MAKE THE
WORLD SEE

Milestone Systems

XProtect® Smart Client 2019 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.

Overview

About this manual

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 Management Client. See the Administrator guide.

What will you find in the different sections of the manual?

Overview

Introductory information about XProtect Smart Client, including what is new in the current release, and add-on products.

Licensing

Everything you need to know about licensing in XProtect Smart Client.

Requirements and considerations

Things you should be aware of before installing XProtect, for example system requirements.

Installation

Information about how to install XProtect Smart Client.

Configuration

Most of the configuration is done by your system administrator in Management Client, but there are some areas that must be configured in XProtect Smart Client, for example views.

If you know that your system administrator has already configured the necessary views for you, or prepared other features, you may skip parts of this manual.

Optimization

Things you can do to optimize the user experience, for example enabling hardware acceleration.

Operation

This section is all about how to use the features in XProtect Smart Client, for example how to play back recorded video and export video recordings and still images.

Even if you are not a system administrator, there are things you can do to change the behavior of these features. In many cases, the help topics in the **Operation** section provides helpful links to the **Configuration** section, and vice versa.

Troubleshooting

Sometimes you run into problems. Try the **Troubleshooting** section if you cannot make things work - before contacting support.

Upgrade

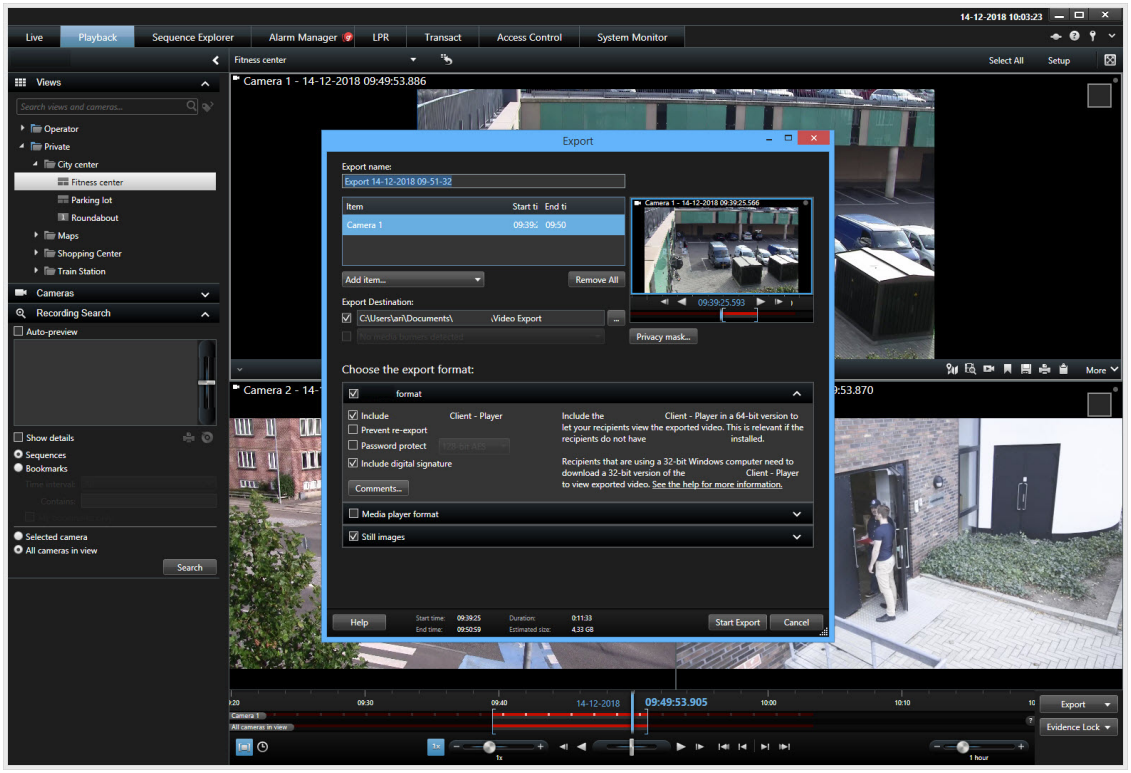
Information about when an upgrade is required.

> Depending on your user rights and the type of XProtect system you connect to, certain features in XProtect Smart Client may not be available to you. Ask your system administrator if in doubt.
>
> References made to the positioning of user interface elements presume that you are using a visual left-to-right interface. For some languages, you can change this to a visual right-to-left interface. If you set the interface to right-to-left, buttons, toolbars, and panes may be reversed compared to where its position is described in this documentation.

XProtect Smart Client (explained)

Designed for Milestone XProtect® IP video management software, the XProtect Smart Client is an easy-to-use client application that provides intuitive control over security installations. Manage security installations with XProtect Smart Client which gives users access to live and recorded video, instant control of cameras and connected security devices, and an overview of recordings.

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.



The interface allows you to tailor your viewing experience to specific working environments by selecting a light or dark theme. It also features work-optimized tabs and an integrated video timeline for easy surveillance operation.

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.

XProtect Smart Client must be installed on operators' computers. Surveillance system administrators manage access to the surveillance system through the Management Client.

What's new?

In XProtect Smart Client 2019 R1

Export: During export, you can include a 64-bit XProtect Smart Client – Player, which supports H.265 video compression.

New help system (F1):

- The content is organized according to where you are in the software usage life-cycle, for example **Installation**, **Configuration**, and **Operation**. See About this manual on page 18
- The connection between configuring and operating XProtect Smart Client is more transparent through links
- Improved terminology support: hover over terms to view their definitions
- Improved navigation: a breadcrumb bar always tells you where in the manual you are. When you open a topic, for example through **Search**, the table of contents immediately syncs up
- More dynamic and responsive look and feel, for example clickable thumbnail images

In XProtect Smart Client 2018 R3

Smart map:

- Not only can you jump to a camera on the smart map, but you can jump to a camera on a specific level inside a building. For more information, see Jump to camera on smart map on page 217.
- When you share the smart map through a Smart Wall, the current zoom level, location, and layers are maintained.
- Improved Windows scaling support.
- Add MIP plug-in elements to smart maps and to buildings in smart maps.

XProtect Smart Wall: In Smart Wall view items, each Smart Wall is listed by its name.

In XProtect Smart Client 2018 R2

Multistory buildings on the smart map:

- You can create buildings with any number of levels. You navigate the levels through a pane that appears when you select a building. For more information, see Add buildings to smart map on page 87
- You can specify a default level for a building. When you select the building, you immediately jump to the default level. For more information, see Set default level for buildings (smart map) on page 90

- You can add cameras and attach them to specific levels. This helps you navigate the cameras level by level. For more information, see Add cameras to buildings (smart map) on page 93
- To help you illustrate the interior of a building, you can add floorplans as custom overlays to the levels. This lets you position cameras in a precise manner. For more information, see Add floorplans to levels (smart map) on page 91

In XProtect Smart Client 2018 R1

- The computer running XProtect Smart Client can use NVIDIA® and Intel® display adapters for hardware accelerated decoding. You can add multiple NVIDIA display adapters for better XProtect Smart Client performance and monitor the CPU and NVIDIA GPU load from the system monitor. For more information, see Hardware acceleration (explained) on page 122
- Users with sufficient rights can temporarily lift privacy masks and thereby view the video underneath. This applies only for privacy masks created as liftable masks in the Management Client. For more information, see Privacy masking (explained) on page 208
- You can use hotspots to quickly shift between cameras on your smart map. By selecting a camera on the smart map, the video feed is displayed in the hotspot view item. For more information, see Use hotspot to view video from cameras on smart map on page 216
- The help is now available as webhelp that you can navigate using your standard browser. It has a more 'webbish' look and feel

Surveillance system differences

Most of the features available in XProtect Smart Client are available in all versions of the XProtect products, but some features work differently depending on what XProtect product you connect to. If in doubt, ask your surveillance system administrator about which type of XProtect surveillance system you connect to. For a detailed outline of the features available on your particular system, see the XProtect software key features on: https://www.milestonesys.com/solutions/platform/product-index/.

In general, 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.

Add-on products

XProtect Smart Wall (explained)

This add-on product is available only for selected surveillance systems (see Surveillance system differences on page 21). Your user rights may restrict your access to certain features.

XProtect Smart Wall is a collaboration tool that lets you provide security personnel with a rich visual overview of the areas you want to keep an eye on. One or more operators can share a variety of content, such as video, images, maps, text, and HTML pages on monitors and video walls to help security teams respond to incidents quickly and effectively.

Typically, Smart Wall is used by operators in command centers, city surveillance, traffic control centers, and so on.

XProtect Access (explained)

The use of XProtect Access requires that you have purchased a base license that allows you to access this feature within your XProtect system. You also need an access control door license for each door you want to control.

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.

- On the **Live** tab, you can monitor access control events in real time from the cameras associated with a door (see XProtect Access (explained)). In setup mode, you can customize your **Access Monitor** view items with overlay buttons (see Customize your view on page 106). In a map view item you can drag Access Control units onto the map (see Monitor doors via maps on page 244)
- On the **Access Control** tab, you can view and investigate events, door states, or cardholders (see Investigating access control events on page 245). 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 (see XProtect Access (explained)). 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 for previewing video associated with individual LPR events. Below the preview, information about the license plate appears together with details from the license plate match list it is associated with.

You can filter the event list according to the period, country module, LPR camera, or license plate match list. Use the **Search** field to search for a particular license plate number. By default, this list shows LPR events from the last hour.

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

You can make updates to the existing match lists by using the **License Plate 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 video previewer that allows you to review the recordings. Below the video previewer, 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.

Requirements and considerations

Minimum system requirements

For information about the minimum system requirements to the various components of your system, go to the Milestone website (https://www.milestonesys.com/systemrequirements/).

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

- Click **Start**, select **Run** and type **dxdiag**. When you click **OK**, the **DirectX Diagnostic Tool** window opens

The version information is displayed near the bottom of its **System** tab. Should the server require a DirectX update, the latest versions of DirectX are available from the Microsoft website (https://www.microsoft.com/downloads/).

Installation

Install XProtect Smart Client

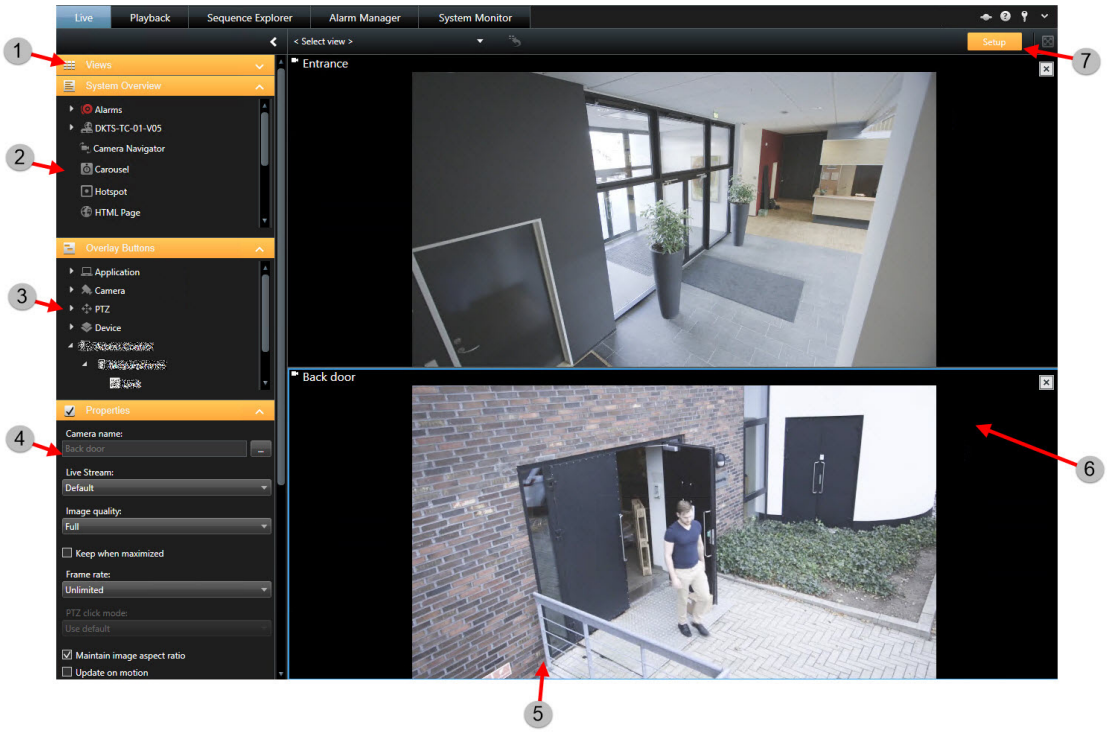
You must install XProtect Smart Client on your computer before you can use it. You download XProtect Smart Client from the surveillance system server and install it on your computer.

1. Open Internet Explorer and connect to the management server using the URL or IP address of the server. Enter one of the following:
   - Local server (http://localhost/installation)
   - IP address of the remote server (http://[IP_address]/installation)
2. On the **Welcome** page, click **Language** and select the language you want to use.
3. The **XProtect Smart Client setup** wizard starts. 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

Setup mode overview

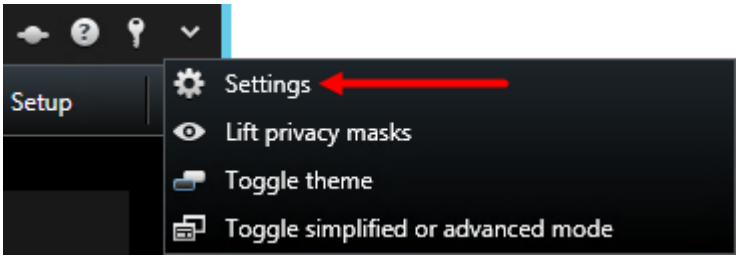


1. Create views (see Create view on page 43).
2. Add content to views (see Adding content to views or Smart Wall on page 45).
3. Add overlay buttons (see Overlay buttons (explained) on page 61).
4. Set the camera properties (see Camera settings (explained) on page 55).
5. Create and manage views (see Configuring views on page 40).
6. Add cameras to views (see Add camera to view on page 45).
7. In setup mode, in the navigation pane, buttons and panes are highlighted in orange.

Settings window (explained)

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. For languages where your normally read and write from right to left, you can choose to enforce a visual left-to-right interface if needed.

Open the **Settings** window from the application toolbar:



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	Select how the XProtect Smart Client reacts when you maximize it by clicking the **Maximize/Restore** button in the application toolbar. If you select **Maximize to full screen**, the XProtect Smart Client will cover any Windows task bar on your screen when maximized.  Maximization is not the same as full screen viewing (see Application settings).
Camera error messages	Select how the XProtect Smart Client displays camera-related message texts. These can be displayed as an overlay on top of the camera image or on a black background. You can also choose to hide such messages completely.
Server error messages	Select how the XProtect Smart Client displays server-related message texts. These can be displayed as an overlay or hidden completely.
Default for video indicator	Select whether to show or hide the green video indicator on the camera title bar. Lights up when connection to the camera is established. You can override this setting on individual cameras by adjusting camera properties (see Camera settings (explained) on page 55) in setup mode.

Name	Description
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 (see Camera names and colored indicators (explained) on page 145) signifying events, detected motion, and video recordings.  You can override this setting on individual cameras by adjusting camera properties (see Camera settings (explained) on page 55) for the camera(s) in setup mode.
Show current time in title bar	Select 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	Select what to show if there are empty positions in views, for example, you can select a logo or have just a black background displayed.
View grid spacer	Select the thickness of the border between camera positions in views.
Default image quality	Select a default for the quality of video viewed in the XProtect Smart Client. 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**.  You can override this setting on individual cameras by adjusting camera properties (see Camera settings (explained) on page 55) 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 (see Camera settings (explained) on page 55) for the camera(s) in setup mode.
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.
Start mode	Select 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	Select whether the XProtect Smart Client displays a view immediately after you have logged in. Options are: the view you last used, no view, or that you decide after you have logged in.

Name	Description
Hide mouse pointer	Lets you select 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 • 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.

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 rights or the surveillance system (see Surveillance system differences on page 21) 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 on the **Live** tab) 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.

Functions:

Name	Description
Live > Camera playback	The ability to play back recorded video from individual cameras on the **Live** tab.
Live > Overlay buttons	The ability to view and use overlay buttons on the **Live** tab 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 (see Bookmarks (explained) on page 194) from the view position toolbar or through ready-made overlay buttons on the **Live** or the **Playback** tab. Enabling or disabling this option on the **Playback** tab will control whether or not the corresponding button is enabled on the **Sequence Explorer** tab. The bookmark feature is only available if connected to certain surveillance systems (see Surveillance system differences on page 21). Depending on your user rights, access to adding bookmarks from some cameras may be restricted. You may be able to view bookmarks even though you may not be able to add them, and vice versa.
Live and **Playback > Print**	The ability to print from the **Live** and **Playback** tab. Enabling or disabling this option on the **Playback** tab will control whether or not the corresponding button is enabled on the **Sequence Explorer** tab.
Live and **Playback > Bounding boxes**	The ability to show bounding boxes on live video on the **Live** tab or on recorded video on the **Playback** tab on all cameras. Bounding boxes are used for, for example, tracking objects. The bounding box feature is only available if connected to certain surveillance systems (see Surveillance system differences on page 21) and to cameras that support metadata. Depending on your user rights, access to bounding boxes from some cameras may be restricted.
Playback > Independent playback	The ability to play back recorded video from individual cameras independently on the **Playback** tab, where all cameras in a view otherwise by default display recordings from the same point in time (the playback time).

Name	Description
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 (see Camera settings (explained) on page 55) 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.
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 you want to export to.

Name	Description
Privacy mask	Select if 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 the Management Client, on the **Privacy masking** tab.
Media player format	Select whether or not you can export in media player format.
Media player format - Video texts	Select whether you want video texts to be optional, required or unavailable when you export in media player format. With video texts, the user can add overlay text on the exported recordings.
Media player format - Video codec properties	Select if you want codec configuration to be available or not when you export in 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 XProtect format.
XProtect format - Project comments	Select whether you want project comments to be optional, required or unavailable when you export in 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 Management Client.

Name	Description
OpenStreetMap geographic background	Specify whether the OpenStreetMap service can be used as a geographic background. If you select **Unavailable**, XProtect Smart Client does not display it as an option.
Alternative OpenStreetMap tile server	To use a different tile server (see Change OpenStreetMap tile server on page 74) for your OpenStreetMap than the one specified in the configuration, 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 Add custom overlay on smart map on page 78.

Name	Description
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.
Remove cached Smart Map files	Smart map saves to the cache on your local computer so that it can load faster. Use this setting to specify how often you want to remove the cached files.

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 (explained) on page 143), 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 **Playback** tab • **Live mode**: Only on the **Live** tab • **Setup mode**: Only in setup mode
Categories	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 position 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 position (view position 1).

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).
Axis setup: Action	Select the function for an axis: Camera PTZ Pan, Camera PTZ Tilt, Camera PTZ Zoom, or 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.

Name	Description
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 position 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 position (view position 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.

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 Control Notifications**.

Alarm settings

In **Alarm** settings, you can:

- Select whether or not you want alarms to play sound notifications
- 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

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 21), 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 Management Client's 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 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.

Name	Description
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 camera position. **Auto** is the default setting. Auto means means that the computer uses as many threads per camera position 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. 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 camera positions, in all views, in live as well as playback mode. You cannot specify the setting for individual camera positions or views. Because this setting may not be equally ideal for all of your camera positions 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.

Name	Description
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 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%.

Name	Description
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 system performance.
Time zone	Select a predefined time zone or a custom time zone. The available options are: **Local**: the time zone of the computer running the XProtect Smart Client **Master Server's 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 from, for example, XProtect Access.
PDF report font	Select a font to be used in your PDF reports.

Language settings

Specify the language version of your XProtect Smart Client. Select from the list of available languages and then restart the XProtect Smart Client for the change to take effect.

Configuring views

In setup mode, you can create groups and views, and specify which cameras should be included in each view. 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.

Your ability to edit views and groups depends on your user rights. Basically, if you can create the view or group, you can also edit it. If in doubt, contact your system administrator.

Private and shared views (explained)

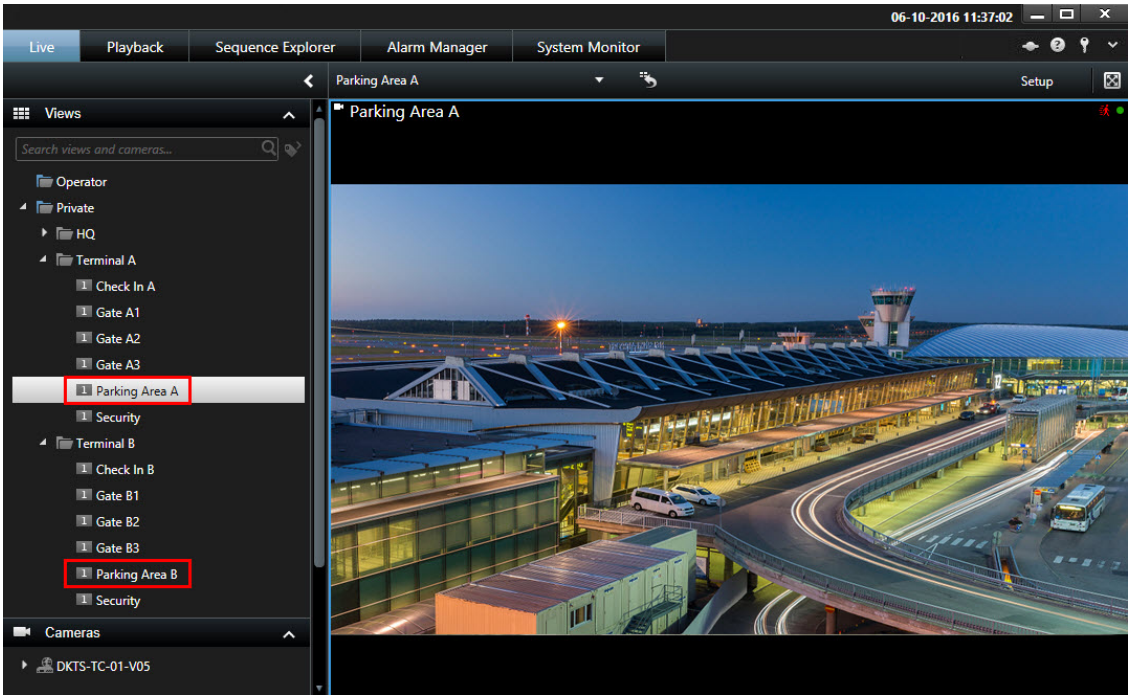
Views can be private or shared:

- **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 many XProtect Smart Client users to share the same views. This is possible because all views are stored on the surveillance system server. Depending on your type of surveillance system (see Surveillance system differences on page 21):
    - There may be a default folder for shared views named **Shared** or **Default group**
    - Shared views can be shared by all XProtect Smart Client users, or access to selected shared views can be given to certain XProtect Smart Client users. Typically, only a few people in an organization can create and edit shared views. For example, the system administrator may create and maintain a number of shared views, so users do not need to create their own views

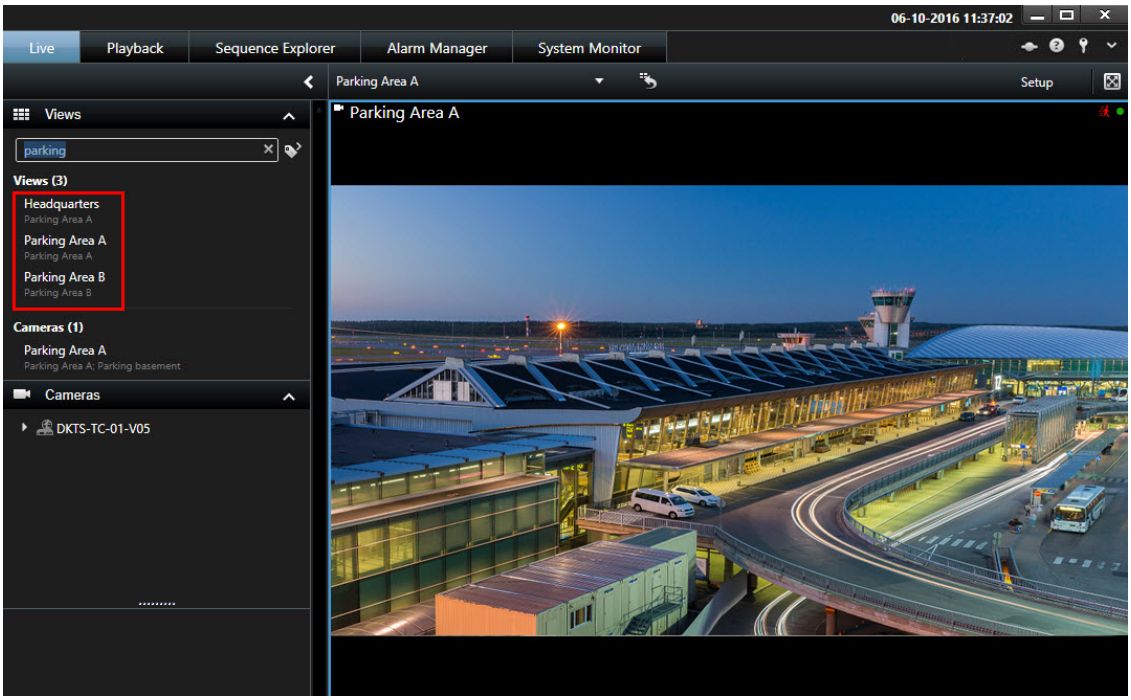
Not all users may have access to all cameras on the surveillance system. Some of the features you include in your shared view may not be supported in earlier versions of XProtect Smart Client. Always make sure that the users you want to share with have the necessary rights and are running the same XProtect Smart Client version as yourself. To check your XProtect Smart Client version, click in the top right corner of the XProtect Smart Client window.

Views and view groups (explained)

If you have a large or complex hierarchy of view groups, the search function does not only ease the navigation. It also adds the ability to search across the existing structure. How well this goes, depends on your organization having worked out a well considered and consistent naming convention for views and cameras.



The example below shows the benefit of searching instead of navigating through a complex hierarchy when you need to get an overview of related views:



You can search for views that contain specific cameras or view item types. For example, if you want to see all views that contain PTZ cameras, cameras from a certain manufacturer or views that contain these view item types:

- Map
- Alarm
- Matrix
- HTML
- Name of camera in view
- Add-on products

Finally, you can search for keywords.

Create a view group

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 view

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. For more information, see Create a view group on page 43.

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 the setup mode.

Views can be private or shared (see Private and shared views (explained) on page 41).

Copy, rename, or delete a view or group

Views can only be copied within the same session; you cannot copy views from one XProtect Smart Client to another.

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.

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 copy the view, 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, click **Rename**.

   Or right-click and select **Rename**.

- To delete a view, select the relevant view, and either click **Delete**.

  Or right-click and select **Delete**.

Deleting a group will delete all views and any subgroups within the group as well.

Adding content to views or Smart Wall

Apart from cameras, there are other elements that you can add to the views or Smart Wall, for example alarms, hotspots, and maps. For more information, see Content inside views (explained) on page 139 or the topics in this section.

Add camera to view

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

   Often, you will only see a single server, but if you are connected to a large surveillance system, you may see a hierarchy of several servers. 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 the position in the view. An image from the camera appears in the selected position. If a connection cannot be established, just the camera name is displayed.

   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 208).

4. You can specify the camera properties (such as quality, frame rate and more) in the **Properties** pane. For more information, see Camera settings (explained) on page 55.

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 under a server, drag the folder to the view. Make sure a sufficient number of positions are available in the view.

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

Add Smart Wall overview to view

After your system administrator has set up your Smart Wall in the Management Client, you can add it to one or more views.

Steps:

1. Click **Setup** to enter setup mode.
2. Select the view where you want to add the Smart Wall.

   Wide layouts are especially suitable for displaying Smart Wall content. The bottom of the 1+1+2 view provides a wide position ideal for displaying Smart Wall content. The 1×3 view can graphically represent three different Smart Wall setups at the same time.

3. In the **System Overview** pane, drag the **Smart Wall** element to the relevant view item. The view item now contains a graphical representation of the Smart Wall.
4. Click **Setup** again to exit setup mode.
5. If your organization has more than one Smart Wall, select the relevant Smart Wall.
6. If the Smart Wall has more than one preset, select the relevant preset in the **Preset** list. Presets contain predefined settings that determine which cameras are displayed, and how content is structured on each monitor on the video wall.

After selecting a Smart Wall and a preset, other users can select a different Smart Wall, preset, or both.

Add image to view or Smart Wall

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

If you are sharing an image with users or Smart Walls that cannot access the network location of the image file, you can embed the image. When you embed an image it is stored in Smart Client, and the connection to the original file location is removed. If you remove or replace an embedded image from a Smart Wall and want to display it again, you must add the image file to the Smart Wall again.

Steps:

1. Click the **Setup** button to enter setup mode.
2. In the **System Overview** pane, drag the **Image** item to a position in the view.
3. Select the image file that you want to add, and then click **Open**.
4. 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.
5. To send the image to your Smart Wall, in the toolbar of the view item, click **More** > **Send to Smart Wall**.
6. Select the Smart Wall, the monitor, and the tile where you want the image to appear.
7. Repeat steps 5-6 for each Smart Wall that you want to send the image to.

Add text to view item or Smart Wall

You can add text to a view item. If you are using XProtect Smart Wall, afterward you can add the text to your Smart Wall. 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** item to the view item, where you want the text to appear. The **Text Editor** 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.
6. To add the text to your Smart Wall, in the text view item, click **More** > **Send to Smart Wall** and select the monitor and tile in the Smart Wall, where you want the text to appear.

You can insert tables from products such as Microsoft Word and Microsoft Excel, but you cannot make changes to the tables. Additionally, to accommodate for the dark and light themes in XProtect Smart Client, the system tries to change the color format of light or dark

text.

For more information about displaying text on a Smart Wall, see Display text on one Smart Wall on page 233 or Display text on more than one Smart Wall on page 233.

Add carousel to view or Smart Wall

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, click and drag the **Carousel** item to the position in the view.
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.
8. (optional) To change settings for the carousel, in the setup mode, go the **Properties** pane and click **Carousel Setup**.
9. To send the carousel to your Smart Wall, see Display carousel on Smart Wall on page 231.

Add hotspot to view or Smart Wall

When clicking a view item or tile with a camera in a Smart Wall, 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 position in the view. The position 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.
5. To send the hotspot to your Smart Wall, see Display hotspot on Smart Wall on page 231.

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

Add camera navigator to view or Smart Wall

Camera navigators let you set up a complete overview of an area by adding all cameras that cover the area in a single view. For example, this is useful if you want to be able to follow someone around a building. As the person moves, you can switch to the next camera. For more information, see Camera navigator (explained) on page 181.

Steps:

1. Click **Setup** to enter setup mode.

   To get the most out of the camera navigator and to be able to see the camera views in the pane on the right, select a 1 x 1 view.

2. From the **System Overview** pane, drag the **Camera Navigator** to your view.
3. In the **Select Home Map and Camera** window, select the map that you want to base your navigation on.
4. Click the camera that you want to select as the default camera whenever you open the **Camera Navigator**, and then click **OK**.
5. Click **Setup** to exit setup mode.
6. To send the camera navigator to your Smart Wall, see Display camera navigator on Smart Wall on page 234.

Add map to view or Smart Wall

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.
3. In the **Map Setup** window that appears, 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.
9. To display the map on your Smart Wall, see Display map on Smart Wall on page 234.

