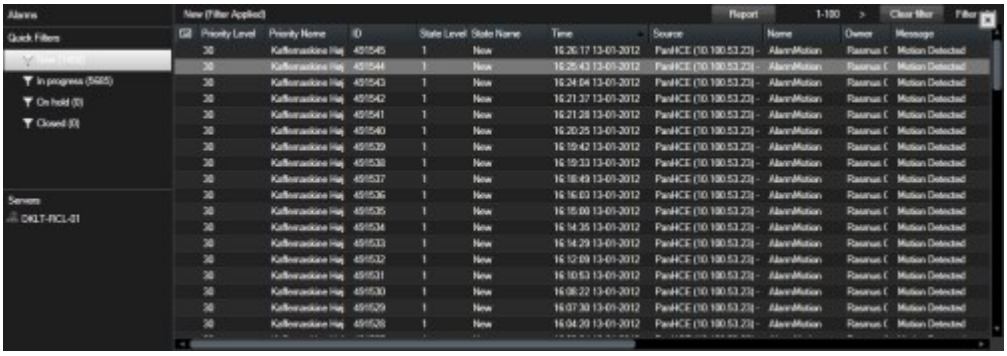
The **Alarm List** displays incoming alarms by default, with the most recent alarms at the top of the list. Alternatively, the alarm list can display a list of MIP plug-in and analytic events, for example, access control or license plate recognition.

Alarms or events with associated video are displayed with an icon . To preview a still image from the time of the alarm or event, hover over the icon. To preview recorded video from the camera or cameras associated with the alarm or event, select the alarm or event in the list. To stop a repeating alarm sound, select the alarm associated with the sound in the list.

You can decide how you want the list to appear, you can filter the columns, you can drag the columns to different positions, and you can right-click to show or hide certain columns.

> The event list does not display system- or user-generated events, such as motion detection or archive failure.

The list is updated every 3 seconds.



To see a list of events, enter setup mode and select **Event** in the **Properties** pane. See also Alarm list settings on page 82.

Servers in alarm list (explained)

On the left-hand side of the alarm list, you can view the servers that the alarms originate from. Many XProtect VMS systems only have a single server, but some systems may consist of several servers in a hierarchy. All the servers you have access to are listed, and you can filter alarms by servers.

Alarm states (explained)

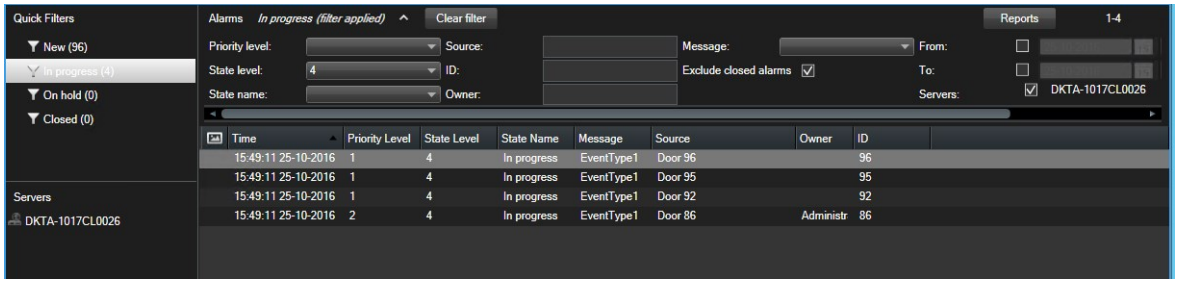
Alarms can be in one of the following states: New, In progress, On hold, or Closed. You can see the state of each alarm in the **Alarm List**, in the **State Name** column. The **Filters** pane lets you filter according to certain criteria. Initially, all alarms will be in the **New** state, but when an alarm is being handled, its state is updated.

Filter alarms

There are several ways you can filter the alarm list, so it displays just the alarms or events that you are interested in.

Steps:

1. In the toolbar of the alarm list, click the **Custom (filter applied)** or **No filter** text. The text may differ depending on the filter selected.



2. Enter filter criteria on any of the columns you want to filter on. For example, if you enter a user ID in the **ID** field, the list will only display alarms assigned to that particular user.
3. You can combine filters, for example **State name** and **Owner** (assigned to).
4. To return to the unfiltered alarm list, click the **Clear filter** button.
5. To sort the content of the alarm list, click the title of the column.

If your alarm handling views contain map content, you can also filter the alarm list by right-clicking an element (camera, server, or similar) on the map, then selecting **Show alarms**. This will make the alarm list show only alarms from the selected element.

Responding to alarms

Viewing and editing details of an alarm

You can respond to alarms in different ways. You can go to any view where you have added the **Alarm List** and double-click an alarm. The alarm opens in a separate window, where you can preview the alarm incident and live video. You can also respond to the alarm by changing the fields in the table below.

Depending on how your XProtect VMS system is configured, you may also receive alarm desktop notifications. Such notifications stay on your screen for 15 seconds. When you click a notification, it takes you directly to the **Alarm Manager** tab and opens the alarm window.

Field	Description
State	The state of the alarm indicates if someone has addressed the event. You can change the state of the alarm. Typically, you would change the state from **New** to **In progress**, and then later to **On hold** or **Closed**.
Priority	Lets you change the priority of the alarm.
Assigned to	Lets you assign the alarm to a user in your organization, including yourself. The person to whom you assign the alarm becomes the owner of the alarm, and will appear in **Owner** column of the alarm list.
Comment	Write comments and remarks that are added to the **Activities** section. Comments typically relate to the actions you have taken. For example, "Suspect detained by Security", "Suspect handed over to police," or "False alarm." The **Comment** field appears at the bottom of the window.
Activities	The activities summarize how you have handled the alarm. Any changes you or your colleagues make to alarm state or priority, any reassigning of alarms between users as well as any comments added will automatically be included in the **Activities** section.

Field	Description
	Depending on the configuration of the XProtect VMS server, the alarm can contain instructions about what to do when receiving the alarm. The instructions are defined on the server-side as part of the alarm definition. When that is the case, the activities are automatically displayed when you edit the alarm.
Print	Lets you print a report that contains information about the alarm, such as the alarm history and a still image from the time of the alarm, if an image is available.

Acknowledge alarms

When you have received an alarm, you can acknowledge it to record that you will do something about it.

Steps:

1. In the alarm list, right-click the alarm and select **Acknowledge**. The alarm state changes to **In progress**.

   You can only acknowledge new alarms.

2. To acknowledge multiple alarms simultaneously, press and hold down the **CTRL** key, and then select the alarms you want to acknowledge.
3. Double-click an alarm to edit the details of the alarm, for example assigning the alarm to someone and adding instructions.

Disable all new alarms on selected event types

If an event is triggering false alarms, you might want to disable all new alarms on this type of event for some time.

For example, if there is a lot of movement around a camera and this is causing several false alarms, you can disable alarms on motion detection for this camera for 10 minutes. Then, motion detection for the camera will not trigger alarms for 10 minutes. This way, false alarms will not disturb you, and you can focus on the alarms that need your attention.

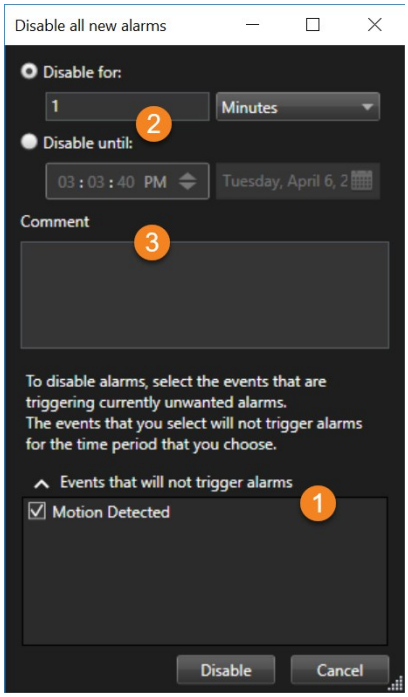
Disabling alarms affects all operators who are connected to the XProtect VMS system that you are also connected to.

You can disable all new alarms using the **Alarm Manager** or a map.

1. Using the **Alarm Manager**: in the alarm list, right-click an alarm and select **Disable all new alarms**.

   Using a map: right-click an alarm and select **Disable all new alarms** > **Disable**.

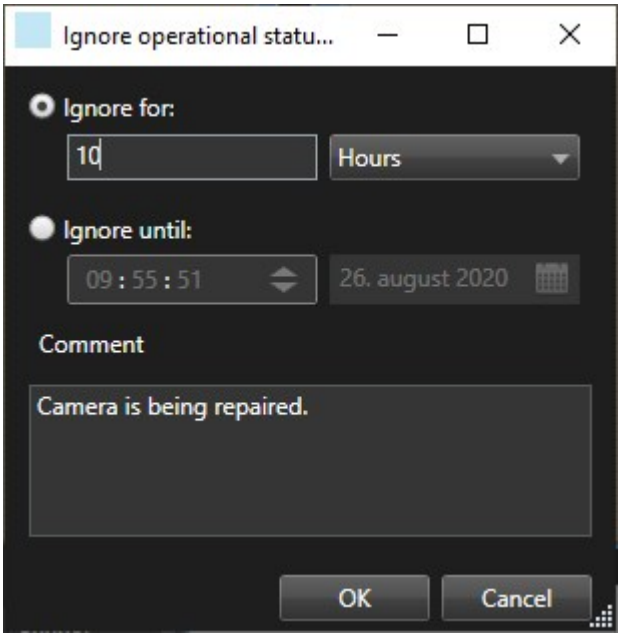
   The **Disable all new alarms** window appears.



2. In the **Events that will not trigger alarms** list ❶, select which event types should not trigger alarms.
3. Specify until when or for how long the selected event types should not trigger alarms ❷.
4. Optionally, add a comment about why you are disabling alarms on the selected event types ❸.

Ignore alarms on maps

On a map, you can ignore an alarm for an element for a duration of time. For example, if a camera is being repaired and therefore disconnected, you might want to ignore the error showing up on the map during the repair. When you ignore an alarm on a map, this does not remove the alarm from the alarm list, just the map.



Close alarms

After acknowledging an alarm, typically you assign it to someone who investigates what is going on. During that time, the alarm will be in the state **In progress**. After handling the alarm, you can close it.

To close an alarm, in the **Alarm List**, do one of either:

- Right-click the alarm and select **Close**.
- Double-click the alarm, and in the **State** list, select **Closed**.

Print alarm reports

You can print a report with information about the alarm, including the alarm history and, if available, a still image from the time of the alarm. However, you cannot use this feature if you have selected multiple alarms in the alarm list . To comply with GDPR rules, by default, the name of the report creator is not shown in the printed report, while the name of the person who printed the report is. To display all names connected to the report, select the **Display names** button.

1. In the alarm list, right-click the alarm.
2. Select **Print**. A window appears.
3. To add a note, enter the text in the **Note** field.
4. Click the **Print** button.

Get statistics on alarms

Get statistical data about the alarms triggered in your XProtect VMS system over the:

- **Last 24 hours**
- **Last 7 days**
- **Last 30 days**
- **Last 6 months**
- **Last year**

The **Alarm Report** window shows two graphs that display the number of alarms filtered by categories, for example **Priority** or **State**, allowing you to compare the two graphs side by side.

Steps:

1. In the **Alarm List**, click the **Reports** button. A window appears.
2. Above the graphs, select the timespan, for example **Last 24 hours**.
3. In the **Select report** list, select one of these categories:
    - **Category**
    - **State**
    - **Priority**
    - **Reasons for closing**
    - **Site**
    - **Response time**
4. For each graph, select a sub-filter. For example if you selected **State**, you can select **New** in the first graph and **In progress** in the second. The graphs are populated.
5. To print the graphs as a PDF report, click  .

Alarms on maps (explained)

If your alarm handling view contains one or more map positions, you can view alarms on the maps too. Maps display alarms based on the geographical location of the camera, server or other device triggering the alarms, so you can instantly see where the alarm originates from. You can right-click and acknowledge, disable, or suppress the alarm directly from the map.

Camera elements display video in thumbnail format when you move your mouse over it. When used together with alarms, the graphical elements on maps display red circles around them if alarms occur. For example, if an alarm associated with a particular camera occurs, the graphical element representing that camera will immediately get a red circle around it, and you can then click the camera element and not only view video from the camera, but also handle the alarm through a menu that appears.

If red is not an ideal color for signifying alarms on your maps, you can change this color.

Now, say the camera which has an alarm associated with it, is located on a street level map, but you are viewing a city level map. How will you then notice the alarm? No problem, thanks to hot zones—graphical representations linking different map hierarchy levels together. If an alarm is detected on the street level map, the hot zone on the city level map will then turn red, indicating that there is an alarm on a lower level map—even if there are map levels in between.

To return to an alarm list mode where you can see alarms from more than just the one element, click the required server, priority or state in the alarm list.

Alarms on smart maps (explained)

Smart map displays alarms if they are triggered by a device and if the device is added to the smart map. See also Adding, deleting, or editing devices on smart map on page 95.

For more information about smart map icons, see Camera icons (explained) on page 223.

Events (explained)

An event is a predefined incident on the XProtect VMS system that can be set up to trigger an alarm. Events are either predefined system incidents or user-defined events, for example analytics events or generic events. Events are not necessarily linked to an alarm, but they can be.

Typically, events are activated automatically and in the background, for example, as a result of input from external sensors, detected motion or by data from other applications. However, events can also be manually activated. Events are used by the VMS system to trigger actions, such as starting or stopping recording, changing video settings, activating output, or combinations of actions. When you activate an event from your XProtect Smart Client, it automatically triggers actions on the VMS system, for example recording on a particular camera with a particular frame rate for a particular period of time.

Your system administrator determines what happens when you manually activate an event.

Manually activate events

The list of selectable events is grouped by server, and the camera or device that the event is associated with. You can manually activate an event. There is no confirmation once you have activated an event.

1. In live mode, expand the **Event** pane.
2. Click **Activate**.
3. Alternatively, if available for the camera, click the overlay button that appears when you move your mouse over the image.

Hierarchically, global events will appear under the relevant server. If a server is listed with a red icon, it is unavailable and you cannot activate events on it.

Privacy masking (usage)

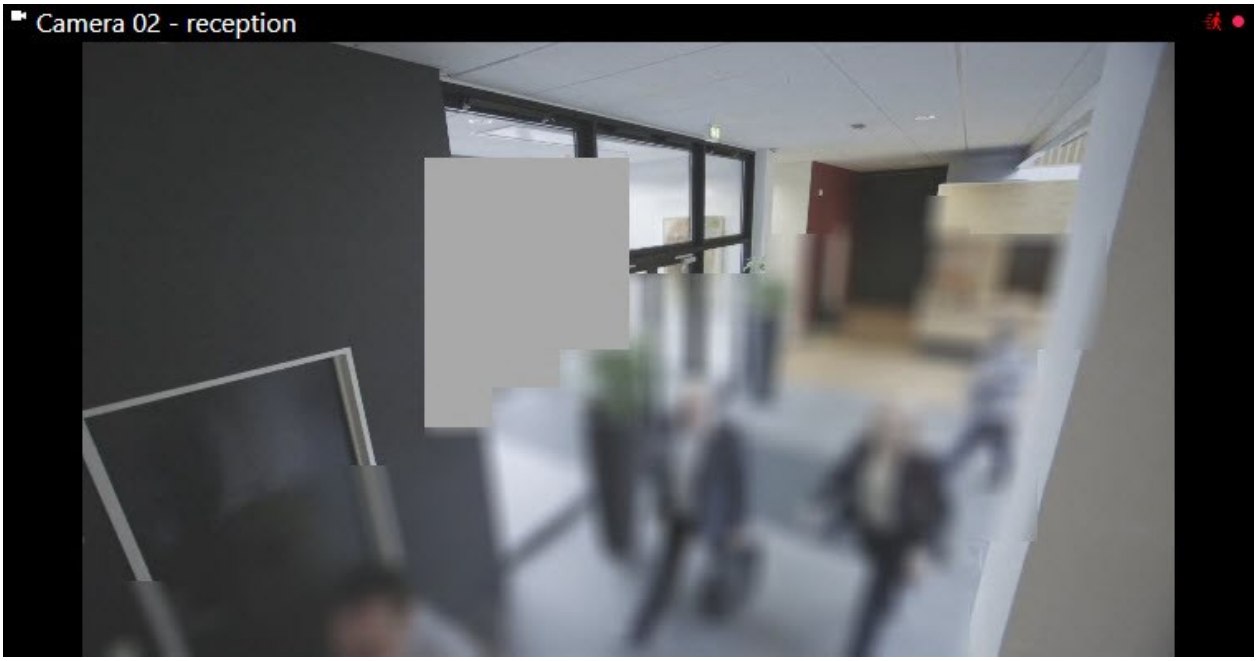
This feature is only available in certain XProtect VMS systems. For more information, see the product comparison chart:
https://www.milestonesys.com/solutions/platform/product-index/

Privacy masking (explained)

You can use privacy masking to protect private or public areas in live and recorded video by blocking out certain areas in the field of view of a camera. For example, if a camera overlooks the windows of a private residence, you can apply privacy masks to the windows.

In this example, privacy masks are applied to five windows in an adjacent building.

In this example, two types of privacy masks are applied. The solid gray area is covered permanently while the blurred area can be lifted, but only by users with sufficient user permissions to lift privacy masks.



Privacy masks are applied to areas in cameras' field of view by system administrators, and as such you cannot add or remove them from views in XProtect Smart Client. You can, however, temporarily remove liftable privacy masks from the views, depending on your surveillance system and user permissions.

You can also add additional privacy masks when you export. See also Add privacy masks to recordings during export on page 182.

If you export video that contains privacy masks, the export process may take significantly longer and the export file size may be larger than usual, particularly if you export in the XProtect format.

Lift and apply privacy masks

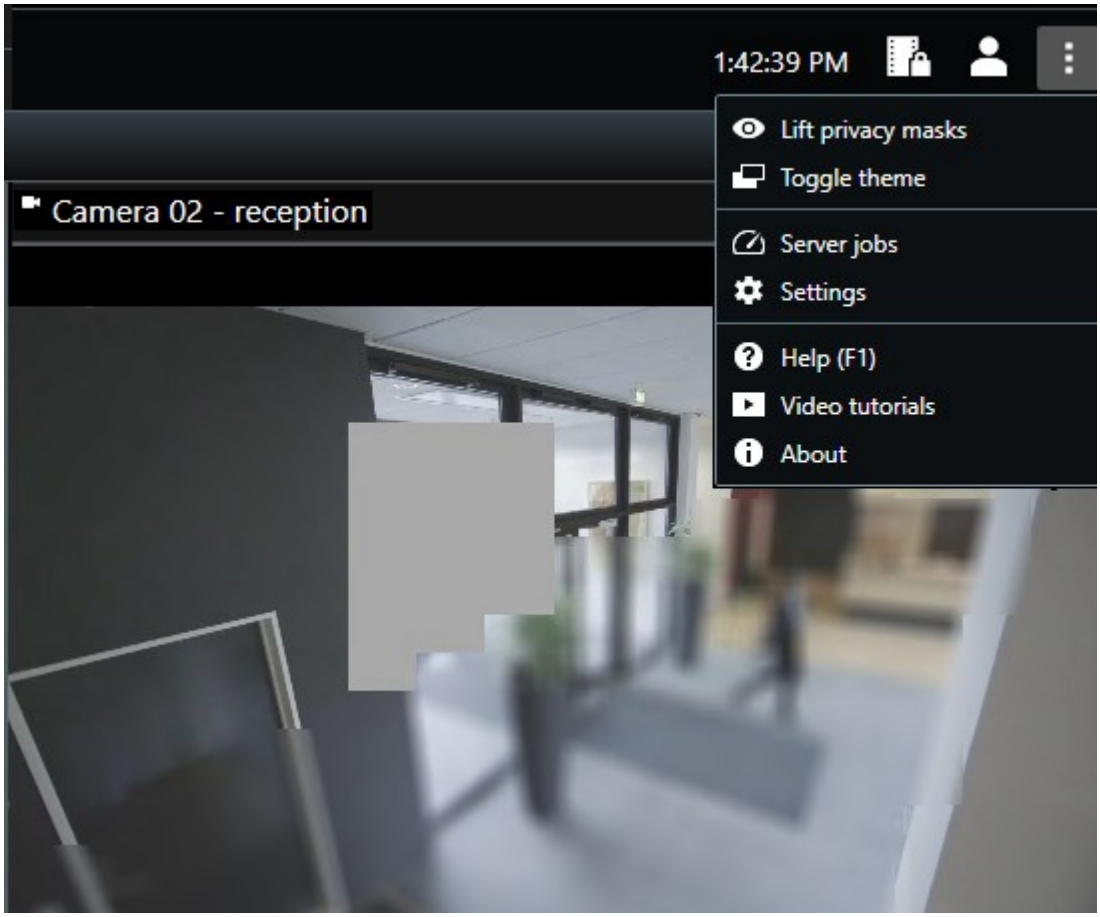
This feature is only available in certain XProtect VMS systems. For more information, see the product comparison chart: https://www.milestonesys.com/solutions/platform/product-index/

It can sometimes be necessary to view the video beneath the areas covered by privacy masks. This is only possible for privacy masks that your system administrator has defined as liftable privacy masks in the Management Client and if you have the necessary user permissions.