Add smart map to view

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. For more information, see Change geographic backgrounds on smart maps on page 74.

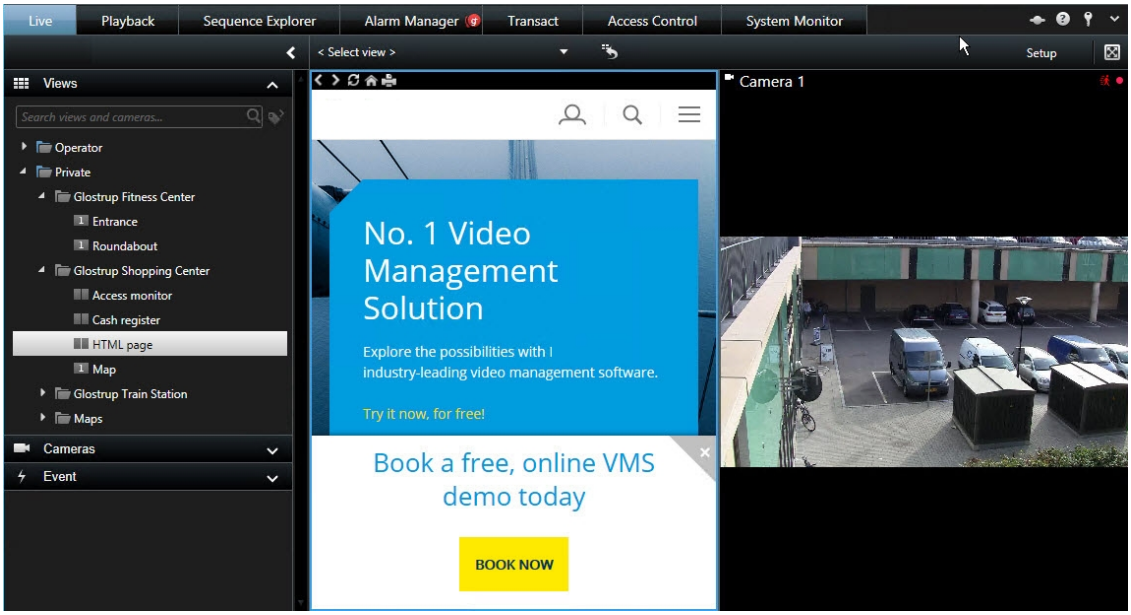
Steps:

1. On the **Live** or **Playback** tabs, select the view where you want to add the smart map.
2. Click **Setup**.
3. Expand the **System Overview** pane, and then drag the **Smart map** item to the view.

For more information, see Smart map (explained) on page 213.

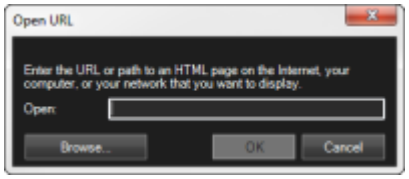
Add HTML page to view or Smart Wall

You can add HTML pages to views and your Smart Wall. For example, this is useful for displaying instructions, company web pages, Internet map services, collections of links, e-learning pages, and so on.



Steps:

1. Click **Setup** to enter setup mode.
2. In the **System Overview** pane, click and drag the **HTML Page** item to the view. The **Open URL** window appears.



3. In the **Open** field, enter the location of the required HTML page (example: **http://www.mywebsite.com/mywebpage.htm**).

   -Or-If the HTML page is stored locally on your computer, do one of the following:

   - Specify its location on your computer (example: C:\myfiles\mywebpage.htm)
   - Click **Browse** to browse for the required HTML page

4. Click **OK**.
5. Click **Setup** again to exit setup mode.
6. (optional) To set the properties, see Set properties for HTML page on page 51.
7. To display the HTML page on your Smart Wall, see Display HTML page on Smart Wall on page 234.

Set properties for HTML page

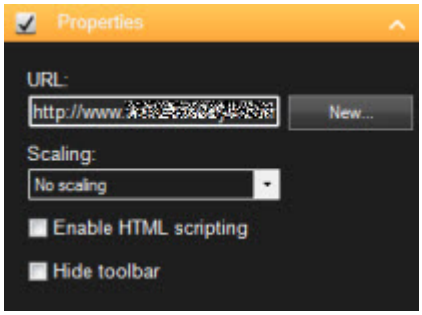
When you have added an HTML page to a view or Smart Wall, you can set the properties, for example the size of text displayed on the HTML page.

Requirements

You have added the HTML page to your view or Smart Wall. For more information, see Add HTML page to view or Smart Wall on page 50.

Steps:

1. Click **Setup** to enter setup mode.
2. Select the imported HTML page in the view.
3. In the **Properties** pane, change one or more of these properties:



- **URL**: Click **New** to specify a new URL or location of the HTML page
- **Scaling**: Select the scaling of the HTML page. The optimal scaling depends entirely on the content of the imported HTML page and how you want to display it

> As a rule, with a high scaling value such as 1280×1024, text on the HTML page will appear relatively small. With a low scaling value, such as 320×200, text on the HTML page will appear relatively large.

- **Enable HTML scripting**: Only select this feature if the HTML page is a custom-made HTML page for navigating or triggering features inside the XProtect Smart Client itself (see examples of custom-made HTML pages in Scripting HTML page for navigation on page 117)

> If selected, a client script required for navigating and controlling a number of features inside the XProtect Smart Client will be added to the HTML page. For HTML pages which are not going to be used for such purposes, the client script cannot be used, and may even cause the HTML page to malfunction.

- **Hide toolbar**: By default, a simple navigation bar is inserted above each imported HTML page. The navigation bar has the following five buttons: **Back**, **Forward**, **Refresh**, **Home** and **Print**:

If you do not want the navigation bar, you can hide it by selecting **Hide toolbar**

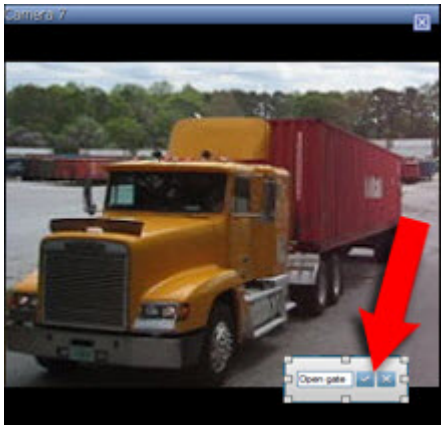
4. Click **Setup** again to exit setup mode.

Add an overlay button to a view

You can activate speakers, events, output, and more through overlay buttons which appear when you move your mouse over individual camera positions in views on the **Live** tab.

You can add as many buttons as needed.

1. In setup mode, in the **Overlay Buttons** pane, select and drag the action onto the camera position.
2. When you release the mouse, the overlay button appears. To resize the button, drag the handles that appear.



3. If you want to change the text of the overlay button, double-click the text, overwrite it, and then click the check mark button to save. To undo, click the cancel button. When you save, the text scales to the largest possible size on the button.

Add alarms to views or Smart Wall

By adding the **Alarm List** to your view or Smart Wall, you can share a list of prioritized alarms that people should address, or just an individual alarm to put focus on one particular incident.

Steps:

1. On the **Views** pane, select the view where you want to add the **Alarm List**.
2. Click **Setup** to enter the setup mode.
3. On the **System Overview** pane, expand **Alarms** and drag the **Alarm List** overview to a view item.
4. Click **Setup** to exit setup mode.
5. To send the alarm list to your Smart Wall, see Display alarms on Smart Wall on page 236.

Permanently 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. On the **Live** or **Playback** tab, 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.

The setting you make in setup mode is stored on the server, so that the change impacts other XProtect Smart Client operators.

Assign a shortcut number to a view

In setup mode, you can assign shortcut numbers to views to let users select views using standard keyboard shortcuts (see Keyboard shortcuts (explained) on page 143).

1. In setup mode, in the **Views** pane, select the view you want to assign a shortcut to.
2. In the **Shortcut** field, specify a shortcut number, and then press ENTER. The shortcut number appears in parentheses in front of the view's name.
3. Repeat as necessary for other views.

Add or edit views in simplified mode

You can select or search for existing views or cameras in the **Select view** list. However, to add or edit views, for example renaming the view or changing a camera, you need to switch to advanced mode.

Steps:

1. In the toolbar, click  and then  to switch to advanced mode.
2. Click **Setup** to enter setup mode.
3. To add a view, see Create view on page 43.
4. To edit a view:
    1. Select the view.
    2. Edit the view.
    3. Click **Setup** again to save the changes.

If the  button is not available, you cannot switch to advanced mode. In that case, please contact your system administrator.

For more information, see Modes in XProtect Smart Client (explained) on page 135.

Configuring camera settings

Camera settings (explained)

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 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.

Name	Description
Image quality	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.  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.

Name	Description
Keep when maximized	When you view live or recorded video, you can double-click a particular camera position in a view 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 **Unlimited** (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 60) 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.
Maintain Image Aspect Ratio	If selected, video will not be stretched to fit the size of the camera position. 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 position in the view; this may lead to slightly distorted video, but you will avoid any black bars appearing around the video.

Name	Description
Update on motion	If selected, video from the selected camera will only be updated on the XProtect Smart Client's **Live** tab 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 position in the view 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 on the **Live** tab, 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 with certain surveillance systems. For a detailed outline of the features available on your particular system, see the XProtect Product Comparison Chart on: https://www.milestonesys.com/. 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 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 on the **Live** tab, 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.

Name	Description
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 camera position. The title bar helps users quickly identify cameras. When displayed on the **Live** tab, the title bar displays information about detected motion and events, whether the camera is recording, etc. See Camera names and colored indicators (explained) on page 145. 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 61) 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 window (explained) on page 27) **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 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**.

Name	Description
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)

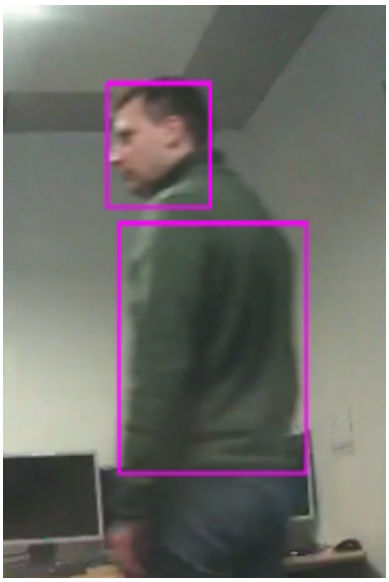
The effect of the frame rate selection can be illustrated as follows:

Effect	Unlimited	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 pink border in video.



You can show/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 (see XProtect format settings on page 168) video in the XProtect format or print (see Print video evidence on page 173) still images.

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 the camera positions in the view 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 21). Auxiliary commands differ from camera to camera; for details, 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 202) 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, consult your surveillance 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 hotspots, carousels, or Matrix (see Matrix) positions.

Frequently asked questions: cameras

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.

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.

What is an event?

An event is a predefined incident occurring on the surveillance system. Depending on the surveillance system's configuration, events may be caused by input from external sensors connected to cameras, by detected motion, by data received from other applications, or manually through user input. Events are used by the surveillance system for triggering **actions**. Typically, most events on the surveillance system are generated automatically. For example, detected motion can be defined as an event which in turn triggers an action, for example, recording.

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- as well as motion-detection notifications. You cannot use different sound files for different cameras or to distinguish between event- and motion-detection notifications.

Configuring camera navigator

Before you can use the camera navigator, you must set up a map (see Add map to view or Smart Wall on page 49) and add cameras to it. When you have added the camera navigator to a view (see Add camera navigator to view or Smart Wall on page 49), you can define properties (see Camera navigator settings on page 62) for how you want the camera navigator to display the views.

Camera navigator settings

In the **Properties** (see Camera settings (explained) on page 55) pane, you can specify these settings for the camera navigator.

Name	Description
Home map and camera	Displays the map and default camera that your camera navigator is based on. You can change these settings, by clicking the … button to open the **Select Home Map and Camera** window.
Maximum camera indicators	Select the maximum number of cameras that you want to include in your main view. Each camera is shown with a camera icon. You can display an unlimited number of cameras.

Name	Description
Camera indicator orientation	Select **Relative to selected camera** if you want to display the location and orientation of the cameras as seen from the camera's perspective or Select **Relative to map** if you want the location and orientation of the cameras to always reflect the layout of the map as seen from above. The selected camera is always the centered one.
Maximum preview cameras	Select the maximum number of cameras that you want to display in your preview pane. Only the cameras that are visible on the screen will use your system's resources. The maximum number of cameras that you can display is 20. The more cameras that you preview, the more of your system resources they will take up.

Carousel settings

In the **Properties** (see Camera settings (explained) on page 55) pane, you can specify the settings for the carousel. The **Live Stream**, **Image Quality**, **Frame Rate**, and **Maintain Image Aspect Ratio** settings apply to all cameras in the carousel.

Hotspot settings

In the **Properties** (see Camera settings (explained) on page 55) 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.

Audio settings

You can listen to recorded audio independently of the views/cameras you are watching. You must specify a time in the **Playback** tab's navigation feature to determine what recorded audio to hear.

Name	Description
Microphones	Select the microphone you want to listen to audio from. 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 (muting speakers is only available on the **Playback** tab).
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 rights 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 **Level 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.

Name	Description
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 (explained) on page 179).

Configuring PTZ presets and patrolling profiles

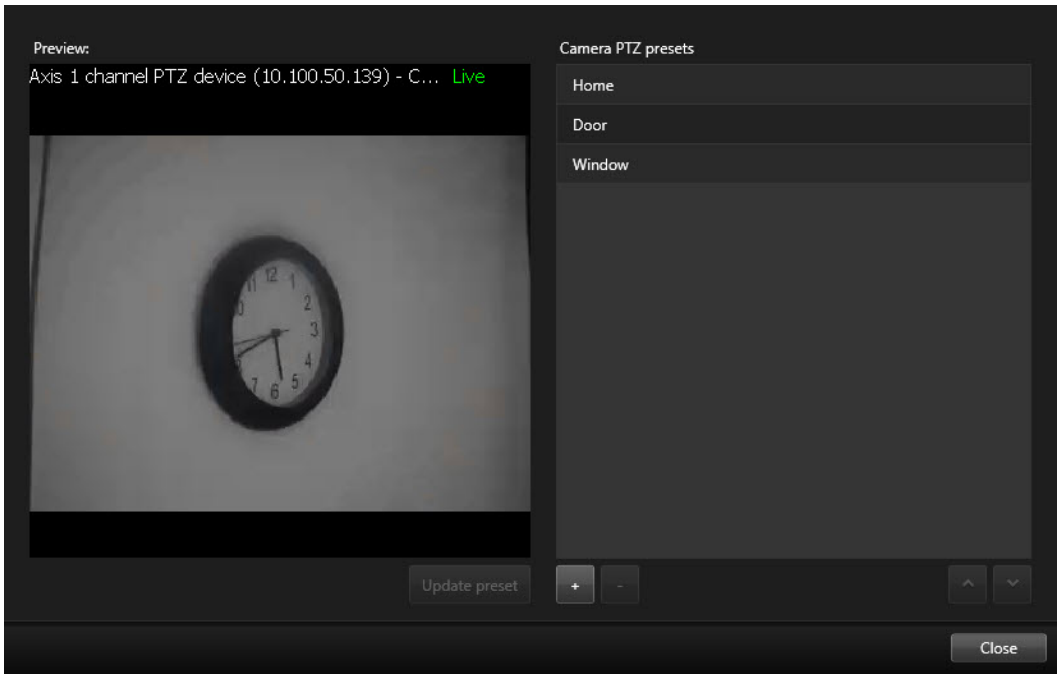
Adding, editing, or deleting PTZ presets

Depending on your surveillance system (see Surveillance system differences on page 21), you can create, edit and delete PTZ presets.

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 dialog box.



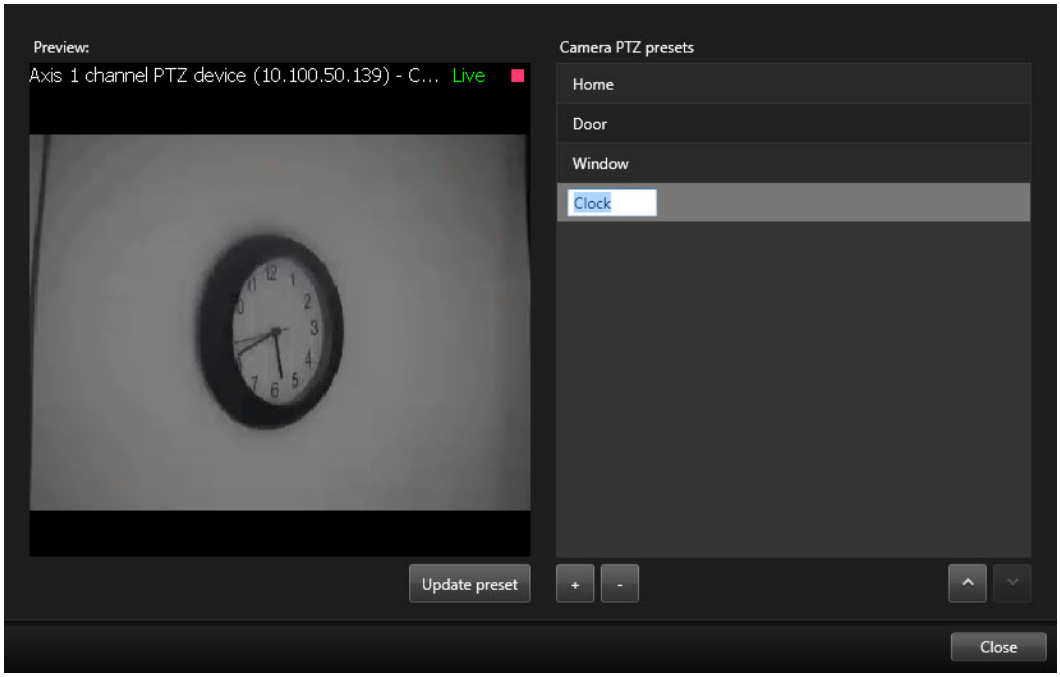
4. Click + to add a new preset entry.
5. Select the PTZ preset entry and type a new name for the PTZ preset.
6. Use the PTZ buttons to navigate to the relevant position and click **Update preset** to save.
7. Use the arrows to move a PTZ preset up or down in the list. This can be useful if your list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

Adding, editing, or deleting patrolling profiles

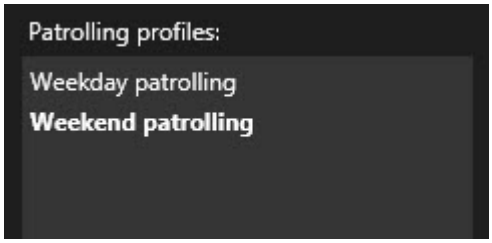
Depending on your surveillance system (see Surveillance system differences on page 21), you can create, edit and delete patrolling profiles.

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. Type 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.

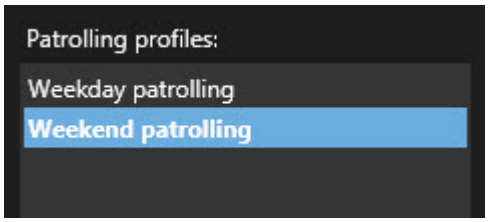
Delete patrolling profile

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

Edit patrolling profile

Specify positions in a patrolling profile

1. Select the patrolling profile:

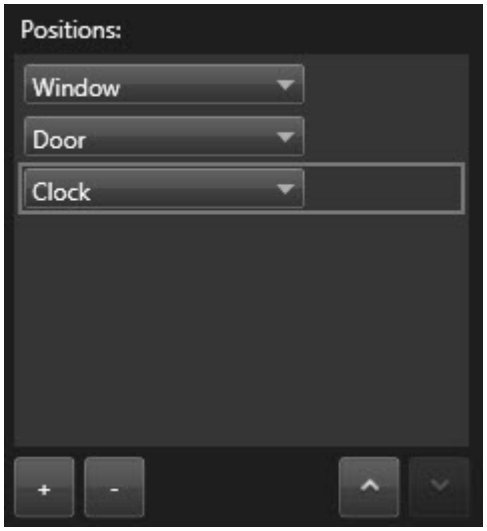


2. Click + below the **Positions** list to add a PTZ preset.

   PTZ presets are defined by your administrator or, depending on user rights, you can do this by clicking the **Manage PTZ presets** (see Adding, editing, or deleting PTZ presets on page 65) button.

3. In the drop-down 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.

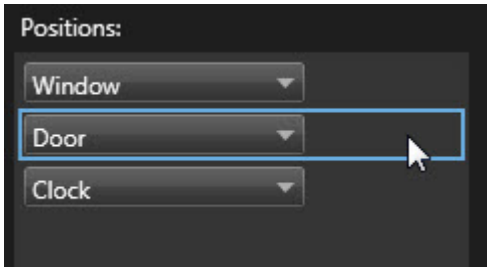
   The camera uses the PTZ preset at the top of the list as the first stop when it patrols according to the patrolling profile. The PTZ preset in the second position from the top is the second stop, and so forth.

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**.

Configuring bookmarks

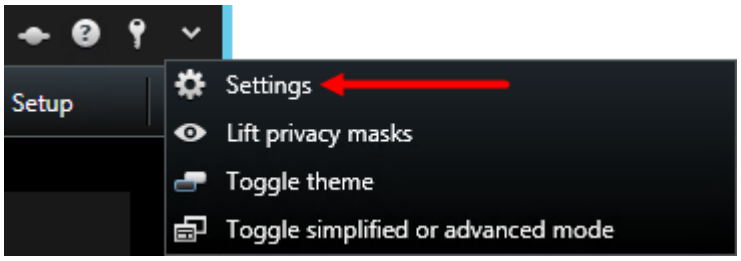
> The bookmark feature is only available for selected surveillance systems (see Surveillance system differences on page 21).

Enable detailed bookmarks

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

Steps:

1. Open the **Settings** window.



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

Configuring alarms and events

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.

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. We recommend that you keep this option selected, because the navigation tree provides an overview of alarm priorities and states, and—not least—the number of alarms in each priority and state.

Name	Description
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 lines, that is up to 100 alarms or events at a time. This provides a good response time, since fetching and displaying larger numbers of alarms or events can take time. There can of course easily be more than 100 alarms or events, and if you want to view more than the first 100 alarms or events, you simply use the buttons in the top right part of the alarm list to browse to the next alarms or events, which will then be fetched and displayed.  In the field, you can set the maximum numbers of rows from 1 to 999, but remember that the more alarms or events in the list, the longer it takes to display the list. If you change the number, note that the number of rows in the list will not be updated until you select another element than the **Max. rows to fetch** field, for example a row in the alarm list.
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.

Configuring smart maps

Before you can take advantage of the smart map features, you are required to perform certain configuration tasks in XProtect Smart Client.

You can only view your smart map if it has been added to a view. See Add smart map to view on page 50.

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 219

- **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 use the Bing Maps and Google Maps services, or the OpenStreetMap map project as geographic backgrounds, and add computer-aided design (CAD) drawings, shapefiles, and images as overlays. For more information, see Smart map (explained) on page 213

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 cameras again. You cannot transfer maps with cameras 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 83.

Geographic backgrounds (explained)

You can use the OpenStreetMap, Google Maps, or Bing Maps services as the geographic background of your smart map. You can also just use the default basic world map. Afterwards, you add the devices, for example cameras, or custom overlays, for example shapefiles. For more information, see Custom overlays (explained) on page 77.

To put custom overlays into focus, you can hide the geographic background. For more information, see Layers on smart map (explained) on page 75.

Types of geographic backgrounds (explained)

After you add a smart map to a view, you can choose 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 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.

- **OpenStreetMap** - connect to the OpenStreetMap (https://www.openstreetmap.org/) (OSM) open source mapping project. This option requires access to the Internet. The map data for OSM is provided under the organization's Open Database License (https://www.openstreetmap.org/copyright/)
- **None** - this hides the geographic background. However, the geo-reference data is still there. For more information, see Layers on smart map (explained) on page 75

By default, Bing Maps and Google Maps display satellite imagery (Satellite). You can change the imagery, for example to aerial or terrain, to see different details. For more information, see Change geographic backgrounds on smart maps on page 74.

Change geographic backgrounds on smart maps

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

Requirements

The Bing Maps and Google Maps geographic backgrounds are available only if your system administrator has set them up.

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**.

Changing OpenStreetMap tile server

If you use OpenStreetMap as the geographic background for your smart map, you can change the location where the tiled images are retrieved. The tiled images make up the map. You do this by changing the tile server address. This allows you to use a local tile server, for example if your organization has its own maps for areas such as airports or harbors. Using a local server means that XProtect Smart Client can retrieve the map images without Internet access.

You can also use a commercial tile server. Milestone does not provide a tile server solution for OpenStreetMap.

The tile server address can be specified in two ways:

- In Management Client - you set the tile server address on the Smart Client profiles. The server address applies to all Smart Client users assigned to the individual Smart Client profiles
- In XProtect Smart Client - you set the tile server address in the **Settings** dialog (see Change OpenStreetMap tile server on page 74). The server address applies only to that Smart Client installation

Change OpenStreetMap tile server

You can specify a different tile server for OpenStreetMap than the standard server specified in the configuration for your type of user profile. For example, if your VMS is not connected to the Internet, you can use a local server. Or you can use a commercial server.

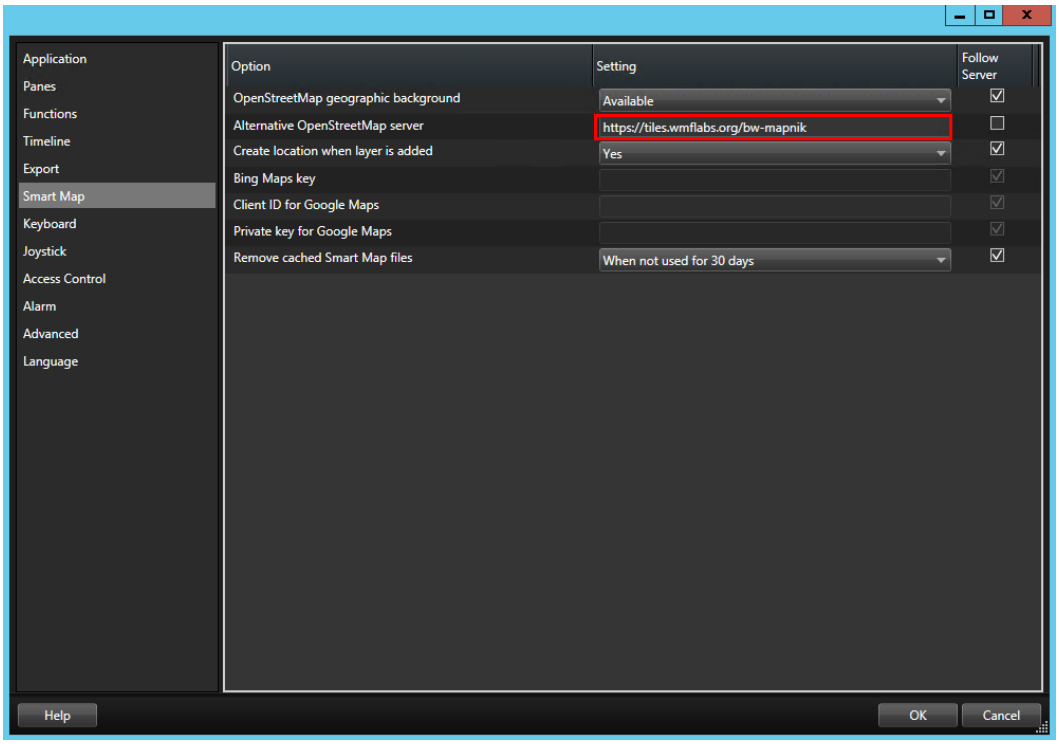
Requirements

If the tile server specified in the configuration has been locked for editing, the field is grayed out in XProtect Smart

Client, and you cannot change the server. Please contact your system administrator to help you enable the feature on the Smart Client profile in Management Client.

Steps:

1. In the upper right corner, click and then **Settings** to open the **Settings** dialog.



2. In the left section, click **Smart map**.
3. In the **Alternative OpenStreetMap tile server** field, do one of the following:
   - Enter the server address. If the field is grayed out, it has been locked in the configuration
   - To use the server specified in the configuration, select the **Follow Server** check box
4. Click **OK**. The geographic background changes.

For more information, see Changing OpenStreetMap tile server on page 74.

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, Bing Maps, Google Maps, or OpenStreetMap

Bing Maps and Google Maps are available as geographic backgrounds only if your system administrator has enabled them in Management Client. For more information, see Geographic backgrounds (explained) on page 73.

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 cameras 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 ap. You rearrange the order by configuring default settings for the map. For more information, see Manage default settings for a smart 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 will still use the spatial reference to place the file on the map.

Manage 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**.

For more information, see Smart map default settings (explained) on page 77.

Smart map default settings (explained)

In the **Manage default settings** window, you can specify the default settings for the custom overlays on your smart map. The default settings include:

- Whether to show or hide one or more custom overlays
- The order, from top to bottom, in which custom overlays display. The first custom overlay in the list is the highest in the order. For example, the order can be helpful when you want to stack overlays to represent levels on a building
- Removing custom overlays from the smart map

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

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 overlay on smart map on page 218. 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 79.

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 77.

Add locations to custom overlays (smart map)

You can enable a setting that allows operators to find and jump to custom overlays, for example images, through the **Select a location** list. When enabled, automatically a location is created when you add a custom overlay to your smart map.

Steps:

1. In the application toolbar, click 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 78.

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 85.

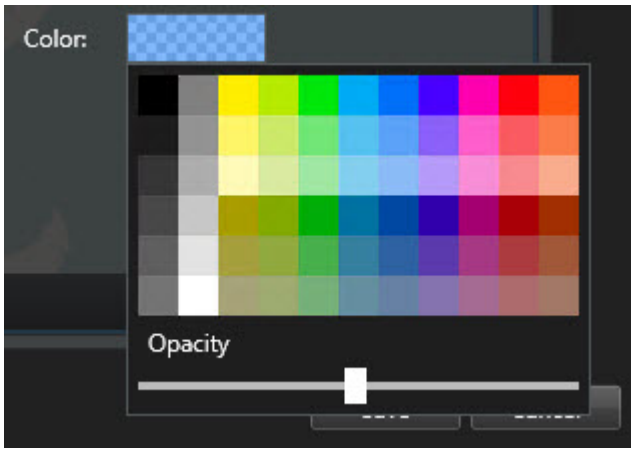
Make areas in shapefiles more visible (smart map)

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 78.
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 cameras on smart map

You can add cameras 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.

Add cameras to smart maps

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

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

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

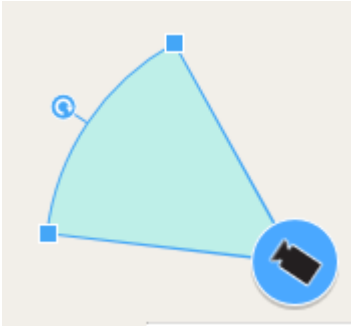
   - Expand the **System Overview** pane, find the camera or camera group, and then drag it to the point on the smart map where you want to display it. You can drag cameras afterward to reposition them
   - On the smart map toolbar, click **Add a camera**, and then select the camera
3. To save the change, 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 you want to work with.
2. Click **Setup** to edit the camera icon.
3. Clickthecameraicon.



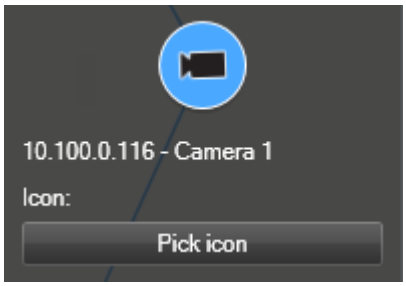
4. Use the rotate handle to point the camera in the right direction.

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 the icon for camera

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

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



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

Show or hide information about cameras

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

1. Select the view that contains the smart map 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.

Deleting cameras on smart map (explained)

All the cameras defined in the system are displayed on the smart map. You can reposition a camera, but you cannot delete it.

If the position of the camera has not been specified in Management Client, it will not appear on the smart map.

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 214.

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**

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. For more information, see Exploring your 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 Custom overlays and locations (explained) on page 78.

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**

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 83.

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 floorplan. For more information, see Add floorplans to levels (smart map) on page 91.

Buildings are automatically given a name, for example **Building 4**. Milestone recommends that you change the name. This will make 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 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.

Edit buildings on smart map

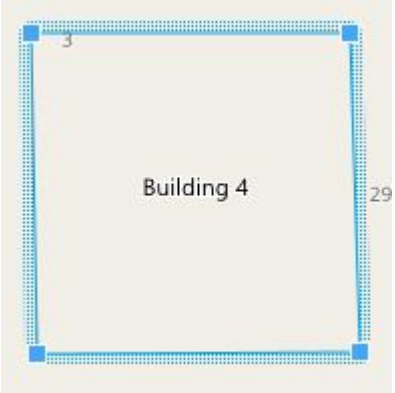
Once a building has been added to the smart map, you can change the name of the building, and adjust the position, the size, dimensions, and angles. You can also add, remove, or reorder levels.

Requirements

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

Steps:

1. Navigate to the building on your smart map. If necessary, zoom in.
2. Click **Setup** to enter setup mode.
3. Clickanywhereinsidethebuilding.Ablue-ridgedborderindicatesthatyoucaneditthebuilding.



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 89.
7. Click **Setup** again to exit setup mode.

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 Management Client.

Steps:

1. Open the smart map.
2. Click **Setup** to enter setup mode.
3. Do one of the following:
   - Right-clickthebuildingandselect**Delete**,orpress**DELETE**onyourkeyboard
     -Or-
     1. Click  **Manage default settings**.
     2. Scroll down to the **Buildings** section.
     3. Hover on the building you want to delete. The text **Delete** appears.
     4. Click **Delete** and **Save**. The building disappears from the smart map.

Managing levels and cameras in buildings (smart map)

Cameras and levels in buildings (explained)

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

More facts:

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

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

Floorplans and cameras in buildings (explained)

To help you visualize the interior of the levels in a building, you can add floorplans as custom overlays. With a floorplan in place, it is easier to precisely position the camera. For more information, see Add floorplans to levels (smart map) on page 91.

The cameras you position are associated with levels, not custom overlays. If you delete a level inside a building with cameras and a custom overlay, the cameras 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 cameras and the custom overlay stay with the level. The cameras maintain their geographical position.

Add or remove levels from buildings (smart map)

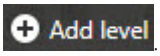
After adding a building to your smart map, you can add any number of levels. The first level is assigned the number **1**, the next **2**, and so forth. Afterwards, you can rename and reorder the individual levels.

Requirements

Smart map editing has been enabled on your Smart Client profile in 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**. Cameras on this level stay in their geographical position, but 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 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 cameras and custom overlays stay with the level.
5. Click **Setup** again to exit setup mode.

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 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.

Add floorplans to levels (smart map)

You can add custom overlays, for example floorplan 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 floorplans are displayed.

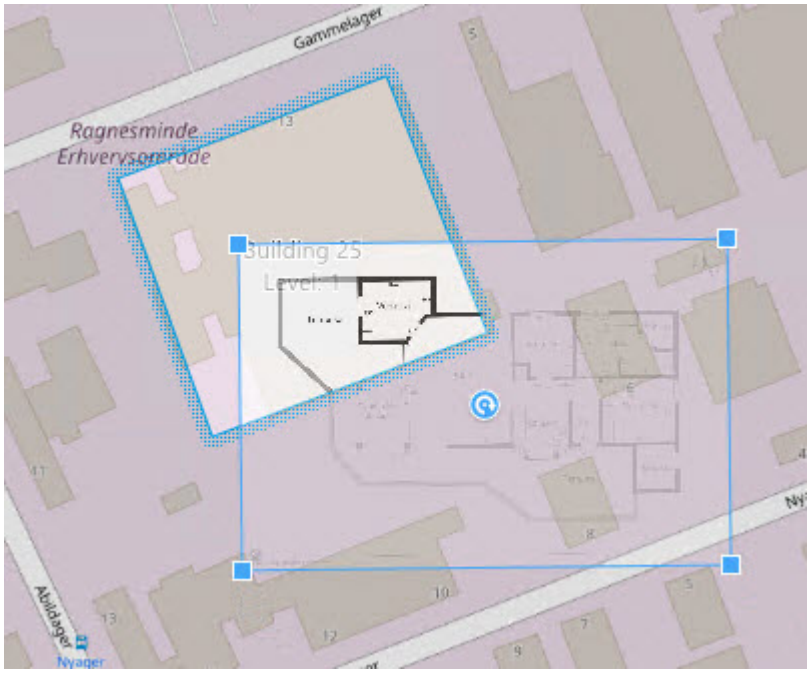
Requirements

Smart map editing has been enabled on your Smart Client profile in 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 77.

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.

Delete floorplans on levels (smart map)

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

Requirements

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

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

Add cameras to buildings (smart map)

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

Requirements

Smart map editing has been enabled on your Smart Client profile in 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  **Add a camera**.
4. Click again on the location where you want to position the camera. A dialog appears.
5. Select the required camera and click **OK**. For each camera you want to add, repeat steps 3-5.
6. To associate a camera with one or more levels, right-click the camera and select the required levels.
7. Click **Setup** again to exit setup mode.

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

Configuring maps

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 **Map Setup** window.
Change Background	Change the map, but keep the elements on the map in their relative positions to each other.
Rename Map	Edit the name of your map.

Name	Description
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. 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 **Video indicator** settings for previews. **Title bar**: select to display a title bar with the name of the camera. **Video indicator**: select to display the video indicator (see Camera names and colored indicators (explained) on page 145), which flashes green when the image is updated. You can only select **Video indicator** if you have also selected **Title bar**.
Status visualization	Select to graphically display the status of the elements (see Maps (explained) on page 219) 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.
Toolbox icons

Maps - the right-click menu (explained)

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

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 rights). 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**.

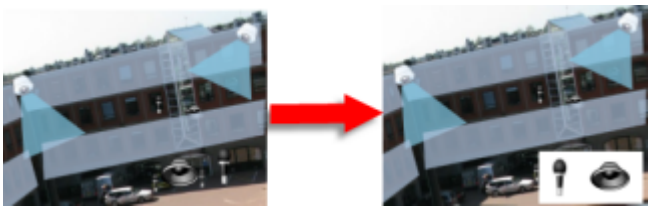
Add and remove elements from maps

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: type 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 95).
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 21), 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

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

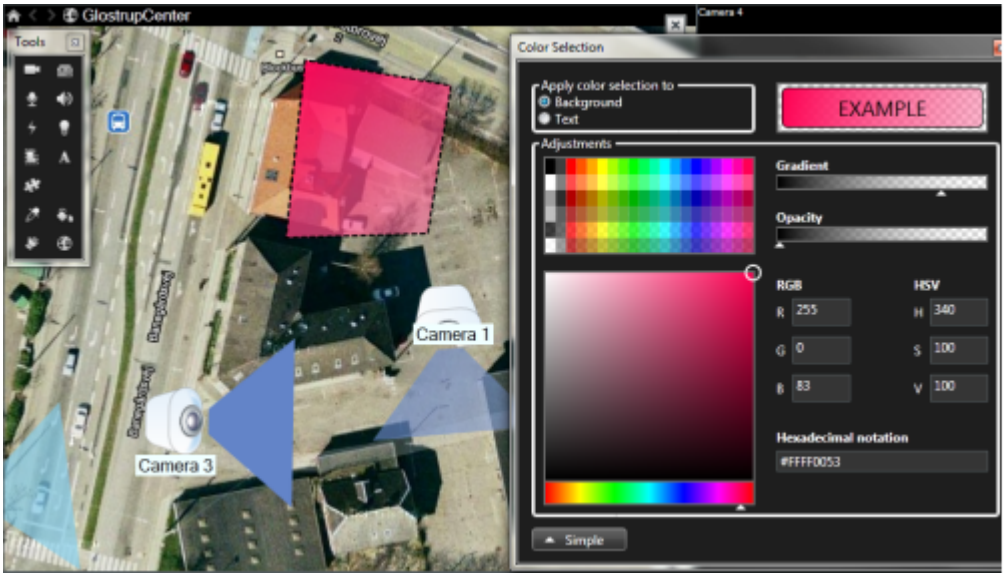
4. Only relevant for text elements: Select whether you want the color change to apply to text or background.
5. Select the color from the color palette—you can see a preview of the selected color in the EXAMPLE box.
6. Click the map element to fill it with the new color.

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.

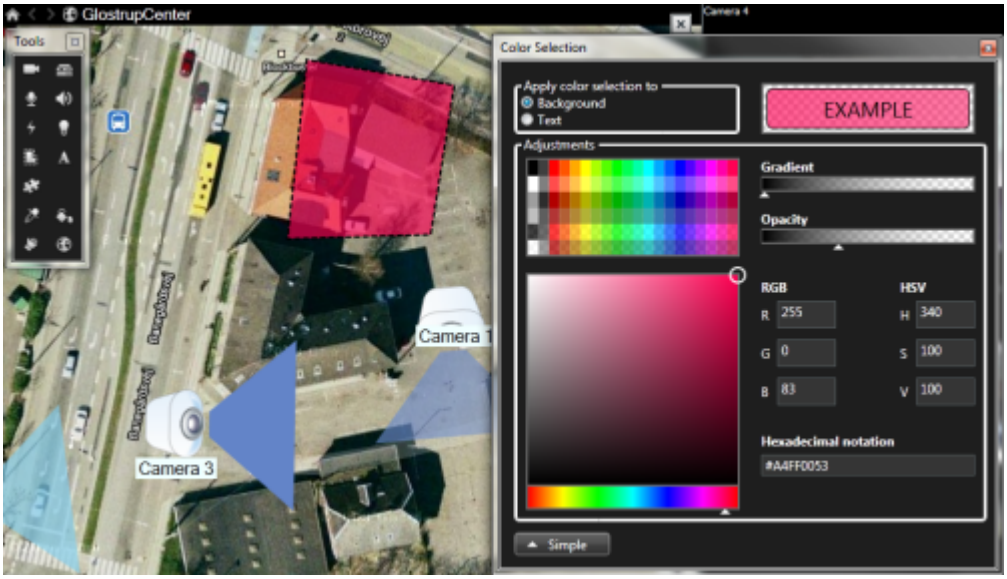


Adjusting Opacity

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.
- Type 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 typing in 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 93).

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. Type 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.

Configuring Matrix

Matrix settings

In setup mode, in the **Properties** (see Camera settings (explained) on page 55) pane, you can specify the settings for Matrix positions.

Name	Description
Window index	Change the Matrix position's ranking by choosing a different number. You can only choose a number in the range that corresponds to the number of Matrix positions in your view. **1** is the primary position 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 position **2**, and so on.
Connection Settings...	Lets you specify the **TCP port** and **Password** for transferring Matrix-triggered video from the surveillance server to the XProtect Smart Client view. This is only available when Matrix position **1** is selected; other Matrix positions inherit the connection settings specified for position **1**. By default, the TCP port used for Matrix is 12345. Consult your surveillance system administrator about which port number or password to use.

Add Matrix content 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** item to the position in the view where you want to add Matrix content. A blue border appears indicating that the position in the view has Matrix content.

2. When you select a Matrix position, you can specify its properties in the **Properties** pane.

> When viewing live or recorded video, you can double-click a Matrix position (or any other camera position in a view) to maximize it. When maximized, video from cameras in the Matrix position 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 Matrix position you want to add.

Configuring Smart Wall

Setting up Smart Wall (explained)

System administrators define the layout and behavior of a Smart Wall. This includes the following:

- General properties, such as the name of the Smart Wall, and whether it displays status text, a title bar, or a live indicator
- Presets that control the layout of the display, and the default cameras that it shows video from
- The user roles that can view, operate and add content, or play back content, and when they can do so
- Events that can be combined with rules to trigger system actions, such as displaying an alarm or content
- Rules that determine whether an action is triggered by an event, or based on a schedule

If you want to change any of these settings of behaviors, talk to your system administrator.

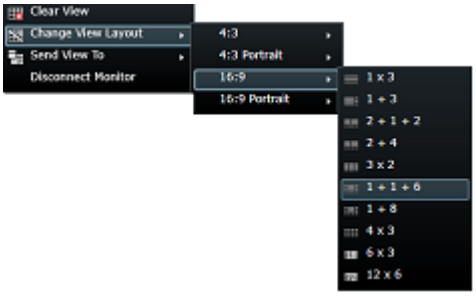
However, you can add content, for example alarms, to your Smart Wall, see Adding content to views or Smart Wall on page 45.

Change the layout of Smart Wall monitors

There are several ways you can change the layout of monitors, and how content is arranged on them.

Apply a different layout to a monitor on a Smart Wall

- In a Smart Wall overview, click the icon for the monitor, select **Change View Layout**, select the display format (for example, 4:3 or 16.9), and then select the layout.

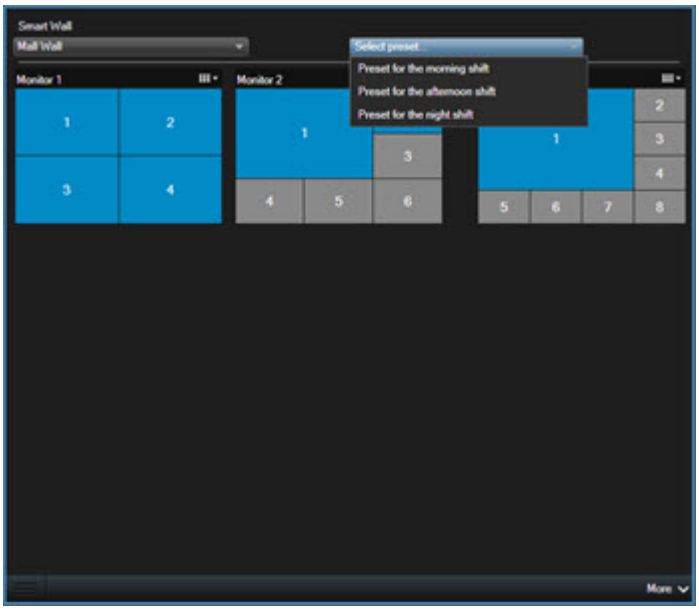


Apply a different preset

You can select a different preset for the Smart Wall overview. However, changing the preset can change all monitors in the Smart Wall.

- If you want to apply a different preset, use the **Select preset** menu

Other users can change the preset manually, or rules can change it automatically.



Content in Smart Wall (explained)

The image displays a Smart Wall overview with a 3x3 layout. Blue tiles in the Smart Wall overview are displaying content. Gray tiles are empty.

You can identify the type of content that a tile is displaying by doing the following:

- Hover the pointer over a tile. The number of the tile changes to an icon, such as a camera, that indicates the type of content
- Click the tile to view the content in a **Preview** window. The toolbar in the **Preview** window provides options for printing the content, or sending it to another Smart Wall

Adding content to Smart Wall

Apart from cameras, there are other elements that you can add to Smart Wall, for example alarms, hotspots, and maps. For more information, see Adding content to views or Smart Wall on page 45.

Configuring XProtect Smart Client – Player

Managing views in XProtect Smart Client – Player

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

Project pane (explained)

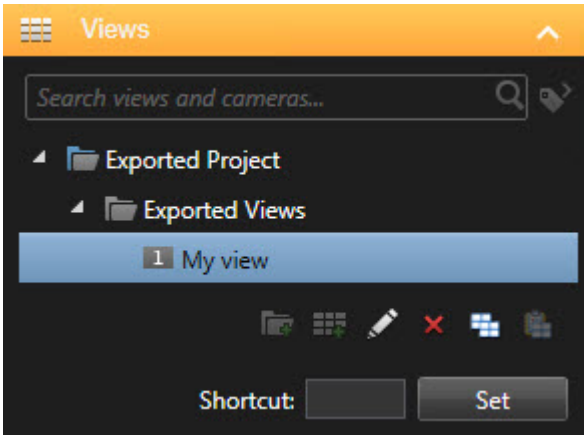
A project in XProtect Smart Client – Player is a collection of files that are created when video is exported in database format from XProtect Smart Client. Your user settings, including information about your views, are stored as part of a project.

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, HTML, 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.

Configuring XProtect Access

Add Access Monitors to views

You start by defining a view item for access control:

1. On the **Live** tab (see Live tab (explained) on page 131), in setup mode, select the view you want to use for access control 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 105) 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.
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

On the **Live** tab, 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 105) 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 105

Steps:

1. On the **Live** tab, click **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 functionality, including cardholder information and access rights.
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. Click  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 Control Notifications**.

Configuring XProtect LPR

Add LPR cameras to views

1. On the **Live** tab, 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 on the **Live** tab in the **Properties** pane (see Adjust LPR view settings on page 107).

Adjust LPR view settings

1. On the **Live** tab, 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 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:

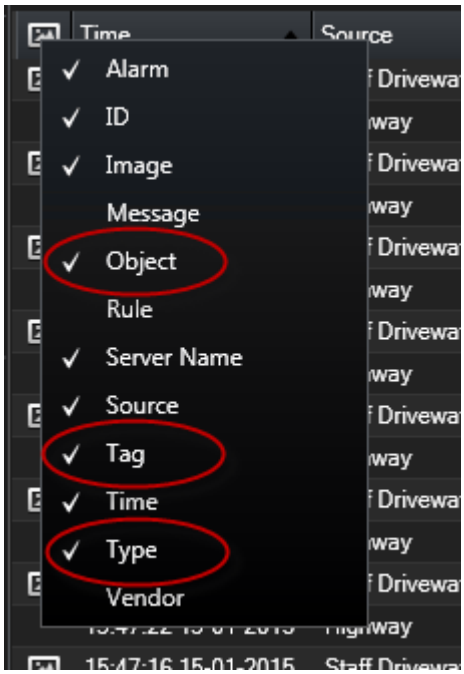
1. On the **Live** tab, click **Setup**.
2. In **Views**, select the relevant map.
3. Right-click the map and select **Toolbox**.
4. In the toolbox, click the  **Add Plug-In Element** icon to open the **Element Selector** window.
5. Select the relevant LPR server and drag it onto the map.
6. On the map, 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 Alarms list by adding the map on the **Alarm Manager** tab.

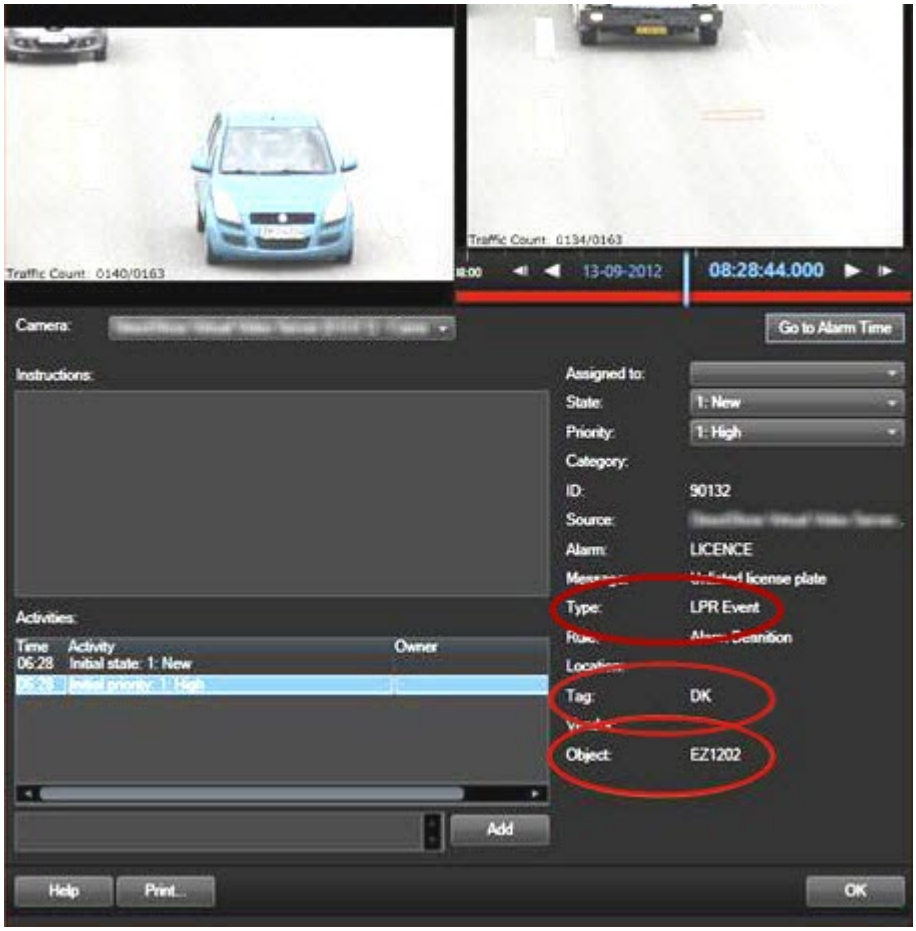
Enable LPR-specific elements

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.



Configuring XProtect Transact

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 111.

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 on the **Live** tab or investigate transactions on the **Playback** tab. For more information, see Set up views for transactions on page 111.

XProtect Transact trial license

With an XProtect Transact trial license, you can try out the XProtect Transact functionality 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.

If you are using XProtect Express or XProtect Professional, the trial license is a built-in license. The trial license is activated when the system administrator adds a transaction source in the configuration.

For other products, you need to acquire the trial license from Milestone. The system administrator must activate the trial license in the configuration.

Setting up a view for transactions

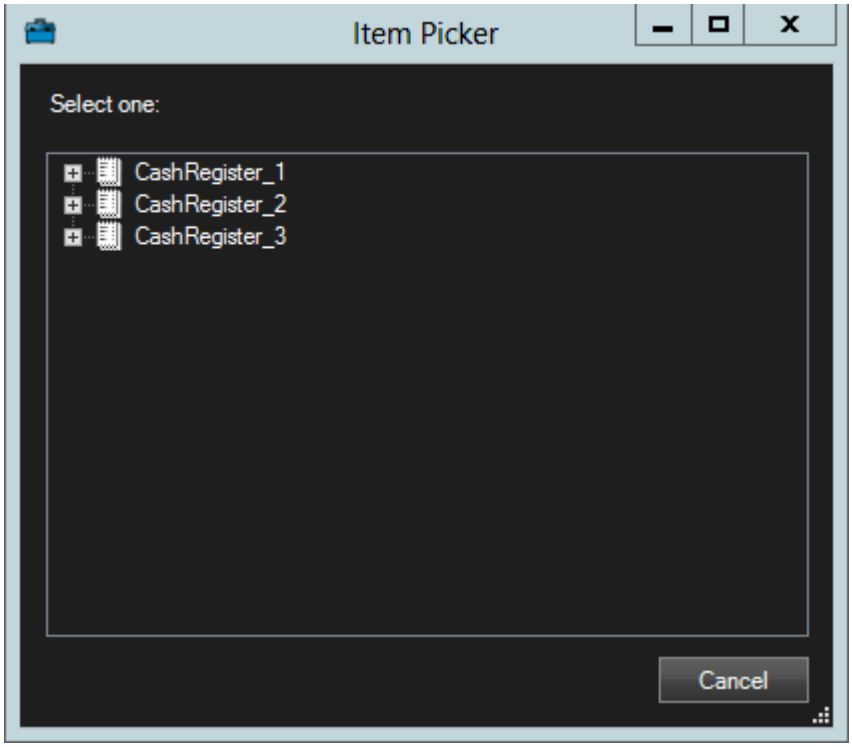
Set up views for transactions

Before viewing transactions on the **Live** or **Playback** tab, 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:

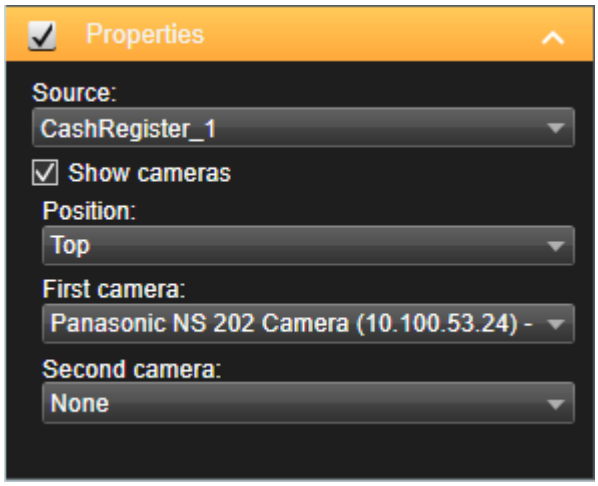
1. On the **Live** tab or **Playback** tab, click **Setup** in the upper right corner to enter the setup mode.
2. Create a new view or select an existing one.
3. Expand the **System Overview** pane.

4. Draganddroptheitemintotheviewitem,whereyouwantthetransactionsandvideofeedtobe displayed.Apop-upwindowappears.



5. Select a transaction source, for example a cash register, and click **OK**. A receipt preview is displayed inside the view item.

6. Expandandselectthecheckboxtoaddcamerasassociatedwiththetransaction source.Bydefault,thefirstcameraaddedtothetransactionsourceintheconfigurationisselected.



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.

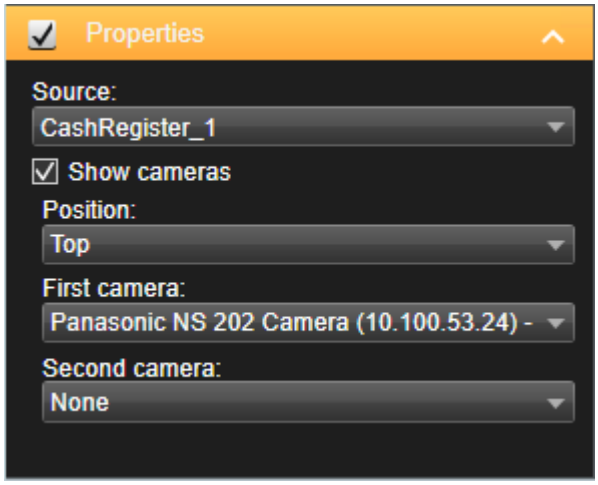
Adjust settings for transaction view items

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. On the **Live** tab or **Playback** tab, 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** checkbox 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 111).

Scripting

Scripting for log in (explained)

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

Examples:

- 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.

> Some authentication methods are only available if the XProtect Smart Client user logs in to certain Milestone surveillance systems. For a detailed outline of the features available on your particular system, see the XProtect Product Comparison Chart on: https://www.milestonesys.com/.

Scripting for log in - parameters

You can use these parameters:

ServerAddress

Refers to the URL of the server to which XProtect Smart Client connects.

For XProtect Corporate, XProtect Expert, XProtect Professional+, XProtect Express+, and XProtect Essential+, this is the URL of the management server.
For XProtect Professional, or XProtect Express it is the URL of the image server.

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

In addition to displaying video, the XProtect Smart Client is able to display static images and HTML pages. Such HTML pages may be used for intuitively switching between different views in the XProtect Smart Client.

For example, you may insert a clickable floor plan of a building, and you would be able to simply click a part of the floor plan to instantly switch to a view displaying video from the required part of the building.

In the following, you will see examples of HTML pages for XProtect Smart Client navigation: a simple HTML page with buttons, and a more advanced HTML page with a clickable image map. For surveillance system administrators wishing to create and distribute such HTML pages to XProtect Smart Client users, a check list outlining the tasks involved is also provided.

The XProtect Smart Client is highly flexible when it comes to customizing navigation and other features. For advanced users it is possible to create approximately 100 different function calls in the XProtect Smart Client.

The **Enable HTML scripting** check box must be enabled in the **Properties** pane, which is visible only in setup mode.

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 tabs: **Live** and **Playback** Bear in mind that, depending on their user rights, some users may not be able to access all tabs.

  Required HTML syntax:

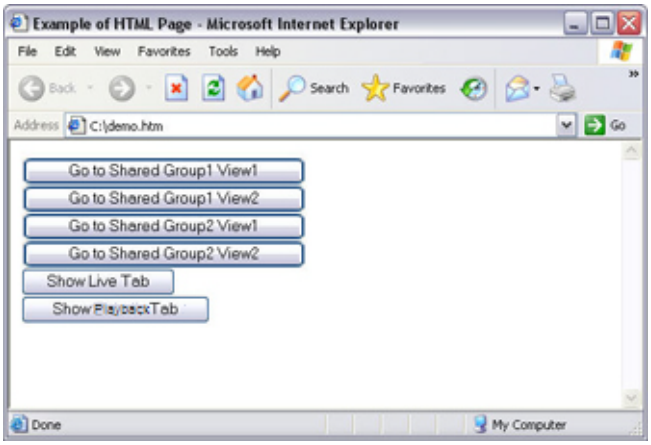
  Live tab: `<input type="button" value="Buttontext" onclick="SCS.Application.ShowLive ();">`

  Playback tab: `<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. See Scripting for more information.

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 two of the XProtect Smart Client 's tabs, **Live** and **Playback**. When viewed in a browser, our HTML page looks like this:

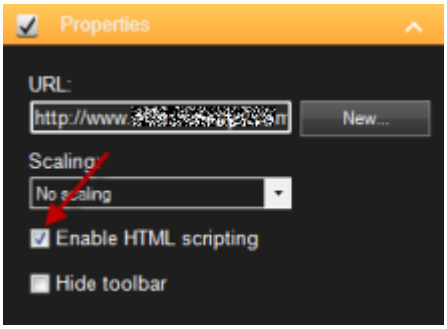


HTML page with buttons for navigating between views and tabs

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 because of security features in Internet Explorer.

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. When importing the HTML page, we made sure to select **Enable HTML scripting** in the HTML page's **Properties** in setup mode.

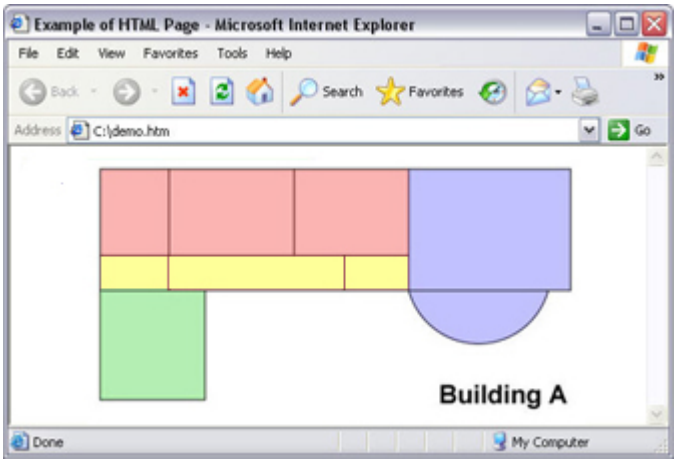


Selecting **Enable HTML scripting** ensures that the scripting required for the buttons to work is automatically inserted in the HTML page.

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 . The two important things to remember are:

- The HTML page should be stored locally on the user's PC

You should make sure HTML scripting is enabled on the HTML page when importing it To import the HTML page:

1. In setup mode, in the **System Overview** pane, drag the **HTML Page** item to the required position in the required view.
2. In the **Open URL** window, specify the HTML page.
3. Select the position in the view, and in the **Properties** pane, select **Enable HTML scripting**.