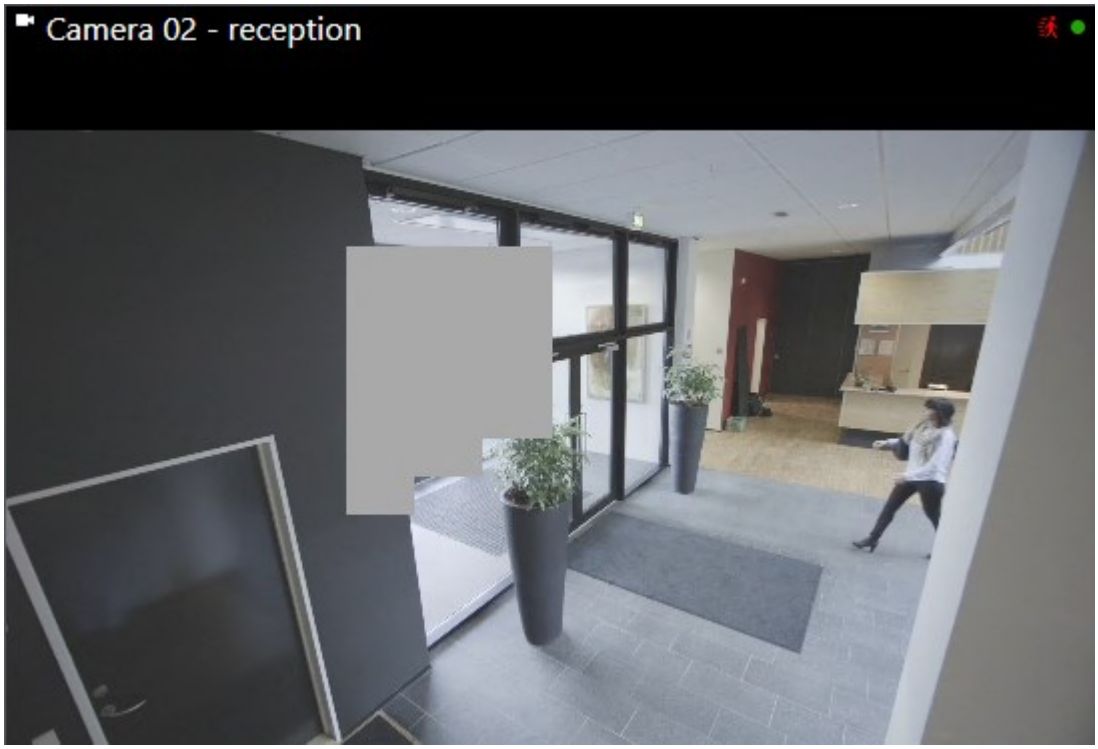
If you do not have the necessary user permissions, you will be asked for additional authorization. Contact a person who has the user permissions to authorize you, so he or she can enter their credentials. If you do not know who can authorize you, ask your system administrator.

To lift privacy masks:

1. In live or playback mode, select **Settings and more** > **Lift privacy masks** on the application toolbar.



If you have the user permissions to lift privacy masks, liftable privacy masks now disappear for all cameras and permanent privacy masks remain.



If you do not have sufficient user permissions, a dialog box appears.

2. Contact a person who has the user permissions to authorize you, so he or she can enter their credentials.

   Liftable privacy masks disappear and permanent privacy masks remain.

3. The lift ends (times out) after 30 minutes, if your system administrator has not changed the default value, but you can apply the masks any time. On the application toolbar, select **Settings and more** > **Apply privacy masks**.

If you log out of XProtect Smart Client with lifted privacy masks and log in again, the masks will always be reapplied.

PTZ and fisheye lenses (usage)

PTZ and fisheye lenses are described in the same section, because they are closely related.

Fisheye lens images (explained)

If your views include fisheye cameras or lenses, you can navigate fisheye cameras images by clicking either the arrow mouse pointer (the virtual joystick) or the PTZ navigation buttons that appear inside the image (some types of fisheye cameras have their own zoom buttons). The PTZ middle navigation button lets you quickly move the camera to its default position.

Zoom in and out using the **plus** and **minus** buttons. If your mouse has a scroll wheel, you can use scroll to zoom in and out. Click the scroll wheel or middle mouse button to return to the default view.

On individual mice, the scroll wheel may have been reserved for special purposes, in which case zooming may not be possible. Refer to your mouse configuration manual.

You cannot use presets (see Move cameras to PTZ preset positions on page 253) for navigating fisheye lens images but you can save a favorite position.

Define a favorite fisheye lens position

You can only save positions for fisheye cameras.

1. Navigate to the position in the fisheye lens image that you want to save.
2. On the camera toolbar, select **PTZ** to open the PTZ menu.
3. To save the position, select **Save Fisheye Lens Positions**.

4. When you want to return to the fisheye lens position, on the camera toolbar, select **PTZ** > **Load Fisheye Lens Positions**.

PTZ and fisheye lens images (explained)

The use of fisheye cameras is not supported by all surveillance systems and some fisheye cameras are not supported by the 64-bit version of Microsoft Windows.

Depending on your user permissions, access to pan-tilt-zoom (PTZ) controls from some cameras may be restricted. PTZ features may be limited when connecting to selected surveillance systems.

For information about the features available in your XProtect VMS, see Surveillance system differences on page 33.

PTZ images (explained)

If your views (including those in a carousel or a map preview) contain PTZ camera images, you can control the PTZ cameras using the overlay PTZ navigation button.

In **Setup** mode, on the **Properties** pane, you can define the PTZ click mode for the view item. You can choose between click-to-center and virtual joystick. Click-to-center is the default mode when you start using XProtect Smart Client. You can change the default selection in XProtect Smart Client settings (see Settings in XProtect Smart Client on page 37).

Most PTZ cameras support joystick and point-and-click control. You can customize (see Joystick settings on page 46) the joystick control.

You can also control most PTZ cameras simply by pointing and clicking inside the camera images. If you see a set of crosshairs when placing your mouse pointer over the images from a PTZ camera, the camera supports point-and-click control.

Crosshairs indicate point-and-click control. For some cameras, crosshairs may look different.

Some cameras have crosshairs surrounded by a square. When this is the case, you can zoom in on an area by dragging a square around the area in the image you want to magnify. For such cameras, zoom level is controlled by holding down the SHIFT key on your keyboard while moving the mouse up or down; this will display a zoom level slider inside the image.

Move cameras to PTZ preset positions

To make the PTZ camera move to a predefined position, select a PTZ preset from the list of available positions defined for the PTZ camera.

1. On the camera toolbar, select **PTZ**  to open the PTZ menu.
2. Select a PTZ preset in the menu to move the camera to the required position. The icon turns green.

> If you select the preset **Home**, the camera moves to its default position. You define a camera's Home preset position on the camera's homepage. The PTZ capabilities available on the homepage depend on the camera.

Locked PTZ presets (explained)

Depending on your surveillance system (see Surveillance system differences on page 33), you may experience that a PTZ preset is locked.

A system administrator can lock a PTZ preset to protect it from being renamed or deleted or to avoid that someone changes its position. The system administrator decides whether a PTZ preset is locked or unlocked.

Starting, stopping, or pausing PTZ patrolling

With certain XProtect VMS systems, you can manually start and stop a patrolling. You can always pause an ongoing patrolling.

Stop PTZ patrolling

A PTZ camera can continuously move between a number of PTZ presets according to a schedule. You can stop an ongoing system patrolling.

> Only stop system patrolling when there is an important reason to do so. Normally your system administrator has planned the patrolling carefully to meet your organization's surveillance needs.

1. In live mode, select the required view and camera.
2. On the camera toolbar, select **PTZ**  to open the PTZ menu.

   The red color of the icon indicates that the camera is patrolling or that another user is controlling the camera.
3. Select **Stop PTZ patrolling** and you can patrol manually.
4. To resume the system patrolling, select the **Stop PTZ patrolling** command again.

Manual patrolling (explained)

Depending on your surveillance system (see Surveillance system differences on page 33), you can start and stop patrolling manually.

You may want to start a patrolling manually if, for example, the system patrolling does not screen an area of a room properly or there is no system patrolling. If the camera is already patrolling, you need a higher PTZ priority than the patrolling user or rule-based patrolling to be able to start a manual patrolling session.

Patrolling profiles can be created by your system administrator, other users, or yourself (see Patrolling profiles (configuration) on page 79), if you have the necessary user permissions.

Users with a higher PTZ priority than you can take control of the camera while you are running a manual patrolling. When they release the session again, the system resumes your manual patrolling.

With a sufficient PTZ priority, you can stop manual patrolling started by other users by clicking the patrolling profile, by pausing it (see Pause patrolling on page 256) or starting another manual patrolling. You can always stop a manual patrolling that you have started.

Start and stop manual patrolling

You can only start and stop PTZ patrolling manually with certain XProtect VMS systems. See Surveillance system differences on page 33.

Steps:

1. In the view, select the PTZ camera that you would like to start patrolling on.
2. On the camera toolbar, select **PTZ**  to open the PTZ menu.
3. Below the **Manage PTZ presets** entry, you find the list of patrolling profiles configured for this camera.

Example of a PTZ menu

4. Select the patrolling profile you want to start.

   While the patrolling profile is running, there is a check mark  in front of it for all users. The PTZ icon turns green for you and red for all other users, so they can see that someone controls the camera.

5. To stop the manual patrolling, select the profile again.

   The system resumes its regular patrolling or the camera is made available for other users.

6. If the camera is available and you have the sufficient PTZ permissions, you can take control of the camera, by clicking on the video within the view item or moving your joystick. You keep the control until you have not done any movements for 15 seconds.

   > The timeout for manual control is 15 seconds by default, but your system administrator can change it.

7. To control the camera for a longer period, select **Pause patrolling** (see Pause patrolling on page 256) from the PTZ menu.

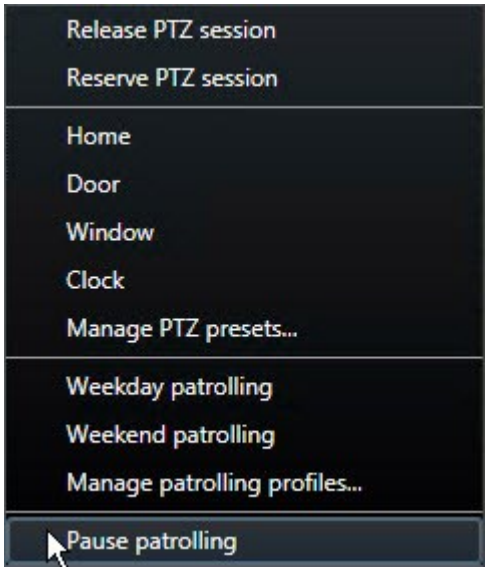
Pause patrolling

Depending on your surveillance system (see Surveillance system differences on page 33), you can pause a patrolling.

If you have the necessary PTZ priority, you can pause a system patrolling or a manual patrolling started by another user. You can always pause your own manual patrolling. This can be useful when you need a longer timeout to control the camera.

1. In the view, select the PTZ camera that you would like to pause patrolling on.
2. On the camera toolbar, select **PTZ**  to open the PTZ menu.

   The red color of the icon indicates that the camera is patrolling or that another user is controlling the camera.
3. Click **Pause patrolling**.



   While patrolling is paused, there is a check mark  in front of the **Pause patrolling** menu item for all users. The PTZ icon turns green for you and red for all other users, so they can see that someone controls the camera.

   If you start a manual patrolling, you lose the pause patrolling session.
4. To stop pausing, select **Pause patrolling** again.

   The system resumes its previous patrolling or the camera is made available for other users.

If a user with a lower PTZ priority than you has started a manual patrolling, for example **Weekday**, you can pause it and take control of the camera:

1. Click **Pause patrolling**.

   While you have paused another user's manual patrolling, there is a check mark ✓ in front of the **Pause patrolling** menu item and the patrolling profile for all users. The PTZ icon turns green for you and red for the other users, so they can see that someone controls the camera.

2. To stop pausing, select **Pause patrolling** again.

   The system resumes to the manual patrolling, in this example **Weekday**.

   Patrolling is paused for 10 minutes by default, but your system administrator may have changed this.

Reserved PTZ sessions (explained)

Depending on your surveillance system (see Surveillance system differences on page 33), you can reserve PTZ sessions.

Administrators with security permissions to run a reserved PTZ session can run the PTZ camera in this mode. This prevents other users from taking control over the camera. In a reserved PTZ session, the standard PTZ priority system is disregarded to avoid that users with a higher PTZ priority interrupt the session.

You can operate the camera in a reserved PTZ session both from XProtect Smart Client and the Management Client.

To reserve a PTZ session can be useful, if you need to make urgent updates or maintenance to a PTZ camera or its presets without being interrupted by other users.

You cannot start a reserved PTZ session, if a user with a higher priority than yours controls the camera, or if another user has already reserved the camera.

Reserve PTZ sessions

1. In live mode, select the required view item.
2. On the camera toolbar, select **PTZ** to open the PTZ menu.
3. Select **Reserve PTZ session**. If you have started a manual patrolling it automatically stops.
   The PTZ camera is now reserved to you, and the timer shows the remaining time of the session.

> Remember to release the session when done, as the PTZ camera will remain reserved until the current session times out.

Release PTZ sessions

When you are done controlling a PTZ camera, you can manually release the PTZ session, so other users with lower priority can take control over the camera or the system can resume its regular patrolling. Otherwise, the camera will not be available until the session times out.

1. Select the PTZ camera that you are controlling.
2. On the camera toolbar, select **PTZ** to open the PTZ menu.

   The green color of the icon indicates that you currently controls the PTZ session.
3. In the menu, select **Release PTZ session**.

   The PTZ session is released and available for other users or system patrolling, indicated by the PTZ icon turning gray .

Virtual joystick and PTZ overlay buttons (explained)

If your views include fisheye cameras or lenses, or PTZ devices (see PTZ and fisheye lens images (explained) on page 252), you can navigate the images by clicking either the arrow mouse pointer (the virtual joystick) or the PTZ navigation buttons that appear inside the image.

The virtual joystick

PTZ overlay

If you don't want the camera toolbar to pop up when you move your mouse over the view, press and hold the **CTRL** key while moving the mouse.

Audio (usage)

Audio (explained)

Support for specific audio features may vary from system to system (see Surveillance system differences on page 33). Access to recorded audio, or certain recorded audio features, may be restricted depending on your user permissions. Ask your system administrator if in doubt.

XProtect Smart Client supports both incoming and outgoing audio. You can listen to live recordings from microphones attached to cameras and use loudspeakers connected to cameras to talk to audiences. When you play back recorded video, you can hear the corresponding audio if the cameras have microphones, speakers, or both, attached. When you select a camera or view, the corresponding microphone or speaker is also selected by default.

The XProtect VMS system can record incoming audio from microphones attached to cameras, even if no video is being recorded.

If your views contain maps, these maps may contain microphones, speakers, or both. You can listen to audio by clicking the relevant microphone or speaker element. Click and hold down the mouse button for as long you want to listen or talk.

Talk to an audience

Talking to audiences through speakers attached to cameras is possible by using:

- The **Audio** pane on the left-hand side
- Overlay buttons
- Speaker functionality on maps

Outgoing audio transmitted through speakers attached to cameras may be recorded, but only on certain XProtect systems. See also Surveillance system differences on page 33.

Smart map (usage)

Smart map (explained)

> This feature is only available in certain XProtect VMS systems. For more information, see the product comparison chart: https://www.milestonesys.com/solutions/platform/product-index/

Smart map lets you view and access devices at multiple locations around the world in a geographically correct way. Unlike maps, where you had a different map for each location, smart map gives you the big picture in a single view.

You can zoom out to see all of your locations in multiple cities, regions, countries and continents, and quickly go to each location to view video from the cameras.

Example

You can preview footage from cameras at your sales office in Rome, then zoom out, pan across the world with a single drag, and then zoom in to the cameras in your office in Los Angeles.

One key benefit of a smart map is the spatial reference data behind-the-scenes. For more information, see Geographic backgrounds (explained) on page 85.

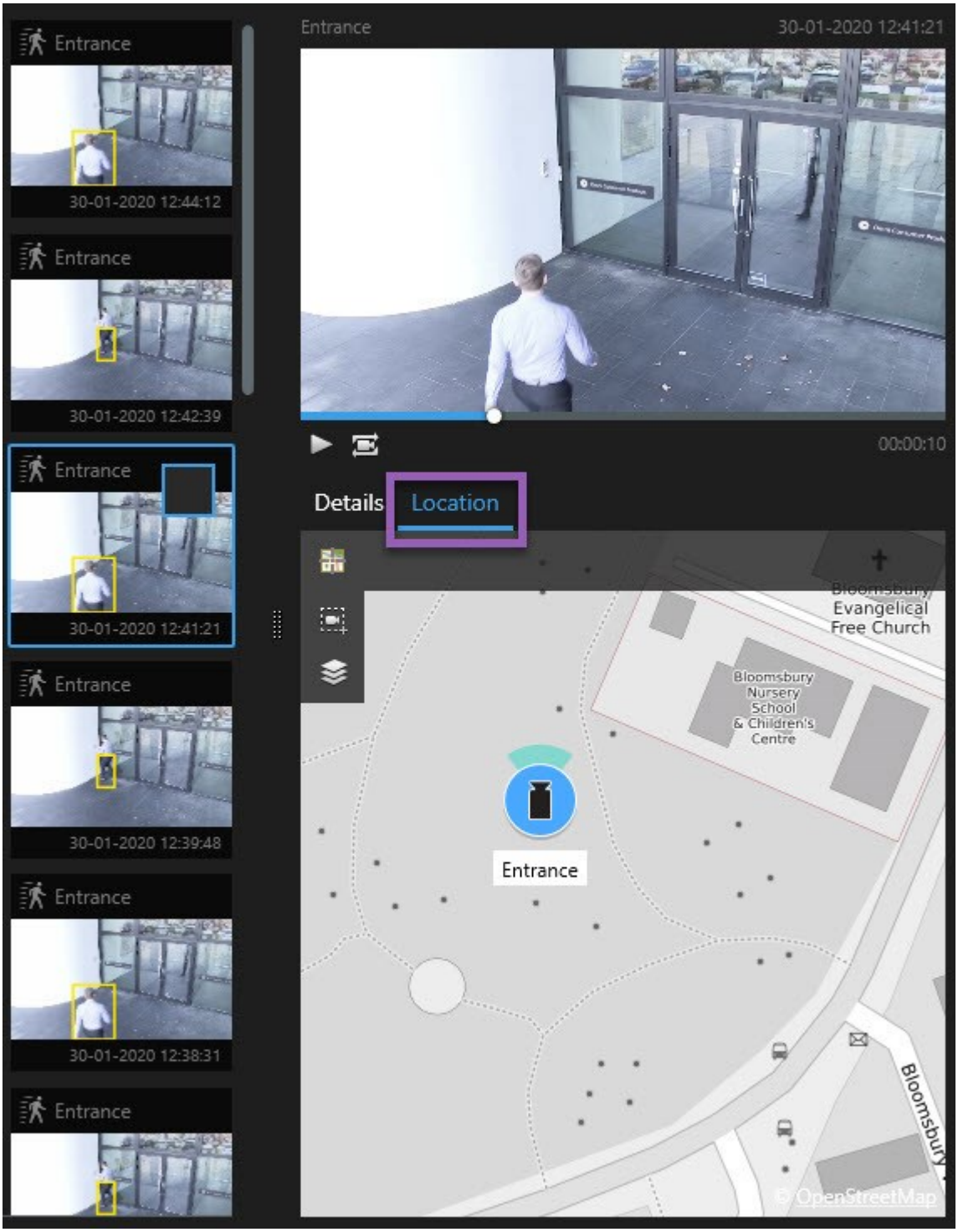
Smart map and alarms (explained)

Smart map displays alarms if they are triggered by a device and if the device is added to the smart map. See also Adding, deleting, or editing devices on smart map on page 95.

Depending on your user permissions, you may be able to see alarms on smart maps.

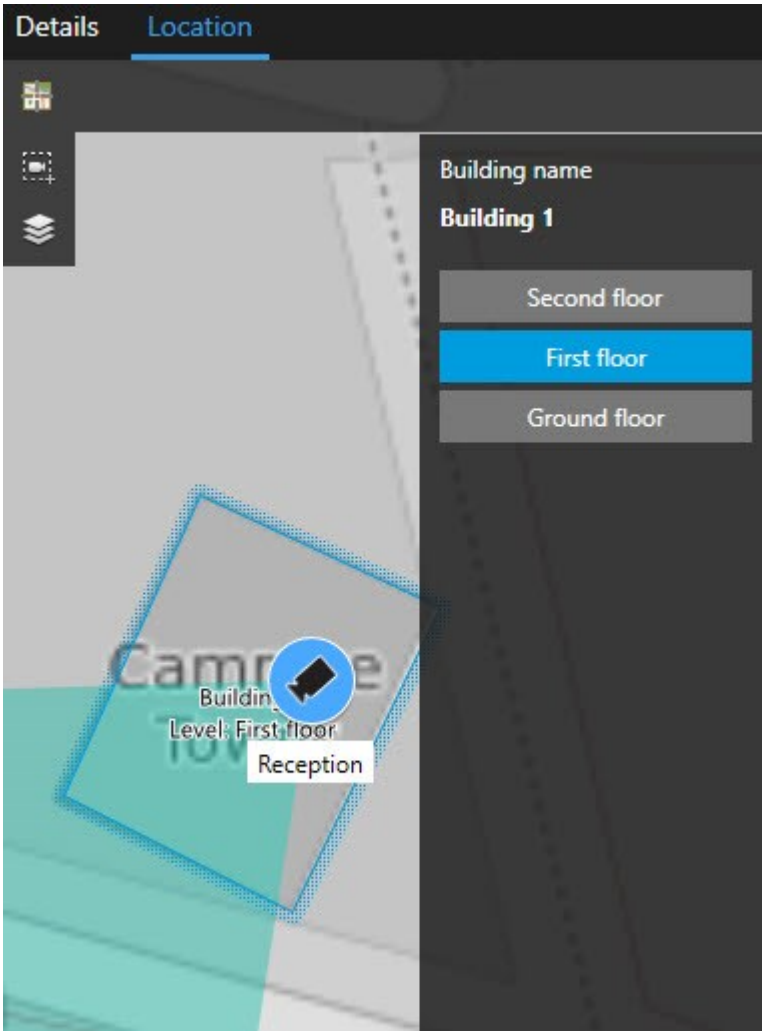
Smart map and search (explained)

While searching for video and related data on the **Search** tab, you can locate the devices geographically in the preview area:



When you select a search result, the smart map zooms in on the associated device in its geographic location. You may need to zoom out to get a better overview of the surroundings.