   Selecting **Enable HTML scripting** ensures that the scripting required for your buttons or other navigation features to work is automatically inserted in the HTML page.
4. Depending on the navigation features you have included on your HTML page, you may often want to import the HTML page into several views in order for the navigation to fully work.

System administrator's check list

Surveillance system administrators wanting to create and distribute navigation HTML pages to XProtect Smart Client users, 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 XProtect Smart Client views in which it will be used. Having imported the HTML page, select its position in the view, go to the **Setup** tab's **Properties** pane, and verify that **Enable HTML Scripting** is selected.
4. **Test** that the navigation controls on the imported HTML page work as intended.
5. **Enjoy** simple and intuitive XProtect Smart Client navigation, tailored to meet your organization's needs.

Troubleshooting

If your HTML navigation page does not work as intended, consider the following:

- Have you used the correct syntax in your HTML?
- Have you selected **Enable HTML Scripting** after importing the HTML page?
- Does the intended audience have the rights to required benefit from the HTML navigation page? Bear in mind that depending on their user rights, some users may not have access to certain cameras, views, features or tabs in their XProtect Smart Client.

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.

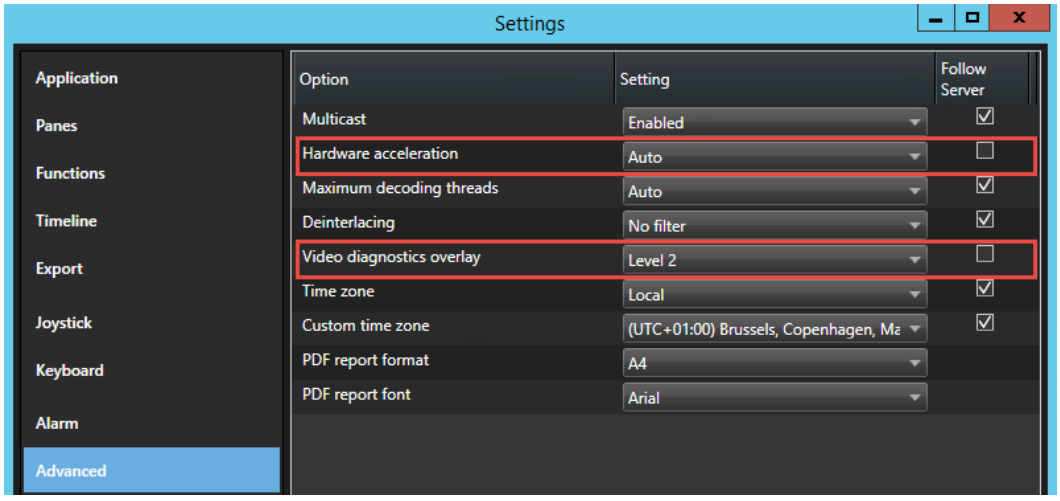
> XProtect Smart Client supports hardware accelerated decoding using Intel® and NVIDIA® GPUs. Milestone does not recommend the use of Scalable Link Interface (SLI) configuration of your NVIDIA display adapters.

Follow the steps described in the next sections to examine your PC to make sure that all hardware acceleration resources are available.

Check hardware acceleration settings

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

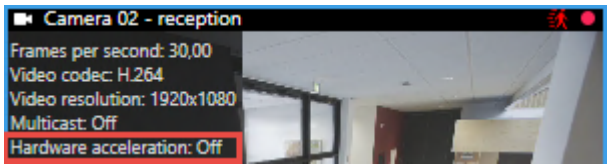
   Select the default setting **Auto**.



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.

Next, Verify your operating system on page 123.

Verify your operating system

Make sure your operating system is Microsoft® Windows® 8.1, Windows® Server 2012, or newer.

Only non-virtual environments are supported.

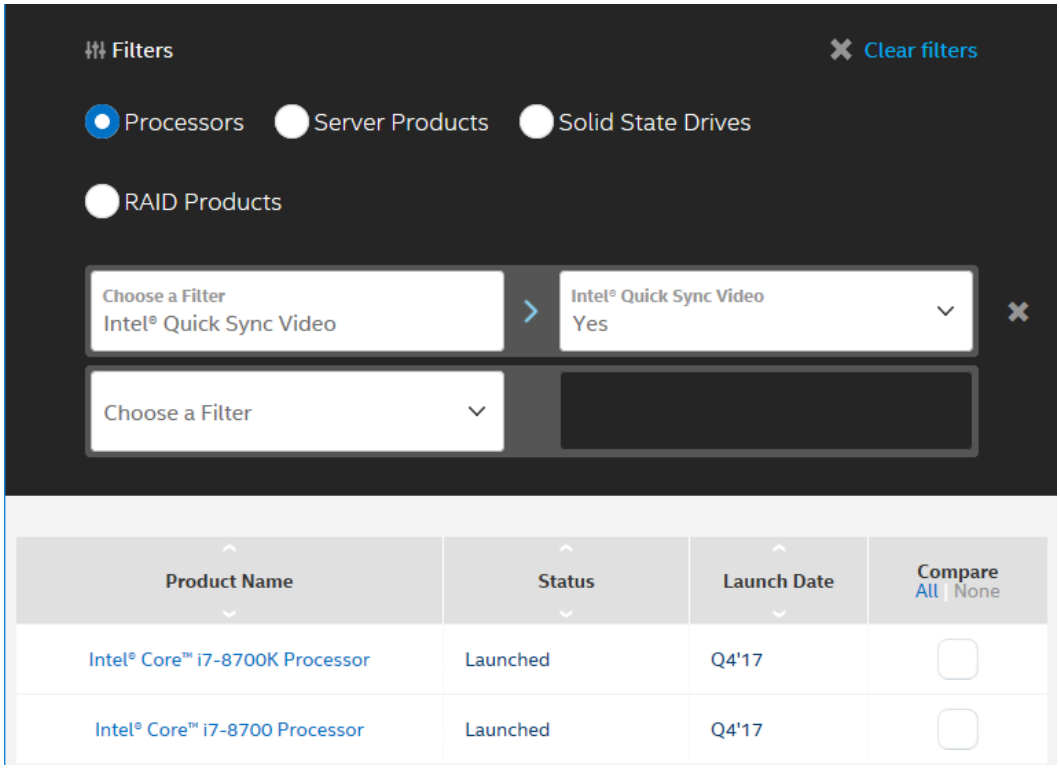
NVIDIA hardware acceleration is only supported by 64-bit operating systems.

Next, Check CPU Quick Sync support on page 123.

Check CPU Quick Sync support

To verify that your processor supports Intel Quick Sync Video:

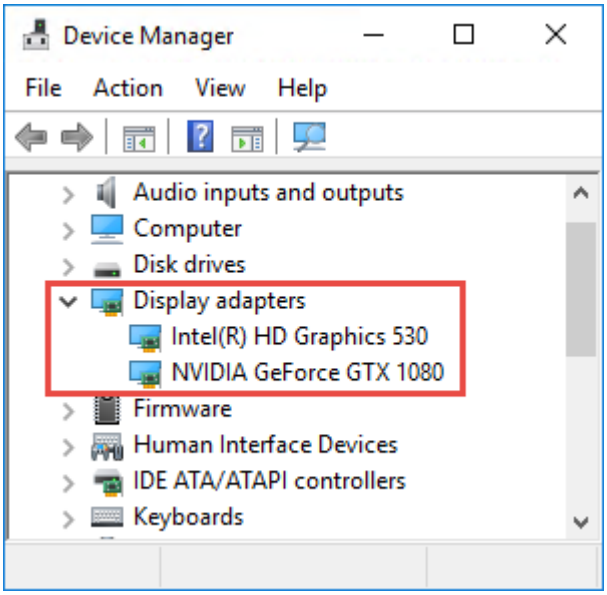
1. Visit the Intel website (https://ark.intel.com/Search/FeatureFilter?productType=processors/).
2. In the menu, set **Processors** and **Intel Quick Sync Video** filter to **Yes**.
3. Find your CPU in the list.



Next, Examine the Device Manager on page 124.

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. Check NVIDIA hardware acceleration support on page 125.

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 126).

Next, Update the video driver on page 126

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/).

Next, Update the video driver on page 126.

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.

Next, Update the video driver on page 126.

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.

Next, Check memory modules configuration on page 127.

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.

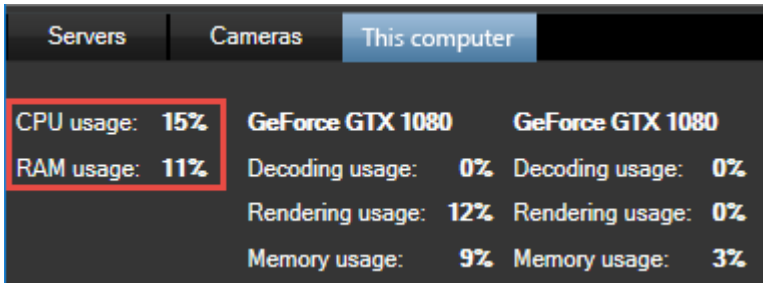
If you use a 1 x 8 GB memory module configuration, you only use one of the memory channels.

Next, Monitor client resources on page 127.

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. To monitor the load of the current view, select the **Live** or **Playback** tab.



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.

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 System Monitor tab (explained) on page 132.

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

First time you log in (explained)

The first time you log in, you need to determine whether any views exist. Views determine how video is displayed and are required to use XProtect Smart Client. One or more views may already have been created for you, or you may need to create views yourself. Read more about views - including how to determine if views have already been created for you, in Views (explained) on page 138.

Your user settings (including views) are stored centrally on the surveillance system. This means that your login can be used on any computer that has a Smart Client installed, and that you can restore views from your last log-in.

If you encounter a second dialog box during login, you need additional login authorization (see Login authorization (explained) on page 129) to get access to the XProtect Smart Client.

Log-in settings

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 the rights to authorize you to enter their credentials along with yours in the login form. After that, you are good to go.

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

Logging into access control systems (explained)

When you log into XProtect Smart Client, you may be asked for additional logins to 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, 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.

Log in and out

1. Open XProtect Smart Client.
2. Specify your login information, and click **Connect**. If a problem occurs during login, you may receive an error message (see Logging in (troubleshooting) on page 262).
3. If you have logged in before, you can restore the views used during the last session. Depending on the configuration, the XProtect Smart Client may ask you if you want to restore the views:
   - **Main view**: If you select this option, the view that you used last time in the main window of XProtect Smart Client is restored
   - **Detached views**: If you select this option, the view that you used last time in a floating window of XProtect Smart Client is restored. Only available when connecting to specific Milestone surveillance systems (see Surveillance system differences on page 21)
4. To log out of the XProtect Smart Client, simply click the **Log out** button in the XProtect Smart Client title bar.

If you encounter a second dialog box during login, you need additional login authorization (see Login authorization (explained) on page 129) to get access to the XProtect Smart Client.

Tabs in XProtect Smart Client

The XProtect Smart Client has the following tabs:

- The **Live** tab (see Live tab (explained) on page 131) for viewing live video
- The **Playback** tab (see Playback tab (explained) on page 131) for viewing recorded video
- The **Sequence Explorer** tab (see Searching for video sequences on page 151) for navigating video sequences
- The **Alarm Manager** tab (see Alarm Manager tab (explained) on page 131) for investigating incidents and alarms
- The **System Monitor** tab (see System Monitor tab (explained) on page 132) for viewing system information

If some of the tabs are unavailable, it is because you do not have the rights required to access all the areas.

These tabs are visible only if you have acquired licenses for XProtect Transact, XProtect LPR, or XProtect Access:

- The **Access Control** tab (see Access Control tab (explained) on page 132) for controlling your access control system and associated cameras.
- The **LPR** tab for (see LPR tab (explained) on page 250) identifying vehicles by their license plates, and investigating LPR related events.
- The **Transact** tab for (see Transact tab (explained) on page 133) monitoring and investigating transactional data in combination with the associated video streams.

Live tab (explained)

On the **Live** tab, 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.

Here, you can also set up views.

Playback tab (explained)

On the **Playback** tab, you can investigate recorded video by playing it back, searching for bookmarks, and then document what you find by exporting evidence.

Advanced features for browsing recorded video:

- The timeline (see Time navigation controls (explained) on page 148)
- Smart search - lets you search for motion in selected areas of recordings from a particular camera
- Recording Search - lets you search for sequences motion or bookmarks (see Search for sequences or bookmarks in Recording Search pane on page 159. You can browse through a simple list with a preview option

You can also:

- Listen to audio when connected to selected Milestone surveillance systems
- Use hotspots, digital zoom (see Use digital zoom on page 192), navigate fisheye lens images (see PTZ and fisheye lens images (explained) on page 185), print images (see Print video evidence on page 173), and more.

Sequence Explorer tab (explained)

On the **Sequence Explorer** tab, you can investigate incidents by examining sequences of video. You can use **Sequence Search** to find video sequences with motion or bookmarks, or Smart Search to find sequences based on motion in a selected area.

Alarm Manager tab (explained)

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 map if one is available.

System Monitor tab (explained)

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**, 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.

Access Control tab (explained)

On the **Access Control** tab, you can investigate access control events with search and filtering, and view the associated video recordings and access control data. You can also monitor door states, investigate cardholders and create reports.

You can drag the **Access Control** tab to its own separate floating window, while you keep the main window in the background to watch multiple views simultaneously. You can also sort columns and drag the columns to different positions.

You can search for, filter, sort, and review data related to:

- **Events**: Logs the events with a time stamp, event type, the associated door or access control unit, and cardholder name if available. If your XProtect system integrates with multiple access control systems, the list displays from which access control system the event was triggered
- **Doors**: Lists the doors, access points and other access control units in each access control system, and their current state
- **Cardholders**: Lists the cardholders in each access control system and their details

Depending on your access control system, you may be able to connect to the access control system applications via the **Access Control Administration** button in the top right corner to, for example, specify access rights or manage cardholders.

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 for previewing video associated with individual LPR events. Below the preview, information about the license plate appears together with details from the license plate match list it is associated with.

You can filter the event list according to the period, country module, LPR camera, or license plate match list. Use the **Search** field to search for a particular license plate number. By default, this list shows LPR events from the last hour.

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

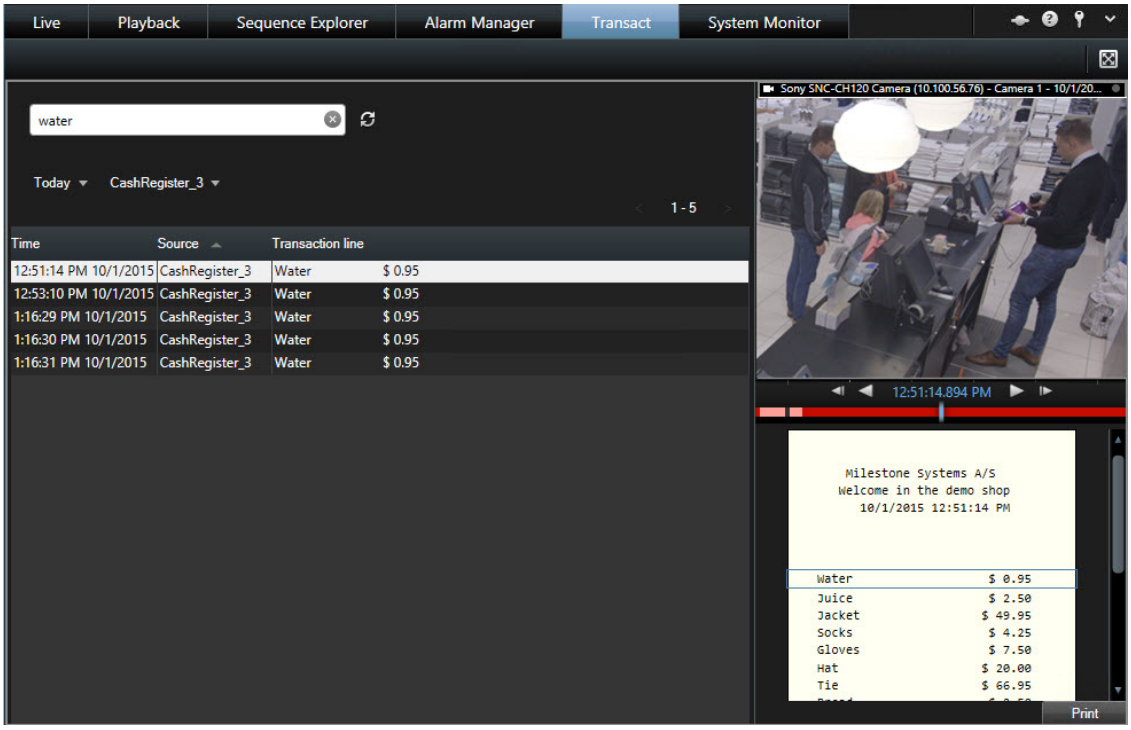
You can make updates to the existing match lists by using the **License Plate Match List** function.

Transact tab (explained)

On the **Transact** tab, you can investigate transactions through search and filtering, and view receipts and video recordings in a combined view.

There is a search field and two filters:

- Search field: enter your search words here to perform a free text search. The search returns transaction lines that contain your search words and does not distinguish between upper and lower case letters. In the receipt, the transaction lines matching the search are highlighted
- Time interval: use this filter to specify the time interval, for example **Last 7 days**. You can also set a custom interval by your own choice. By default, the filter is set to **Today**
- Source: use this filter to select the transaction sources you want to view transactions for. By default, the filter is set to **All**

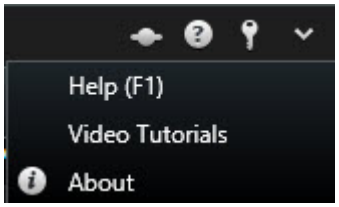


Getting to know your XProtect Smart Client

The topics in this section can help you become familiar with the different areas your XProtect surveillance system.

Get help

- To access the XProtect Smart Client help system, on the XProtect Smart Client toolbar, click **Help** > **Help** or press F1 on your keyboard



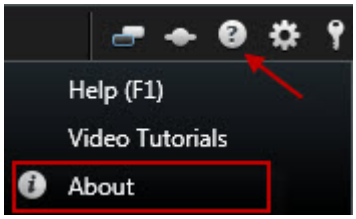
- To access online video tutorials in a browser window, on the XProtect Smart Client toolbar, click **Help** > **Video Tutorials**

The help system is context-sensitive, which means it automatically displays a help topic relevant to the area you are working with.

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.

- To view this information, on the XProtect Smart Client toolbar, click **Help** > **About**



> The version of your XProtect Smart Client affects which XProtect server version it is compatible with. The latest XProtect Smart Client is compatible with the latest server version and the previous server version.

User rights (explained)

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

Basically, your system administrator can restrict your rights to:

- Access the XProtect Smart Client
- Access each of the tabs: **Live**, **Playback**, **Alarm Manager**, and **Sequence Explorer**
- Setup mode.
- Use specific features
- Create views (views determine the way in which video from one or more cameras is displayed)
- View video from specific cameras

The ability to use features of the XProtect Smart Client can vary considerably from user to user. When connected to certain surveillance systems (see Surveillance system differences on page 21), user rights may even vary depending on time of day, day of week, etc. For example, you may only be able to view video from a particular camera during certain hours Monday-Friday, but not outside these hours.

Modes in XProtect Smart Client (explained)

XProtect Smart Client has two modes:

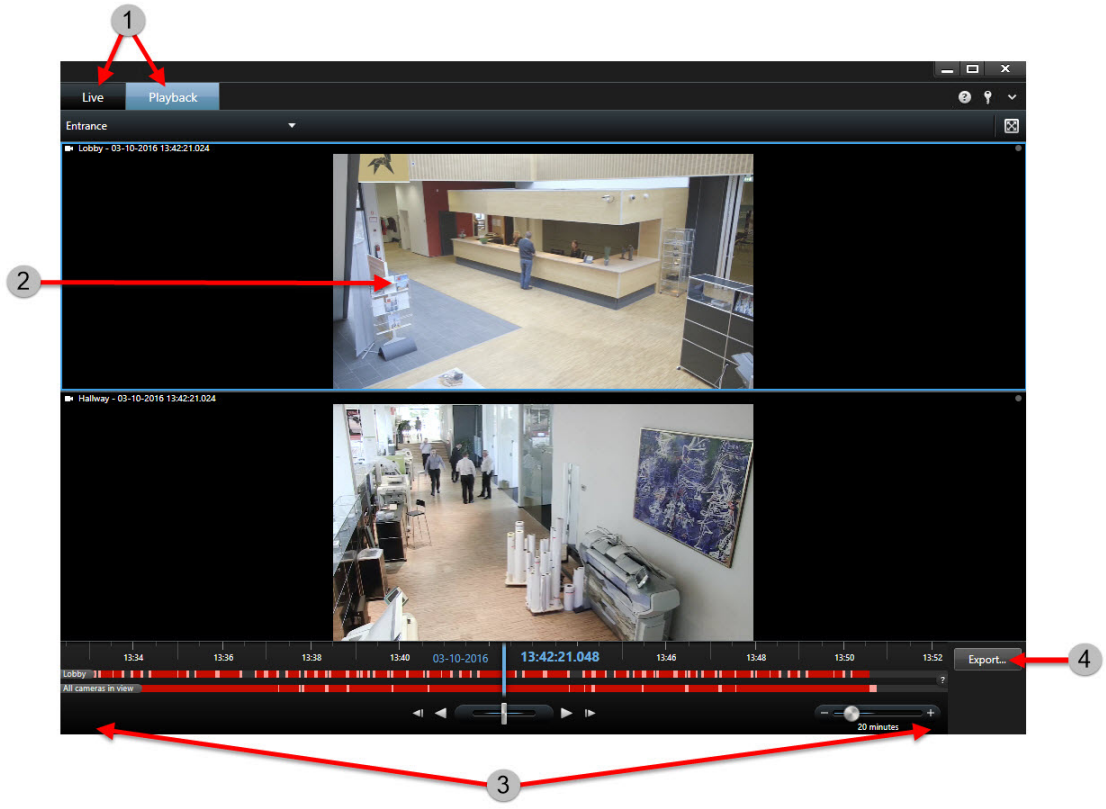
- Simplified mode - only the **Live** and **Playback** tabs are available, and you can perform a limited set of tasks. For more information, see Simplified mode overview on page 136
- Advanced mode - all features and tabs are available, and you can access the setup mode. For more information, see Playback tab (advanced mode) overview on page 137

Depending on your product, XProtect Smart Client opens in simplified or advanced mode. If you change the default mode through the **Toggle simplified or advanced mode** button, XProtect Smart Client opens in the changed mode the next time you open the program.

The table gives you an overview of the XProtect Smart Client default mode according to the product.

Product	Mode
XProtect Corporate	Advanced
XProtect Expert	Advanced
XProtect Professional+	Advanced
XProtect Express+	Advanced
XProtect Essential+	Advanced
XProtect Professional	Simplified
XProtect Express	Simplified

Simplified mode overview



1 View video - view live video, or play back recorded video to investigate an incident. Select a different view to view video from other cameras or other types of content. For more information, see:

- Topic: Add or edit views in simplified mode on page 54
- Video: https://www.youtube.com/watch?v=sn1voRJxXEo/

❷ **Get a closer look** - tap or double-click a video to view it in full-screen mode. Tap or double-click again to exit the full-screen mode. Scroll to zoom in and out.

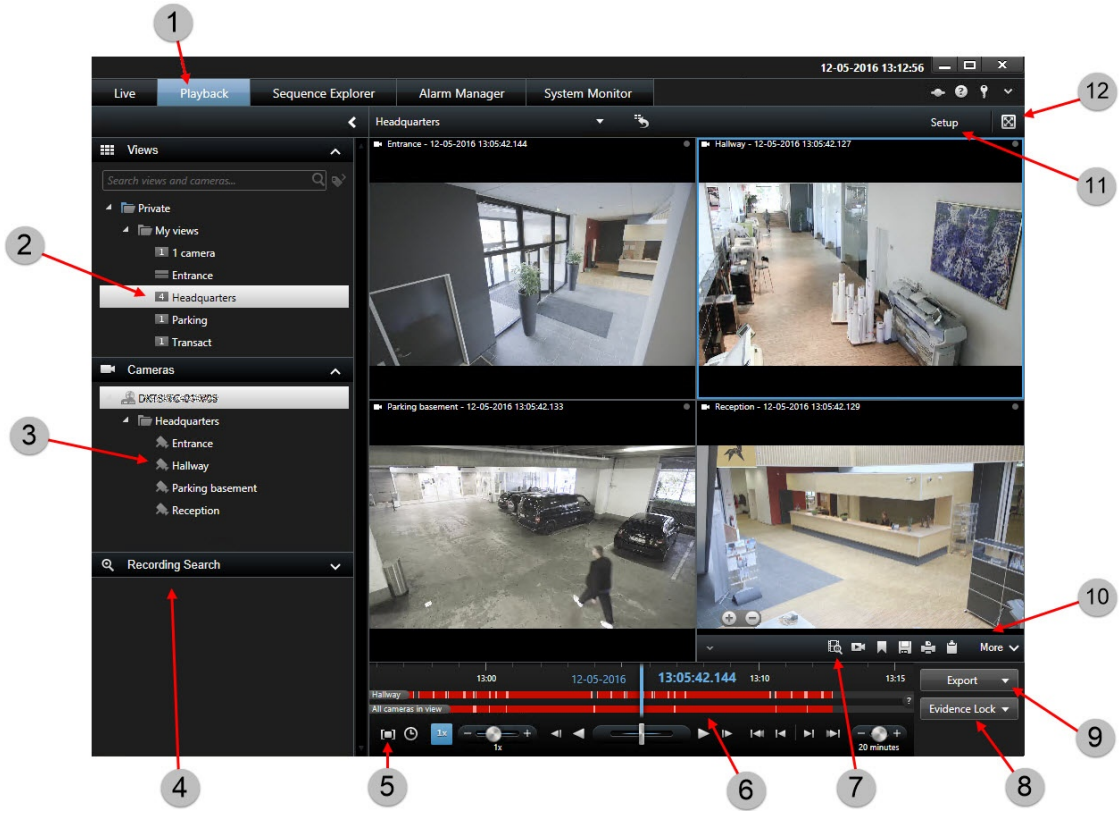
❸ **Investigate recordings** - Play back video forward or backward in time, adjust the timespan, or scroll to quickly browse the recordings. You do this on the **Playback** tab. For more information, see:

- Topic: Time navigation controls (explained) on page 148
- Video: https://www.youtube.com/watch?v=Ev4LZwLAl4c/

❹ **Create documentation** - export a video clip or still image that shows what happened. You do this on the **Playback** tab. For more information, see:

- Topic: Export video in simplified mode on page 163
- Video: https://www.youtube.com/watch?v=r1BIp1PrWJ8/

Playback tab (advanced mode) overview



❶ View recorded video on the **Playback** tab. See Viewing recorded video (explained) on page 149.

❷ Select a view.

❸ Change cameras in views on page 175

❹ Use the **Recording Search** pane.

❺ Select a timespan for exporting video. See Time navigation controls (explained) on page 148.

❻ Browse using the timeline. See Timeline (explained) on page 147.

❼ Search for motion in seleted areas on page 157

❽ Create an evidence lock. See Evidence locks (explained) on page 203.

❾ Export video in advanced mode on page 164

❿ Perform various actions on the camera toolbar. See Camera toolbar overview on page 140.

⓫ Enter setup mode. See Setup mode overview on page 27.

⓬ View in full screen.

Views (explained)

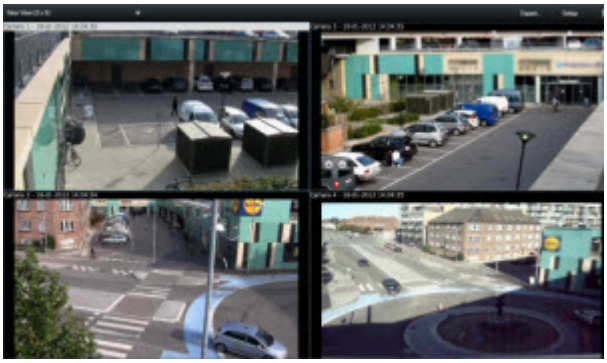
The way video is displayed in XProtect Smart Client is called a view. A view can contain video from up to 100 cameras, depending on your surveillance system. XProtect Smart Client can handle an unrestricted number of views, allowing you to switch between video from various groups of cameras. The layout of each view can be customized to fit its content. To help you maintain an overview, all views are placed in folders called **groups**. A group can contain any number of views and, if required, subgroups.

Views can be private or shared with other users.

In addition to video, views can display web pages and still images (for example, mugshots). For some surveillance systems, views can even display data from other applications (such as receipts from a cash register) alongside video. See Content inside views (explained) on page 139.

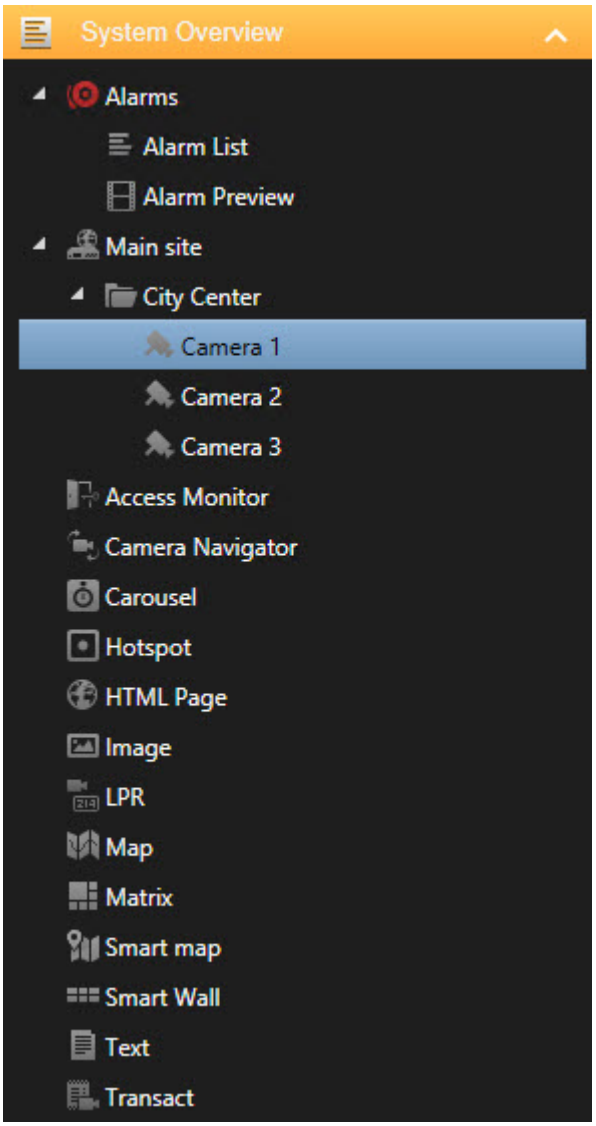
Your user settings, including information about your views, are stored centrally on the surveillance system server, so you can use your views on any computer that has a XProtect Smart Client installed.

Example of a 2x2 view



Content inside views (explained)

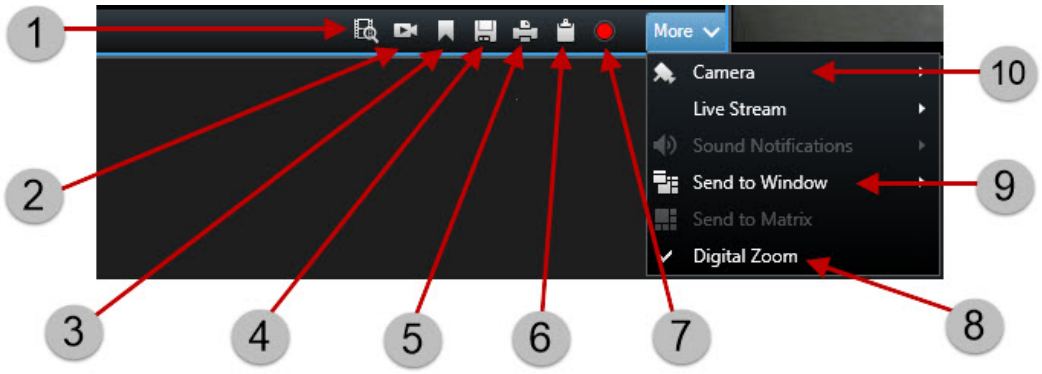
Once you have defined a layout for your view, you can add different types of content to your view items. In setup mode, you can drag and drop these items from the **System Overview** pane into the view item.



- Alarms - the alarm list and alarm preview you can also find on the **Alarm Manager** tab
- Cameras - video feed from a live camera or video played back. The cameras appear under the site name, which is defined by your system administrator.
- Access Monitor - with XProtect® Access installed, you can set up access monitors, for example for a specific door
- Camera Navigator - allows you to navigate cameras on a map
- Carousel - shifts between cameras and at a pace that you define
- Hotspot - a hotspot window shows whatever camera is in focus in a high resolution or frame rate

- HTML page - import a webpage into the view, for example the web address of an online news channel
- Image - add images to views, for example to distribute a picture of a suspect.
- LPR - with XProtect® LPR installed, you can add LPR cameras to views
- Image - allows you to share images, for example of suspects
- Map - a floor plan or a geographical area
- Matrix - add a Matrix position to a view. See Matrix (explained) on page 225
- Smart Map - a geographical world map based on existing online map services, for example Google Maps and OpenStreetMap.
- Smart Wall - if XProtect Smart Wall has been configured by your system administrator, you can add video walls to your views. See XProtect Smart Wall (explained) on page 22
- Text - add text to you views
- Transact - if XProtect Transact has been installed in your system, you can add point-of-sales systems together with cameras.

Camera toolbar overview



1. Searching for motion in selected areas (explained) on page 156
2. View recorded video independently of timeline on page 150
3. Add a bookmark (Bookmarks (explained) on page 194)
4. Take snapshots on page 146
5. Print video evidence on page 173
6. Copy single images
7. Record video manually on page 146
8. Use digital zoom on page 192
9. Send video between open views on page 176

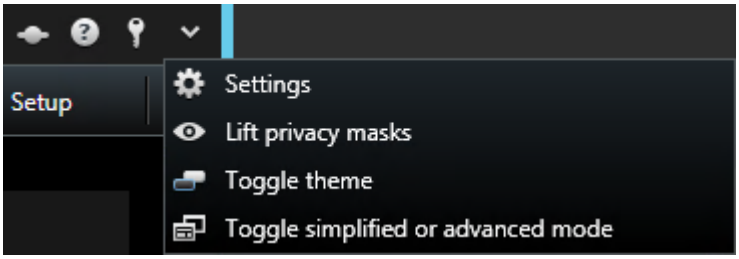
10 Change cameras in views on page 175

Task buttons (explained)

The task buttons are on the XProtect Smart Client toolbar and to the right of the timeline. The task buttons available vary depending on the tab you are on. For example, **Setup** is not available on all tabs. These are the task buttons:

- **Setup**: click to enter setup mode (see Setup mode overview on page 27)
- **Export**: click to export video (see Export video in advanced mode on page 164)
- **Evidence Lock**: click to create an evidence lock (see Create evidence locks on page 203)
- **Retrieve**: Click to retrieve recordings from interconnected hardware devices or cameras that support edge storage
- **Toggle full screen mode**: click to toggle between full screen (see View in full screen) and a smaller window that you can adjust to the size you want

Application buttons (explained)



With the application buttons in the toolbar, you can select basic XProtect Smart Client actions:

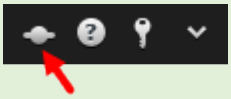
- **Status**: Access the **Status** window. See Status window (explained) on page 141
- **Help**: Access the help system, play online video tutorials or view version number and plug-in information. See Get help on page 134 and View version and plug-in information on page 134
- **Log out**: Log out XProtect Smart Client. See Log in and out on page 130
- **Settings**: Configure XProtect Smart Client settings and behavior, joysticks, keyboard shortcuts, and language. See Settings window (explained) on page 27)
- **Lift privacy masks**: Users with sufficient rights can temporary lift privacy masks. See Privacy masking (explained) on page 208
- **Toggle theme**: Switch the XProtect Smart Client theme to dark or light
- **Toggle simplified or advanced mode**: Switch between simplified mode and advanced mode. See Modes in XProtect Smart Client (explained) on page 135

Status window (explained)

In the **Status** window, you can find information about:

- The status of the surveillance servers that your XProtect Smart Client is connected to through Milestone Federated Architecture. For more information, see **Login information** below.
- The jobs created for retrieving data from interconnected hardware devices or cameras that support edge storage. For more information, see **Jobs** below.
- The existing evidence locks that you have user rights to. For more information, see **Evidence Lock List** below.

To open the **Status** window, click the **Status** button in the application toolbar:



If the button appears with a red circle  , one of more servers are unavailable. When you have viewed the status, the button will stop flashing red even if the server(s) are still unavailable.

Login information

Here you can view the status of the surveillance servers your XProtect Smart Client is connected to. The dialog box is useful if you are connected to a surveillance system that supports Milestone Federated Architecture. Milestone Federated Architecture is a parent/child setup of 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.

If servers are available, they will be displayed in gray:

If servers are not available at the time you log in, you cannot use cameras or features belonging to those servers. Unavailable servers are displayed in red:

The number of servers you see reflects the number of servers retrievable from the surveillance system at the time you logged in. Particularly if you connect to large hierarchies of servers, more servers may occasionally 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 attempt 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 surveillance system administrator for advice.

Jobs

If your XProtect Smart Client is part of a Milestone Interconnect™ system and you have sufficient rights to retrieve data from interconnected hardware devices or cameras that support edge storage, you can view the jobs created

for each data retrieval request for these devices.

Each camera where retrieval has been requested is displayed as a separate job. You can view the progress of the running jobs and you can stop the jobs from here. Related audio will automatically be retrieved, but these jobs will not show up anywhere. Once a job has completed, the timeline (see Timeline (explained) on page 147) for the device is automatically updated.

If you would like to only see the jobs you have requested, click the **Only show my jobs** filter.

Evidence Lock List

You can sort, filter and search the evidence locks list and see additional information about them. You can only see evidence locks with devices that you have user rights to. For more information see View existing evidence locks on page 204.

Keyboard shortcuts (explained)

When you work on the **Live** and **Playback** tabs, a number of simple keyboard shortcuts are available.

The PLUS SIGN in the following shortcuts does not indicate the key but the combination of pressing two or more keys. For example, the keyboard shortcut /+ENTER indicates that you press the slash (/) key and then the ENTER key.

These shortcuts cannot be used for positions in views containing Matrix content or static images.

Press these keys	To do this
ENTER	Toggle maximized/regular display of the selected position in the view.
ALT	Select a specific view item. When using ALT, you can navigate to a view item by typing the numbers displayed on the screen. When a view item is in focus, it is marked with a blue frame. If you are using a PTZ camera or a hotspot (see Hotspots (explained) on page 181), this allows you to control cameras with a joystick or to send the view item directly to the hotspot without using the mouse.
/+<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 surveillance system. Camera shortcut numbers are defined on the server.

Press these keys	To do this
/+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**. View shortcut numbers may not necessarily be used. If view shortcut numbers are used, you can see them on the **Live** tab in the **Views** pane, where they appear in parentheses before the views' names. View shortcut numbers are defined on the **Live** tab in setup mode.
6 (numeric keypad only)	Move the view position selection one step to the right.
4 (numeric keypad only)	Move the view position selection one step to the left.
8 (numeric keypad only)	Move the view position selection one step up.
2 (numeric keypad only)	Move the view position selection one step down.

You can also assign your own custom shortcut key combinations (see Keyboard settings on page 34) for particular actions in XProtect Smart Client.

Viewing live video

You view live video mainly on the **Live** tab in one of the views that are set up in XProtect Smart Client. There are different actions available on the view items that show the live video. For example, if something catches your attention, you can zoom in to take a closer look, or start manual recording.

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 surveillance system detects special events, for example, motion generated by a person entering a room.

If title bars have been enabled in the **Settings** window, the title bar above the images indicates if video is being recorded. Sometimes the camera is recording for short periods only. This is because the surveillance system server may have been configured to only record when there is motion, when a door is open, 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, go to the **Playback tab** or the **Sequence Explorer** tab.

Camera names and colored indicators (explained)

By default, the camera title bar displays the name of the camera. You can change this in setup mode on the **Live** tab, in the **Properties** pane (see Camera settings (explained) on page 55).

The round video indicator is placed in the upper right corner of the camera title bar. This indicator changes color to display the current status of the video in the view item. The list below describes the different colors:

- **Green** - A connection to the camera is established
- **Red** - Video from the camera is being recorded
- **Yellow** - Playing back recorded video
- **Gray** - The video has not changed for more than two seconds

The motion indicator appears when motion is detected. Click inside the image to reset the motion indicator. This indicator will not appear if no motion has been detected.

The event indicator appears when specific events occur. This is defined by the surveillance system administrator. Click inside the image to reset the event indicator. The indicator will not appear if event indication has not been specified for the camera, or if no specified events have occurred.

This feature is only available in certain surveillance systems (see Surveillance system differences on page 21) and requires that notifications on events have been configured on the server.

Event and motion indications can be accompanied by sound notifications (see Sound notifications (explained) on page 61).

The camera connection indicator appears when the server connection to the camera is lost. A camera 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 surveillance system server.

Record video manually

The functionality of the manual recording feature depends on the surveillance system you are connected to and on your user rights. Recording while watching live video is useful if you see something of interest. On the camera toolbar for the position in the view you want to record, select:

- Start recording for # Minutes

  Once started, recording will continue for the number of minutes determined by your surveillance 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 surveillance 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, although you must select them one by one.

Take snapshots

As an alternative to exporting video evidence, you can take a quick snapshot of an image if you want to save or share a still image. You can take a snapshot from the **Live**, **Playback** or **Sequence Explorer** tab, or from a carousel, hotspot or the camera navigator.

- To take a snapshot, on the camera toolbar of a selected camera, click the snapshot icon: . When a snapshot is taken, the snapshot icon momentarily turns green

You can view your snapshot by browsing to the snapshot file location. Snapshot files are saved in the default file location specified in **Application settings** (see Settings window (explained) on page 27).

If the image contains a privacy mask, this privacy mask is also applied to the snapshot image.

Investigating incidents

You investigate incidents mainly on the **Playback** tab using the timeline. However, you can also search for sequences based on motion detection, events, or bookmarks on the **Sequence Explorer** tab. 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.

Timeline (explained)

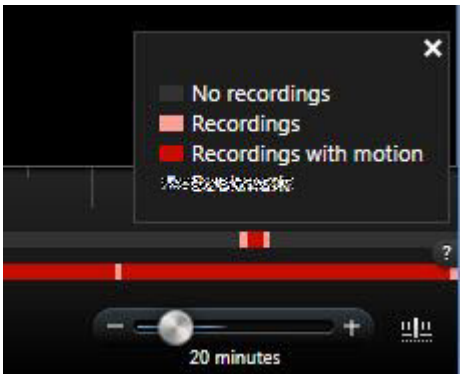
The timeline displays an overview of periods with recordings from all cameras displayed in your current view.

Two timelines are displayed in the timeline area. The upper timeline shows the selected camera's recording periods and the lower one 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 to move backward in time; drag to the left to move forward in time. You can also use the scroll wheel of your mouse to move the timeline backward and forward. To adjust the range of the timeline, press **CTRL** and use the scroll wheel at the same time.

The timeline is displayed in light-red to indicate recording, red for motion, light-green for incoming audio, and green for outgoing audio. If there are additional sources of data available, these will be shown as other colors. See Additional data (explained) on page 161 and Additional markers (explained) on page 161.

On the timeline, to the far right, click the small question mark for a legend of color codes.



Timeline and Milestone Interconnect (explained)

If the selected camera is part of a Milestone Interconnect setup, and it is an interconnected device, the timeline for the selected camera displays the retrieval data. Retrievals that have taken place are displayed as recordings. On the timeline, shading lets you quickly identify which periods contain recordings and which periods you need to request a retrieval (see Retrieve data from Milestone Interconnect on page 162) for.

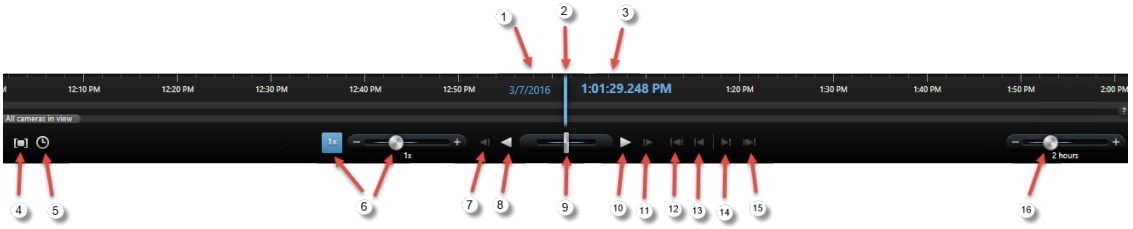
- Dark gray indicates that there are no recordings for the time
- A dark checkerboard pattern indicates that no recordings have been requested and therefore it is unknown

whether there are recordings

- Red shading indicates that there is a recording
- A light checkerboard pattern indicates that data has been requested for retrieval

The timeline with dark checkerboard pattern where no recordings have been requested and therefore it is not known whether there are recordings and the lighter checkerboard pattern where video has been requested for retrieval

Time navigation controls (explained)



1 and 3 - The playback date and time is the time to which all the cameras are tied, except if you are in independent playback mode. When you play back recordings, all video in the view will be 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 camera's database prior to the specified point in time will be displayed in the view, and the image will be dimmed.

2 - The **Timeline time** is indicated by a blue vertical line.

4 - : Select a period of time by dragging the start and end time indicators on the timeline (typically when you are exporting video (see XProtect format settings on page 168). Click again to see the timeline with no time selected.

5 - : Jump to a specific point in time by specifying the date and time.

6 - 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.

7 - : Move to the image just before the one currently viewed.

Play buttons

8 - : Play backward in time.

 **Pause**: When you click either **Play backward in time** or **Play forward in time**, the button turns into a pause button. This lets you pause playback without having to move your mouse pointer.

9 -  : Adjust the speed. Drag it to the right to increase forward play speed. Drag to the left to increase backward play speed.

10 -  Play forward in time.

11 -  Move to the image just after the one currently viewed.

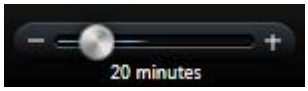
Navigation buttons

12 -  Move to the first image in the database for the selected camera.

13 -  Move to the first image in the previous sequence.

14 -  Move to the first image in the following sequence.

15 -  Move to the last image in the database for the selected camera.

16 - 

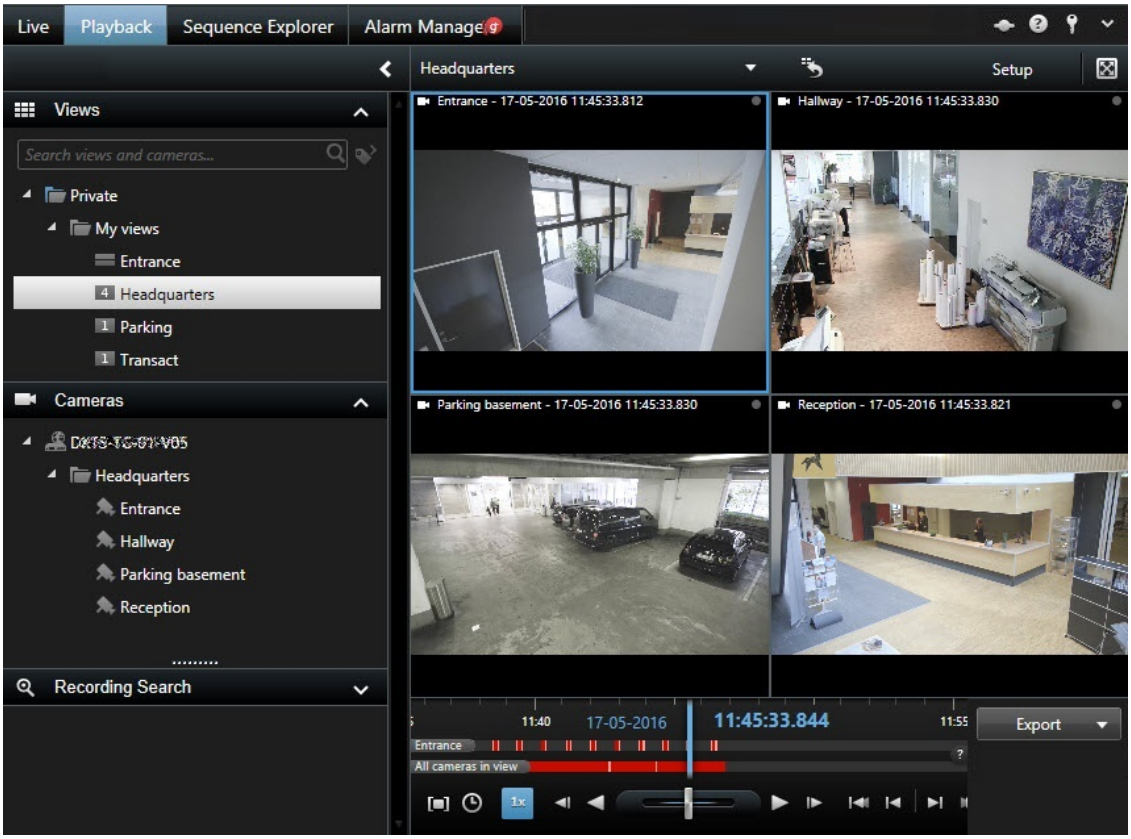
Specify the time span of playback in the timeline.

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.

Viewing recorded video (explained)

You view recorded video on the **Playback** tab of the XProtect Smart Client. When you select the **Playback** tab, the XProtect Smart Client connects to the surveillance system server and displays recorded video from the cameras in the selected view. In this way, you can play back recorded video.



On the **Playback** tab, all cameras in a view display recordings from the same point in time (the master time) by default . However, you can view and navigate recordings from individual cameras independently of the master time (if this is enabled in the **Settings** (see Functions settings on page 30) window). You can also use independent playback to view recorded video from the **Live** tab.

Particular user rights may be required in order to access the **Playback** tab, and, depending on your user rights, access to browsing video from some cameras may be restricted.

View recorded video independently of timeline

When you play back video on the **Playback** tab, all recordings in the view are synchronized with the timeline. For individual cameras, you can play back video independently of the timeline.

You can only use this feature for ordinary single-camera positions, not for hotspots, carousels, or Matrix positions.

Requirements

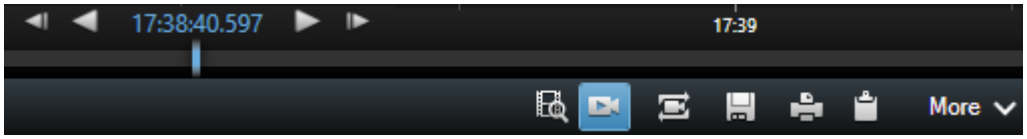
In the **Settings** window > **Functions** tab, the **Independent playback** option must be set to **Available**.

Steps:

1. Move your cursor to the bottom of the camera that you want to view recorded video from. On the toolbar that appears, click the **Independent Playback** button.

   The independent playback timeline appears:

2. Drag the timeline to set the start time.
3. If you want to view recorded video for the selected time on all the cameras in your view at once, on the toolbar, click the **View recordings from selected time on Playback tab** button: . This displays the **Playback** tab with all cameras synchronized to the time you have selected.

Searching for video sequences

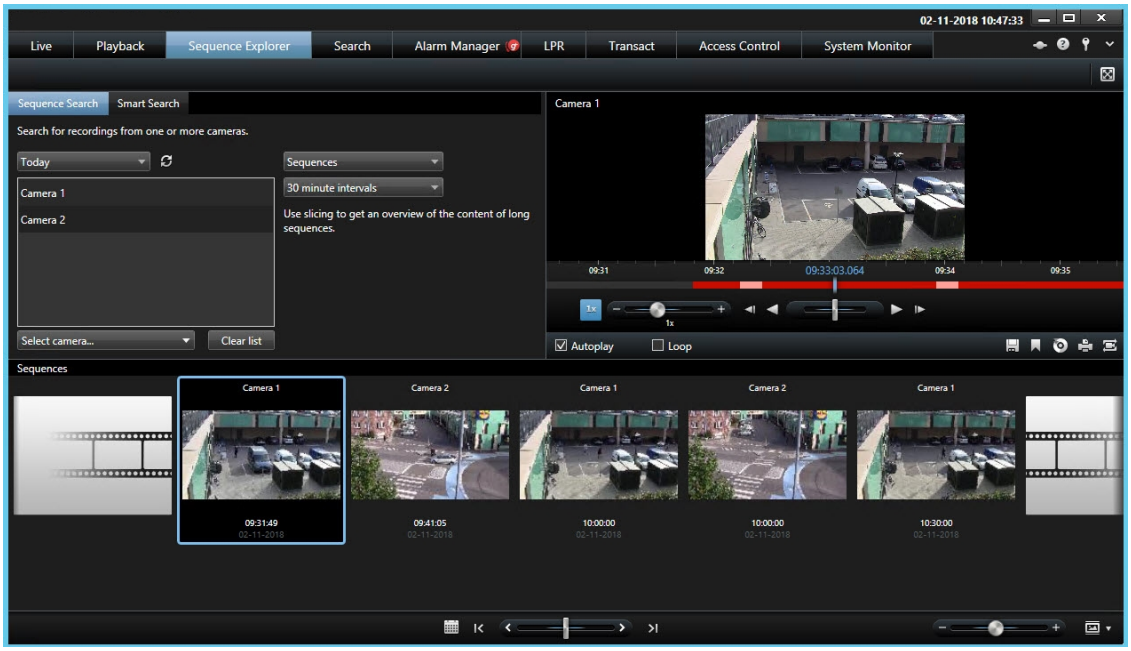
The **Sequence Explorer** tab lets you investigate an incident by searching sequences of video. There are two ways of doing this:

- **Sequence Search** - search recordings from several cameras based on motion detection and events. Depending on your XProtect VMS, you may be able to search based on bookmarks, too.
- **Smart Search** - search for motion only in selected areas on a single camera

> You can also search for sequences with motion or bookmarks in the **Recording Search** pane on the **Playback** tab. See Search for sequences or bookmarks in Recording Search pane on page 159.

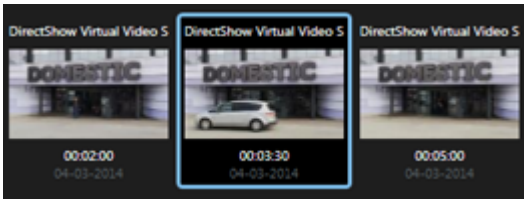
Searching for sequences or bookmarks (explained)

With **Sequence Search** on the **Sequence Explorer** tab, you can investigate recordings from selected cameras. You specify whether you want to search for **Sequences** with motion **or Bookmarks**. The recorded video is shown in a thumbnail overview where you can browse recordings and play them instantly in the player window.



You can adjust the size of the thumbnails by dragging the slider below the thumbnail overview:

The thumbnails can relate to an individual selected camera or several selected cameras in a view. To view video associated with a particular thumbnail, click the thumbnail. When you click a thumbnail, it becomes highlighted and (if **Autoplay** is selected) the associated sequence is played back in the right-hand side.



If you have clicked a thumbnail, and then navigated away from it by dragging the thumbnail overview left or right, you can quickly return to the selected thumbnail by clicking the refresh button.

The thumbnail overview only shows recording within the time interval you have specified. Unless you have selected to view all sequences, you can navigate the timespan backward or forward by placing the mouse in the left or right side of the thumbnail overview.

Sequence Explorer - search for sequences

When you are in Sequence Explorer > Sequence Search, you must specify that you want to search for **Sequences**.

1. Select **Sequences** in the list.
2. Select a time interval, for example **Today** or define a **Custom interval**.
3. In the **Search for camera** list, select one or more cameras, or search for a camera. You can add up to 100 cameras in a sequence search.
4. In the list just below **Sequences**, select a value to display thumbnails for specific intervals of time, for example one thumbnail for every 30 seconds. You can also specify your own intervals with **Custom slicing interval...**.

   If you have continuous recordings, or recordings of long duration, it is especially useful to use slicing to divide the thumbnails into shorter sequences.

5. As the list of thumbnails update, you can start selecting the thumbnails to view the sequences.

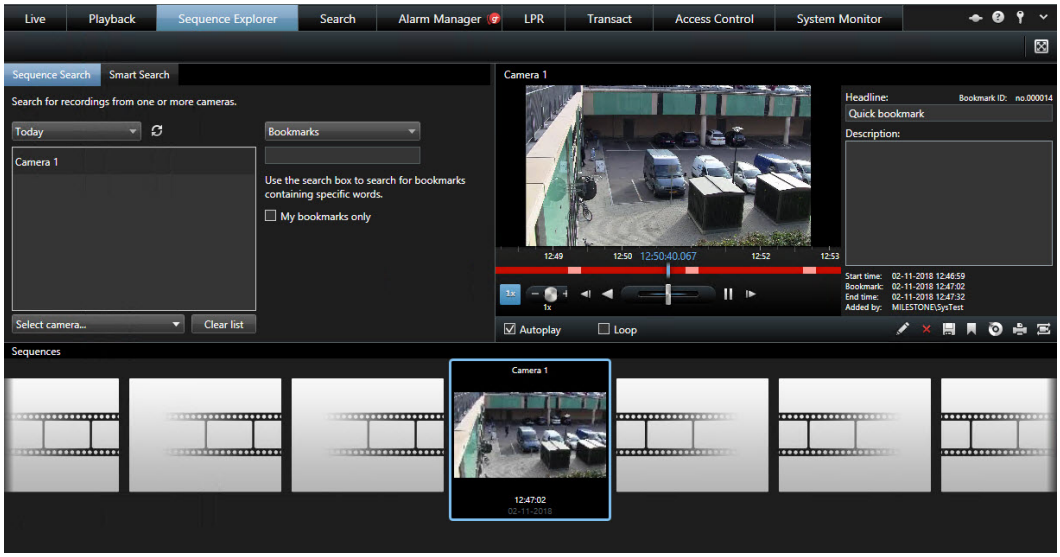
Sequence Explorer - search for bookmarks

The bookmark feature is only available with certain XProtect products. For more information, see Surveillance system differences on page 21.

When using **Sequence Search** on the **Sequence Explorer** tab, you must specify that you want to search for **Bookmarks**.

1. Select **Bookmarks** in the list.
2. Use the search field to search for bookmark headlines or descriptions. Matching results are shown instantly in the thumbnail overview.
3. To get only the bookmarks created by you, select the **My bookmarks only** check box.

4. If the system finds any bookmarked sequences, click the thumbnail to play back the video and view details about the bookmark.



5. Depending on your user rights, you may be able to edit, delete, print, or export the bookmark:

When you delete a bookmark, the bookmark is deleted not only from the thumbnail overview but from the entire surveillance system.

Thumbnail overview (explained)

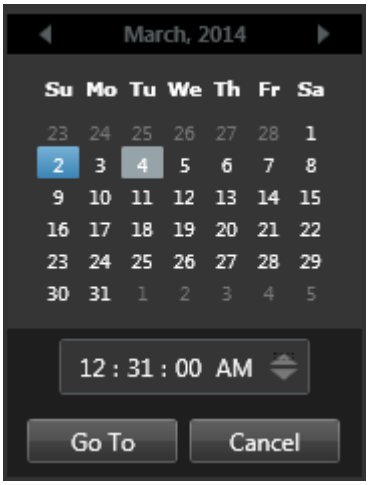
In **Sequence Explorer** > **Sequence Search**, you can navigate forward and backward in time by dragging the thumbnail overview left or right, or you can use the navigation controls below the thumbnail overview.

The sequence slider

Drag the sequence slider, located below the thumbnail overview, to the left (backward in time) or right (forward in time).

Pick date and time

Click the  icon below the thumbnails to access a calendar where you can specify a date and time.



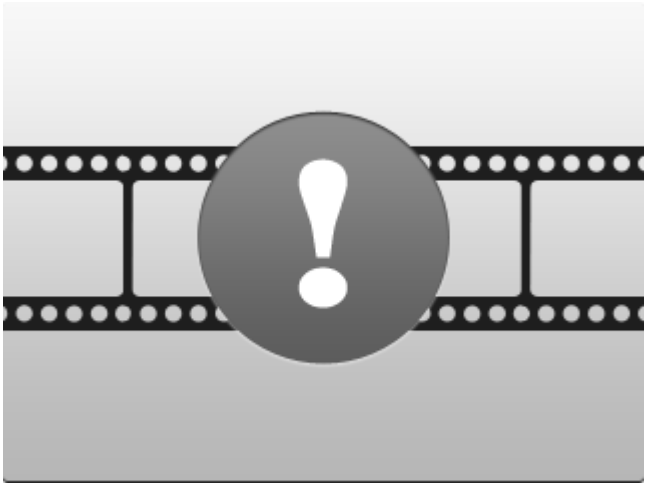
Navigate within time interval

The thumbnail overview only shows recordings within the specified time interval. Using the buttons in the thumbnail overview, you can navigate the sequences within the time interval you have specified. Here is a description of some of the buttons:

Button	Description
	z
	Go to latest sequences.
	Expand time interval to show earlier sequences.
	Expand time interval to show later sequences.
	End of database. No more sequences available.

Thumbnails with exclamation marks (explained)

In **Sequence Explorer** > **Sequence Search**, you may occasionally see placeholder thumbnails with exclamation points if there is no recorded image from a specific point in time:



These appear when the **Sequence Explorer** cannot retrieve a proper thumbnail, for example, because of a server communication error, a decoding error, or similar. However, placeholder thumbnails may also appear when thumbnails retrieved from the surveillance system do not exactly match requested points in time. This is because deviating thumbnails could otherwise cause confusion.

If you have selected slicing in **Sequence Search**, a placeholder thumbnail appears if the retrieved thumbnail is outside of the requested time interval. Example: You request a time interval of 12:00:00, 12:00:30, and the first available thumbnail is at 12:00:33. If there are no recording sequences that cover this interval, the system makes no attempt to retrieve a thumbnail. The next thumbnail displayed is from the next interval (12:00:30-12:01:00). If there are recording sequences that cover this interval, a placeholder thumbnail will appear instead.