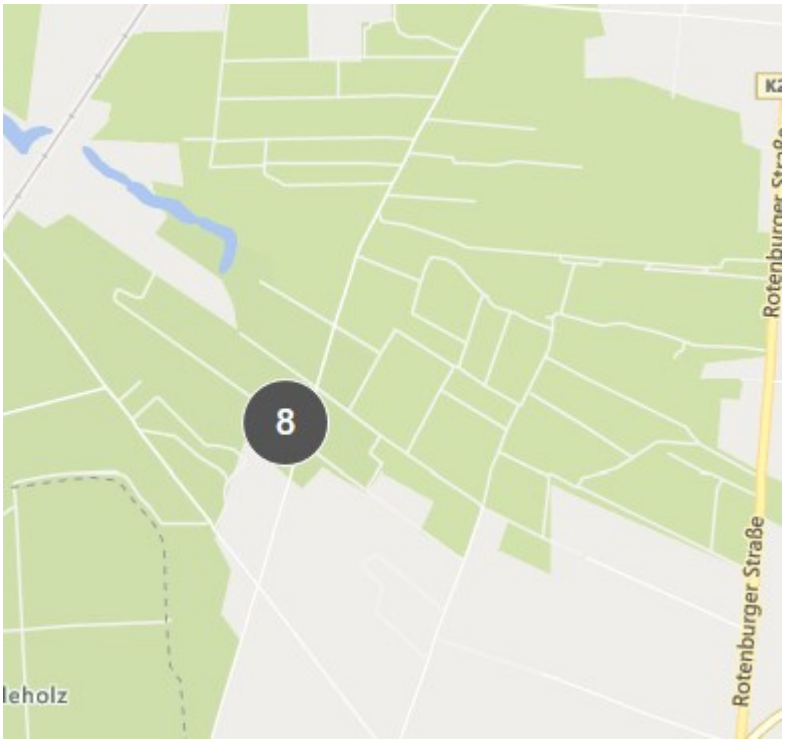
If the device is placed somewhere inside a multistory building, an indication of the level of the device appears:



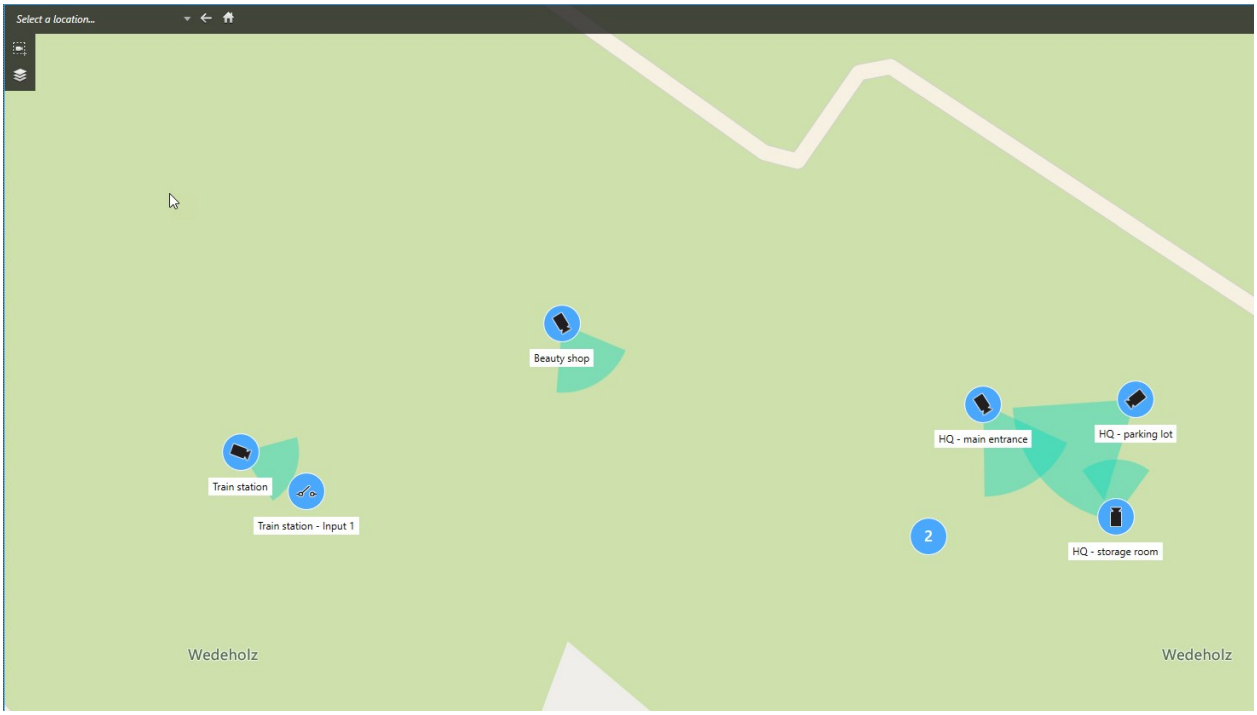
If a device is visible on multiple levels, only the first level specified is displayed, from the bottom and up.

Grouping of devices (explained)

When cameras and other types of devices are placed close to each other and you zoom out, the devices are grouped and displayed visually as circular icons.



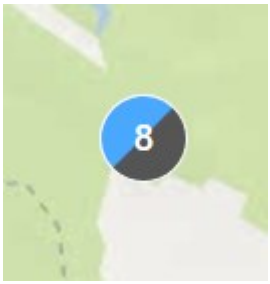
The cluster shows the number of devices inside the cluster. As you zoom in again, for example by double-clicking the cluster, it turns into devices and possibly sub-clusters.



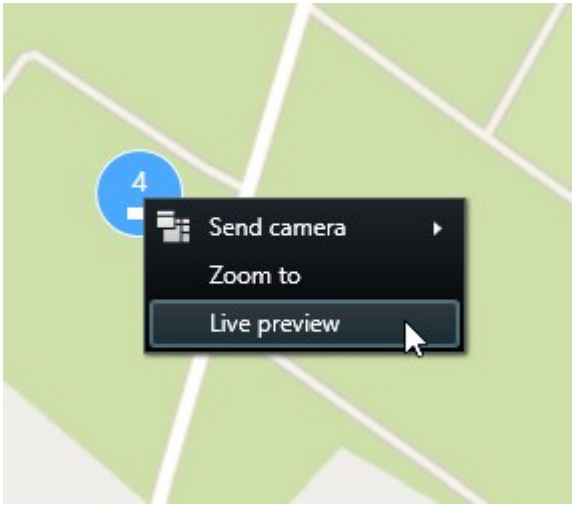
Clusters turn blue when you select them.

If a cluster contains different types of devices, for example cameras and microphones, then the cluster only shows the number of devices. However, if a cluster contains only one type of device, then the cluster shows both the type of device and the number of devices. This scenario is illustrated in the following image:

If you see a cluster that looks this way, only some of the devices inside the cluster are selected:



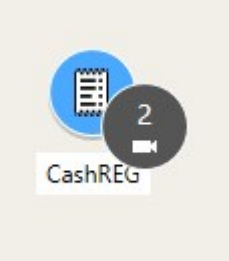
You have different options when you right-click a cluster - or one or more selected devices - for example **Live preview**:



The options differ depending on the situation. For example, you can only remove devices in setup mode.

MIP elements do not cluster with any type of device. They only cluster with MIP elements of the same type.

Example 1: If an area has two cameras and one MIP element, the cluster will look as follows:

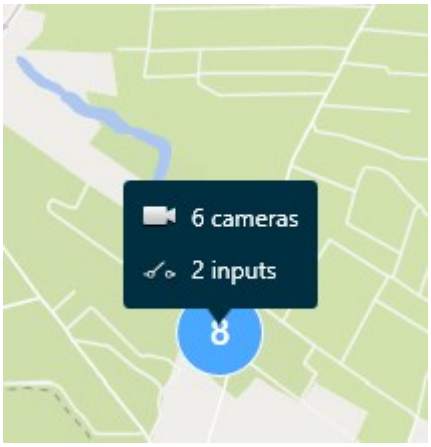


Example 2: If an area has two MIP elements of different types, there will be no cluster.

In addition, MIP elements have their own layer that you can turn on or off by clicking **Show or hide layers and custom overlays** in the smart map toolbar.

Get overview of grouped devices

Clusters can contain different types of devices, for example cameras and input devices. To get an overview of the devices in a cluster, click the cluster once.



Zoom in and out

There are different ways of zooming in or out:

- Use the scroll wheel on your mouse
- If there is a cluster, double-click it, or right-click and select **Zoom to**. The map zooms to a level where all the devices or sub-clusters within the cluster are visible

- Press and hold the **SHIFT** key and drag the pointer to select an area on the map. The map zooms in and centers on your selection

There may be a limit to how much you can zoom in on a map if you're using one of the following services:

- Bing Maps
- Google Maps
- Milestone Map Service
- OpenStreetMap

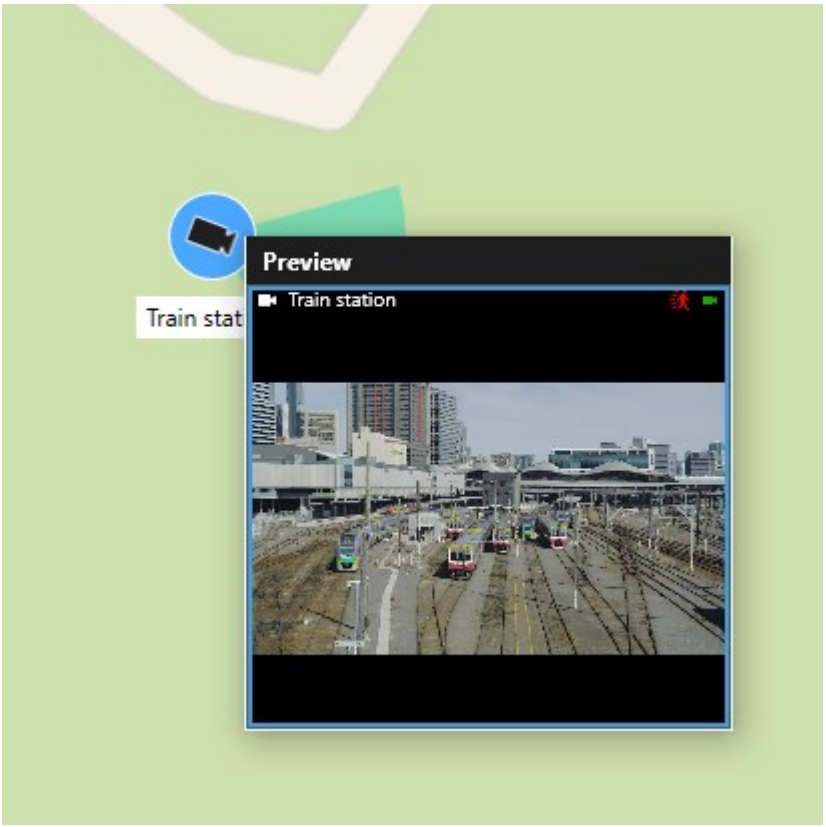
The zoom limitation depends on if the services are able to provide an image at the requested zoom depth. When such a zoom limit occurs, the view item stops displaying the geographic background. Other layers, such as devices or shapefile images continue to display.

Preview live video from one camera

You can preview video from single cameras. The video is displayed in a preview window, which allows you to further investigate the video, for example in a new floating window.

Steps:

1. Navigate to the camera.
2. Double-click the camera, or right-click and select **Live preview**. The live video feed is displayed in the **Preview** window.



3. To play back and investigate the video in more detail, do one of the following actions:
   - In the **Preview** window, click **Independent playback**. The controls of independent playback become available
   - Click **More** > **Send to window** > **New floating window**. A window appears.

Preview live video from multiple cameras

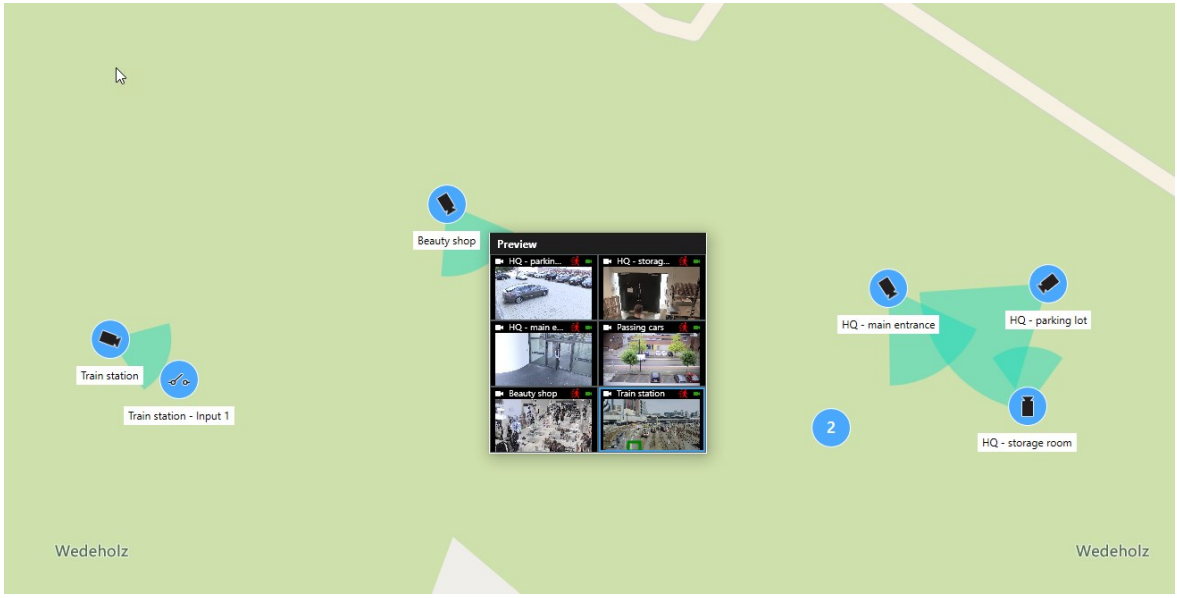
You can preview live video from multiple cameras at the same time - a maximum of 25 live videos can be shown at the same time. The video is displayed in a preview window, allowing you to further investigate the video, for example, in a new floating window.

Steps:

1. Navigate to the place on the smart map, where the cameras are located.
2. Select the cameras using one of these methods:
   - Press and hold the **CTRL** key while you select the cameras.
   - In the toolbar, click **Select multiple cameras**, then click and drag to select the cameras within an area.

     Only cameras are included in the selection.

   - Double-click a cluster to zoom to and select the devices and potential sub-clusters inside the cluster
3. Right-click any of the selected cameras or sub-clusters and select **Live preview**, or press **Enter**.



4. To play back and investigate the video in more detail, do one of the following actions:
   - In the **Preview** window, click **Independent playback**. The controls of independent playback become available
   - Click **More** > **Send to window** > **New floating window**. A window appears.

Use hotspot to view video from cameras on smart map

Instead of previewing video feed from your cameras, or sending the video feed to a secondary display, you can use a hotspot to quickly shift between cameras on your smart map.

Requirements

You have already set up a view with a hotspot. For more information, see Add hotspots to views on page 77.

Steps:

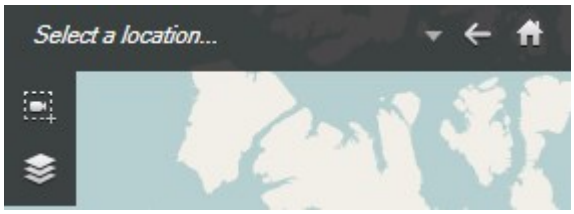
1. Open the view that contains the smart map.
2. If the view also contains the hotspot:
    1. Navigate to the cameras on the smart map.
    2. Click the cameras you are interested in. As you click, the video feed is displayed in the hotspot view item.
3. If the view does not contain the hotspot:
    1. In the **Views** pane, right-click the view that contains the hotspot.
    2. Select **Send view to** and select a display option, for example **Floating window**.
    3. Arrange the views on your monitor or monitors so that you can see both.
    4. Navigate to the cameras on the smart map.
    5. Click the cameras you are interested in. As you click, the video feed is displayed in the hotspot view item.

Go to smart map locations

You can quickly jump to locations added by yourself or others in XProtect Smart Client instead of panning manually to the location on the smart map. The list of locations displays the last location you selected.

Steps:

1. Select the view that contains the smart map.
2. In the upper left corner of the view, open the **Select a location** list.



3. Select the location to go to that location on the smart map.

Jump to device on smart map

If you want to view a device in its geographic context, you can jump to the place on the smart map where the device is. This is useful if, for example, you forgot the location of a device, or if you want to check nearby devices.

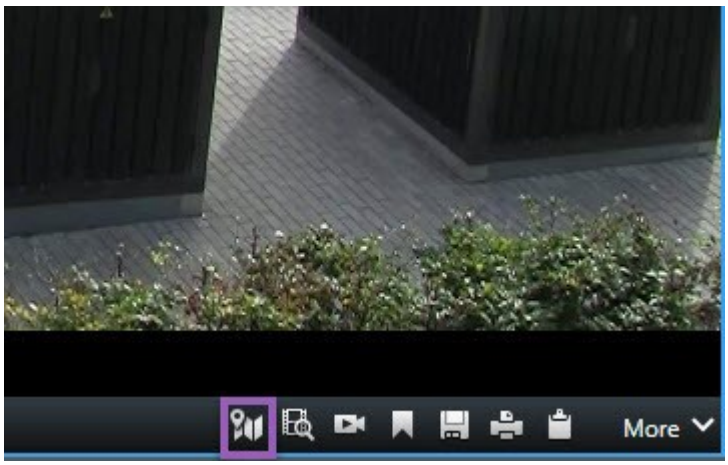
Requirements

You can jump to a device only if the device has been geographically positioned in one of two ways:

- The geo coordinates of the device have been specified in the device properties in XProtect Management Client
- The device has been positioned on the smart map in XProtect Smart Client

Steps:

1. To search for a device and then jump to it:
    1. In live or playback mode, go to the **Views** pane.
    2. Search for the device. If the device exists, it appears in the search results.
    3. Hover over the device that you want to jump to.
    4. Click to jump to the device. The smart map opens in a floating window.
2. To jump to a camera from a view item:
    1. In live or playback mode, select the view item that contains the camera.
    2. Inside the view item, at the bottom, hover over the black bar to make the camera toolbar appear.



    3. Click to jump to the camera. The smart map opens in a floating window.

Jump to custom overlays on smart map

If you need to quickly navigate to a custom overlay on the smart map, you can jump to the location where the overlay is.

1. On the smart map, click **Show or hide layers and custom overlays**. A window appears.
2. Go to the **Custom overlays** section.
3. Click next to the overlay you want to find. This will take you to the location on the smart map.

Backtracking to previous locations (explained)

When you go from one location to another, XProtect Smart Client keeps a history of the locations you visit. This lets you backtrack by clicking **Back**. The history is based on the locations that you click. That is, if you pan to a location, but do not click it, the location is not added to the history.

When you backtrack, XProtect Smart Client removes the location you just left from the history. The history includes only forward movements.

The system clears the history when you leave the view.

Maps (usage)

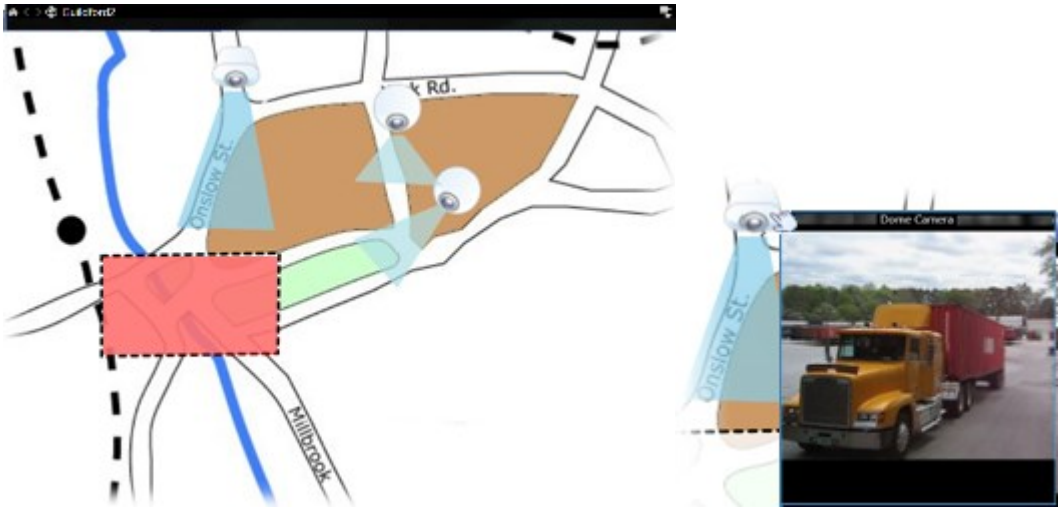
> If you are connected to a surveillance system that supports Milestone Federated Architecture, you can only add maps from the surveillance system server you logged in to.