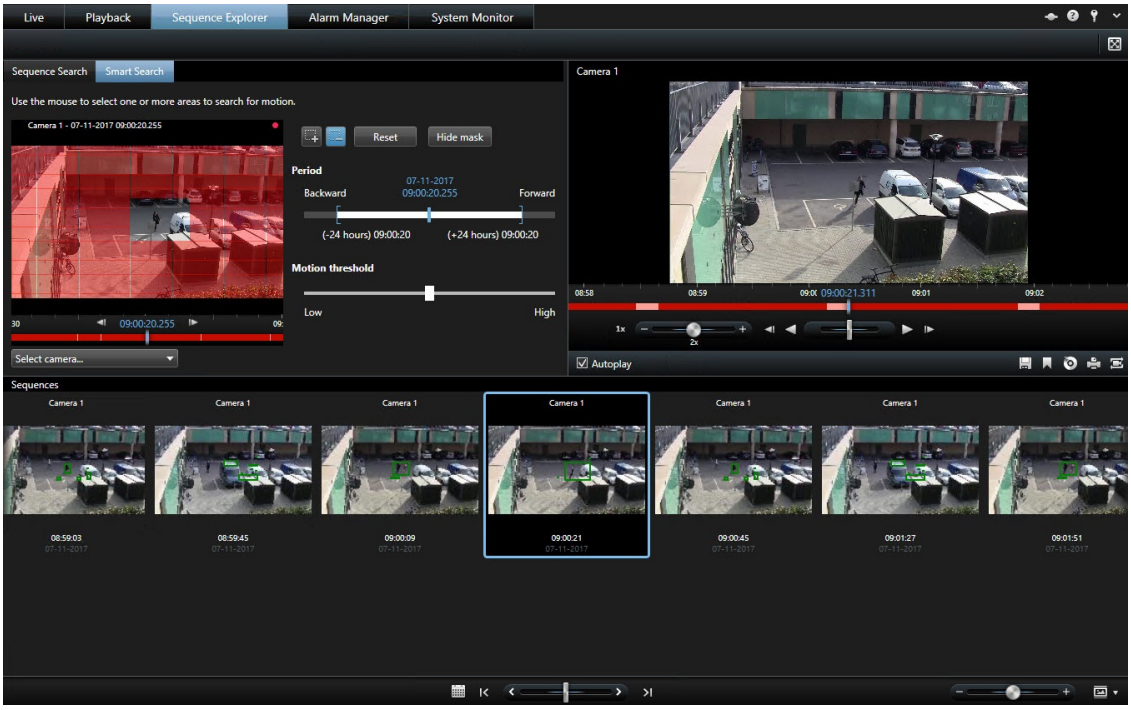
In **Sequence Search**, a placeholder thumbnail appears if the retrieved thumbnail is more than three seconds off compared with the requested time, for example the time when recording of the sequence in question was triggered on the surveillance system.

You can still click a placeholder thumbnail to view video; it will take you to the first available recording after the point in time represented by the placeholder thumbnail.

Searching for motion in selected areas (explained)

Use Smart Search to search for motion in selected areas of a recording. For example, Smart Search is useful when you want to identify when a package was removed from a shelf, or when a person entered through the back door. If you know where an incident occurred and the camera that covers the area, you can look for motion in that specific area in the recording.

By default, the whole selection image is masked. To search for motion in a specific area, you must unmask that area. The system displays search results as thumbnail sequences with green boxes around areas with motion.



Smart Search is based on motion metadata that is generated along with the motion-recorded video. Your system administrator can enable or disable Smart Search for cameras on the server, and can specify settings such as sensitivity, processing time, and detection methods. If your search does not produce results, Smart Search may not be enabled for the camera.

Search for motion in seleted areas

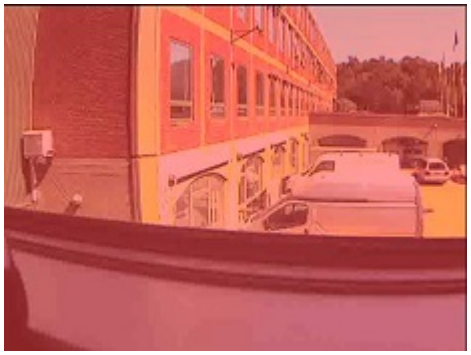
Use Smart Search to investigate an incident by searching for motion in selected areas of a recording. For more information, see Searching for motion in selected areas (explained) on page 156.

Depending on your product, you can activate Smart Search in one or both of these ways:

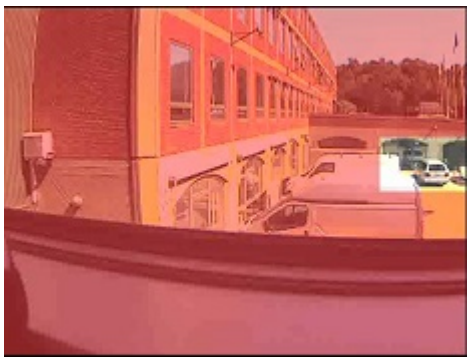
- By clicking the button in the camera toolbar on the **Playback** tab
- By clicking **Smart Search** on the **Sequence Explorer** tab.

Steps:

1. When you have activated smart search, if the camera is not already selected, select the camera that recorded the video. An image is displayed from the camera with a mask applied.



2. To specify where to search, click the button, and then click and drag in the image to unmask the area. Repeat this step to unmask more areas.



> To temporarily switch between mask and unmask modes, press and hold the **CRTL** button.

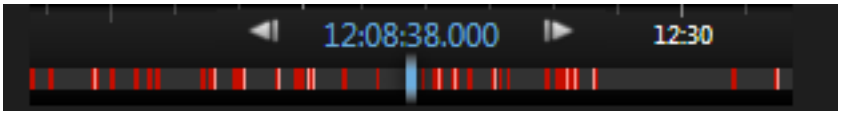
3. Under **Period**, use the time selector to specify a time-frame for the search.
4. Under **Motion threshold**, use the slider to specify how much motion to search for. Higher thresholds require more motion and produce fewer search results, and lower thresholds produce more.
5. Optional: Use the timeline to specify the time to start searching from. You can search forward and backward in the recording.
6. The search results are displayed in the lower section as thumbnails. Click them to play back the recordings.

Smart Search - adjusting time (explained)

You can set the time that you want Smart Search to search from. The preview image is shown from the selected time.

You can also define a period to search within. The period is always based on the start time that you have selected. To select a start time, you have two options:

- Drag the timeline below the preview grid left or right to set the start time. Available recordings are indicated with colors. You can also use the arrows to go to previous or next frame
- Click the current time to access a calendar where you can specify a date and time. Click **Go To** to set this time as start time



Smart Search - motion threshold (explained)

The motion threshold allows you to define the smart search sensitivity.

The **higher** the threshold you select, the more motion you need in the selected areas before the motion is detected by Smart Search.

The **lower** the threshold you select, the less motion you need in the selected areas before the motion is detected by Smart Search.

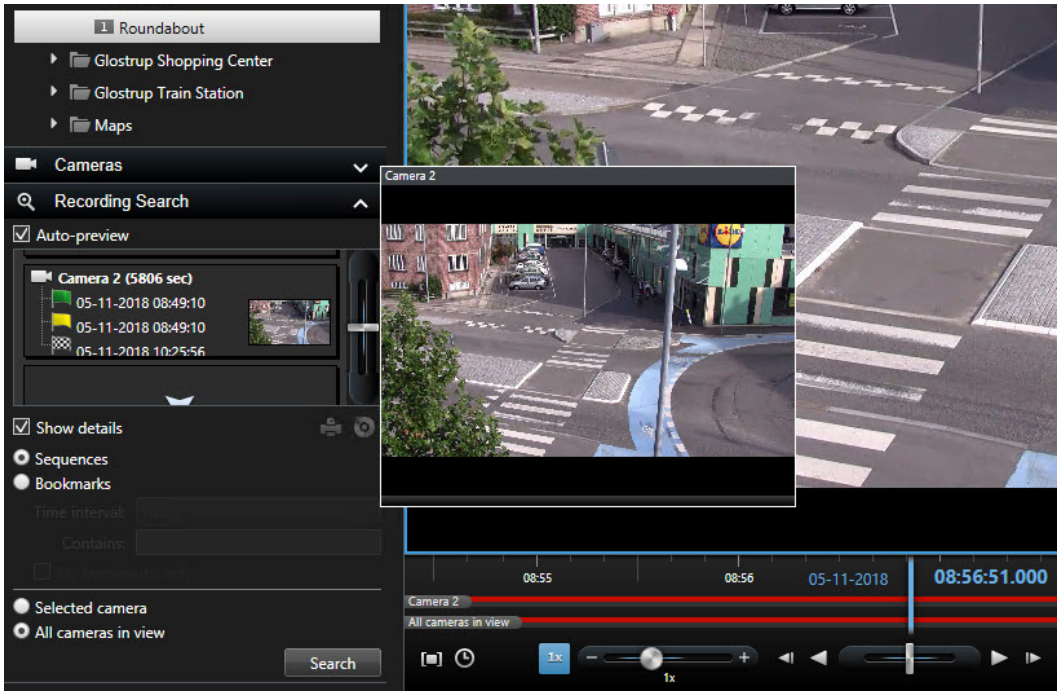
> A low threshold does not necessarily give more results. A high threshold does not necessarily give less results.

Search for sequences or bookmarks in Recording Search pane

There are different ways of searching for video recordings. You will find most options on the **Sequence Explorer** tab, but you can also search for sequences or bookmarks in the **Recording Search** pane on the **Playback** tab.

Steps:

1. On the **Playback** tab, open the view that contains the cameras that you are interested in.
2. Use the timeline to specify time and date. This is the starting point of the search.
3. Expand the **Recording Search** pane in the left-hand side.



4. To select a specific camera, select a camera in the view and then select the **Selected camera** radio button at the bottom of the **Recording Search** pane.
5. To select all cameras, select the **All cameras in view** radio button.
6. To search for sequences:
    1. Select the **Sequences** check box.
    2. Click **Search**.
7. To search for bookmarks:
    1. Select the **Bookmarks** check box.
    2. Select the search criteria you are interested in, for example, time interval, your bookmarks only, or search words that may be part of the bookmark information.
    3. Click **Search**.

    The sequence closest to the time you have selected appears in the middle of the list.
8. Select a sequence to move the video in the view to the time of the selected sequence.
9. To quickly preview the video, hover over the sequence or bookmark. The **Auto-preview** check box must be selected.

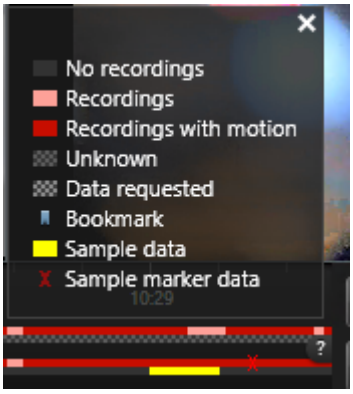
10. When you have selected a sequence or bookmark in the list, you can generate a printed report or export it . For a bookmark (depending on your user rights), you can also edit or delete it.

To display more details about each sequence or bookmark in the list, select **Show details**. For sequences, this displays the date and time of the first image in the sequence (green flag), the last image (checkered flag), and the motion detection, event, that triggered the recording (yellow flag). For bookmarks, **Show details**, displays additional information, consisting of an image from the bookmark time as well as a detailed description (if one is available).

Additional data (explained)

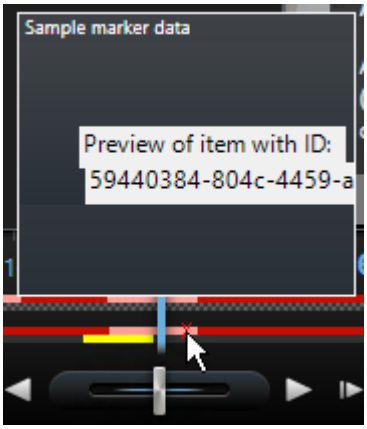
If you have additional data under **Timelines** enabled for the Smart Client profile and additional sources are available, you will be able to see an additional layer in the timeline that designates the defined data. This allows you to view additional data that is added by other sources.

The color and the name of the additional data are defined by the source. You can see these in the legend.

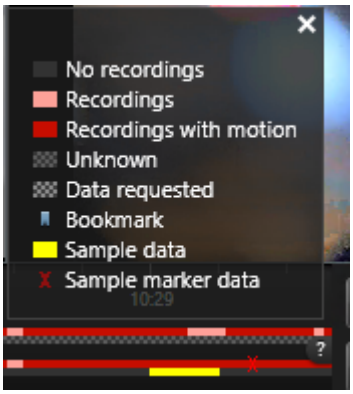


Additional markers (explained)

If you have **Additional markers** under **Timelines** enabled for the Smart Client profile and additional sources are available, you will be able to see additional markers in the timeline that designate incidents provided by the source. These can appear as popups in the timeline.



The icon and the name of the additional markers are defined by the source. You can see these in the legend.



Retrieve data from Milestone Interconnect

Milestone Interconnect™ allows you to integrate a number of independent surveillance systems, for example, mobile installations on ships or busses, with a central site.

If your XProtect Smart Client is part of a Milestone Interconnect setup and at least one of your cameras supports edge storage and you have the necessary user rights, you can retrieve data from one or more interconnected devices.

1. On the **Playback** tab, in the timeline, click the **Time Selection Mode** button to select the start and end time of the sequence you want to retrieve data for.
2. To the right of the toolbar, click **Retrieve** to open the **Retrieval** window.
3. Select the relevant camera(s) and then click **Start Retrieval**.

You can view the progress of your retrieval jobs in the **Status** window (see Status window (explained) on page 141) by clicking the **Status** button on the Application toolbar.

- To stop a retrieval job that is in progress, either click **Stop** in the notification area at the top of the workspace area, or in the **Status** window, next to the job that is in progress.

Creating 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.

For information about evidence locks and how to export them, see Working with evidence locks on page 203.

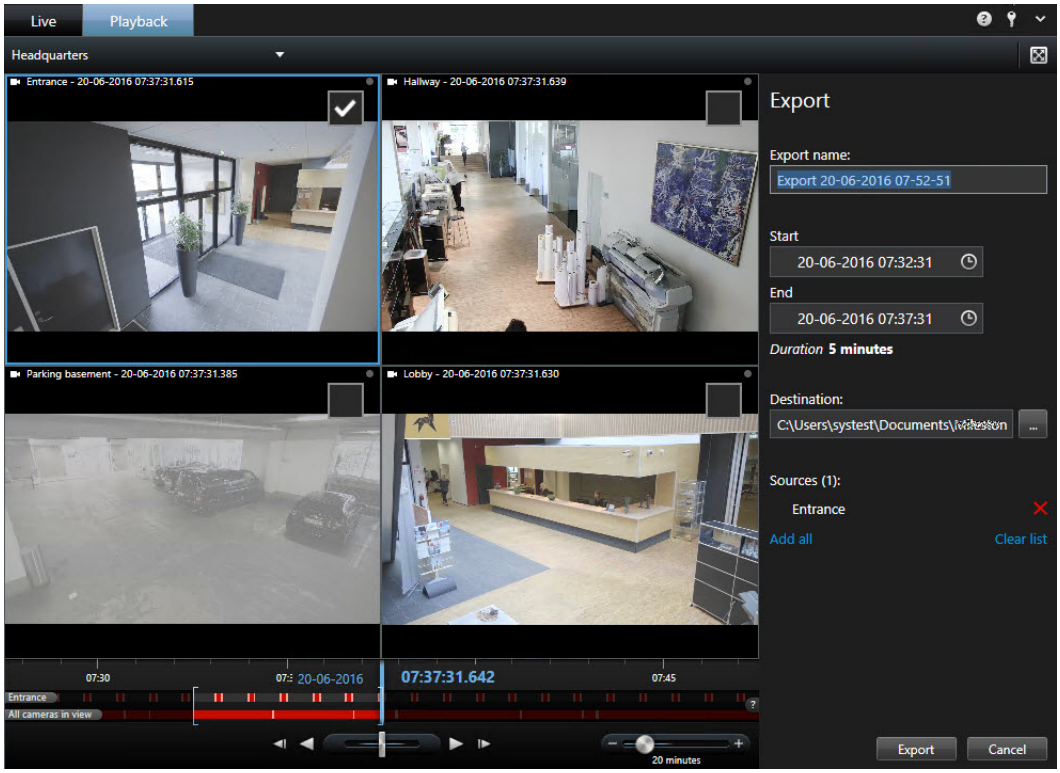
Export video in simplified mode

In the simplified mode, you can export video to document an incident.

Privacy mask, the media player format, and still images are features that are available only in advanced mode. Click  and then  to switch to advanced mode.

1. Select the view containing the cameras that caught the incident.
2. On the **Playback** tab, to the right of the timeline, click the **Export** button. The **Export** panel appears. Only the camera in focus appears in the **Sources** list.

3. For each camera you want to include in the export, select the associated checkbox. If the same camera appears more than once in a view, automatically all of them are selected.



4. You can also include cameras from other views. If you change the view, you will not lose your export settings.
5. Specify the start and end time. You can also set the time interval in the timeline by dragging the square brackets to the left or right.
6. Click **Export**. The panel is closed, and a green status bar in the upper right corner indicates the progress of the export.
7. When the export is complete, you can click the **Details** button in the status bar to view the exported video.

If a plug-in that supports export is added to the export list, any related cameras are automatically included.

Export video in advanced mode

When working in advanced mode, not only can you export a video clip. You can also export audio, XProtect data, and still images.

1. On the **Playback** tab, in the timeline, click the **Time Selection Mode** button to select the start and end time (see Time navigation controls (explained) on page 148) of the sequence you want to export.
2. For each view item you want to export, select the check box  associated with it.
3. To the right of the timeline, click **Export** > **Export** to open the **Export** window.
4. To include additional view items, click **Add item** button to select them.
5. In the **Export name** field, enter a name for the export. The system automatically creates a name with the current date and time. You can change the name.
6. Specify a path, a media burner, or both, for the destination of the export.
7. Click the relevant tab to select one or more of the following formats to export to:
   - **XProtect format** - use the XProtect database format, with the option to include the XProtect Smart Client – Player along with the export. If you choose this option, other media players will not work
   - **Media player format** - use a format that most media players can play. This requires that a media player is installed on the computer that will play the video
   - **Still images** - export a still image file for each frame for the selected period
8. If you want the receiver to be able to verify that the exported evidence has not been tampered with, select the **XProtect format** and **Include digital signature** check boxes. This will enable the **Verify Signatures** button in the XProtect Smart Client – Player.
9. Click **Start Export** to export your evidence.

If you want to cover specific areas of a video in the export, you can add privacy masks. 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 Mask areas in a recording during export on page 166.

For information about the settings for the format you selected, see Export window settings on page 167.

Export items directly from the Export window

To export items by adding them directly in the **Export** window, follow these steps:

1. On the **Playback** tab, to the right of the timeline, click **Export** > **Export** to open the **Export** window with an empty **Item** list.
2. Click **Add item** to add the items, for example cameras, that you want to add to the export list.

3. Click each export item and then specify its start and end time in the preview pane to the right of the list. Repeat for all items in the list.
4. In the **Export name** field, enter a name for the export. By default, the system uses the current date and time. You can change the name.
5. Specify a path or media burner for the destination of the export.
6. Click the relevant tab to select a format to export to.
7. Specify the necessary settings (see Export window settings on page 167) for the format you have chosen. Based on these settings, the program estimates and displays the size of the export at the bottom of the window.

   If the video contains items or information that you do not want to be visible in the export, you can add a privacy mask to hide those areas in the video. For more information, see Mask areas in a recording during export on page 166.

8. Click **Start Export** to export your evidence.

If you want to make changes or add more items later, click **Cancel**. When asked if you want to remove the selected export items, click **No**. This ensures that your list of export items is available in the Export window when you open it again.

Mask areas in a recording during export

When you export video, you can add privacy masks to cover selected areas. When someone watches the video, the areas with privacy masks appear as solid blocks.

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. For more information, see Privacy masking (explained) on page 208.

Steps:

1. In the **Export** window, click the **Privacy mask** button. A window appears.
2. Click the button, and then drag the pointer over the area that you want to mask. To mask more areas, repeat this step.
3. To unmask part of a privacy mask, click the button, and then drag the pointer over the area of the mask that you want to unmask. Repeat this step for each part to unmask.

4. You can temporarily switch between mask and unmask modes by pressing the **CRTL** button while you make a selection.
5. Click **OK** to return to the **Export** window.

The preview image contains an invisible grid with cells. If the area you select includes any portion of a cell, the system masks the entire cell. The result can be that the system masks slightly more of the image than you intended.

If you just want to view the image without masks applied, click and hold the **Hide mask** button. The mask reappears when you release the button.

Export window settings

Depending on your user rights, type of server, and what has been set up on the server, certain export settings may be restricted and unavailable.

You can use privacy mask, the media player format, and still images only in the advanced mode.

With XProtect Smart Client you can quickly export recorded evidence in movie clip, audio, still images, or in the XProtect format. The export can be either a single sequence or a storyboard (see Exporting storyboards (explained)). The format and settings you choose are stored and displayed next time you export.

Name	Description
Export name	The program automatically fills this in with the local date and time, but you can rename it. The folder or disk that you save or burn to inherits the export name.

Name	Description
Item	Lists the items selected for export, for example video sequences. For each item, you can change the time and date. If you click the date, a calendar opens. Here, you can select a new date to view. Click **Go To** to change date. You can change the start and stop time of the item by using the time indicator underneath the calendar. Click an item to see a preview of the export clip in the preview pane to the right of the **Item** list. If you select more items by holding down the SHIFT or CTRL button and clicking extra items, you get access to multiple previews. You can adjust the start and stop time on the timeline for each preview. 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 pane, you can edit the start and end time of each item.
Add Item	Use the **Add item...** button to select other items that you want to include in the list for exporting. Use the **Remove All** button to clear the list in the **Item** window.
Export destination	**Path** - You can specify a path yourself (the field may suggest a path for you). When you specify a path this way, the folders you specify do not have to be existing ones. If they do not already exist, they are created automatically. **Media burner** - Select a 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 on 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 208.

XProtect format settings

Export in the XProtect format is available when connected to selected surveillance systems (see Surveillance system differences on page 21) only. Depending on your user rights, access to exporting evidence from some or all cameras may be restricted.

Name	Description
Include XProtect Smart Client – Player	Select to include the XProtect Smart Client – Player application with the exported data. The XProtect format can only be viewed with the XProtect Smart Client – Player.
Prevent re-export	Select that you do not want to allow the video or audio to be re-exported—your recipients will not be able to export in any format.
Password protect	Select the strength of the encryption you want to apply to the exported data. When you click **Start Export**, the system asks you for a password that must contain at least eight characters.
Include digital signature	Select to 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 the recipient opens the exported files, he/she can verify the signature (see Verify digital signatures on page 242) in the XProtect Smart Client – Player. 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. 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.
Comments	Click to open the **Add Comments to Export** window, where you can add comments to individual cameras or to the project as a whole.

Export storyboards

If you want to export a number of items that make up a storyboard (see Export a storyboard), follow these instructions:

1. On the **Playback** tab, in the timeline, click the **Time Selection Mode** button.
2. For each item that you want to export, select the start and end time (see Time navigation controls (explained) on page 148) and then click **Export** > **Add to export list.** This adds each item to the list of exports without opening the **Export** window. Repeat until you have added all items that you need for your storyboard.
3. To the right of the timeline, click **Export** > **Export** to open the **Export** window. All selected items are displayed in the **Item** list, ready for export.

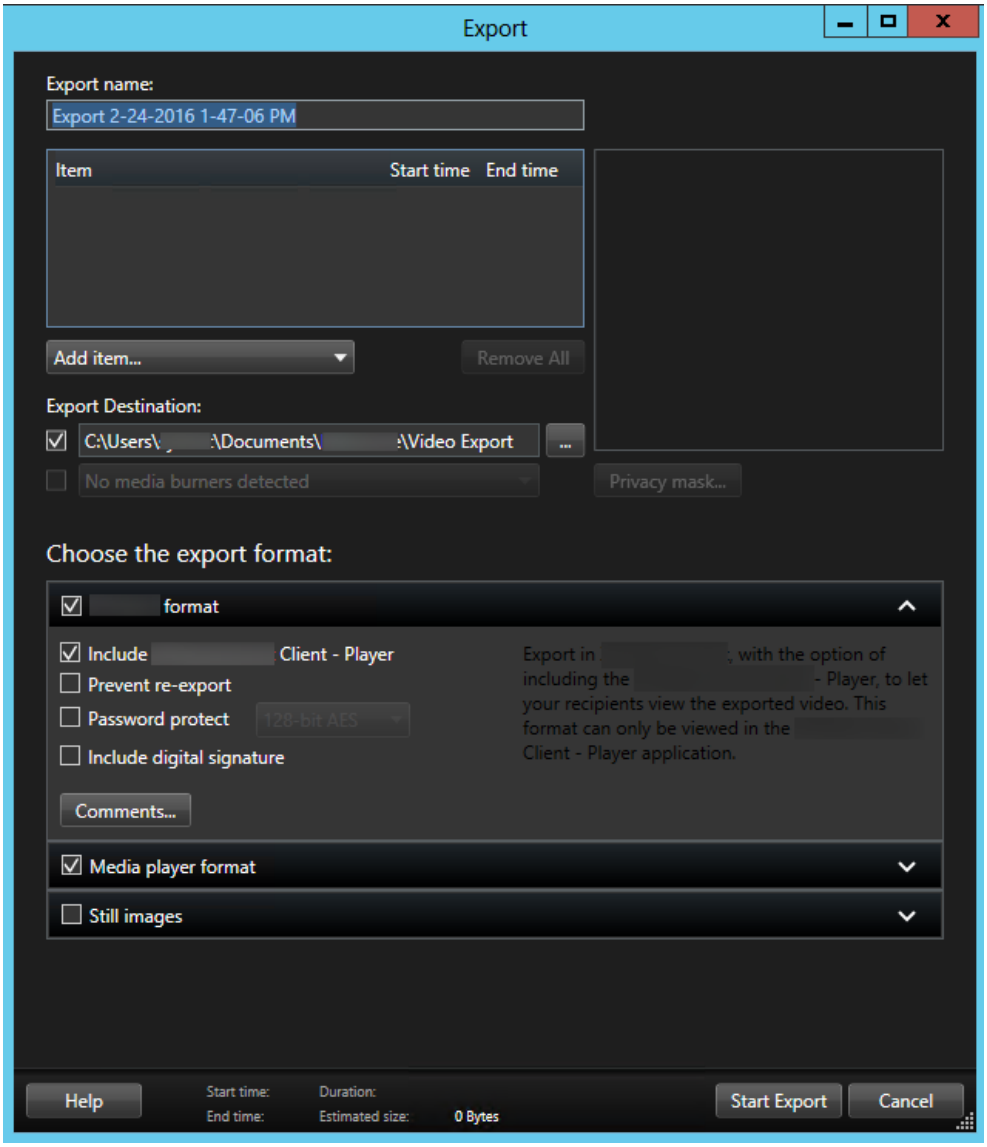
   Click **Add item** to add additional items. Click **Delete All** to clear the list.
4. In the **Export name** field, enter a name for the export. The program automatically creates a name with the current date and time. You can change the name.
5. Specify a path and/or media burner for the destination of the export.
6. Click the relevant tab to select a format to export to.
7. Specify the necessary settings (see Export window settings on page 167) for the format you have chosen. Based on these settings, the program estimates the size of the export and displays this in the bar at the bottom of the window.
8. Click **Start Export** to export your evidence.

If you want to make changes or add more items later, click **Cancel**. When asked if you want to remove the selected export items, click **No**. This ensures that your list of export items is available in the Export window when you open it again.

View exported video

The exports you create in XProtect Smart Client are stored in a default folder on your local computer, unless you have specified a different folder. You can view an export immediately after creating it, or later.

1. To view the exported video immediately after creating it:
    1. Create the export as described in Export a video clip, audio, XProtect data or a still image (see Export video in advanced mode on page 164).



    2. Click the **Details** button in the upper right corner when the export is complete. A dialog box appears with a link to the output folder.
    3. Click the link to open the output folder.

2. If you have exported video at a previous point in time:
    1. Go to the folder where you store export files. The default location is *C:\Users\<username>\Documents\Milestone\Video Export*. You can check the folder location in the **Export** window. 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.

Frequently asked questions: exporting

Can I export audio too?

When exporting in the media player and XProtect formats, you can—if your surveillance system supports this—include recorded audio in the export. Export in the database format is only available if connected to selected surveillance systems. For a detailed outline of the features available on your particular system, see the XProtect Product Comparison Chart on: https://www.milestonesys.com/. When exporting in the JPEG (still image) format, you cannot include audio.

If I export a bookmark video clip, what is included in the export?

The entire bookmark video clip (see Bookmarks (explained) on page 194) is included, from the specified clip start time to the specified clip end time.

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).

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 21), 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 signature to the exported material. See XProtect format settings on page 168.

Print video evidence

You can print single still images or whole views from recorded video in several ways. When you print, the image is automatically included in a surveillance report that you can add notes to. The steps describe how to print on the **Playback** tab.

1. To print a recorded still image, on the Playback tab, open the view that contains the camera you are interested in.
2. Hover over the view item. The camera toolbar appears.
3. Click the  icon. A window appears.
4. Add notes if required.
5. Click **Print**.

You can also print information about alarms (see Alarms (explained) on page 196) if your organization uses the alarm handling features. Or, you can print real-time still images on the **Live** tab.

Working with views

Views are located on the **Live** and **Playback** tabs and contain cameras and other types of content. If views have been assigned shortcut numbers (see Assign a shortcut number to a view on page 54), you can select a view by using keyboard shortcuts (see Keyboard shortcuts (explained) on page 143).

Searching for views and cameras (explained)

You can search directly for available views and cameras. Not only by searching for names, but also by searching for description, type and keywords.

You can find an overview of common keywords if you click  next to the search field.

You can see matching results for views and cameras while you type.

When you search for cameras in live and playback mode, you can view the cameras in a temporary view that is optimized for the amount of cameras you select.

You can click a single camera to view it in a 1:1 view, or you can click the heading of the camera results to view all discovered cameras (or the first 25). You can also select cameras manually if you press either **CTRL** or **Shift** while clicking one or more cameras. Press **Enter** to view the cameras.

You cannot create new views based on temporary views.

Camera characteristics that you can search for

- 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 surveillance 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, all cameras of this type can easily be found.

Change cameras in views

You can temporarily change the cameras that are displayed 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.

You cannot change cameras if the view contains a hotspot, carousel, or Matrix (see Matrix (explained) on page 225) content. If used from the **Cameras** pane, the feature works with Smart Wall (see XProtect Smart Wall (explained) on page 22) positions as well.

Steps:

1. Select the relevant position in the view.
2. Do one of the following:
   - In the **Cameras** pane, drag the relevant camera into the position in the view.
   - On the camera toolbar, click **More** > **Send to window** > **Main Window**, and then select a position 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 on page 176

Swap cameras

You can temporarily swap two cameras in a view. The camera in that position 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 position in your view.

Steps:

1. Click the relevant camera title bar and drag it to a new position.
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 camera position to a single-camera position in another open view, including any views you may have in floating windows or on secondary displays.

This feature is not available for hotspots, carousels, or Matrix (see Matrix) positions.

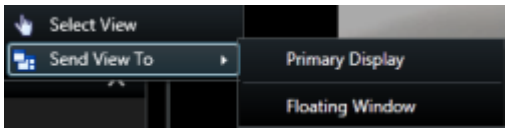
Steps:

1. On the camera toolbar, click **More** > **Send to Window**.
2. Select the destination view, and then select the position in the view where you want the video for that camera to display. If some of the camera positions are not selectable, 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 hotspots, carousels, Matrix positions, still images or HTML pages included in the view will work as usual in a floating window.

Frequently asked questions: 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 21)—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 surveillance 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 surveillance 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 surveillance 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 surveillance 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.

On the **Live** or **Playback** tab, 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 rights to perform the action myself?

Yes. This enables you to make buttons available on shared views, where colleagues with the necessary rights will be able to use the buttons, even if you do not have rights to use them yourself.

When you add a button for an action you do not have rights for, the button will appear dimmed in setup mode and will not appear when you use the **Live** tab. Colleagues with the necessary rights will be able to use the button on the **Live** tab.

What if my rights change after I have added an overlay button?

Changes to your rights 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 rights for those actions. For example, if you add a button for an action you do not have rights to perform and then your user rights change so that you do have the necessary rights, 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.

Multiple windows (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 to show the view in a separate full-screen window on your computer's main display with the main window hiding behind it
- A secondary display to show the view in a full-screen window on another monitor (if available)
- A floating window to show the view in a small separate window. You can use any number of floating windows and you can resize these to suit your needs.

Your view setup is stored in the XProtect Smart Client, so next time you log in, you can reuse it. However, this only applies to the computer on which you set it up. If you want to use multiple windows with the XProtect Smart Client on more than one computer, you must configure your multiple window setup on each computer.

For more information, click the expanding links:

Primary display

Shows the window in full screen with the tabs and controls hidden. To display the tabs and controls, click the **Toggle full screen mode** icon: .

Example of a view sent to the **Primary display**. While you are viewing the separate full screen window, the main XProtect Smart Client window is hidden behind it.

Secondary display

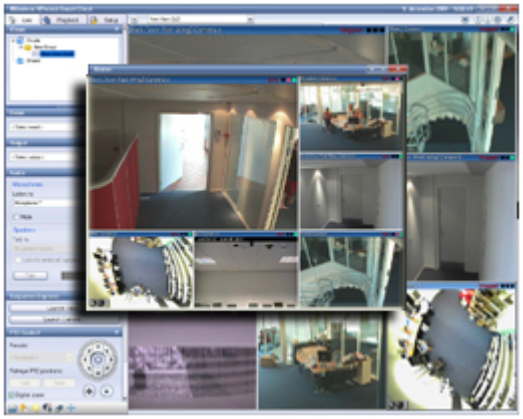
Shows the window in full screen with the tabs and controls hidden. To display the tabs and controls, click the

Toggle full screen mode icon: .

Example of an 8×8 view sent to a **Secondary display**. In this example, the main XProtect Smart Client window is available on the left display.

Floating window

Shows the selected view, with the **Live** and **Playback** tabs. You can select a new view from the toolbar by clicking the dropdown button. You can toggle between displaying the floating window as a full-screen with no tabs and as a smaller floating window with tabs by clicking the **Toggle full screen mode** icon: . You can also choose to link the floating window to the main window to synchronize time or to follow the **Live** or **Playback** tab.



Example of a view sent to a **Floating window**. The main XProtect Smart Client window is immediately available behind the floating window.

Frequently asked questions: multiple 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 Carousel settings on page 63.

Hotspots (explained)

A hotspot lets you view magnified and/or higher quality video from a selected camera in a dedicated position in a view. Hotspots are useful because you can use a low image quality and/or frame rate for cameras in the view's regular positions and a high image quality and/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 view's larger positions, for example, the large position in a **1+7** view:  .

If a position in one of your views contains a hotspot:

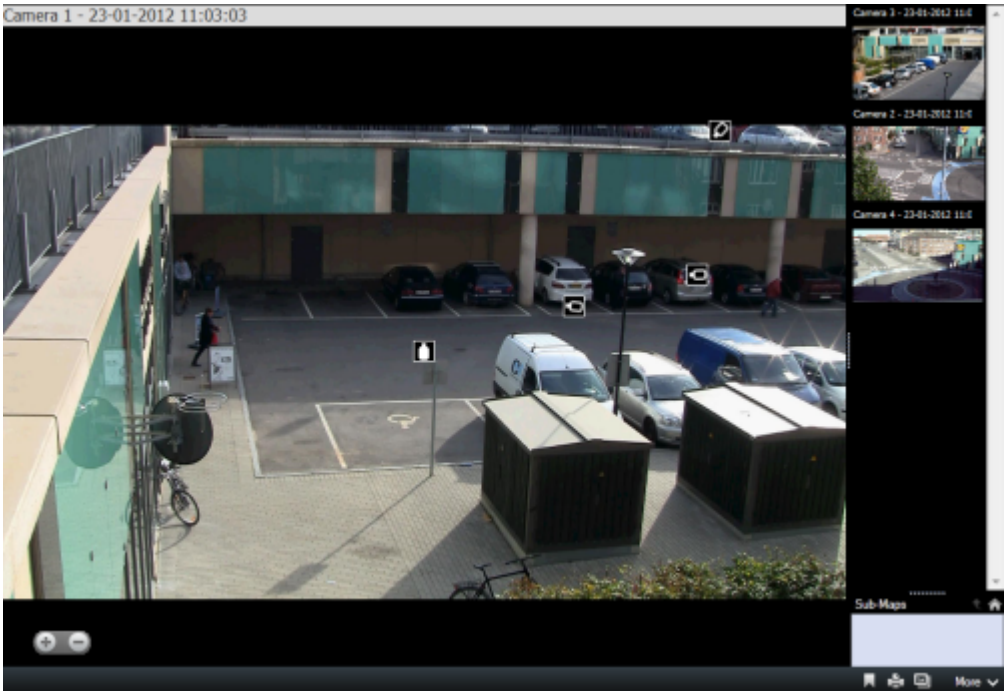
- When you click a camera in a view, the hotspot position updates with that camera's feed
- The title bar displays the hotspot icon: 

When you view live or recorded video, you can double-click a hotspot (or any other camera position 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**.

Working with camera navigator

Camera navigator (explained)

The camera navigator allows you to see several cameras in relation to each other, for example, as they are laid out according to a floor plan. This can be useful if you would like to follow someone or something from one camera to another, for example, to follow suspects as they move around a building. By setting up your cameras according to their location on a map or floor plan, you can navigate from one camera to the next from a single view.



Using camera navigator (explained)

On the **Live** and **Playback** tabs, you can see the video from the current camera in the camera navigator view, with thumbnail views of all the nearby cameras sorted according to proximity on the pane on the right. When you point to any of the other cameras, either in the main view or the pane on the right, the camera is shown highlighted in red. You can click directly on the camera icons or in the pane on the right to change from one camera to the next.

You can base your views on several maps that link to each other through hot zones, allowing you to follow movement from a camera on one map to another camera on a sub-map, just as you would a person moving from one floor to another or outside your building. The **Sub-Maps** pane gives you access to the cameras set up on maps that are linked via hot zones on a map.

When you click from one camera to the next, a **Back** button appears next to the **Home** button above the camera preview pane. This lets you click back through your camera selection or home to your default camera view. In the **Sub-Maps** view, you can also click **Up** to a previous map or **Home** to your default view.

Working with carousels

Carousels must be added to views before you can use them. For more information, see Add carousel to view or Smart Wall on page 48.

Carousels (explained)

A carousel is used for displaying video from several cameras, one after the other, in a single position 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 position. 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 (see PTZ images (explained) on page 185) 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: . You can only see it if **Default for camera title bar** is set to **Show** in the **Settings** window.

Steps:

1. On the **Live** tab, open a view that contains a carousel. When you hover over the view item, this toolbar appears:  .
2. To start or pause the carousel, click the play button.
3. To shift to the next or previous camera in the carousel, click the **Previous camera** or **Next camera** button.
4. With the proper user rights, and if smart map has been set up in your XProtect VMS, you can jump to a camera position on the smart map.
5. To search for motion in specific areas of the recordings, click the **Smart Search** button.
6. To create a snapshot or create a still image, click the **Create snapshot** or **Copy to Clipboard** button.

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

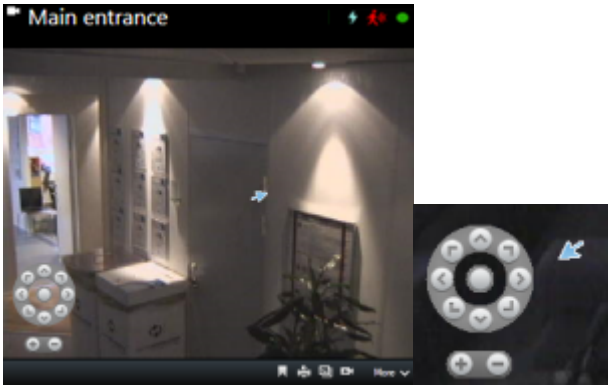
Working with PTZ and fisheye lenses

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 the camera to a PTZ preset position on page 185) 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, click **More** > **Save Fisheye Lens Positions** to save the position.

3. When you want to return to the fisheye lens position, on the camera toolbar, click **More** > **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 rights, 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 a detailed outline of the features available on your particular system, see the XProtect Product Comparison Chart on: https://www.milestonesys.com/.

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 window (explained) on page 27).

Most PTZ cameras support joystick and point-and-click control. You can customize (see Joystick settings on page 35) 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 the camera to a PTZ preset position

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.

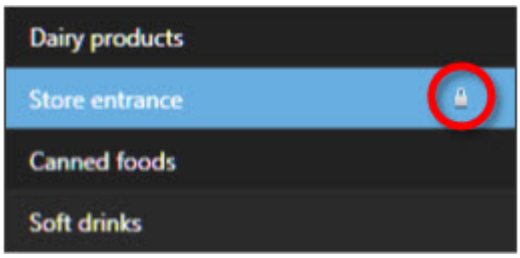
1. On the **Live** tab, on the camera toolbar, click the PTZ icon  to open the PTZ menu.
2. Select a PTZ preset in the menu to move the camera to the required position. The icon turns green.

If you select the preset **Home**, the camera moves to its default position.

Locked PTZ presets (explained)

Depending on your surveillance system (see Surveillance system differences on page 21), 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. On the **Live** tab, select the required view.
2. On the camera toolbar, click the PTZ icon  to open the PTZ menu.
3. Select **Stop PTZ patrolling** and you can patrol manually.
4. To resume the system patrolling, select the **Stop PTZ patrolling** command again.

Starting and stopping manual patrolling (explained)

Depending on your surveillance system (see Surveillance system differences on page 21), you can start and stop patrolling manually. See Start and stop manual patrolling on page 187.

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 Adding, editing, or deleting patrolling profiles on page 67), if you have the necessary user rights.

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.

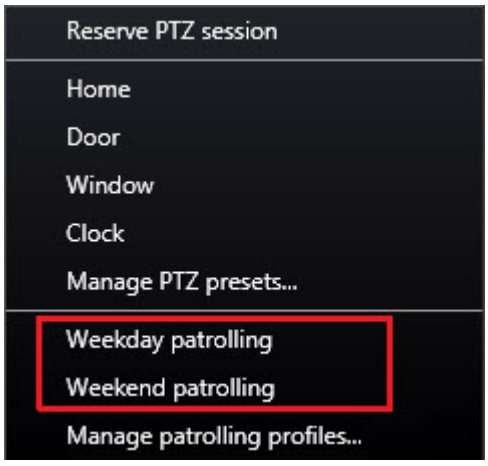
With a sufficient PTZ priority, you can stop manual patrolling started by other users by clicking the patrolling profile, by pausing it (see Pause patrolling on page 188) or starting another manual patrolling. You can always stop a manual patrolling that you have started.

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 21.

Steps:

1. In the view, select the PTZ camera that you would like to start patrolling on.
2. On the camera toolbar, click the PTZ icon  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 rights, 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.

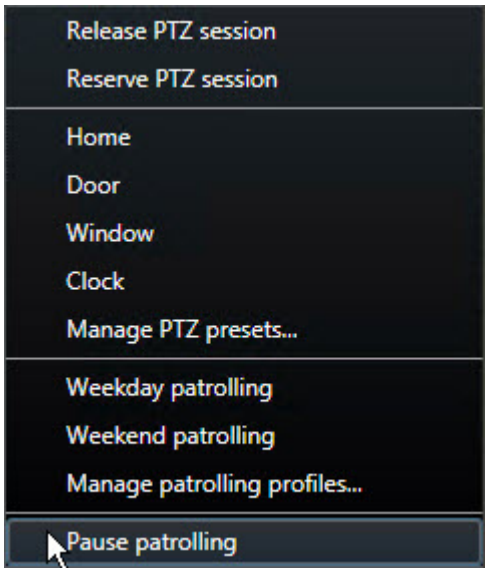
7. To control the camera for a longer period, select **Pause patrolling** (see Pause patrolling on page 188) from the PTZ menu.

Pause patrolling

Depending on your surveillance system (see Surveillance system differences on page 21), 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, click the PTZ icon to open the PTZ menu.
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 21), you can reserve PTZ sessions.

Administrators with security rights 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. On the **Live** tab, select the required view item.
2. On the camera toolbar, click the PTZ icon  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 a PTZ session

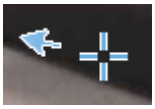
When you are done controlling a PTZ camera, you can manually release the PTZ session, so other users with lower priority can take control over the camera or the system can resume its regular patrolling. Otherwise, the camera will not be available until the session times out.

1. On the camera toolbar for the PTZ camera that you are controlling, click the PTZ icon to open the PTZ menu. (The green color indicates that you currently run the PTZ session).
2. 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 185), 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.

Working with digital zoom

Use digital zoom to take a closer look at a specific area. It works both in live and playback mode.

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. Digital zoom is therefore a useful feature for cameras that do not have their own optical zoom capabilities. Your use of digital zoom will not affect any recording of the video; any recording will still take place in the camera's regular format. If you later wish to play back the recordings, you can use digital zoom on the **Playback** tab as well.

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 evidence (see XProtect format settings on page 168), you can choose to export the regular images or the digitally zoomed images in AVI or JPEG formats. When you export to database format, this is unavailable, because the recipient can use digital zoom on the exported recordings. If you print (see Print video evidence on page 173) an image on which you have used digital zoom, the digitally zoomed area of the image will be printed.

Use digital zoom

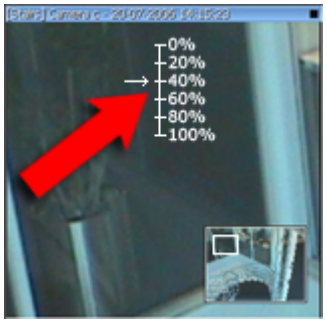
Digital zoom must be enabled, before you can use it. On the camera toolbar, click **More** and select **Digital zoom** to enable it.

Steps:

1. Click and hold down the mouse button inside the image to zoom. The area you select is highlighted by a white border. 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 using the zoom level slider, press and hold down the SHIFT key, click inside the image and while holding both down, move your mouse up or down the zoom level slider.



4. Selecting a zoom level of **0%** lets you view the full image again.
5. Click the **Home** icon inside the virtual joystick to return to the normal zoom level.

> If your mouse has a scroll wheel, you can also use the scroll wheel to control the zoom level.

Frequently asked questions: 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 rights 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.

Working with bookmarks

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 70.

Bookmarks (explained)

The bookmark feature is only available for selected surveillance systems (see Surveillance system differences on page 21). Depending on your user rights, the ability to add bookmarks from some cameras may be restricted. You may be able to view bookmarks even if you cannot add them, and vice versa.

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 you and other users 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 surveillance system administrator) to ensure that the incident is recorded, regardless of any delays.

You can find and edit bookmarked video by using:

- The **Playback** tab's **Recording Search** (see Search for sequences or bookmarks in Recording Search pane on page 159) pane
- The Sequence Explorer
- The timeline (see Bookmarks in the timeline (explained) on page 149)

If you cannot find a particular bookmark, it can be because:

- Your user rights do not allow you to view it
- The bookmark has been deleted (users with sufficient rights can delete bookmarks from the **Playback** tab's **Recording Search** (see Search for sequences or bookmarks in Recording Search pane on page 159) pane or the **Sequence Explorer**)
- The bookmarked video no longer exists on the surveillance system

Bookmark window

To add details to bookmarks, you must first specify this for both the Live and the **Playback** tab in the **Settings** window, under **Functions** (see Functions settings on page 30). If you have not specified this, you will only be able to create quick bookmarks.

When you create a detailed bookmark, or when you edit a bookmark, there are a number of settings you can specify.

Name	Description
The timeline	Although the bookmark time and the clip start and end time are specified by the surveillance system administrator, you can change these settings. To change the time, drag the indicators on the timeline (see Time navigation controls (explained) on page 148) to the required time.  **Clip start time**: The suggested start time of the bookmark clip (a certain number of seconds before the bookmark time), specified by the surveillance system administrator. **Bookmark time**: The time in the video clip that you bookmarked. **Clip end time**: The suggested end time of the bookmark clip (a certain number of seconds after the bookmark time), specified by the surveillance system administrator.
Headline	Lets you specify a headline containing a maximum of 50 characters.
Description	Lets you specify a description.

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 timespan. Later, you can find and edit the bookmark details.

Requirements:

Detailed bookmarks must be enabled. For more information, see Enable detailed bookmarks on page 70.

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 **Recording Search** pane on the **Playback** tab, or the **Sequence Explorer** tab, and search for **Bookmarks**.

Working with events and alarms

Alarms (explained)

The Alarm and Map features are only available when connected to certain types of surveillance system (see Surveillance system differences on page 21). Particular user rights may be required.

On the surveillance server, virtually any kind of incident or technical problem (events) can be set up to trigger an alarm. These can all be viewed from the **Alarm Manager** tab, which provides a central overview of your surveillance system incidents, status, and possible technical problems.

The **Alarm Manager** tab is either displayed or hidden depending on the settings defined by your surveillance system setup.

You cannot set up alarm triggers in the XProtect Smart Client, this is done by the surveillance system administrator as part of the surveillance system configuration.

The **Alarm Manager** tab provides a dedicated view for your alarm or event handling. The tab itself displays the number of active alarms (up to nine—more alarms than this are shown with a 9+) . The **Alarm Manager** tab includes an alarm list, an alarm preview (for previewing video associated with individual alarms or events), and, if available, a map position (for geographical display of alarm indicators). Click the **Report** button, to display relevant reports on the incidents (see View alarm reports on page 200).

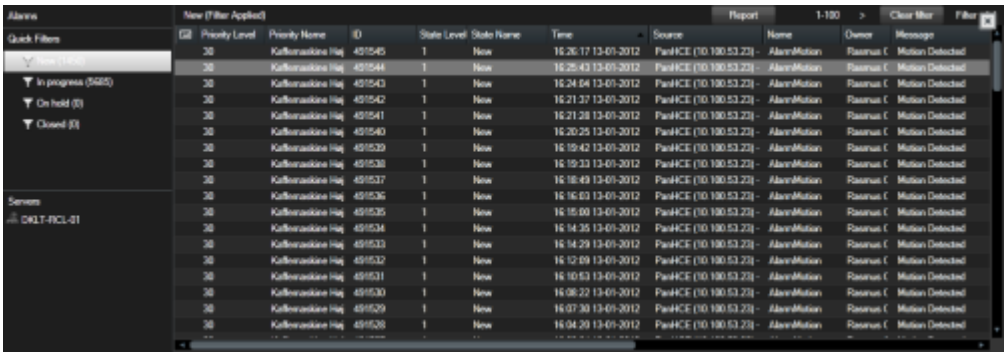
Alarm list (explained)

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. To see a list of events, in setup mode, define that the alarm list displays events (see Alarm list settings on page 71). Alarms or events that have video associated with them are listed with an icon . To preview a still image from the time of the alarm or event, place your mouse 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.

You can decide how you want the list to display, 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.



Servers in alarm list (explained)

On the left side of the alarm list, you can view the servers that the alarms originate from. Many surveillance 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. In the alarm filters, you can filter alarms by servers.

Alarm states (explained)

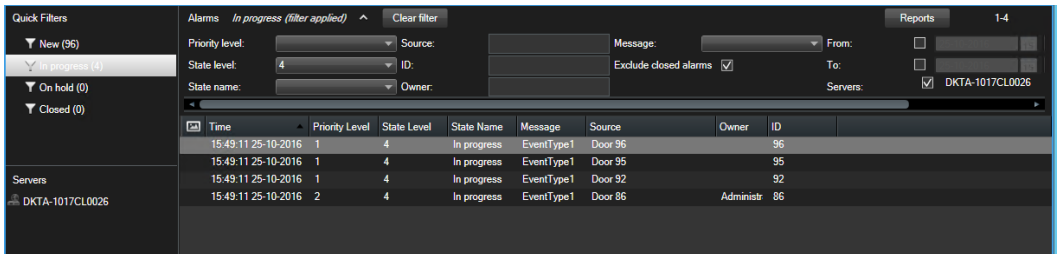
Alarms can be in one of the following states: New, In progress, On hold, or Closed . You can see the state of each alarm in the **Alarm List**, in the **State Name** column. The **Filters** pane lets you filter according to certain criteria (see Filter alarms on page 197). Initially, all alarms will 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 alarm list's content, in 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

After you add the **Alarm List** to a position in a view, you can double-click an alarm to view information about it in a separate window. A window shows a preview of the alarm incident and live video.

You can manage the alarm in the following ways:

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**; but if required you can also change state from, for example, **On hold** to **New**.
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 be listed in the alarm list's **Owner** column.
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,” or “Suspect handed over to police,” or “False alarm.” The comments field appears at the bottom of the window.

Field	Description
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. Depending on the configuration of the surveillance system 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 alarms

If you know that certain activity is causing false alarms, you may want to disable alarms on this type of activity for a period of time. This can make it hard for you to see the real alarms that you need to address. For example, if there is a lot of movement around a particular camera and this is generating several false alarms, you can disable alarms on motion detection for this camera for 10 minutes.

1. In the **Alarm list**, select the alarm.
2. Right-click it and select **Disable new alarms**.
3. In the **Disable alarms** window, specify how long you want to disable the alarm.

Ignore alarms

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. If you have selected multiple alarms in the alarm list, you cannot use this feature.

Steps:

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.

View alarm reports

Alarm reports are available only if you are using XProtect Corporate, XProtect Expert, XProtect Professional+, or XProtect Express+.

- Click the **Report** button to open the **Alarm Report** window, where you can view two graphs representing one of the following predefined reports:
    - Category
    - State
    - Priority

- Reasons for closing
- Site
- Response time

You can filter the interval of the report, so it displays alarms over a period of 24 hours, 7 days, 30 days, 6 months, or a year.

Select the categories, states, priorities, reasons for closing, sites, or response times to display in each of the two graphs so you can compare these side by side. The graphs display the number of alarms on the vertical axis and the time frame on the horizontal axis.

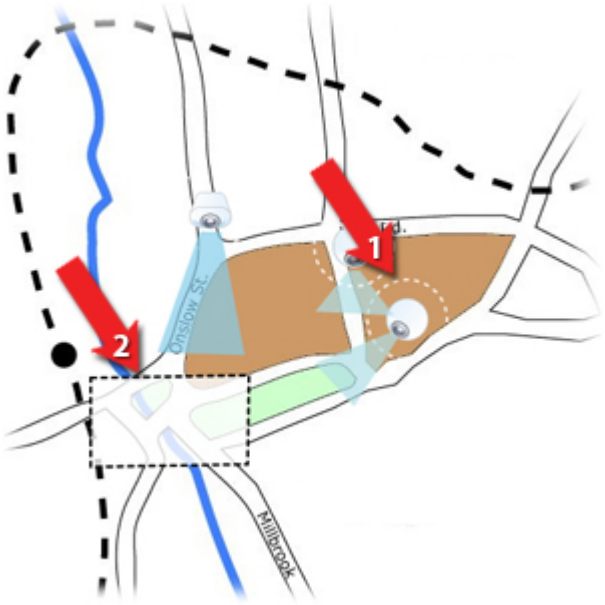
Alarms on maps (explained)

If your alarm handling view contains one or more map (see Maps) 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 white 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 white circle around it (**1** in the following illustration), 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 white 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 white (**2** in the following illustration), 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.

Events (explained)

An event is a predefined incident on the surveillance system that can be set up to trigger an alarm. Events are either predefined system incidents or user-specified events (for example, analytics events, generic events, or user-specified). 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), but can also be manually activated. Events are used by the surveillance 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 surveillance system, for example recording on a particular camera with a particular frame rate for a particular period of time as well as sending of a mobile phone text message with a predefined incident description to a particular security officer.

Your surveillance system administrator determines what happens when you manually activate an event. Your surveillance system administrator may use the terms event buttons, user-defined events or custom events for manually activated events.

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 output.

1. On the **Live** tab, 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.

Working with evidence locks

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 protects the data from being deleted. This means that neither you nor other XProtect Smart Client users can delete the data until a user with sufficient user rights unlocks the evidence. With an evidence lock, the data is also protected from automatic deletion that would otherwise take place based on the system's default retention time.

Depending on your user rights defined by your system administrator, you may or may not be able to create, view, edit and delete evidence locks.

Create evidence locks

You can create an evidence lock to prevent video recordings and other data from being deleted.

1. Select the **Playback** tab.
2. In the timeline, click the **Time Selection Mode** or the **Set Start/End Time** button.

3. Select the start and end time for the video sequences you want to protect from deletion.
4. Select one or more cameras that have video sequences and data from related devices that you want to protect.
5. To the right of the timeline, click **Evidence Lock** and select **Create**.
6. In the **Create Evidence lock** window, give the evidence lock a headline and optionally add a description.

7. Click **Select camera** to add more cameras to the evidence lock.
8. Click **Remove** or **Remove All** to remove cameras from the evidence lock.
9. You can adjust the time interval and define for how long you want to keep the evidence protected. See Evidence lock settings on page 206 for more information.
10. Click **Create**.
11. A window shows if your evidence lock was created successfully. Click **Details** to see what went well and what did not. See Evidence lock status messages on page 207 for more information.

View existing evidence locks

1. Click the **Playback** tab.
2. To the right of the timeline, click **Evidence Lock** and select **View**.
3. If you want to stay on the **Live** tab instead of the **Playback** tab, click the **Status** button  on the application toolbar and select **Evidence Lock List**. A list appears with the existing evidence locks with devices that you have user rights to.
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. See Evidence lock filters on page 206 for more information.
5. Select an evidence lock and click **Details** to see the cameras included in the evidence lock and other information. See Evidence lock settings on page 206 for more information.

Edit evidence locks

You can edit evidence lock, depending on your user rights, for example the time interval, the cameras, and how long the evidence lock should apply.

1. Select the **Playback** tab.
2. To the right of the timeline, click **Evidence lock** and select **View**, or click the **Status** button  on the application toolbar and select **Evidence Lock List**.
3. Select an evidence lock and click **Details**. A window appears. See Evidence lock settings on page 206.
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 Evidence lock status messages on page 207 for more information.

Play back video with evidence locks

You can always play back video on the **Playback** tab 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. Click the **Playback** tab.
2. To the right of the timeline, click **Evidence Lock** and select **View**.
3. If you want to stay on the **Live** tab instead of the **Playback** tab, click the **Status** button  on the application toolbar and select **Evidence Lock List**. A list appears with the existing evidence locks with devices that you have user rights to.
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 evidence locks

When you export evidence locks, also the data from devices related to the cameras are included in the export.

1. Click the **Playback** tab.
2. To the right of the timeline, click **Evidence Lock** and select **View**.
3. If you want to stay on the **Live** tab instead of the **Playback** tab, click the **Status** button  on the application toolbar and select **Evidence Lock List**.
4. Select an evidence lock and click **Export**.
5. The **Export** window opens. Define your settings. See Export window settings on page 167 for more information.

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. Click the **Playback** tab.
2. To the right of the timeline, click **Evidence Lock** and select **View**.
3. If you want to stay on the **Live** tab instead of the **Playback** tab, click the **Status** button  on the application toolbar and select **Evidence Lock List**.

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 Evidence lock status messages on page 207 for more information.

Evidence lock settings

Name	Description
Headline	The headline of the evidence lock.
Description	A description of the evidence lock.
Evidence lock interval start	Adjust the start date and time for the video sequences you want to protect.
Evidence lock 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 you user rights, you can 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: The evidence lock is created/updated/deleted but without including some of the selected cameras and/or their related devices.	**Scenarios**: Some of the recording servers with devices included in the evidence lock are offline. Your system administrator has changed your evidence lock user rights after you logged into XProtect Smart Client. **Solution**: Depending on scenario. Try again later or 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.	**Scenarios**: All the recording servers with devices included in the evidence lock are offline. The management server is offline. Only for update and deletion: You do not have user rights to one or more devices in the evidence lock. **Solution**: Depending on scenario. Try again later or contact your system administrator.

Working with privacy masking

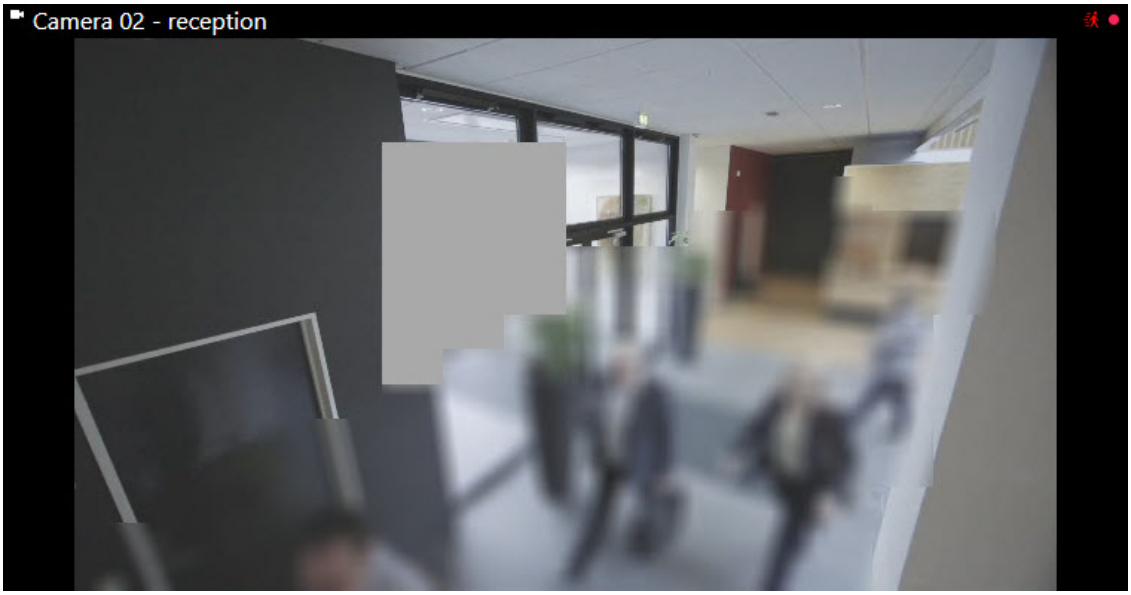
Privacy masking (explained)

> Privacy masking functionality and availability depend on the selected surveillance system (see Surveillance system differences on page 21).

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 rights 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 rights.

You can also add additional privacy masks when you export. For more information, see Mask areas in a recording during export on page 166.

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 XProtect format.