Maps (explained)

With a map, you get a physical overview of your surveillance system. You can instantly see which cameras are placed where, and in what direction they are pointing. You can use maps for navigation. Maps can be grouped into hierarchies, so you can drill down through hot zones, from large perspectives to detailed perspectives, for example, from city level to street level, or from building level to room level.

A map position does not display live video, a map is always a still image.

Maps may contain elements representing cameras, microphones, and similar technology. You can view recorded video from cameras in a preview window when you move your mouse over a camera icon on the map. The status information in playback mode is **not** based on recorded data, but retrieved from the elements' current status, as displayed in live mode.



Map with camera elements and hot zone

Maps do not have to be geographical maps, although they often are. Depending on your organization's needs, photos and other kinds of image files can also be used as maps.

Maps are not the same as a smart map. For more information, see Differences between maps and smart maps (explained) on page 83.

How elements interact with maps

You can use map elements to interact with the actual devices in the following ways:

Cameras

Place your mouse pointer over a camera on a map to see a live preview from the camera. Click the title bar of the preview to display it as a separate floating window. You can resize the floating window by pulling its corners. To start recording, right-click the required camera and select **Start recording for # minutes**. Particular user permissions may be required to use this feature.

A **fixed camera** is displayed on the map with an associated view zone that shows the camera's angle of view. Note that the angle on the map is very likely to need adjustment to match the camera's angle of view. To adjust the angle, simply drag it to a suitable size and position.

A **PTZ camera** is displayed on the map with any PTZ presets defined for the camera on the surveillance system. The presets are illustrated as colored angles that radiate from the PTZ camera icon. Each angle represents a particular preset. Note that the angles are very likely to need adjustment to match the camera's preset angles. To adjust an angle, simply drag it to a suitable size and position. If a camera has more than 25 presets, no angles are initially displayed since the angles would be too small to be useful. In such cases, you can add required angles individually by dragging the presets from the required camera from the **Element selector** window onto the map. To go to one of a PTZ camera's presets, simply click the preset on the map. This works in the floating preview window, on the map itself, as well as in hotspot positions (see Hotspots (explained) on page 159). Alternatively, right-click the camera, select **PTZ presets**, then select the required preset.

Microphones

Place your mouse over a microphone; press and hold the left mouse button to listen to incoming audio from a microphone, or right-click the microphone and select **Listen to microphone**. You cannot use microphones in map views in playback mode.

Speakers

Place your mouse over a speaker; press and hold the left mouse button to talk through the speaker. You cannot use speakers in map views in playback mode.

Events

Click an event on the map (see Alarms (explained) on page 237) to activate it, or right-click the event and select **Activate event**. When left-clicking an event, the mouse pointer briefly changes to a lightning symbol to indicate that the event is being activated.

Alarms

Click an alarm on the map (see Alarms (explained) on page 237) to view it, or right-click the alarm and select **Activate Alarm**. Right-click to acknowledge the alarm.

Output

Click an output on the map to activate it, or right-click the output and select **Activate output**. When you click an output, the mouse pointer briefly changes to a lightning symbol to indicate that the output is being activated.

Hot zones

A hot zone is usually colored, so it is easy to recognize. Click a hot zone to go to the sub-map associated with the hot zone, or right-click the required hot zone and select **Go to sub-map**.

If the hot zone appears with a dotted outline, no map is associated with the hot zone.

On some surveillance systems, maps from several different servers may be in a map hierarchy. This can mean that when you click a hot zone, the sub-map is unavailable because its server is unavailable. Servers can become unavailable because of scheduled maintenance or network problems. Contact your system administrator if the problem persists.

A hot zone can point to a map that you do not have access permissions to and the XProtect Smart Client will inform you about this. Because user permissions can be time-based, you might not be able to access a map that you could previously. This can be because you do not have access during certain hours of the day or certain days of the week. Contact your system administrator if in doubt about your user permissions.

Plug-ins

Plug-in elements are available only if used on your surveillance system. Examples of plug-in elements: access control systems, fire detection systems, etc.

Interconnected hardware

Because interconnected hardware that is part of a Milestone Interconnect system is offline at times, you may often see error statuses on the interconnected hardware element on a map.

Status visualization

Status visualization is a feature that graphically displays the status of elements added to a map. When a map is fully operational and in the normal state, no visual status indication is presented. The **Status visualization** window lets you define the visual appearance of maps' status indication.

Indicator	Description
	**Attention needed** - when an element requires attention, but is still working; for instance when a server is running out of disk space. Note that the device in question is not necessarily included on the map. The default display color is yellow.
	**Not operational** - when there is an error on the element, for example if a server cannot connect to a microphone or speaker. The default display color is orange.
	**Alarms** - when an element has an alarm attached to it. The default display color is red.
	**Disabled/status unknown** - when an element has been disabled on the surveillance server, or when it is not possible to obtain status information from a server. The default color is purple.
	**Ignore status** - when an element has a status that does not need attention, for example, if you are already aware of what the issue is. The default color is blue.

The status of a map mirrors the status of all elements on the map. Up to four names of affected servers can be listed in the map title bar. In cases where an unavailable server causes disabled elements on the map, but the server itself is not included on the map, the map is displayed in the **not operational** state, even though the map only contains **disabled** elements. If the unavailable server **is** included on the map, the map is simply displayed with the **disabled/status unknown**. Status information is also available in the **Map overview**.

Example of map with status visualization
Change the appearance of status visualization

Map overview window (explained)

The **Map overview** window provides you with an overview of the map hierarchy set up in the XProtect Smart Client. To open the **Map overview** window, right-click the map and select **Map overview** or click the icon on the map title bar.

A plus sign (+) next to a map indicates that the map could have one or more sub-maps attached to it as hot zones. Clicking a map in the **Map overview** immediately displays the selected map in the view.

Content in the **Map overview** may take some time to load if you are connected to a very large surveillance system with many maps.

If you are connected to a surveillance system that supports Milestone Federated Architecture, you can only add maps from the surveillance system server you logged in to. Milestone Federated Architecture is a system setup with related but physically separate surveillance systems. Such a setup can be relevant for, for example, chains of shops with many separate—but related—surveillance systems.

See the XProtect Comparison Chart on https://www.milestonesys.com/ for information about which surveillance systems support Milestone Federated Architecture.

Send cameras from a map to a floating window

To view all the cameras (a maximum of 25 in one view) on a map simultaneously in a floating window:

1. In live or playback mode, select the map that contains the cameras you want to view in a floating window.
2. At the top of the map title bar, click the **Send all cameras to floating window** icon:  .

The floating window displays a maximum of 25 cameras in the view.

If you have more than 25 cameras on a map, when you click this button, it will not always be the same cameras you see.

View recorded video from cameras on a map

You can view recorded video from cameras in a preview window when you move your mouse over a camera icon on the map. The status information in playback mode is retrieved from the camera's current live status.

- You can use digital zoom and PTZ controls from the camera preview if the camera supports this. In the preview window, either click the More button and select digital zoom or use the PTZ (see PTZ images (explained) on page 252) controls that appear. If you have PTZ presets set up for a particular camera, you can activate the preset by selecting the preset in the preview
- To view all the cameras (a maximum of 25 in one view) on a map simultaneously in a floating window, click the **Send all cameras to floating window** icon at the top of the map title bar: 

If you have more than 25 cameras on a map, when you click this button it will not always be the same cameras you see.

View status details

Status details are available for cameras (for example, resolution, image size, and bit-rate) and servers (for example, CPU usage, memory, network usage).

- To display status details, right-click the required element and select **Status details**. Status details are displayed in a separate, floating window

If you see an error message saying that the event server has insufficient access permissions to the recording servers, you will not be able to view status details from recording servers. The error message relates to the Event Server service, which handles map-related communication on the surveillance system. The Event Server service is managed on the surveillance system server. Contact your system administrator, who will be able to handle the issue.

Zoom and auto maximize

If the map is larger than the view area in the XProtect Smart Client, or if you have zoomed in on the map, you can pan the map to see otherwise hidden areas. Click the map anywhere outside of added elements, and the map centers on the clicked spot. Pan the map by clicking and dragging the map in any direction.

- To use the zoom function on a map, right-click the map and select **Zoom in** or **Zoom out** as required. Or use the **Zoom to standard size** function to zoom back to normal size

Alternatively, use your mouse's scroll wheel to zoom; scroll up to zoom in, scroll down to zoom out.

If **Auto maximize map** is enabled and your map position in the view is part of a view with several view positions, the map is automatically maximized to full screen after a period of time as defined in setup mode in the **Properties** pane. To revert to the original view, double-click the map anywhere outside of any added elements.

Matrix (usage)

This feature is only available in certain XProtect VMS systems. For more information, see the product comparison chart: https://www.milestonesys.com/solutions/platform/product-index/

Matrix (explained)

Matrix is a feature that lets you send or receive video from any surveillance system camera to any monitor (known as a Matrix-recipient) on a network. A typical Matrix configuration automatically presents live video on the required Matrix-recipient when a defined event occurs, for example, when motion is detected or when another user wants to share important live video. Provided Matrix has been configured on the surveillance system server, you can include Matrix content in your XProtect Smart Client views. When a particular event occurs, or another user wants to share video with you, live video will automatically appear in your Matrix views.

Viewing Matrix content (explained)

The event or the camera used in the Matrix setup depends entirely on the Matrix configuration on the surveillance system server or on what other users want to share with you. You cannot control this in XProtect Smart Client. However, you can add Matrix content to as many view items in the view as required, so you can watch live video from several Matrix-triggered sources at the same time.

A view item with Matrix content has a Matrix icon on the toolbar:  . You can maximize a Matrix view item by double-clicking it.

A view can contain several view items with Matrix contents. This lets you watch live video from several Matrix-triggered sources at the same time. If your view contains several view items with Matrix content, the view items are always ranked—one of the view items will be the primary view item with Matrix content, another the secondary, and so on. When the first Matrix-triggered live video stream is received, it is automatically presented in the primary view item with Matrix content. When the next Matrix-triggered video stream is received, a first-in-first-out principle applies: the previously received video stream is transferred to your view's secondary view item with Matrix content, and the newest video stream is presented in your primary view item with Matrix content, and so on. The ranking of the view item with Matrix content is applied automatically: the first view item you add Matrix content to is the primary Matrix view item, the next one you add is the secondary one, and so on. You can change this ranking in setup mode.

In playback mode, view items with Matrix content display video from the cameras with which the Matrix view items were last used in live mode.

Manually send video to Matrix recipients

You cannot send video to a hotspot (see Hotspots (explained) on page 159) or carousel (see Carousels (explained) on page 159).

Requirements

Matrix content has been added to a view. See Add Matrix to views on page 118.

1. Select the view.
2. On the camera toolbar, click **More** > **Matrix**, and then select the relevant Matrix recipient.

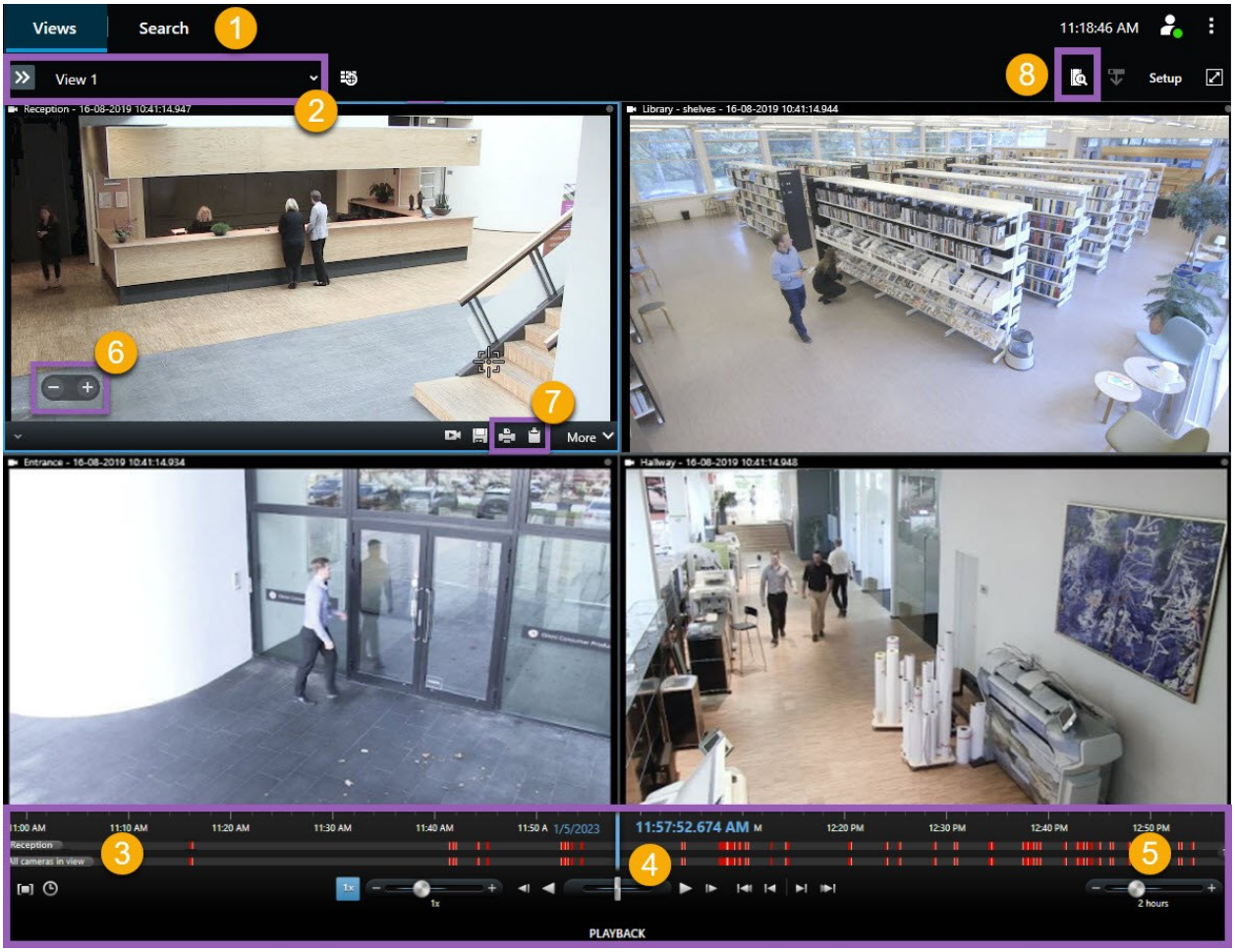
XProtect Smart Client – Player (usage)

XProtect Smart Client – Player is a light version of XProtect Smart Client that can be included with exported video data. XProtect Smart Client – Player lets the recipient view the exported files without having surveillance software installed.

XProtect Smart Client – Player is also automatically included in video archives and recording database folders to ensure availability of recordings if the disk with the recordings is removed.

You can use XProtect Smart Client – Player to view video data and archives and to repair corrupted databases. The application has many of the features of the XProtect Smart Client and looks similar.

XProtect Smart Client – Player (overview)



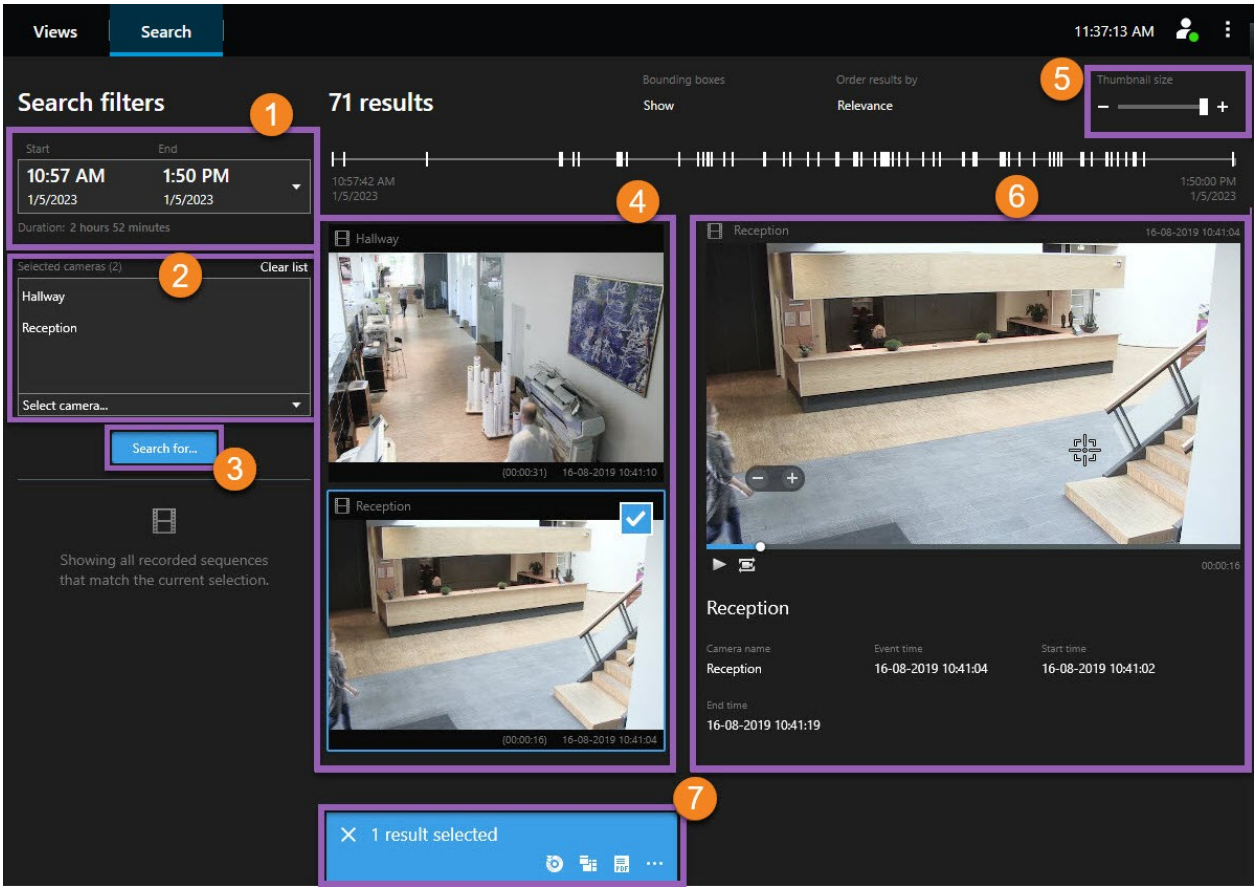
Number	Description
1	Investigate the exported recordings in playback mode, and run searches on the **Search** tab.
2	Select the view that contains the cameras that you are interested in.
3	Drag the timeline back and forth to browse the recorded video. See Timeline (explained) on

Number	Description
	page 174.
4	Use the time navigation controls to play back video or jump to a specific moment in time. See Time navigation controls (overview) on page 175.
5	Change the time span. The range is five minutes to four weeks.
6	Zoom in or out.
7	Copy a still image to the clipboard, so you can paste it into, for example, a document, or print a surveillance report with a still image and related information.
8	Start search in a new search window with the cameras in the current view preselected.

Search in XProtect Smart Client – Player

On the **Search** tab, you can search the recordings included in the export, for example if you want to search a subset of the cameras.

You can search for recordings, motion, and bookmarks.



Number	Description
1	The time span is set automatically based on the export time span. You can define your own time span, for example **Custom interval**.
2	Add the cameras that you want to search.
3	Specify what to search for, for example **Motion**. You can combine search categories.
4	Review the list of search results. Scroll to view the next or previous search results.
5	Use the **Thumbnail size** slider to make the thumbnail images smaller or bigger.
6	Play back video from the search results.
7	Take further action based on your search results, for example create PDF reports to share or print evidence. The action bar appears when you select the blue check box inside the search results.

For more information about the features on the **Search** tab, see Search for video on page 202.

Verify digital signatures

If you are reviewing video evidence in XProtect Smart Client – Player, and the exported material has digital signatures, you can verify that the recording has not been tampered with since it was recorded, or since the export was made, or both.

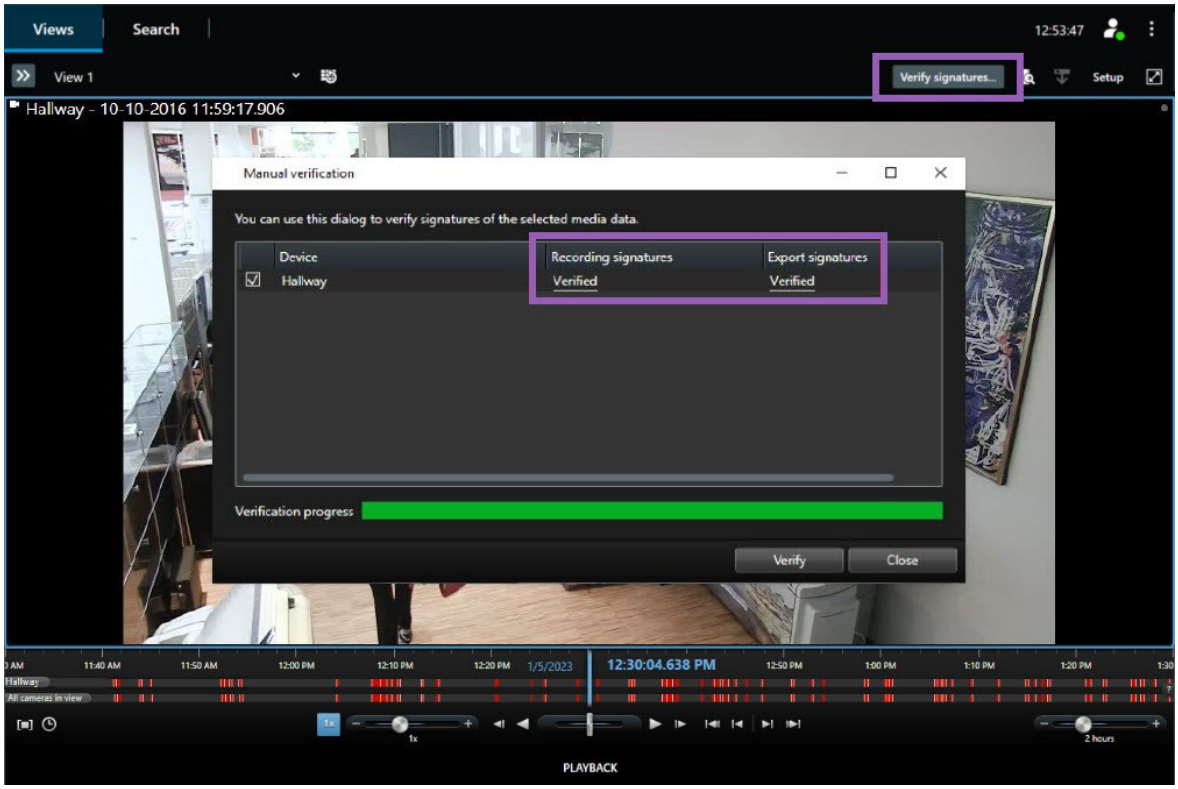
Digital signing does not work for XProtect Smart Client 2017 R1 or earlier that connects to XProtect VMS 2017 R2 or newer. The video export will not succeed.

Requirements

- In XProtect Management Client, signing has been turned on for the recording server
- In XProtect Smart Client, during the export process, the **Export as XProtect format** and the **Include digital signature** check boxes were selected

Steps:

1. On the toolbar, click the **Verify signatures** button. The **Manual verification** window appears. Here you can see the devices selected for the export.
2. Click **Verify** to start the verification process. The system checks the authenticity of the recording signature and the export signature.



3. To verify that you can rely on the verification of the recording signature:
    1. In the **Recording signatures** column, click the **Verified** link. The **Certificates** dialog appears.
    2. Compare the value of the **public_key** and **signature** with the corresponding values in the **PublicKey.xml** file (**C:\Program Files\Milestone\Management Server\Tools\CertificateIssuer**). If the values differ, the recording has been modified.
4. To verify that you can rely on the verification of the export signature:
    1. In the **Export signatures** column, click the **Verified** link. The **Certificates** dialog appears.
    2. Compare the value of the **public_key** and **signature** with the corresponding values in the **Public Key Certificate.xml** file (**<export destination folder>\<export name>\Client Files\Data\Mediadata\<camera name>\<camera name>\Export signatures**). If the values differ, the export material has been modified.

A database can be verified, partially verified (if some of the files have not had signatures attached), or not signed.

View database or previously exported evidence

The **Open database** wizard lets you open a database from an archive or previously exported material and add it to your project. The **Open database** wizard also repairs corrupted databases automatically.

Steps:

1. Click the **Setup** button in the upper-right corner. The panes on the left-hand side turn orange.
2. Expand the **Overview** pane.
3. Click  . The **Open database** wizard appears.

   > Do not attempt to open a live database or live archive because it can damage your system.

4. Select the folder containing the relevant files. When you select a database, the name of the device appears next to the **Camera**, **Microphone**, or **Speaker** field.

   > If the system cannot identify a camera, for example, if you open archived recordings, the name will be **Unknown** and all three types of devices will be added as **Unknown** devices (even if they don't exist) with the database file name assigned. If there is no device, the field contains **N/A**.

5. If the database you are trying to open is corrupted, the wizard can repair it.
6. After adding the database, you can see whether or not the database contains digital signatures. Then you can verify the authenticity of the recordings. See Digital signatures (explained) on page 121.

Edge storage and Milestone Interconnect

There are two types of cameras with edge storage:

- Cameras with memory cards on which the recordings are saved.
- Interconnected cameras that are part of another XProtect VMS installation and that you have access to through Milestone Interconnect™.

When you have the necessary user permissions, you can manually retrieve recordings from cameras with edge storage. Retrieval of recordings can also happen automatically through rules defined by your XProtect VMS administrator. See also the Milestone Interconnect setups section in the administrator manual for XProtect VMS.

The timeline and edge retrieval

If you select a camera with edge storage, the checkerboard pattern in the timeline indicates whether the recordings have been retrieved to your local recording server:

- A dark checkerboard pattern indicates that the recordings have not yet been retrieved. Before a retrieval attempt, you can't see whether recordings actually exist.
- A light checkerboard pattern indicates that retrieval is in process.

When the recordings are retrieved, the timeline uses the same colors as for all your recordings: Red for recordings and dark gray for no recordings.

Retrieve recordings manually

You can manually retrieve recordings to store them on your recording servers. Usually, you do this when an incident has occurred that you want to investigate and/or when you need to store the recordings for a longer time.

1. Select a camera with edge storage.
2. In the timeline, select **Time selection mode** to select the start and end time of the relevant recordings.
3. In the workspace toolbar in the top-right corner, select **Retrieve data**.
4. Optionally, select more cameras that you want to retrieve recordings from.
5. Select **Start retrieval**.

   In the notification area at the top, you can view the progress or stop the retrieval job.

View all edge retrieval jobs

If you want to see all ongoing and recent retrieval jobs started by rules, yourself, or other operators, in the top-right corner, in the **Settings and more** menu, select **Server jobs**. You can see the status of the retrieval jobs and stop ongoing jobs if needed.

XProtect Access (usage)

If one or more access control systems have been integrated with your VMS system through the XProtect Access add-on, you can monitor doors, control door states, investigate access control events, respond to access requests, and manage cardholder information.

Access control in live mode (explained)

In live mode, you can view live video from the cameras associated with access control sources, together with the list of events on the right-hand side of the video.

When you click any of the events in the list, the live video automatically pauses and changes to independent playback of the event. To go back to viewing live video, either click the event again or click the **Independent playback** icon on the camera toolbar (see View recorded video independently of timeline on page 177).

If the system and the event hold cardholder information, you can click the search icon next to the cardholder name on a selected event to jump to the **Access control** tab and view all events associated with this person.

Monitor doors via maps

If you use the map functionality to support your surveillance and access control tasks, you can add access control units to a map:

1. In setup mode, expand the **System overview** pane.
2. Select **Map** from the list and drag it to a view item.
3. Locate the map file and click **OK**.
4. From the map toolbox that appears, click **Add access control**.
5. In the list that appears, drag the relevant access control unit, for example a door, onto the map. A door icon appears on the map.
6. Click **Setup** to change to live viewing.
7. When a person requests access, the door unlocks. The door unlocks because someone grants access via a command button on the access request notification or even on the map itself. Once the access is granted, the door icon turns green and appear as an open door.
8. When the door is locked again, automatically or manually, the door icon turns red and appear as a closed door.
9. You can right-click the door icon to, for example, trigger commands.

   Since the state of the access control units are always visible, a map used in this way is a quick way to get a graphical overview of the states of the access control units for the area or building you are monitoring.

Investigating access control events

Search and filter access control events

There are several ways you can filter the event list, so it displays the data that you are interested in.

1. On the **Access control** tab, select **Events** list.
2. Click any of the filters at the top of the list and specify the criteria.
3. Alternatively you can right-click a specific time, event, source or cardholder within the list and filter using that value.

Any filters you apply are immediately reflected in the list.

You can filter on:

Events list	Description
Time	Select one of the available periods to see data for that particular period. For example, click **Today** to see only events that took place today or use the custom interval to specify a particular period. If you select **Live update**, the list of events is updated instantly if new events occur that meet the filter criterion. The list displays maximum 100 events. You cannot search for cardholders when you work in live update mode.
Event	Select one or more of the available event types directly from the list of event categories and uncategorized events or select between specific access control events.
Source	Select one or more of the available sources directly from the list of doors or select between other sources (for example access points or controllers from the access control system) to view only events for those units.
Access Control System	If your XProtect system integrates with multiple access control systems, select from which access control system you want to view events.
Cardholder	Select one or more of the available cardholders.

Events list (explained)

On the **Access control** tab, when you select an event, the preview on the right lets you view the related video sequence for the event. The preview camera title bar shows the camera related to the unit that triggered the event.

- If you have multiple cameras associated with a door, they all appear in the preview
- Standard playback options are available from the toolbar
- Related cardholder information appears below the video preview together with details about the selected event
- Click  to view live video or play back recorded video in a floating window

Export an access report

On the **Access control** tab, you can create and export a report of the event list to a PDF file when you are not in live update mode.

1. Filter or search for the events you want in the report.

   If the event count is very high, you will receive a recommendation to refine the search and thereby reduce the number of search results.

2. Click the **Access Report** button.
3. Fill out the fields. The report contains:
   - Report name
   - Report destination
   - A list of the applied filters
   - A comment field
   - An option to include snapshots
4. Click **OK** and await that the report is completed.
5. In the top right corner, click **Details** and in the dialog box that appears, click **Open**.

   The report opens in PDF format.

Switch to or from live update mode of the Events list

Instead of viewing live video of access control events in live mode, you work in live update mode on the **Access control** tab. The list of events is updated instantly if new events occur that meet the filter criterion.

1. On the **Access control** tab, select **Events** list.
2. In the dropdown list of the filter where you usually select a period, select **Live Update**.

   Next to the search field, you see that you have changed mode and the list is updated instantly when an event that meets the filter criterion occurs.

   > When you work in live update mode, you cannot search for cardholders and you cannot create an access report.

3. To switch back from the live update mode, filter on a new period.

Monitor and control door states

The **Doors** list provides a list of the doors, access points and other access control units in each access control system, and their current state. This is useful if you, for example, need to know the state of a specific door.

There are several ways you can filter the doors list, so it displays the data that you are interested in.

1. On the **Access control** tab, select **Doors** list.
2. Click any of the filters at the top of the list and specify the criteria.
3. You can combine the filters or enter your criteria in the search field to search for doors.
4. Alternatively you can right-click a door or a state within the list and filter using that value.

   Any filters you apply are immediately reflected in the list.

What can you filter on?

Doors list	Description
Name	Select one or more of the available doors, access points and uncategorized types or select between other access control units to view only states of those selected.
Access Control System	If your XProtect system integrates with multiple access control systems, select from which access control system you want to view doors.
State	Select one or more of the available states directly from the list of state categories and uncategorized states or select between specific access control states.

Another way that you can monitor the door states for your surveillance area is by adding doors to a map (see Monitor doors via maps on page 286).

Doors list (explained)

On the **Access control** tab, when you select a door in the **Doors** list, the associated camera shows live video on the right-hand side of the screen together with detailed information.

- If you have multiple cameras associated with a door, they all appear in the preview
- Standard independent playback options are available from the toolbar
- Action buttons allow you to perform certain commands related to that door, for example lock/unlock door. Available commands depend on your system configuration
- Information related to the selected door appears below the live video preview
- Click  to view live video or play back recorded video in a floating window

Investigate cardholders

The **Cardholders** list provides a list of the cardholders in each access control system and their details. This is useful if you, for example, need detailed information about a specific person.

There are several ways you can filter the cardholders list, so it displays the data that you are interested in.

1. On the **Access control** tab, select **Cardholders** list.
2. Click the filter at the top of the list to specify the access control system from which you want to investigate cardholders. You can only work with one access control system at a time.
3. You can combine the filters or enter your criteria in the search field to search for cardholders.
4. Alternatively you can right-click a cardholder or a type within the list and filter using that value.

   Any filters you apply are immediately reflected in the list.

What can you filter on?

Cardholders list	Description
Name	Select one of the available cardholders to view detailed information about this person.
Type	Select one of the available cardholder types to view the list of cardholders with this type.

When you select a cardholder, the detailed information about this person appears on the right-hand side of the screen. Depending on your system this may include a picture or a link to manage the cardholder record in the access control system (see Manage cardholder information on page 124).

Access request notifications (explained)

Your organization may have chosen that only security personnel must open the doors, when people want to enter your building. If such conditions apply, you may, for example, receive access request notifications when a person wants to enter one or more areas. All conditions that trigger an access request notification have to be specified in the video management system. The notification displays live video related to the access request, allowing you to see the person who is requesting access. The name of the door that should open is shown as a headline, indicating, for example, **Access Request - Front door**. The door state (for example open, closed, or forced open) also appears. If you have multiple cameras associated with a door, they appear below each other.

Access request notifications are temporary. When you close an access request notification, the notification is no longer present in your system. If you close XProtect Smart Client while an access request notification is shown, the notification is not restored when you restart.

Managing access request notifications (explained)

Provided that XProtect Smart Client is running, access request notifications pop up on your screen even when you work in other applications.

Click  if you want to view the live video in a floating window.

Access requests stack up on each other in the access request notification window so that you can handle all incoming access request notifications from the same notification window. You can drag a notification to the other side of the screen or even to another screen if connected.

If needed, you can minimize the access request notification window to allow the functionality to continue in the background. The XProtect Smart Client icon blinks in the taskbar when you have new notifications.

Respond to access requests

Provided that your VMS system supports two-way audio and if a speaker and microphone is attached to the relevant camera that shows the access request notification, access request notifications allow you to speak and listen to the person who wants to enter:

1. To listen to what the person requesting access is saying, click the  button.
2. To speak to the person requesting access, for example to give instructions on how to proceed or behave in the area, click and hold the  button.
3. To carry out other actions, use the command buttons to the right of the microphone and speaker buttons. The most typical action is to unlock a door for a person requesting access, but could also be to turn on the lights in the area close to the relevant entry.

Cardholder information may be available if your access control system provides such information to the XProtect system. Examples of cardholder information: Cardholder's ID number, name, department, phone number, and authority level. Depending on your system configuration, you may be able to manage cardholder information (see Manage cardholder information on page 124).

XProtect LPR (usage)

LPR in live mode (explained)

In live mode, you can view live video from the cameras that have been configured for license plate recognition (LPR). You can view video from several LPR cameras in a view at the same time. On the right-hand side of the view item, the LPR events appear whenever there is a match. In setup mode, you can change the settings that define how the list of license plate numbers displays.

When you click a license plate in the LPR event list, the live video automatically pauses and changes to independent playback. To go back to viewing live video, either click the license plate again or click the **Independent playback** icon on the camera toolbar.

LPR on the Search tab (explained)

On the **Search** tab, you can search for video recordings associated with vehicles.

LPR tab (explained)

On the **LPR** tab, you can investigate LPR events from all your LPR cameras and view the associated video recordings and license plate recognition data. Keep match lists updated and create reports.

The tab includes an LPR event list and an LPR camera preview. In the preview, you can view video associated with LPR event details. Below the preview, information about the license plate appears together with details from the match list and the license plate style that it is associated with.

You can filter the event list according to the period, country module, LPR camera, match list, or license plate style. Use the **Search registration number** field to search for a particular license plate registration number. By default, this list shows LPR events from the last hour. See also LPR event list (explained) on page 292.

You can specify and export a report of relevant events as PDF.

You can make updates to the existing match lists by using the **Match list** function.

LPR event list (explained)

The LPR event list displays all LPR events. By default, the list displays LPR events from the last hour and with the newest at the top, but your system administrator can change this.

When you select an LPR event from the list, you can see a preview to the right with the related video sequence for the event. The title bar of the preview shows the name of the LPR camera that the LPR event was triggered from. You also see the:

- License plate number
- Country module
- Time of the event
- Match list that triggered the event
- License plate style (see License plate styles on page 293)

You can change how the LPR event list displays events; you can sort the columns and you can drag them to different positions. You can use the filters at the top of the list to filter LPR events or use the **Search registration number** field to search.

> The LPR event list only displays LPR events from the time of your search or filter. If you want to see the latest LPR events, click the **Refresh** button.

License plate styles

A license plate style is a set of characteristics of a license plate, including the:

- Plate size and shape
- Text format and font
- Colors
- Type of vehicle that the license plate is used on

Your system administrator can group license plate styles and give that group a custom name.

> You can only add those license plate styles to match lists that were grouped and named by your system administrator.

Filtering LPR events (explained)

There are several ways you can filter the LPR event list, so it displays just the LPR events that you are interested in; you can click any of the filters at the top of the list to see only LPR events associated with that filter. Any filters you apply are immediately reflected in the list.

- **Period**: Select one of the available periods to see LPR events within that particular time
- **Country module**: Clear or select country modules to view only LPR events linked to a license plate from a particular country, state, or region

- **LPR camera**: Select one or more of the available LPR cameras to view only LPR events for those cameras
- **Match list**: Select one or more license plate lists to view only LPR events generated by those lists
- **License plate style**: Select one or more license plate styles to view only LPR events associated with those license plate styles

You can combine the filters, for example, for a particular country module on a certain date.

You can also use the **Search registration number** field to search for a particular license plate. Enter a combination of characters to find results with combinations of those characters. For example, if you enter the characters **XY 12** you will get license plates that have both XY and 12 in their number. If you enter **XY12** you will only get license plates that have XY12 in their number.

Edit match lists

You can add and delete license plates from match lists.

1. On the **LPR** tab, in the top-right corner of the window, click **Match lists** to open the **Match lists** dialog box.
2. In **Select match list**, select the list that you want to edit.
3. To add a license plate registration number or a license plate style, click **Add**. Enter relevant information and click **OK**.

   You can only add those license plate styles to match lists that were grouped and named by your system administrator.

4. To edit an existing license plate registration number, you can use the search function to find the relevant registration number.
5. Double-click a single row to edit or select multiple rows and click **Edit**.
6. In the dialog box, enter information and click **OK**. If the match list contains muliple columns, you can edit the information in all fields.
7. To remove a license plate registration number, you can use the search function to find the relevant registration number.
8. Select multiple rows if needed and click **Delete**.
9. Click **Close**.

Alternatively, you can add a license plate to a match list by right-clicking an unlisted LPR event and selecting **Add to list**. You can also remove a license plate by selecting the relevant LPR event, and on the right, below the preview, clicking the **Remove from list** icon.

Import or export match lists

You can import a file with a list of license plates that you want to use in a match list. You have the following import options:

- Add license plates to the existing list
- Replace the existing list

This is useful if, for example, the lists are managed from a central location. Then they can keep all local installations updated by distributing a file.

Similarly you can export the complete list of license plates from a match list to an external location.

1. To import a match list:
    1. On the **LPR** tab, at the top right of the window, click **Match Lists** to open the **Match Lists** dialog box.
    2. Select the relevant list.
    3. To import a file, click **Import**.
    4. In the dialog box, specify the location of the import file and the import type. Click **Next**.
    5. Await the confirmation and click **Close**.
2. To export a match list:
    1. Click **Export**.
    2. In the dialog box, specify the location of the export file and click **Next**.
    3. Click **Close**.
    4. You can open and edit the exported file in, for example, Microsoft Excel.

Supported formats are .txt or .csv.

Export LPR events as a report

You can export a report of LPR events to a PDF file.

1. On the **LPR** tab, filter or search for the events you want to include in the report.

    If the number of found events is very high, you will receive a recommendation to refine the search and thereby reduce the number of search results.

2. Click the **LPR Report** button.

3. Specify the following values and click **OK**:
    - Report name
    - Report destination
    - A comment field
    - An option to include snapshots

    A progress bar appears at the top right of the XProtect Smart Client window.
4. Click **Details** to view the report.

If you want to change the paper format or font, open the **Settings** window, select **Advanced**, and change the **PDF report format** or **PDF report font** settings.

LPR on the Alarm Manager tab

On the **Alarm Manager** tab, you can view and investigate alarms related to LPR. Some customization is required before you can view the information:

- Enable LPR-specific elements on page 126
- Alarms list must be in Event mode (see View LPR recognitions on page 296)

In general, read the sections about alarm management for more details on XProtect Smart Client functionality.

View LPR recognitions

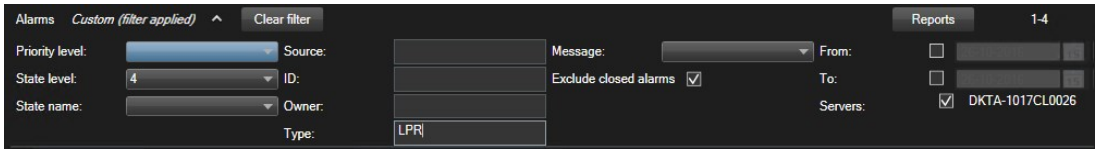
You can view LPR recognitions in the alarm list. If you select events as the data source, all recognitions are displayed. If you select alarms as the data source, only the recognitions associated with an alarm are displayed.

Requirements

To use the **Type** field referred to in the steps below, the field must be enabled in XProtect Management Client by your system administrator.

Steps:

1. Go to the **Alarm Manager** tab.
2. Click the **Setup** button to enter setup mode.
3. To view recognitions associated with an alarm:
    1. In the **Data Source** list, select **Alarm**.
    2. Click **Setup** again to exit setup mode. Your changes are saved. The recognitions are displayed in the alarm list.
    3. To view incoming LPR alarms, enter **LPR** in the **Type** field.



4. To view all recognitions:
    1. In the **Data Source** list, select **Event**.
    2. Click **Setup** again to exit setup mode. Your changes are saved. The recognitions are displayed in the alarm list.
    3. To view all incoming LPR events, enter **LPR** in the **Type** field.

The alarm list will display the filtered results only when you leave the field you modified.

XProtect Transact (usage)

If XProtect Transact has been configured in your system, you can observe live transactions, investigate transactions in several ways, and print transactions.

XProtect Transact (overview)

This topic gives you an overview of what you can do with XProtect Transact in XProtect Smart Client. The features are described according to the tabs.

Tab	Description
Views	On the **Views** tab you can view live and recorded video with transactions. In live mode, you can observe live transactions and surveillance video from the cameras monitoring the transactions. The view can contain several transaction view items, where

Tab	Description
	transactions are displayed as receipts that roll over the screen in sync with the video stream from up to two cameras. In playback mode, you can browse recorded transactions and surveillance video from the cameras monitoring the transactions. The view can contain several transaction view items, where transactions are displayed as receipts that roll over the screen in sync with the video stream from up to two cameras. You create and modify the transaction views in setup mode.
Alarm Manager	On the **Alarm Manager** tab, you can view and investigate events and alarms related to transactions. The events are displayed in the event list. To group transaction events, you need to filter for events of the type transaction. When you click a line in the event list, the video associated with the event is displayed in a preview.
Transact	On the **Transact** tab, you can investigate transactions by performing free text searches and applying filters. The transaction lines appear in a list that you can sort by time, transaction source, and line name. When clicking a line, the associated video still frames from the associated cameras are displayed. Below the preview area, the receipt is displayed.

Observe live transactions

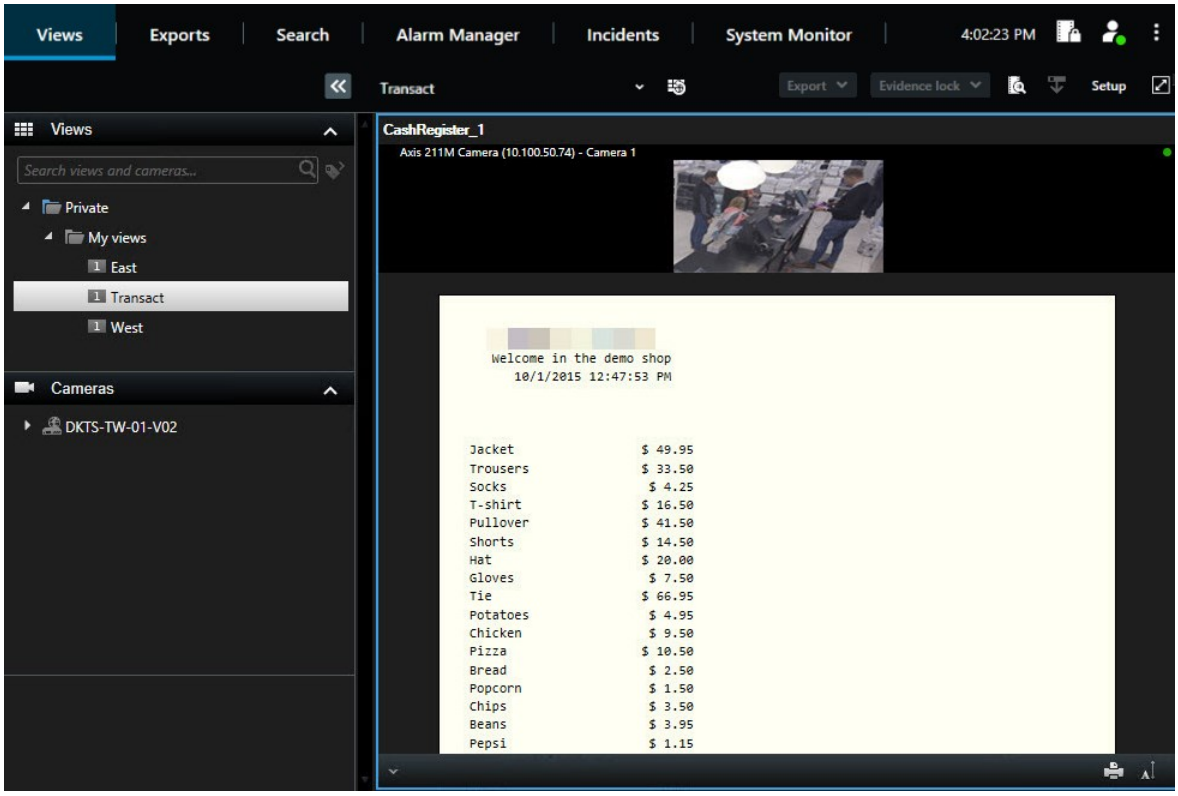
You can observe real time transactions in combination with live video surveillance from the cameras recording the transactions. For example, you may want to observe a cash register, the sales clerk, and the ongoing transactions.

Requirements

You have set up a view to display transactions. For more information, see Set up views for transactions on page 128.

Steps:

1. In live mode, expand the **Views** pane.
2. Select a view set up for transactions. Receipts roll over the screen if there are ongoing transactions, and the live video from the associated cameras are displayed.



If the transaction view item is narrower than the receipt, a horizontal scroll bar allows you to view the part of the receipt that is hidden. If you try to access the scroll bar, the view item toolbar appears covering the scroll bar. To access the scroll bar, press and hold down **Ctrl** while moving the cursor into the view item area.

Select  to change the font size of receipts.

Investigating transactions

Investigate transactions in a view

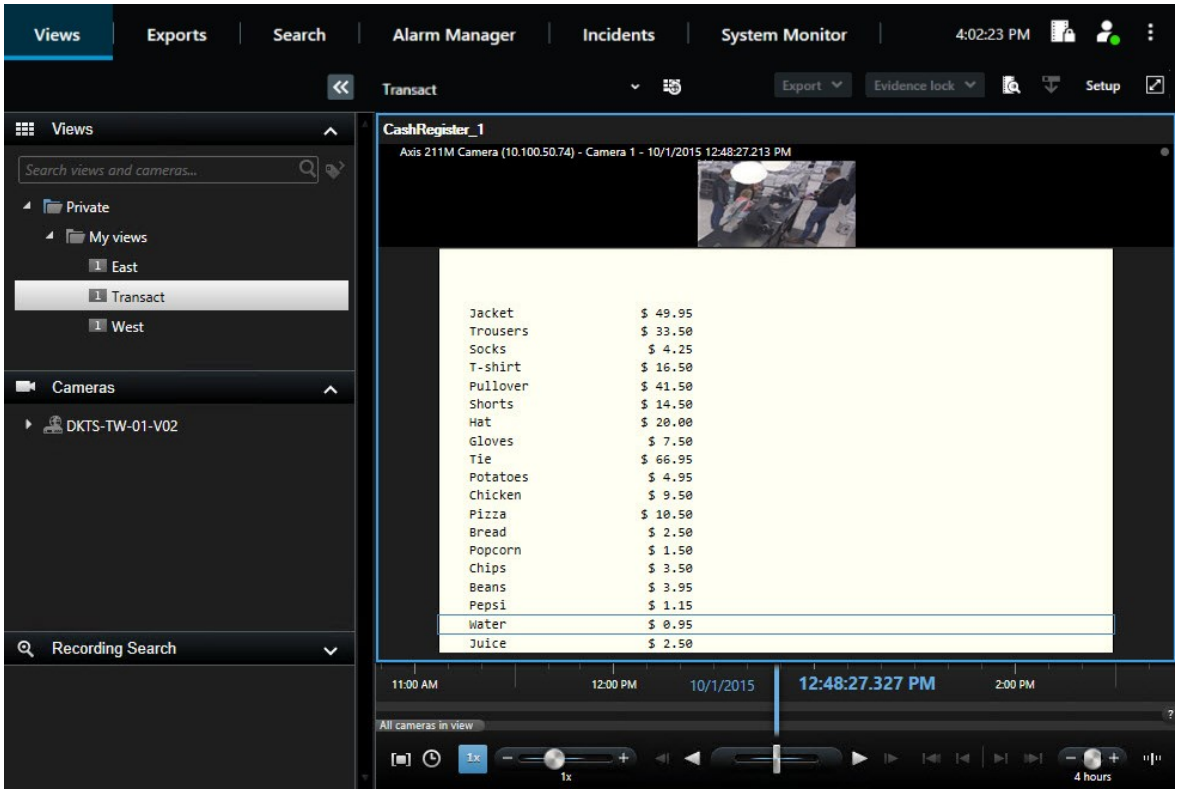
The simplest method of investigating transactions is to view transactions in a view, where the receipts roll over the screen in sync with the video recordings.

Requirements

You have set up a view to display transactions. For more information, see Set up views for transactions on page 128.

Steps:

1. Select the relevant view and switch to playback mode.
2. In the **Views** pane, select the transaction view. Depending on how the view has been configured, one or more receipts appear together with the cameras associated with the transaction source.



3. To browse the video sequences in backward mode, drag the time line to the right.
4. To browse the video sequences in forward mode, drag the time line to the left.
5. Use the  or  button to play the video backwards or forwards.

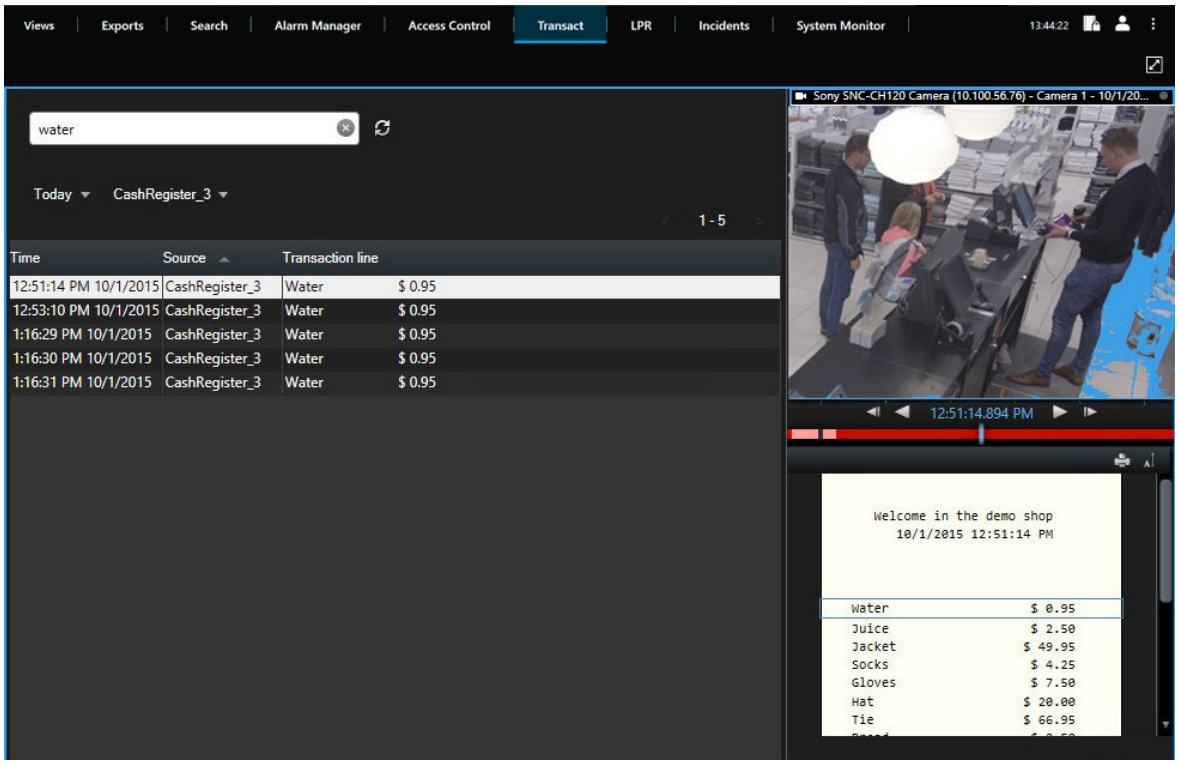
If the transaction view item is narrower than the receipt, a horizontal scroll bar allows you to view the part of the receipt that is hidden. If you try to access the scroll bar, the view item toolbar appears covering the scroll bar. To access the scroll bar, press and hold down **Ctrl** while moving the cursor into the view item area.

Select  to change the font size of receipts.

Investigate transactions using search and filters

You can investigate transactions and the associated video recordings by using filters and search words. The filters help you narrow down your search, for example transactions from the last seven days, or a specific cash register. Search words help you identify specific data from the transactions, for example the name of the sales clerk or unauthorized discounts.

1. Click the **Transact** tab.
2. In the **Today** drop-down list, select a time interval.
3. In the **Source** drop-down list, select the transaction sources you want to investigate. Disabled sources are marked with "()", for example "(CashRegister_)".



4. Enter your search words. The search results are displayed as transaction lines below the filters, and in the receipt, the search item is highlighted.
5. To update the list, click .
6. Click a transaction line to view the associated video still frame. Use the or button to start the video in backward play or forward play mode.

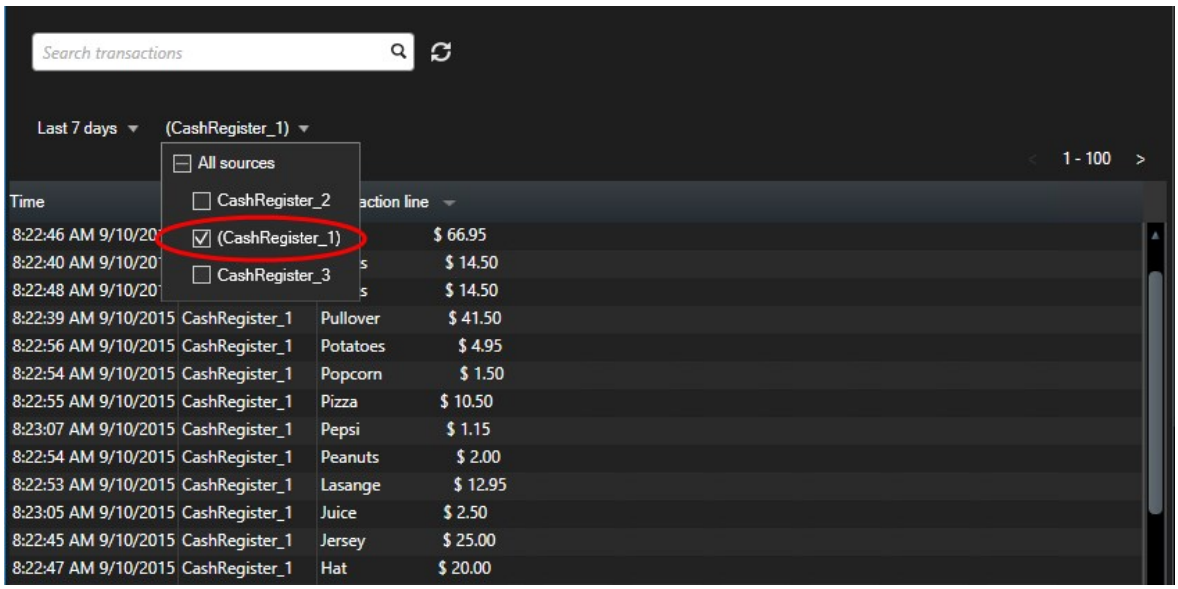
By default, transaction data is stored for 30 days, but depending on the configuration, data can be stored up to 1000 days.

Investigate transactions from a disabled source

Even if a transaction source has been disabled by your system administrator, you can still view past transactions from that source in combination with the associated video recordings.

Steps:

1. Click the **Transact** tab.
2. In the **All sources** drop-down list, select a disabled transaction source. Parentheses indicate that the source is disabled, for example "(CashRegister_1)".



3. Select a time interval, for example **Last 7 days**, or set a custom interval.
4. Click  to view the transaction lines for the specified time interval.
5. Select a transaction line to view the associated video still frame from that exact point in time.
6. Use the  or  button to play the video backwards or forwards.

> By default, stored transaction data is deleted after 30 days. However, your system administrator may have changed the retention period to anything between 1 and 1000 days.

Investigate transaction events

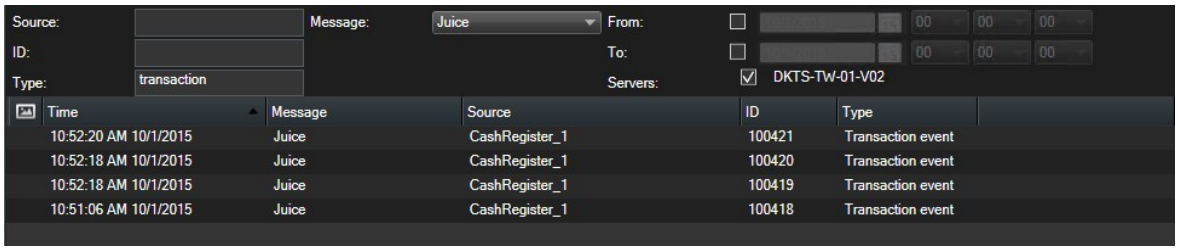
You can investigate transaction events, for example by identifying transactions where a specific item has been purchased. Investigating a transaction event involves viewing the details about the event in the alarm list and the associated video recordings.

Requirements

To filter by transaction events, the **Type** field must be added to XProtect Smart Client. This can only be done by your system administrator.

Steps:

1. Click the **Alarm Manager** tab.
2. Click **Setup** in the upper right corner to enter the setup mode.
3. Expand the **Properties** pane.
4. In the **Data Source** list, select **Event** and click **Setup** again to exit the setup mode. All events are displayed in a list with the most recent at the top.
5. To view only the transaction events, expand the **Filter** section and enter **transaction event** in the **Type** field. Automatically the filter is applied, and only transaction events appear in the list.



6. If you want to view a specific event defined by your system administrator, open the **Message** list and select the event.
7. To view the video recordings associated with an event, click the event in the list. The video starts playing in the preview area.

Investigate transaction alarms

You can investigate alarms that have been triggered by transaction events. The alarms appear in the alarm list, where you can view the details about the alarm and the associated video recordings.

Requirements

To filter by transaction events, the **Type** field must be added to XProtect Smart Client. This can only be done by your system administrator.

Steps:

1. Click the **Alarm Manager** tab.
2. Click the **Setup** button in the upper right corner to enter the setup mode.
3. Expand the **Properties** pane.
4. In the **Data Source** list, select **Alarm** and click **Setup** again to exit the setup mode. The most recent alarms are displayed at the top.

5. To view only the alarms triggered by transaction events, expand the **Filter** section and enter **transaction event** in the **Type** field. Automatically the filter is applied to the list.
6. To view alarms triggered by a specific event, open the **Message** list and select the event.
7. To view the video recordings associated with an alarm, click the alarm in the list. The video starts playing in the preview area.

Print transactions

When you are viewing transactions in the **Transact** workspace, you can print the transactions, one at a time. The printout displays the receipt and still images from the associated cameras at the time matching the transaction line.

Steps:

1. Click the **Transact** tab.
2. Find the transaction you want to print as described in Investigating transactions on page 299.

3. Click **Print** below the transaction to print it. A Windows dialog box appears.
4. Select the required printer and click **OK**.

Maintenance

Check the status of your server connection

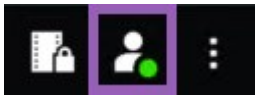
In the **User menu**, you can check the status of your server connection, for example, to see if you are using an older security model (HTTP) or the newest security model (HTTPS). If multiple sites are connected through Milestone Federated Architecture, you can also check the connected sites.

Connection statuses

- HTTPS
- HTTP
- Not connected

Steps:

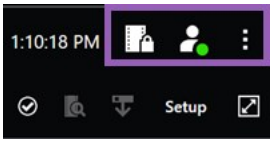
1. On the global toolbar, select the **User menu**.



2. Select **Login information** and check the status of your connection.

Global toolbar

From the Global toolbar, in the upper-right corner of the XProtect Smart Client, you have access to:



- Evidence lock list
  The **Evidence lock list** shows evidence locks with devices that you have permissions to access. You can sort, filter, and search the evidence locks list and see detailed information about the evidence locks. For more information, see View evidence locks on page 196.

- User menu
  From your **User menu**, you can see your **Login information**, and you can log out from the XProtect Smart Client. See Log out on page 150. **Login information** contains information about the status of the XProtect VMS servers that your XProtect Smart Client is connected to. This is useful if you are connected to an XProtect VMS system that is configured to use Milestone Federated Architecture. Milestone Federated Architecture enables organizations to connect related but physically separate XProtect VMS systems. For example, such a setup can be relevant for chains of shops.

  A red circle on the **User menu**  indicates that one or more servers are unavailable.

  Select **Login information** to view the server status.

  - Available servers are displayed in green.
  - Unavailable servers are displayed in red.
    If servers are not available at the time you log in, you cannot use cameras or features belonging to those servers. When you have viewed the status, the red button will stop flashing even if the server is still unavailable.

  The number of servers you see reflects the number of servers retrievable from the XProtect VMS system at the time you logged in. Particularly if you connect to large hierarchies of servers, occasionally, more servers may become available after you log in. The server list is a static representation of server status. If a server is unavailable, it will display a reason in the **Status** field when you click it. To connect to the server, click the **Load Server** button. The server status for that server will then be updated. If a server continues to be unavailable for longer periods of time, contact your system administrator for advice.

- Settings and more
  The **Settings and more** window covers **Toggle theme**, **Server jobs**, XProtect Smart Client **Settings**, **Help**, **Video tutorials**, and the **About** button. See also Buttons on page 24.

Troubleshooting

Installation (troubleshooting)

Error messages and warnings

You cannot install Milestone XProtect Smart Client (64-bit) on this operating system. The OS is not supported.

You have tried to install a version of XProtect Smart Client that does not support the current version of your computer's Windows operating system. To resolve the problem, install an older version of XProtect Smart Client or upgrade your operating system.

For information about system requirements, see https://www.milestonesys.com/systemrequirements/.

Logging in (troubleshooting)

Error messages and warnings

Your user permissions do not allow you to log in at this point in time. User permissions may vary depending on time of day, day of week, and so on.

You have tried to log in at a time when your user permissions do not allow you to log in. To resolve this issue:

Wait until you are permitted to log in. Contact your system administrator if in doubt about your user permissions.

You do not have access to any part of the application. Contact the system administrator.

You currently have no access permissions to any part of the XProtect Smart Client, and therefore you cannot log in. To resolve this issue:

Contact your system administrator, who will be able to change your access permissions if required.

Application is not able to start, because two (or more) cameras are using the same name or ID...

This error message only appears in a very rare scenario, where a backed-up configuration from one XProtect VMS system is mistakenly used without any modification on another XProtect VMS system. This can cause different cameras to "fight" over the same identity, and that can in turn block your access to the XProtect VMS system. If you see such a message, contact your system administrator.

Authorization failed: You cannot authorize yourself.

You have entered your own credentials in the **Authorized by** field. You cannot authorize yourself. To resolve this issue:

You must contact the person who has authorization permissions. This could be your supervisor or your system administrator. This person must enter his or her credentials to authorize your login.

Authorization failed: You do not have permission to authorize.

You have tried to authorize a user but you do not have the user permissions to do so. To resolve this issue:

Ask your system administrator to check that you have the necessary permissions to authorize other users or ask someone else with sufficient user permissions to authorize the user.

Failed to connect. Check the server address.

It was not possible to connect to the XProtect VMS server at the specified server address. To resolve this issue:

Verify that you have entered the correct server address. The *http://* or *https://* prefix and port number are required as part of the server address (example: *https://123.123.123.123:80*, where *:80* indicates the port number). Contact your system administrator if in doubt.

Failed to connect. Check the user name and password.

It was not possible to log in with the specified user name and/or password. To resolve this issue:

Verify that you have entered your user name correctly, then enter your password again to ensure it does not contain errors. User names and passwords are case sensitive. For example, there may be a difference between entering **Amanda** and **amanda**.

Failed to connect. Maximum number of clients are already connected.

The maximum number of clients allowed to connect to the surveillance system server simultaneously has been reached. To resolve this issue:

Wait for a while before connecting again. If access to the surveillance system is urgent, contact your system administrator, who may be able to extend the number of simultaneously connected clients.

Connection using an old security model. You cannot connect to the web page using the newest security model.

Occurs if you try to log in to a server that does not have a certificate installed. To resolve the issue, contact your system administrator, or click the **Allow** button to log in using HTTP, a network protocol that operates without the use of a certificate.

You no longer have permission to do this

Occurs if your time-dependent user permissions no longer allow you to do something that you have previously been able to do. This is because, when connected to certain types of surveillance system (see Surveillance system differences on page 33), your user permissions may vary depending on time of day, day of week, etc. Therefore, you may well be able to perform the action again at a later stage.

Due to system settings, your XProtect Smart Client session will expire within the next [...]

Occurs if your current XProtect Smart Client session is about to end. When connected to certain types of surveillance system (see Surveillance system differences on page 33), your permissions to use the XProtect Smart Client may depend on time of day, day of week, etc.

When that is the case, you will typically see this message a number of minutes or seconds before your session will be closed; the exact number of minutes or seconds is defined on the surveillance system server.

No user activity detected recently, your XProtect Smart Client session will expire within the next [...]

Occurs if you have not used your XProtect Smart Client for a while (the exact time is defined on the surveillance system server), in which case your XProtect Smart Client session will be closed for security reasons.

When that is the case, this message will typically be presented a number of minutes or seconds before your session will be closed; the exact number of minutes/seconds is defined on the surveillance system server.

Audio (troubleshooting)

I cannot hear sound from a camera that has a speaker attached

The speaker may have been muted, or the speaker has been disabled by your system administrator. To unmute a speaker, select the view item with the camera, and open the **Audio** pane on the left-hand side. Clear the **Mute** check box.

Exporting (troubleshooting)

At least one database file is using an unsupported encryption algorithm

If you see this warning, your current XProtect VMS system uses AES-256 for encrypting exported video data to comply with the FIPS 140-2 security standard. However, the system which was used to create the export uses a different encryption standard.

To resolve the issue, do one of the following:

- Re-export the video data using an upgraded version of XProtect Smart Client. The version must be equal to or newer than your current version
- Though Milestone recommends always using the latest version of XProtect Smart Client, you can open the export using an older version of XProtect Smart Client in offline mode
- Open the export on a computer where FIPS mode is disabled. See also https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation#using-windows-in-a-fips-140-2-approved-mode-of-operation

Milestone recommends that you password-protect your data. To do this, select the **Encrypt with password** check box in the **Export settings** window > **XProtect format**.

Could not validate the integrity of this project...

No tampering key is included in the video export. Either the tampering key was removed, or the video export was created using a stand-alone third-party application based on the MIP SDK 2020 R2 or older. If the tampering key is missing, there is no way of verifying the authenticity of the video project file.

To resolve the issue, do one or more of the following:

- Request a new video export and make sure the tampering key is included
- Re-export the video data using a third-party application which is based on MIP SDK 2020 R3 or later

Searching (troubleshooting)

Error messages and warnings

Unable to create report

You have tried to create a surveillance report based on one or more search results, but the report could not be created. There may be different reasons:

- You have already created a report with the same name in the same location, and the report is currently open. To resolve the issue, close the report, and try again.
- You do not have the user permissions to save reports in the report destination. To resolve the issue, specify a different path in the **Create report** window.

You cannot open this search, because certain data sources are not available to you

These are some of the possible reasons why you cannot open the search:

- The person who created the search used one or more search categories that are not available to you. To resolve the issue, create a new search.
- The search that you are trying to open uses search categories that are not available in the version of XProtect Smart Client that you are using. To resolve the issue, download a newer version of XProtect Smart Client.
- The search categories that are not available to you may require additional licenses. Please contact your system administrator.

This device has not been placed on the smart map

You have selected a search result, but the associated device is not displayed on the smart map in the preview area. The reason is that the device has not been geographically positioned. To resolve this issue, do one of the following:

- Go to your smart map and add the device. See Add devices to smart map on page 96
- Ask your system administrator to specify the geo coordinates in the device properties in XProtect Management Client

Smart map (troubleshooting)

I do not see any devices on my smart map

If you do not see any cameras or other devices on your smart map, then likely the system elements layer is hidden. To enable the system elements layer, see Show or hide layers on smart map on page 90.

My device does not appear on the smart map

If there are one or more devices that should, but do not appear on the smart map, then likely the devices have not been geographically positioned. To resolve this issue, do one of the following:

- Drag the devices onto the smart map from the device hierarchy. This requires that editing of devices is enabled on your user profile
- Ask your system administrator to specify the geo coordinates in the device properties in XProtect Management Client

Error messages and warnings

Cannot save the map. Cannot perform the operation.

You are trying to add devices to a smart map manually in XProtect Smart Client. A probable cause is that you are running XProtect Smart Client 2017 R1 against an XProtect Corporate 2017 R2 installation. XProtect Smart Client looks for the position of the device on the event server, but in version 2017 R2 or newer of XProtect Corporate the geo coordinates are stored on the management server.

To resolve the issue, upgrade XProtect Smart Client to version 2017 R2 or newer.

This device has not been placed on the smart map

You have selected a search result, but the associated device is not displayed on the smart map in the preview area. The reason is that the device has not been geographically positioned. To resolve this issue, do one of the following:

- Go to your smart map and add the device. See Add devices to smart map on page 96
- Ask your system administrator to specify the geo coordinates in the device properties in XProtect Management Client

Web pages (troubleshooting)

I am getting a script error when adding a web page to a view

The web page uses scripts that are not supported by the browser used to render the web page. It may resolve the issue to change the **Display mode** in the web page properties.

I am getting a script error when loading a view that contains a web page

The web page uses scripts that are not supported by the browser used to render the web page. It may resolve the issue to change the **Display mode** in the web page properties.

I have used scripting to add navigation buttons or clickable images to my HTML page, but the HTML page does not work as intended. Consider the following:

- Have you set **Display mode** to **Compatibility**? Only **Compatibility** mode supports scripting.
- Have you used the correct syntax in your HTML code?
- Is HTML scripting enabled in XProtect Management Client or in the **Client.exe.config** file?
- Does the intended audience have the user permissions to access certain cameras, views, features, or tabs in XProtect Smart Client?

XProtect Transact (troubleshooting)

Error messages and warnings

Failed to retrieve transaction data from the event server.

The event server is not running or not responding, or the connection to the server has been lost.

There is an internal error on the event server or in the associated database. This may include issues with the connection to the database. To resolve this issue, please contact your system administrator.

Your search timed out before completion. Try narrowing your search by shortening the search period.

There is an internal error on the event server or in the associated database. This may include issues with the connection to the database. To resolve this issue, please contact your system administrator.

Upgrade

Upgrading XProtect Smart Client

During log-in, if you are using an older version of XProtect Smart Client compared to the server that you are connecting to, a message informs you that a new version of the XProtect Smart Client is available, including where to download the new version of the software. Milestone recommends that you download the new version.

If XProtect Smart Client is newer than the server that you are connecting to, certain features may not be available.

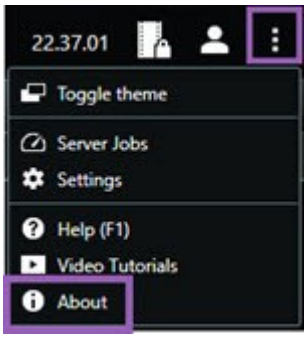
View version and plug-in information

Knowing the exact version of your XProtect Smart Client can be important if you require support or want to upgrade. In such cases, you also need to know which plug-ins your XProtect Smart Client is using.

The version of XProtect Smart Client may also affect which XProtect server version it is compatible with.

Steps:

1. Open XProtect Smart Client.
2. In the **Settings and more** window on the global toolbar, select **About**. A window appears.



FAQ

FAQ: alarms

I see an alarm desktop notification, but it disappears before I can respond. How do I find it again?

Go to the **Alarm Manager** tab and look in the alarm list. If you do not see the alarm, it may have been filtered out. Try changing the filter settings.

If the alarm list is configured to show events instead of alarms, click the **Setup** button. In the **Properties** pane on your left-hand side, select **Alarm** in the **Data Source** list and click **Setup** again.

FAQ: audio

Why is the Speakers list not available?

Some surveillance systems do not support two-way audio.

For information about the features available in your XProtect VMS, see Surveillance system differences on page 33.

Can I adjust the recording volume of a microphone connected to a camera?

This feature does not exist in the XProtect Smart Client. However, you may be able to adjust the recording volume either on the microphone or through the configuration interface of the camera device that has the microphone attached. Contact your system administrator if in doubt.

Can I adjust the output volume of speakers connected to a camera?

This feature does not exist in the XProtect Smart Client. However, the **Level meter** in the **Audio** pane gives an indication of the input level which, in turn, gives an idea of the output level.

You may be able to adjust the output volume either on the speakers or through the configuration interface of the camera device that has the speakers attached. You can also adjust your audio settings in Windows. Contact your system administrator if in doubt.

Will other XProtect Smart Client users be able to hear what I say through speakers?

As a rule, other XProtect Smart Client users cannot hear what you say. However, if microphones are located near the speakers you are talking through, it may be possible to hear you.

Can I talk through multiple speakers at the same time?

Yes, if your surveillance system has speakers attached to multiple cameras (and you have the necessary user permissions to access them), you can talk through all the speakers at once. In the **Audio** pane, in the **Speakers** list, select **All speakers**, then click and hold the **Talk** button when you talk.

If you have selected List only devices from current view in the Audio pane, you will not see all speakers.

Will audio from microphones attached to cameras be recorded?

Incoming audio, from microphones attached to cameras, is recorded, even when no video is being recorded.

Will what I say through speakers be recorded?

The surveillance system can record incoming audio from microphones, even when no video is being recorded. However, outgoing audio transmitted through speakers can only be recorded, played back, and exported on some surveillance systems. For information about the features available in your XProtect VMS, see Surveillance system differences on page 33.

Depending on your surveillance system, recordings can be used, for example, to prove that a XProtect Smart Client operator gave an audience specific instructions through speakers.

Do I get an indication of my voice level when I talk through speakers?

Yes, in the **Audio** pane, the **Level meter** indicates the level of your voice. If the level is very low, you may need to move closer to the microphone. If the **Level meter** shows no level at all, verify that the microphone is connected and correctly set up.

FAQ: bookmarks

How do I find bookmarked incidents?

Go to the **Search** tab, set a timespan, select the cameras that may have recorded the incident, and then click **Search for** > **Bookmarks**.

I cannot find a particular bookmark. Why?

There may be several reasons why you cannot find the bookmark:

- Your user permissions do not allow you to view the bookmark.
- The bookmark has been deleted by a user with permissions to delete bookmarks.
- The bookmarked video no longer exists in the database.

Can I bookmark my search results?

Yes. When you have performed a search that returns a list of search results, you can bookmark any of these search results. See Bookmark search results on page 224.

FAQ: cameras

What is jitter?

Jitter is small variations in the video which the viewer can perceive as irregular movement, for example when viewing a person walking.

Will I receive lots of sound notifications?

If you select **Always on**, the number of motion-related sound notifications will depend on the motion detection sensitivity of the camera. If motion detection for the camera is highly sensitive, you may receive very frequent sound notifications. The camera's motion detection sensitivity is configured on the surveillance system server. If you select sound notifications for more than one camera, you may also hear more notifications—again depending on the cameras' motion detection sensitivity.

Can I change the notification sound?

By default, the XProtect Smart Client uses a simple sound file for its sound notifications. The sound file, called **Notification.wav**, is located in the XProtect Smart Client installation folder, typically **C:\Program Files\Milestone\XProtect Smart Client**. If you want to use another .wav file as your notification sound, simply name the file **Notification.wav** and place it in the XProtect Smart Client installation folder instead of the original file. The file **Notification.wav** is used for event-detection and motion-detection notifications. You cannot use different sound files for different cameras or to distinguish between event- and motion-detection notifications.

What do the camera indicators mean?

The camera indicators show you the status of the video that is displayed in the camera view items. See Camera indicators (explained) on page 168.

Why is the server connection to the camera lost?

Cameras may stop working for various reasons, for example, if it has been configured only to be available during certain hours of the day, or because of camera or network maintenance, or a change in configuration on the VMS server.

Why does the time in the camera toolbar not match my current time?

The time zone that is defined server-side may differ from your current time zone or the time zone of your computer. To change the time in the camera toolbar, open the **Settings** window and go to **Advanced** > **Time zone**.

FAQ: digital zoom

What is the difference between optical and digital zoom?

With optical zoom, a camera's lens physically moves to provide the required angle of view without loss of image quality. With digital zoom, the required portion of an image is enlarged by cropping the image and then resizing it back to the pixel size of the original image—a process called interpolation. Digital zoom simulates optical zoom, but the digitally zoomed portion will have a lower quality than the original image.

Is digital zoom relevant for PTZ cameras?

When viewing live video from a pan-tilt-zoom (PTZ) camera, you can use the PTZ camera's own optical zoom features, so digital zoom is not highly relevant for PTZ cameras. You can, however, use the digital zoom feature if, for example, your user permissions do not allow you to use the PTZ camera's own optical zoom features.

Why can't I see any navigation buttons?

If the camera you are viewing video for is not a PTZ camera, you will only be able to zoom in on an area of the image and you will only see the zoom buttons. Once you have zoomed in on an area of the image, you will have access to the PTZ navigation buttons, which let you navigate within this zoomed area.

FAQ: displays and windows

How many secondary displays can I use?

In the XProtect Smart Client there is no limitation. However, the number of secondary displays you can use depends on your hardware (display adapters, etc.) and your Windows version.

I want to close a view sent to Primary display or a Secondary display; where is the Close button?

In order to allow the maximum possible viewing area, the title bar of a view sent to primary display or a secondary display is hidden. To show the title bar, and get access to the **Close** button, move your mouse pointer to the top of the view.

I watch the same carousel in two different windows; why are they out of sync?

A carousel changes cameras at a specific interval, configured in setup mode. Example: With an interval of 10 seconds, the carousel will show Camera 1 for 10 seconds, then Camera 2 for 10 seconds, etc. The timing begins when you start watching a view containing the carousel. When you later begin watching the same carousel in another view, perhaps even in another window or another display, the timing for that instance of the carousel begins. This is why the carousel appears to be out of sync: in reality, you are watching two separate instances of the carousel. For more information, see Edit the carousel settings on page 76.

FAQ: exporting

Can I export audio too?

When exporting in the media player and in the XProtect formats, you can—if your surveillance system supports this—include recorded audio in the export. Export in the XProtect format is only available if connected to selected surveillance systems. When exporting in the still image format, you cannot include audio.

For information about the features available in your XProtect VMS, see Surveillance system differences on page 33.

If I export a bookmark video clip, what is included in the export?

The entire bookmark video clip (see Bookmarks (explained) on page 232) is included, from the specified clip start time to the specified clip end time.

Can I include local video clip files in my export?

No, you can only include video data from cameras or other devices that are connected to your VMS system.

If I export a sequence, what is included in the export?

The entire sequence, from the first image of the sequence to the last image of the sequence is included.

If I export an evidence lock, what is included in the export?

All data protected from deletion is included: all the cameras and data from devices related to the cameras, from the first images of the selected interval to the last images of the selected interval.

Can I export fisheye lens recordings?

Yes, provided your surveillance system supports the use of 360° lens cameras (i.e. cameras using a special technology for recording 360° images).

What can I do to reduce the file size of the export?

You cannot compress the export files to reduce the size of the export. To get the smallest export size possible, select the MKV media player format. If not enabled, please contact your system administrator.

Why can't I specify an export path?

You can usually specify your own path, but if you are connected to certain types of surveillance systems (see Surveillance system differences on page 33), the surveillance system server may control the export path setting and you cannot specify your own path.

Why have digital signatures been removed in my exported video?

There are two scenarios where digital signatures are excluded during the export process:

- If there are areas with privacy masks, digital signatures for the recording server will be removed in the export
- If the data you are exporting is very close to the current date and time, the digital signature for the recording server might not be included for the whole sequence. In this case, only part of the export will have digital signatures added

The export process will complete, but when you verify the signatures, you will see that the digital signatures for the recording server were removed or partially OK.

Can I protect the evidence I export from being tampered with or ending in the wrong hands?

Yes. When you export in the XProtect format, you can prevent your recipients from re-exporting the material, protect the exported evidence with a password, and add a digital signature to the exported material. See XProtect format settings on page 189.

FAQ: maps

Which image file formats and sizes can I use for maps?

You can use bmp, gif, jpg, jpeg, png, tif, tiff, and wmp file formats for maps.

Image file size and resolution should preferably be kept under 10 MB and 10 megapixels. If you use larger image files, this can cause low performance in the XProtect Smart Client. You cannot use images larger than 20 MB and/or 20 megapixels.

Maps are displayed in the XProtect Smart Client on the basis of the graphic file's properties, and adhering to Microsoft standards. If a map appears small, you can zoom in.

Can I change the background of a map but keep the cameras in their relative positions?

Yes. If you need to update the map but want to keep all the information on it, you can just replace the map background (if you have the necessary map edit user permissions). This allows you to keep all your cameras, and other elements in their relative positions on a new map. Select **Change map background**, by right-clicking the map or in the **Properties** pane.

FAQ: notifications

Why do I not receive any desktop notifications when new alarms occur in my XProtect VMS system?

Desktop notifications for alarms must be enabled by your system administrator in XProtect Management Client. Otherwise, you will not receive any.

I see an alarm desktop notification, but it disappears before I can respond. How do I find it again?

Go to the **Alarm Manager** tab and look in the alarm list. If you do not see the alarm, it may have been filtered out. Try changing the filter settings.

If the alarm list is configured to show events instead of alarms, click the **Setup** button. In the **Properties** pane on your left-hand side, in the **Data Source** list, select **Alarm** and click **Setup** again.

Will I receive multiple desktop notifications if multiple alarms occur within a few seconds?

A desktop notification stays on the screen for 15 seconds. If multiple alarms occur consecutively within a few seconds, you will still only see one desktop notification. When you click the desktop notification, the most recent alarm opens in the alarm window. To view the previous alarms, go to the alarm list.

FAQ: searching

Can I start search from individual cameras?

Yes. When you are looking at a specific camera in live or playback mode, you can send the camera to a new **Search** window. To start search, click  in the camera toolbar.

Can I start search from all cameras in a view?

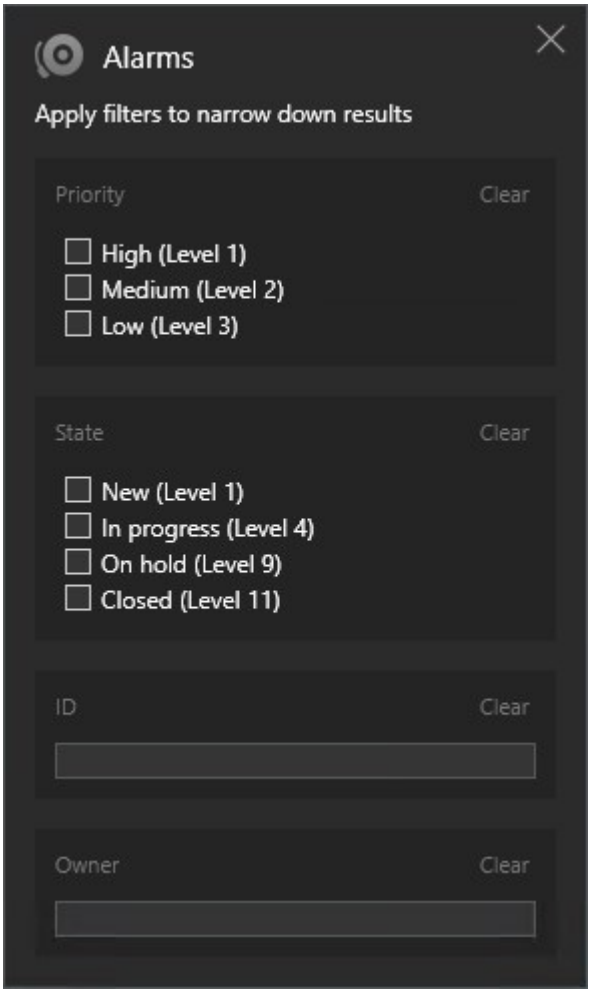
Yes. When you are looking at cameras in a view in live or playback mode, you can send these cameras to a new **Search** window. To start search, click  above the view.

I am running a search, but even after a while XProtect Smart Client still seems to be searching. Why is that?

If the **Duration** covers a wide timespan, for example two weeks, or you have selected many cameras, there may be thousands of search results, and it may take a while for XProtect Smart Client to find all the search results.

Milestone recommends that you refine your search to narrow down the search results.

How do filters work with search?



When you apply multiple filters, for example both **Priority** and **State**, you filter for results that match all the applied filters.

When you select multiple values within one filter, for example **High**, **Medium**, and **Low** within the **Priority** filter, you filter for results that match at least one of those values.

Why are some of the thumbnail images grayed out?

A grayed out thumbnail image in the list of search results means that currently no recordings are available for the camera at trigger time. There may be multiple reasons, for example that the recording server is down.

Why is the action that I need not available in the action bar?

After selecting a search result, certain actions may not be available in the blue action bar.

This happens if you select a search result that matches more than one search category at the same time, and the action that you are trying to perform does not support one of those search categories.

Example: You search for **Bookmarks** and **Motion**, and one of the search results contain both motion and a bookmark. In this case, editing or deleting the bookmark is not possible.

> The scenario described in this section may also apply to actions pertaining to third-party software that is integrated with your XProtect VMS system.

Why is the action that I need only applicable to some of my search results?

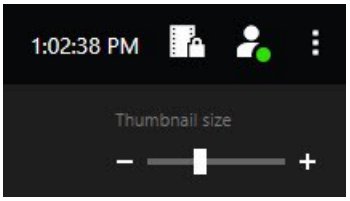
If you are trying to use one of the actions in the blue action bar on multiple search results, you may see a tool tip informing you that the action can only be applied on a subset of the search results.

This happens when at least one of the selected search results is not supported by the action that you are trying to perform.

> The scenario described in this section may also apply to actions pertaining to third-party software that is integrated with your XProtect VMS system.

The thumbnail images in the search results are too small. How do I make them bigger?

You can increase the size of the thumbnails by dragging the slider in the image to the right.



I am trying to save a new search. Why is the Private search check box disabled?

If the **Private search** check box is grayed out and preselected, you do not have the permissions to **Create public searches**. The search that you are about to save is only available to you.

I am trying to open or find a search. Why is the Only show my private searches check box disabled?

If the **Only show my private searches** check box is grayed out and preselected in the **Open search** or **Manage searches** window, you do not have the permissions to **Read public searches**. You can only view your own private searches.

I have changed a search. Why can I not save the changes?

If you change how an existing search is configured, for example if you have added a camera, and the **Save** button is disabled, you do not have the permission to **Edit public searches**. Also, you will not be able to change the details of the search, for example the name and description.

Why can I not delete a search?

If the **Delete** button is disabled in the **Manage searches** window, you do not have the permission to **Delete public searches**.

What happened to smart search?

When the **Sequence Explorer** tab was retired, smart search was moved to the **Search** tab. To use the smart search feature, create a search, select **Motion**, and finally unmask an area. See also Search for motion (smart search) on page 206.

What is the difference between start time and event time?

When you search for video recordings on the **Search** tab, each search result has a start time, end time, and event time. The start time and end time indicate the beginning and end of an event, respectively. The event time is the most interesting or important part of the video sequence. For example, if you are searching for motion, the event time is when the motion starts. Or, if you are identifying objects, the event time is the time of the most reliable identification.

I am searching for bookmarks. Will the search find bookmarks where the start time or end time falls outside of the search timespan?

Yes. As long is there is an overlap in time, bookmarks will be found. Here is an example: If the search timespan is today between 1:00 pm and 3:00 pm, and there is a bookmark where the start time is today 11:00 am and the end time is today 2:00 pm, then the bookmark will be found.

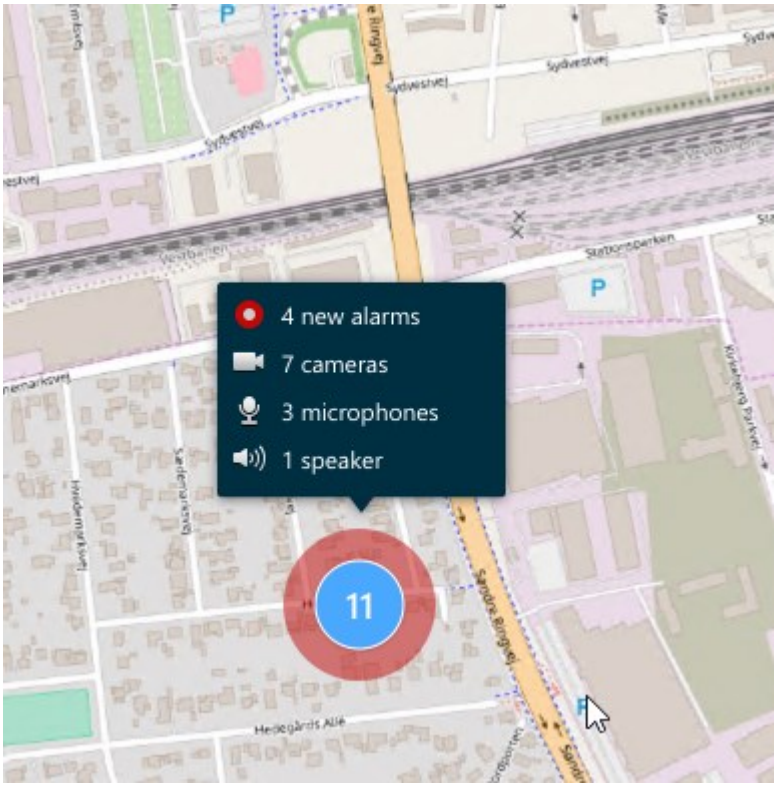
What is a relative timespan?

When you save a search where you have selected a predefined timespan, for example **Last 6 hours**, you will be notified that the timespan is relative. It means that the last six hours are relative to your current time. Regardless of when you run the search, it will always return search results from the last six hours.

FAQ: smart map

Can I see what is inside the clusters?

The cluster icons on the smart map appear when there are multiple devices within an area. Simply click the cluster to see the types of devices and how many devices are inside the cluster.



Can I remove devices from my smart map?

Yes. For more information, see Remove devices from smart map on page 98.

Can I show the same device on multiple levels in a building?

Yes, you start by placing the device on one level. Next, right-click the device, select **[device] visible on levels** and then specify additional levels that you want the device to be associated with.

Can I adjust the building outline to match a round building?

On the smart map, building outlines are square. Milestone recommends that you use the corner handles to adjust the shape of the building to cover the actual building.

What files types can I use as floor plans in a building?

You can use any of the supported custom overlays:

- Shapefiles
- CAD drawings
- Images

For more information, see Adding, deleting, or editing custom overlays on page 91.

What is the maximum size of custom overlays?

The maximum size of custom overlays are as follows:

- CAD drawings: 100 MB
- Images: 50 MB
- Shapefiles: 80 MB

The maximum size can adjusted by changing the values in the **client.exe.config** file. Please contact your system administrator for more information.

Can I add multiple floor plans to the same level?

Yes, you can add any number of floor plans to the same level, for example one for the north-wing and one for the south-wing.

What if a device in a building is not associated with any levels?

In that case, the device is visible an all levels.

Dissociating a device from the levels in a building is relevant, for example, if the device is located inside an elevator. When you add a device to a building, automatically the device is associated with the selected level. To dissociate the device, in setup mode, right-click the device, select **[device] visible on levels**, and make sure that no levels are selected.

If I move a building with a floor plan, will the floor plan move with it?

No, the floor plan stays in its original, geographic location and is visible only in setup mode. You must manually reposition the floor plan.

If I reorder a level within a building, will the devices stay with the level?

Yes, the devices stay with the level.

What happens to floor plans and devices when I delete a building?

The floor plans are deleted, but the devices remain.

FAQ: views

Can I view video immediately without setting up views?

Yes. Many XProtect Smart Client users can view video in their XProtect Smart Client immediately, without the need to set up views first.

Private views: If connected to certain types of surveillance system (see Surveillance system differences on page 33)—primarily small surveillance systems with few cameras—the surveillance system server can automatically generate a single private view with all the system's cameras. Such a view is called a **default view**. If you have access to a default view, you can begin viewing video in your XProtect Smart Client immediately because the default view will automatically be displayed the first time you log in to your XProtect Smart Client.

Shared views: Shared views may already have been created by the system administrator or by some of your colleagues. If shared views already exist, and you have access to them and the cameras they contain, you can begin viewing video in your XProtect Smart Client immediately.

Why do I need to recreate my views?

From time to time your system administrator may make changes to camera or user properties on the surveillance system. Such changes take effect in the XProtect Smart Client when you log in for the first time after the changes were made, and they may occasionally require you to re-create your views.

What if I cannot create private or shared views?

Typically only a few people in an organization are able to create and edit shared views. Your system administrator may create and maintain a number of shared views. When you log in, the shared views will automatically be available to you, so you will not need to create further views.

How can I see which views I have access to?

Typically, your system administrator will have told you if you have access to shared views. If not, you can quickly determine if any shared views are available to you.

In live or playback mode, the Views pane will always contain a top-level folder called Private. The Private top-level folder is for accessing private views, and its content depends upon which views—if any—you have created for yourself.

Any other top-level folders in the Views pane are for accessing shared views. The names of these top-level folders depend on what has been configured.

The fact that the Views pane contains one or more top-level folders for accessing shared views does not in itself guarantee that shared views are actually available. To verify if any shared views are available under the top-level folders, expand the folders.

How can I see which views I can edit?

If a folder has a padlock icon, it is protected and you cannot create new views or edit existing views to it.

Can I see my views on different computers?

Your user settings, including information about your views, are stored centrally on the surveillance system server. This means that you can use your views, private as well as shared, on any computer that has a XProtect Smart Client installed, provided you log in to the XProtect Smart Client with your own user name and password.

Can I add an overlay button for an action if I do not have user permissions to perform the action myself?

Yes. This enables you to make buttons available on shared views, where colleagues with the necessary user permissions will be able to use the buttons, even if you do not have user permissions to use them yourself.

When you add a button for an action you do not have user permissions for, the button appears dimmed in setup mode and doesn't appear in live mode. Colleagues with the necessary user permissions can use the button in live mode.

What if my user permissions change after I have added an overlay button?

Changes to your user permissions will affect the way you can use any buttons and they will either appear dimmed or available depending on whether or not you have user permissions for those actions. For example, if you add a button for an action you do not have user permissions to perform and then your user permissions change so that you do have the necessary user permissions, the button will change to available.

How do I delete an overlay button?

In setup mode, right-click the button, and select **Delete**.

Will overlay buttons appear in exported video?

No, if you export video, overlay buttons are not included in the export.

Glossary

A

access control
A security system that controls the entering of persons, vehicles, or others into a building or area.

adaptive streaming
A feature that improves the video decoding capability and thereby the general performance of the computer running XProtect Smart Client or another video viewing client.

alarm
Incident defined on surveillance system to trigger an alarm in XProtect Smart Client. If your organization uses the feature, triggered alarms are displayed in views that contain alarm lists or maps.

archiving
The automatic transfer of recordings from a camera's default database to another location. This way, the amount of recordings you are able to store will not be limited by the size of the camera's default database. Archiving also makes it possible to back up your recordings on backup media of your choice.

aspect ratio
Height/width relationship of an image.

AVI
A popular file format for video. Files in this format carry the .avi file extension.

B

bookmark
An important point in a video recording, marked and optionally annotated so that you and your colleagues will easily be able to find it later.

C

cardholder
A person that possesses a card that is recognizable to an access control system and gives access to one or more areas, buildings or similar. See also access control.

carousel
A particular position for viewing video from several cameras, one after the other, in a view in XProtect Smart Client.

cluster
a grouping of devices or plug-in elements – or a combination - on the smart map displayed visually as a circular icon with a number. Clusters appear on certain zoom levels indicating the number of devices or plug-in elements within a particular geographical area.

codec
A technology for compressing and decompressing audio and video data, for example in an exported AVI file.

CPU
Short for "central processing unit", the component in a computer that runs the operating system and applications.

custom overlay
A user-defined, graphic element that users can add to a smart map, for example to illustrate a floor plan in a building, or to mark borders between regions. A custom overlay can be an image, a CAD drawing, or a shapefile.

D

deadzone
A deadzone determines how much a joystick handle should be allowed to move before information is sent to the system. Ideally, a joystick handle should be completely vertical when not used, but many joystick handles lean at a slight angle. When

joysticks are used for controlling PTZ cameras, even a slightly slanting joystick handle could cause PTZ cameras to move when it is not required. Being able to configure deadzones is therefore often desirable.

DirectX
A Windows extension providing advanced multimedia capabilities.

E

event
A predefined incident occurring on the surveillance system; used by the surveillance system for triggering actions. Depending on surveillance system configuration, events may be caused by input from external sensors, by detected motion, by data received from other applications, or manually through user input. The occurrence of an event could, for example, be used for making a camera record with a particular frame rate, for activating outputs, for sending e-mails, or for a combination thereof.

evidence lock
A video sequence that is protected, so it cannot be deleted.

external IDP
An external entity that can be associated with the XProtect VMS to manage user identity information and provide user authentication services to the VMS.

F

FIPS
Short for "Federal Information Processing Standards".

FIPS 140-2
A U.S. government standard that defines the critical security parameters that vendors must use for encryption before selling the software or hardware to U.S. government agencies.

fisheye lens
A lens that allows the creation and viewing of 360° panoramic images.

FPS
Frames Per Second, a measure indicating the amount of information contained in video. Each frame represents a still image, but when frames are displayed in succession the illusion of motion is created. The higher the FPS, the smoother the motion will appear. Note, however, that a high FPS may also lead to a large file size when video is saved.

frame rate
A measure indicating the amount of information contained in motion video. Typically measured in FPS (Frames Per second).

G

GOP
Group Of Pictures; individual frames grouped together, forming a video motion sequence.

GPU
Short for "graphics processing unit", which is a processor designed to handle graphics operations.

H

H.264/H.265
A compression standard for digital video. Like MPEG, the standard uses lossy compression.

hotspot
A particular position for viewing magnified and/or high quality camera images in XProtect Smart Client views.

I

i-frame
Short name for intraframe. Used in the MPEG standard for digital video compression, an I-frame is a single frame stored at specified intervals. The I-

frame records the entire view of the camera, whereas the following frames (P-frames) record only the pixels that change. This helps greatly reduce the size of MPEG files. An I-frame is similar to a keyframe.

J

JPEG
An image compression method, also known as JPG or Joint Photographic Experts Group. The method is a so-called lossy compression, meaning that some image detail will be lost during compression. Images compressed this way have become generically known as JPGs or JPEGs.

K

keyframe
Used in the standard for digital video compression, such as MPEG, a keyframe is a single frame stored at specified intervals. The keyframe records the entire view of the camera, whereas the following frames record only the pixels that change. This helps greatly reduce the size of MPEG files. A keyframe is similar to an i-frame.

L

layer
The geographic background on a smart map, a custom overlay, or a system element, for example a camera. Layers are all the graphic elements that exist on the smart map.

LPR
Short for "license plate recognition".

M

MAC address
Media Access Control address, a 12-character hexadecimal number uniquely identifying each device on a network.

map
1) XProtect Smart Client feature for using maps, floor plans, photos, etc. for navigation and status visualization. 2) The actual map, floor plan, photo, etc. used in a view.

Matrix
A product integrated into some surveillance systems, which enables the control of live camera views on remote computers for distributed viewing. Computers on which you can view Matrix-triggered video are known as Matrix-recipients.

Matrix-recipient
Computer on which you can view Matrix-triggered video.

MIP
Short for "Milestone Integration Platform".

MIP element
A plug-in element added through the MIP SDK.

MIP SDK
Short for "Milestone Integration Platform software development kit".

MKV
Short for "Matroska Video". An MKV file is a video file saved in the Matroska multimedia container format. It supports several types of audio and video codecs.

MPEG
A group of compression standards and file formats for digital video, developed by the Moving Pictures Experts Group (MPEG). MPEG standards use so-called lossy compression as they store only the changes between keyframes, removing often considerable amounts of redundant information: Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change. This helps greatly reduce the size of MPEG files.

O

operator
A professional user of an XProtect client application.

output
Data going out of a computer. On IP surveillance systems, output is frequently used for activating devices such as gates, sirens, strobe lights, and more.

overlay button
A button appearing as a layer on top of the video when you move your mouse cursor over individual view items with cameras when in live mode. Use overlay buttons to activate speakers, events, output, move PTZ cameras, start recording, clear signals from cameras.

P

P-frame
Short name for predictive frame. The MPEG standard for digital video compression uses P-frames together with I-frames. An I-frame, also known as a keyframe, is a single frame stored at specified intervals. The I-frame records the entire view of the camera, whereas the following frames (the P-frames) record only the pixels that change. This helps greatly reduce the size of MPEG files.

pane
Small groups of buttons, fields and more located in the left side of the XProtect Smart Client window. Panes give you access to the majority of the XProtect Smart Client features. Exactly which panes you see depends on your configuration and on your task, for example on whether you are viewing live video when in live mode or recorded video when in playback mode.

patrolling profile
The exact definition of how patrolling with a PTZ camera is carried out, including the sequence for moving between preset positions, timing settings, etc. Also known as a "patrol scheme".

port
A logical endpoint for data traffic. Networks use different ports for different types of data traffic. Therefore, it is sometimes, but not always, necessary to specify which port to use for particular data communication. Most ports are used automatically based on the types of data included in the communication. On TCP/IP networks, port numbers range from 0 to 65536, but only ports 0 to 1024 are reserved for particular purposes. For example, port 80 is used for HTTP traffic which is used when viewing web pages.

PoS
Short for "Point of Sale" and typically refers to a cash register or cashier counter in a retail shop or store.

privacy mask
A blurred or solid color that covers an area of the video in the camera view. The defined areas are blurred or covered in live, playback, hotspot, carousel, smart map, smart search, and export modes in the clients.

PTZ
Pan-tilt-zoom; a highly movable and flexible type of camera.

PTZ patrolling
The automatic turning of a PTZ camera between a number of preset positions.

PTZ preset
Can be used for making the PTZ camera automatically go to particular preset positions when particular events occur, and for specifying PTZ patrolling profiles.

Q

QVGA
A video resolution of 320×240 pixels. QVGA stands for "Quarter Video Graphics Array" and is named as such because the resolution 320×240 pixels is a quarter of the size of the standard VGA resolution which is 640×480 pixels.

R

recording
In IP video surveillance systems, the term recording means saving video and, if applicable, audio from a camera in a database on the surveillance system. In many IP surveillance systems, all of the video/audio received from cameras is not necessarily saved. Saving of video and audio in is in many cases started only when there is a reason to do so, for example when motion is detected, when a particular event occurs, or when a specific period of time begins. Recording is then stopped after a specified amount of time, when motion is no longer detected, when another event occurs or similar. The term recording originates from the analog world, where video/audio was not taped until the record button was pressed.

S

SCS
File extension (.scs) for a script type targeted at controlling XProtect Smart Client.

Sequence Explorer
The Sequence Explorer lists thumbnail images representing recorded sequences from an individual camera or all cameras in a view. The fact that you can compare the thumbnail images side-by-side, while navigating in time simply by dragging the thumbnail view, enables you to very quickly assess large numbers of sequences and identify the most relevant sequence, which you can then immediately play back.

smart map
A map functionality that uses a geographic information system to visualize devices (for example, cameras and microphones), structures, and topographical elements of a surveillance system in geographically accurate, real-world imagery. Maps that use elements of this functionality are called smart maps.

smart search
A search feature that lets you find video with motion in one or more selected areas of recordings from one or more cameras.

Smart Wall control
A graphical representation of a video wall that allows you to control what is displayed on the different monitors.

Smart Wall preset
A predefined layout for one or more Smart Wall monitors in XProtect Smart Client. Presets determine which cameras are displayed, and how content is structured on each monitor on the video wall.

snapshot
An instant capture of a frame of video at a given time.

still image
A single static image.

T

TCP
Transmission Control Protocol; a protocol (i.e. standard) used for sending data packets across networks. TCP is often combined with another protocol, IP (Internet Protocol). The combination, known as TCP/IP, allows data packets to be sent back and forth between two points on a network for longer periods of time, and is used when connecting computers and other devices on the Internet.

TCP/IP
Transmission Control Protocol/Internet Protocol; a combination of protocols (i.e. standards) used when connecting computers and other devices on networks, including the Internet.

V

view
A collection of video from one or more cameras, presented together in XProtect Smart Client. A view may include other content than video from cameras, such as HTML pages and static images. A view can be private (only visible by the user who created it) or shared with other users.

VMD
Video Motion Detection. In IP video surveillance systems, recording of video is often started by detected motion. This can be a great way of avoiding unnecessary recordings. Recording of video can of course also be started by other events, and/or by time schedules.

VMS
Short for "Video Management Software".

X

XProtect Transact
Product available as an add-on to surveillance systems. With XProtect Transact, you can combine video with time-linked Point of Sale (PoS) or ATM transaction data.

helpfeedback@milestone.dk

About Milestone

Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone Systems enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone Systems is a stand-alone company in the Canon Group. For more information, visit https://www.milestonesys.com/.