Lift and apply privacy masks

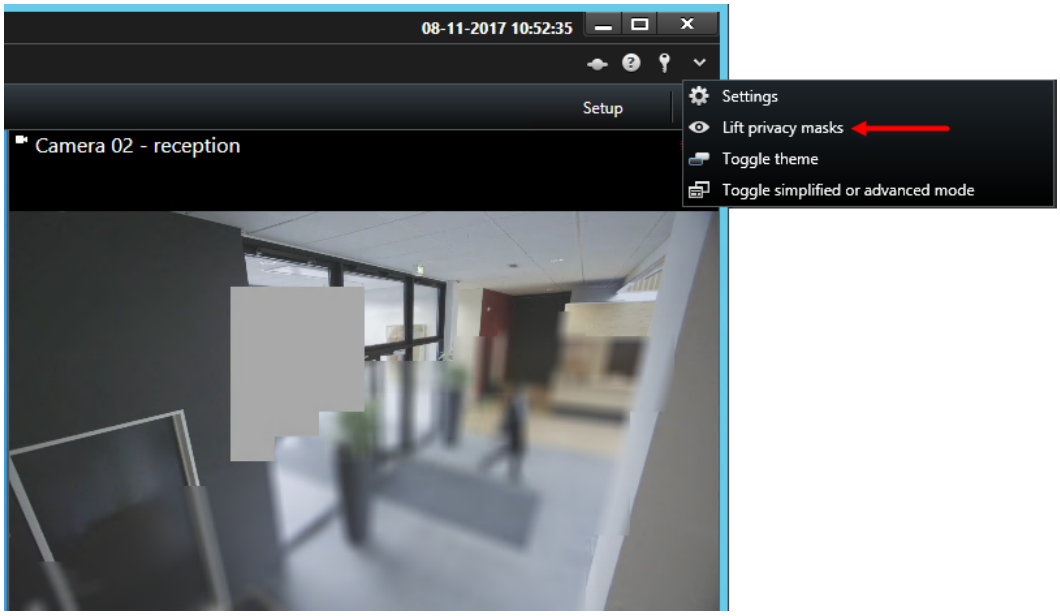
This feature is only available for selected surveillance systems (see Surveillance system differences on page 21).

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 rights.

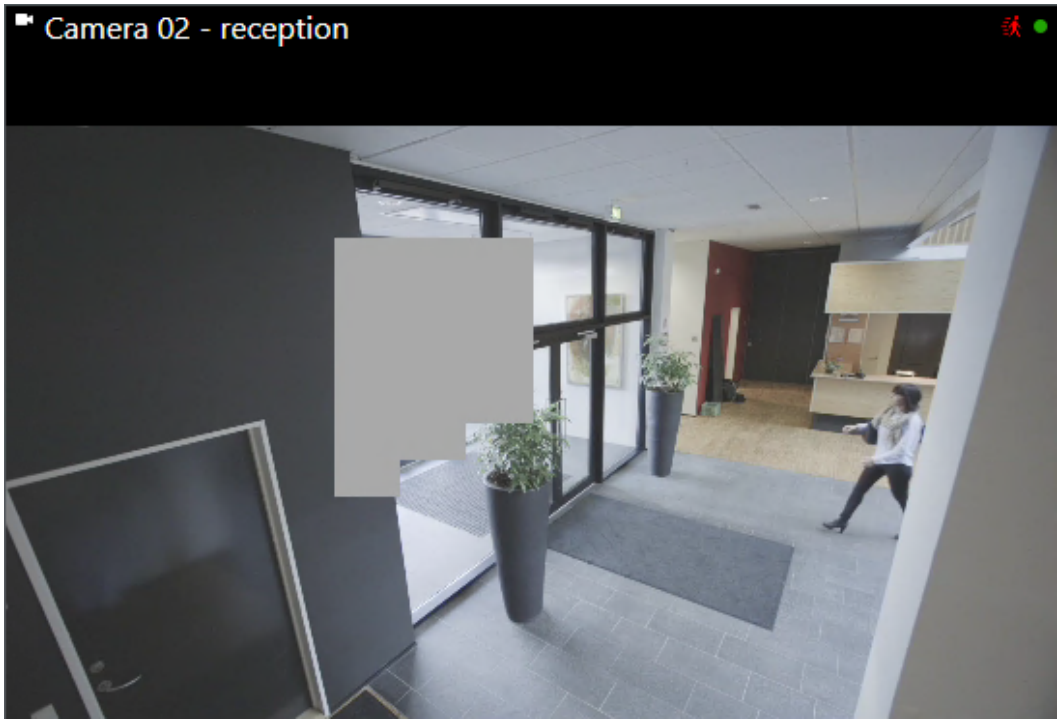
If you do not have the necessary user rights, you will be asked for additional authorization. Contact a person who has the rights to authorize you, so he or she can enter their credentials. If you do not know who can authorize you, ask your system administrator.

To lift privacy masks:

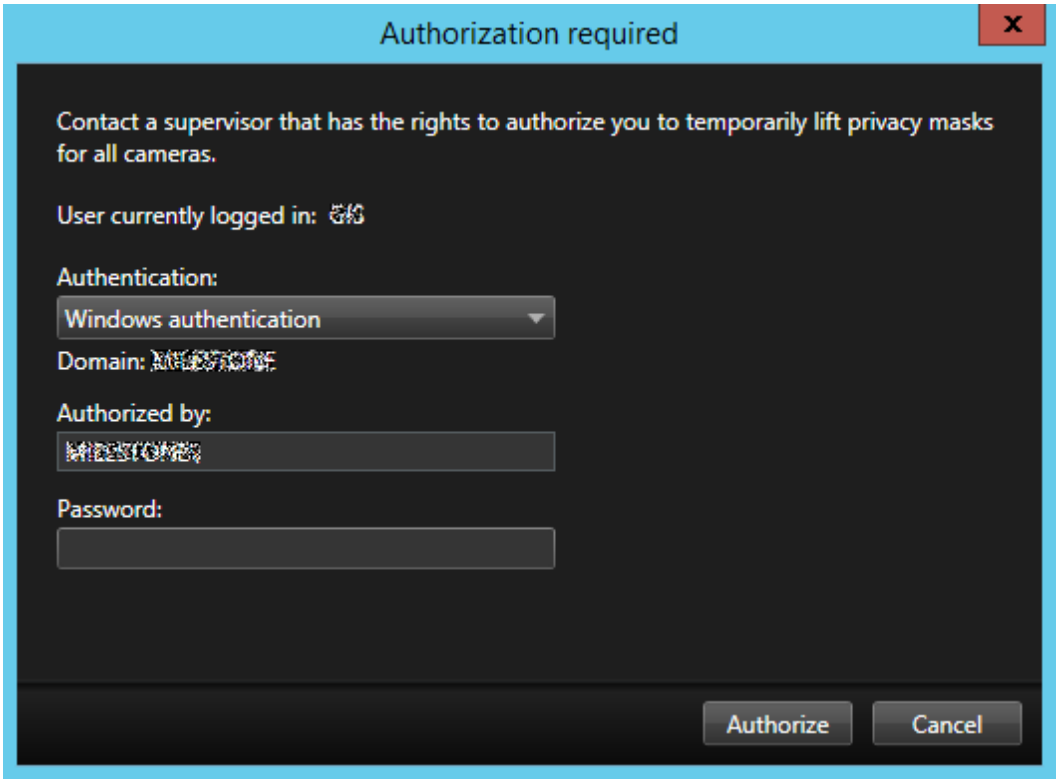
1. On the **Live** or **Playback** tab, click **More** > **Lift privacy masks** on the application toolbar.



If you have the rights to lift privacy masks, liftable privacy masks now disappear for all cameras and permanent privacy masks remain.



If you do not have sufficient rights, a dialog box appears.



2. Contact a person who has the rights 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, click **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.

Working with audio

Audio (explained)

Support for specific audio features may vary from system to system (see Surveillance system differences on page 21). Access to recorded audio, or certain recorded audio features, may be restricted depending on your user rights. Consult your surveillance system administrator if in doubt.

The 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.

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

The surveillance system can record incoming audio from microphones attached to cameras, even if no video is being recorded. However, outgoing audio transmitted through speakers attached to cameras is only recorded on some surveillance systems (see Surveillance system differences on page 21).

Talking to audiences through speakers attached to cameras is possible by using:

- The **Audio** pane
- Overlay buttons
- Speaker functionality on maps

Frequently asked questions: audio

Why is the Speakers list not available?

Some surveillance systems do not support two-way audio.For a detailed outline of the features available on your particular system, see the XProtect Product Comparison Chart on: https://www.milestonesys.com/.

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. Consult your surveillance 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. Consult your surveillance 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 rights 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 a detailed outline of the features available on your particular system, see the XProtect Product Comparison Chart on: https://www.milestonesys.com/.

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.

Working with smart map

Smart map (explained)

> This feature is only available for selected surveillance systems. For a detailed outline of the features available on your particular system, see the XProtect Product Comparison Chart on: https://www.milestonesys.com/.

Smart map lets you view and access cameras 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. For 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. For more information, see Zoom in and out on page 214.

One key benefit of a smart map is the spatial reference data behind-the-scenes. For more information, see Geographic backgrounds (explained) on page 73.

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 219
- **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 use the Bing Maps and Google Maps services, or the OpenStreetMap map project as geographic backgrounds, and add computer-aided design (CAD) drawings, shapefiles, and images as overlays. For more information, see Smart map (explained) on page 213

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 cameras again. You cannot transfer maps with cameras 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 83.

Zoom in and out

If you have multiple cameras covering the different areas on the smart map, the cameras are grouped and displayed with icons. For example, this icon 

indicates that there are 6001 cameras within the area. As you zoom in, these icons multiply into new icons reflecting how the cameras are grouped and distributed across the smart map - on that specific zoom level. If you zoom out, the number of grouping icons decrease, but the number inside them increase.

Steps:

- Use the scroll wheel or double-click the left or right button on your mouse
- 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

With Bing Maps, Google Maps, or OpenStreetMaps as geographic backgrounds, there may be a limit to how much you can zoom in if the services are not able to provide an image at that depth. When this happens, the view item stops displaying the geographic background. Other layers, such as cameras or shapefile images continue to display.

Preview video from one camera

You can preview and investigate video feeds from the cameras on your smart map. If you want to investigate and play back the video, you can open it in a new floating window. In doing so, the smart map will stay in the background in the position where you left it.

Steps:

1. Navigate to the camera.
2. To preview the video feed from the camera, double-click it. The video feed is displayed in the **Preview** window. You can also right-click the camera and select **Live preview**.
3. To play back and investigate the video in more detail, do one of the following:
   - Click the **Independent Playback** button. The controls of independent playback becomes available
   - Close the window, and then right-click and select **Send camera** > **New Floating Window**

Preview videos from several cameras

You can preview video from several cameras on your smart map at the same time. If you want to investigate and play back the video, you can open the cameras in a new floating window. In doing so, the smart map will stay in the background in the position where you left it.

Steps:

1. Navigate to the place on the smart map, where the cameras are located.
2. To view video from more than one cameras in a preview window, do one of the following:
   - Press and hold the **CTRL** key while you select the cameras, and then right-click a camera icon and select **Live preview**
   - Click **Select multiple cameras**, then click and drag on the smart map to select the cameras. After you select the cameras, press **ENTER** on your keyboard
   - Double-click a cluster of cameras. You can preview up to 25 cameras in a group. If one or more cameras are selected in the group, the preview window displays video only from the selected cameras
3. To play back and investigate the video in more detail, do one of the following:
   - In the **Preview** window, click the **Independent Playback** button. The controls of independent playback becomes available
   - When you have selected the cameras, right-click and select **Send camera** > **New Floating Window**

If you chose the cluster option: The icon for the group of cameras indicates whether only some of the cameras in the group are selected, for example  .

Use hotspot to view video from cameras on smart map

Instead of previewing video feed from cameras one at a time, 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 hotspot to view or Smart Wall on page 48.

Steps:

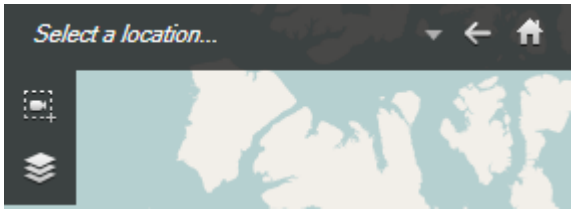
1. Open the view that contains the smart map.
2. If the view also contains the hotspot:
    1. Navigate to the cameras on the smart map.
    2. Click the cameras you are interested in. As you click, the video feed is displayed in the hotspot view item.
3. If the view does not contain the hotspot:
    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 another smart map location

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 camera on smart map

If you want to view a camera in its geographic context, you can jump to the place on the smart map where the camera is. This is useful if, for example, you forgot the location of camera, or you want to check nearby cameras.

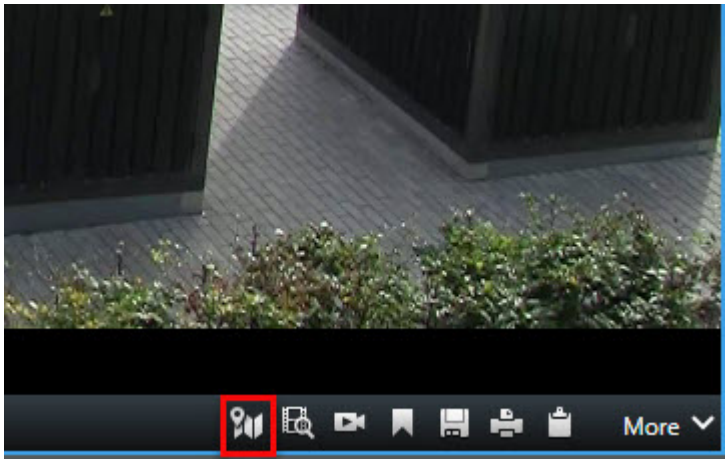
Requirements

You can jump to a camera only if the GPS coordinates of the camera have been specified.

Steps:

1. To search for a camera and then jump to it:
    1. On the **Live** or **Playback** tab, go to the **Views** pane.
    2. Search for the camera. If the camera exists, it appears in the search results.
    3. Hover over the camera you want to jump to.
    4. Click  to jump to the camera. The smart map opens in a floating window.

2. To jump to a camera from a view item:
    1. On the **Live** or **Playback** tab, 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 overlay 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.

Sharing smart map through Smart Wall

If you are using Smart Wall, you can send the smart map to the Smart Wall overview so that other people can view the smart map. The current zoom level, the location that you have navigated to, and the layers that are visible are also sent to the Smart Wall.

The next sections describe different ways of sharing the smart map.

Working with maps

Maps (explained)

> The map feature is only available for selected surveillance systems (see Surveillance system differences on page 21). A map position does not display live video, a map is always a still image.
>
> 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.

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.

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.

Maps may contain elements representing cameras, microphones and similar technology. You can view recorded video from cameras (see View recorded video from cameras on a map on page 223) 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 214.

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 rights 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 181). 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 196) 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 196) 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 surveillance system administrator if the problem persists.

A hot zone can point to a map that you do not have access rights to and the XProtect Smart Client will inform you about this. Because user rights 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 surveillance system administrator if in doubt about your user rights.

Plug-ins

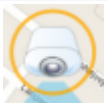
Plug-in elements are available only if used on your surveillance system. Examples of plug-in elements: access control systems, fire detection systems, etc.

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. On the **Live** tab or the **Playback** tab, 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 185) 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 the error message "Event Server has insufficient access rights 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 surveillance 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.

Frequently asked questions: 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 rights). 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.

Working with Matrix

The ability to add Matrix content to views is only available when connecting to selected surveillance systems (see Surveillance system differences on page 21). Matrix is only available if Matrix has been configured on your surveillance system, and you have the required user rights.

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 positions in the view as required, so you can watch live video from several Matrix-triggered sources at the same time.

A Matrix position is displayed with a Matrix icon on the toolbar: . You can maximize a Matrix by double-clicking it.

A view can contain several Matrix positions. This lets you watch live video from several Matrix-triggered sources at the same time. If your view contains several Matrix positions, the positions are always ranked—one of the positions will be the primary Matrix position, another the secondary, and so on. When the first Matrix-triggered live video stream is received, it is automatically presented in the primary Matrix position. 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 Matrix position, and the newest video stream is presented in your primary Matrix position, and so on. The Matrix positions' ranking is applied automatically: the first Matrix position you add is the primary Matrix position, the next one you add is the secondary one, and so on. You can change this ranking in setup mode. See Matrix settings on page 100.

On the **Playback** tab, Matrix positions display video from the cameras with which the Matrix positions were last used on the **Live** tab. You can play back this video using the navigation features of the **Playback** tab.

Manually send video to Matrix recipients

You cannot send video to a hotspot (see Hotspots (explained) on page 181) or carousel (see Carousels (explained) on page 183).

Requirements

Matrix content has been added to a view. See Add Matrix content to views on page 100.

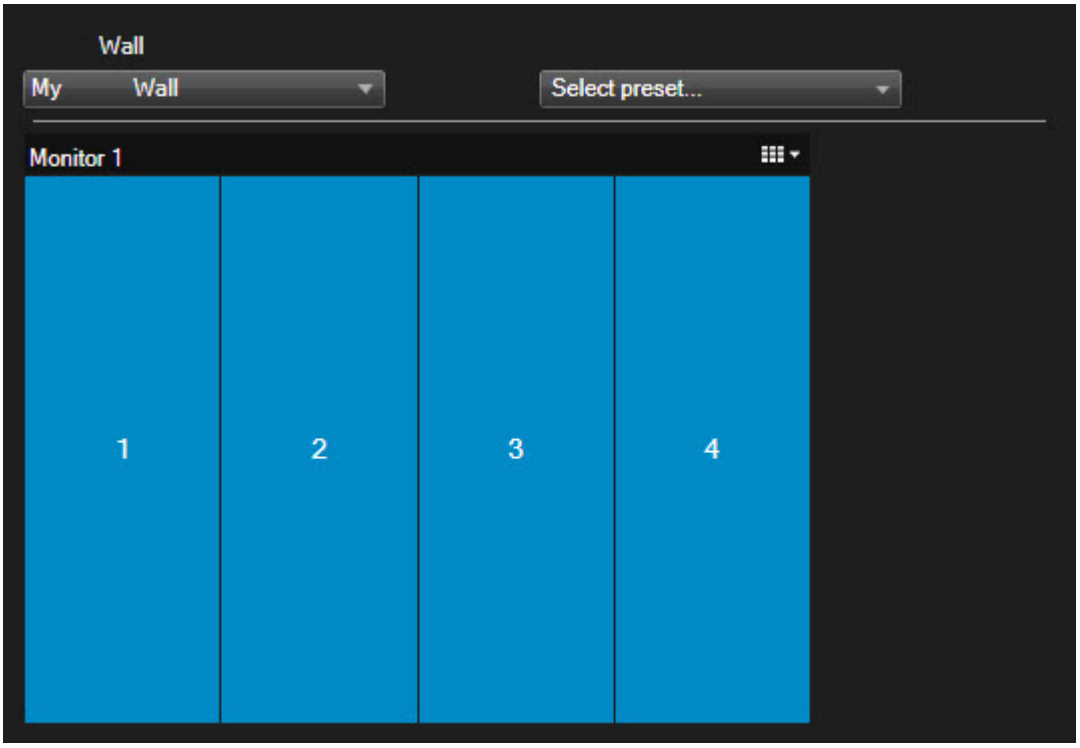
1. Select the view.
2. On the camera toolbar, click **More** > **Matrix**, and then select the relevant Matrix recipient.

Working with Smart Wall

After your system administrator sets up a Smart Wall, you can start working with it in Smart Client. By default, the Smart Wall overview reflects the layout, size, and cameras that your system administrator specified, but you can change those settings and add other types of content. For more information, see Adding content to views or Smart Wall on page 45.

Viewing XProtect Smart Wall content (explained)

You can view the content of your Smart Wall in live or playback mode. The Smart Wall has its own view item inside a view. What you see is the graphical presentation of the Smart Wall, not the video content itself.



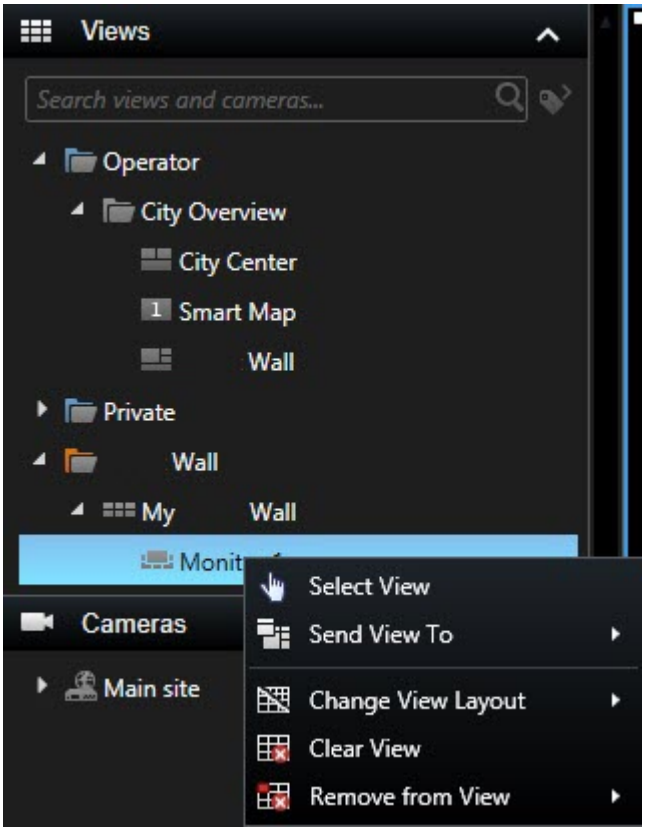
To view the contents, you need to send the Smart Wall to a separate window, either on your main computer monitor, or to secondary computer monitors. See View XProtect Smart Wall content on page 228.

Examples where this is useful

You are setting up a video wall for the first time, and want to display content in full-screen on the monitors.

- If you aren't located in the same room as the video wall, and you want to see what it's showing while you work on other tasks
- If you want to work in Smart Client while you monitor a situation on your Smart Wall. For example, you might want to investigate the situation on the **Playback** tab, or take a snapshot of the suspect

The most direct way of viewing the Smart Wall content is to access the Smart Wall directly from the **Views** pane. In doing so, the Smart Wall content is displayed immediately in the viewing area in XProtect Smart Client



If you want to review Smart Wall content without disturbing what others see on the video wall, you can click the **Disconnect Smart Wall monitor** button. Changes you make will not affect the shared view. At any time, you can reconnect to the server.

View XProtect Smart Wall content

Your Smart Wall displays both live and recorded video depending on the tab you are standing on.

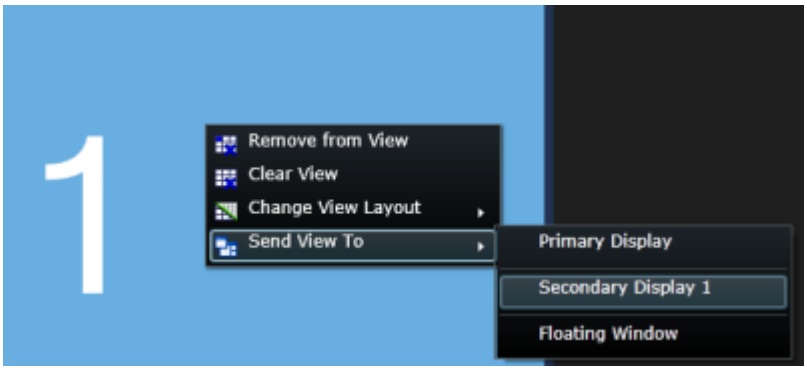
User rights can prevent cameras from displaying video on your Smart Wall.

Steps:

1. To view Smart Wall content in the current window:
    1. Expand the **Smart Wall** folder in the **Views** pane.
    2. Expand the Smart Wall and select the monitor. The Smart Wall overview appears showing, for example, video content.

3. To review content without interfering with what is being displayed on the Smart Wall for others, click **Disconnect Smart Wall monitor**. Changes you make, for example adjusting the time slider, are reversed when you reconnect.

2. To view content in a separate window:
    1. Open the view where you have added your Smart Wall.
    2. In the view item that contains the Smart Wall, click  in the upper right corner.
    3. Select **Send View To** and select a display option.



For more information about display options, see Viewing Smart Wall content in separate window (explained) on page 229.

Viewing Smart Wall content in separate window (explained)

The following table describes ways to view Smart Wall content in a separate window or secondary display.

Option	Description
Primary Display	View content in full-screen on the display that you're currently viewing. Smart Client remains open behind the Smart Wall content. You can minimize or resize the window. This option is useful when you want to focus on the area that the Smart Wall covers. For example, when you want to watch the front parking lot after security has lost track of a suspect inside the building.
Secondary Display	View content on another display, and continue viewing Smart Client on the current display. This option lets you keep an eye on your Smart Wall while working in Smart Client. For example, you can continue to monitor the parking lot while you export video of the incident.

Option	Description
Floating Window	View content in a floating window on the display that you're currently viewing. You can maximize or resize the window. For example, this option is useful when you want to display content from multiple Smart Walls. You can watch the parking lot and the roof at the same time.

For more information, see Viewing XProtect Smart Wall content (explained) on page 226.

Displaying content on Smart Wall

XProtect Smart Wall lets you display content such as video feeds from cameras, HTML pages, images, text, hotspots, and carousels on monitors and video walls.

Depending on the situation and the environment you monitor, you can combine these different types of content to improve response times and effectiveness. For example, if you want to display a picture of a suspect so that people on patrol know who to look for, you can add an image. If you want to provide guidance for response measures, you can add text.

Display video from camera on Smart Wall

Requirements:

You have set up a view that contains your Smart Wall. For more information, see Add Smart Wall overview to view on page 46.

Steps:

1. Go to the **Live** or **Playback** tab.
2. In the **Views** pane, select the view that contains the Smart Wall overview.
3. In the **Cameras** pane, drag the camera to a tile in your Smart Wall overview.
4. To view the contents of the Smart Wall, follow the steps described in View XProtect Smart Wall content on page 228.

Display image or snapshot on Smart Wall

You can display an image from your computer, for example of a suspect, on your Smart Wall, or take a snapshot of an incident and then display it on your Smart Wall.

You can also add images to views and then send it to more than one Smart Wall. For more information, see Add image to view or Smart Wall on page 46.

1. On the **Live** or **Playback** tab, roll the mouse over the view item that is showing the footage.
2. To display a snapshot:
    1. On the view item toolbar, click the **Create Snapshot**  icon . The system saves the image to the location specified in Application options (see Application settings on page 28).
    2. Drag the snapshot from the folder to a tile in the Smart Wall overview.
    3. In the Smart Wall view item, click  and select a display option, for example **Primary Display**. For more information, see View XProtect Smart Wall content on page 228.
3. To display an image located on your computer:
    1. In the folder on your computer where the image is located, find the image.
    2. Drag the image from the folder to a tile in the Smart Wall overview.
    3. In the Smart Wall view item, click  and select a display option, for example **Primary Display**. For more information, see View XProtect Smart Wall content on page 228.

When you drag an image to the Smart Wall overview, the system automatically embeds the image so that the image is available from anywhere.

Display carousel on Smart Wall

If you are using XProtect Smart Wall, you can display carousels.

Requirements

You have added a carousel to your view as described in Add carousel to view or Smart Wall on page 48.

Steps:

1. Go to the view item that contains the carousel.
2. In the toolbar, click **More** > **Send to Smart Wall** and select the Smart Wall, monitor, and the tile where you want to display the carousel.
3. In the Smart Wall overview, click  and select a display option, for example **Primary Display**. For more information, see View XProtect Smart Wall content on page 228.

Display hotspot on Smart Wall

Requirements

You have added a hotspot to your view as described in Add hotspot to view or Smart Wall on page 48.

Steps:

1. Go the view item that contains the hotspot.
2. In the toolbar, click **More** > **Send to Smart Wall** and select the Smart Wall, monitor, and the tile where you want to display the hotspot.
3. In the Smart Wall overview, click  and select a display option, for example **Primary Display**. For more information, see View XProtect Smart Wall content on page 228.

Displaying video or still image from bookmark on Smart Wall (explained)

When you send a video clip or still image from a bookmark to a Smart Wall, the bookmark details are displayed in the tile you have selected in the Smart Wall overview. This includes the video clip or the still images, the bookmark heading, the start and end times of day, the moment the bookmark was made, and the user who made it.

You can view bookmark details by hovering the mouse pointer over the name of the camera.

Display video or still image from bookmark on Smart Wall

Sending a bookmark to a Smart Wall can help you quickly distribute a single image of, for example, a person or a video sequence of an incident.

Steps:

1. If you are on the **Live** tab, in the camera toolbar, click to create a new bookmark.
2. If you are on the **Playback** tab, do one of the following:
   - In the camera toolbar, click to create a new bookmark
   - In the **Recording Search** pane, select the **Bookmarks** check box and click **Search** to locate your bookmarks
   - In the search results, select your bookmark and click  to edit the bookmark
3. In the **Headline** field, enter a name or title for the bookmark.
4. Click **Display on Smart Wall**, point to the Smart Wall, then the monitor, and then click the tile where you want to display the video or image.
5. To send a video clip, click **OK**.
6. To send a still image, select the **Send still image only** check box and click **OK**.
7. Send the Smart Wall to a view as described in View XProtect Smart Wall content on page 228.

Displaying text on Smart Wall

If you are using the XProtect Smart Wall add-on, you can also display text on your video wall. For example, this is useful when you want to provide information to anyone who can see the video wall. The best way to share text depends on whether you want to display it on one Smart Wall, or send it to more than one Smart Wall.

When you send text to a Smart Wall, only the original text displays. That is, if you edit the text in the view, the change does not display on the Smart Wall.

Display text on one Smart Wall

You can copy text directly from a text editor into a tile in your Smart Wall.

Requirements

Your text editor must support drag and drop operations to perform this procedure. If your text editor does not, follow the steps described in Display text on more than one Smart Wall on page 233.

Steps:

1. Select the view that contains your Smart Wall overview.
2. In your text editor, enter the text you want to display.
3. Select the text and drag it to the tile in the Smart Wall overview where you want to display it. The built-in text editor appears.
4. Review the text, and make any changes required.
5. Click **Save**.
6. To edit the text after you save it, in the **Properties** pane, click **Edit text**.
7. In the Smart Wall view item, click  and select a display option, for example **Primary Display**. For more information, see View XProtect Smart Wall content on page 228.

As an alternative, you can add text to a view item and then send it to your Smart Wall. This is described in Add text to view item or Smart Wall on page 47.

Display text on more than one Smart Wall

When you have added text to a view item, you can send the text to more than one Smart Wall.

Steps:

1. Add text to your view item as described in Add text to view item or Smart Wall on page 47.
2. After you save, click **More** > **Send to Smart Wall**.
3. Select the Smart Wall setup and then the monitor.
4. Select the position on the monitor.
5. Repeat these steps for each Smart Wall.

Display HTML page on Smart Wall

HTML pages let you combine web content with video footage on your Smart Wall.

Requirements

You have added an HTML page to a view as described in Add HTML page to view or Smart Wall on page 50.

Steps:

1. Go to the view item that contains the HTML page.
2. In the toolbar, click **More** > **Send to Smart Wall** and select the Smart Wall, monitor, and the tile where you want to display the HTML page.
3. In the Smart Wall overview, click  and select a display option, for example **Primary Display**. For more information, see View XProtect Smart Wall content on page 228.

Display camera navigator on Smart Wall

If you are using XProtect Smart Wall, you can display a camera navigator.

Requirements

You have added a camera navigator to your Smart Wall as described in Add camera navigator to view or Smart Wall on page 49.

Steps:

1. Go the view item that contains the camera navigator.
2. In the toolbar, click **More** > **Send to Smart Wall** and select the Smart Wall, monitor, and the tile where you want to display the camera navigator.
3. In the Smart Wall overview, click  and select a display option, for example **Primary Display**. For more information, see View XProtect Smart Wall content on page 228.

When you send a camera navigator to a Smart Wall, the navigator uses only the original settings. That is, if you select a different camera in the view, the Smart Wall does not display the change.

Display map on Smart Wall

You can send maps to your Smart Wall, so that the map is displayed in the Smart Wall overview.

Requirements

You have added a map to your view as described in Add map to view or Smart Wall on page 49.

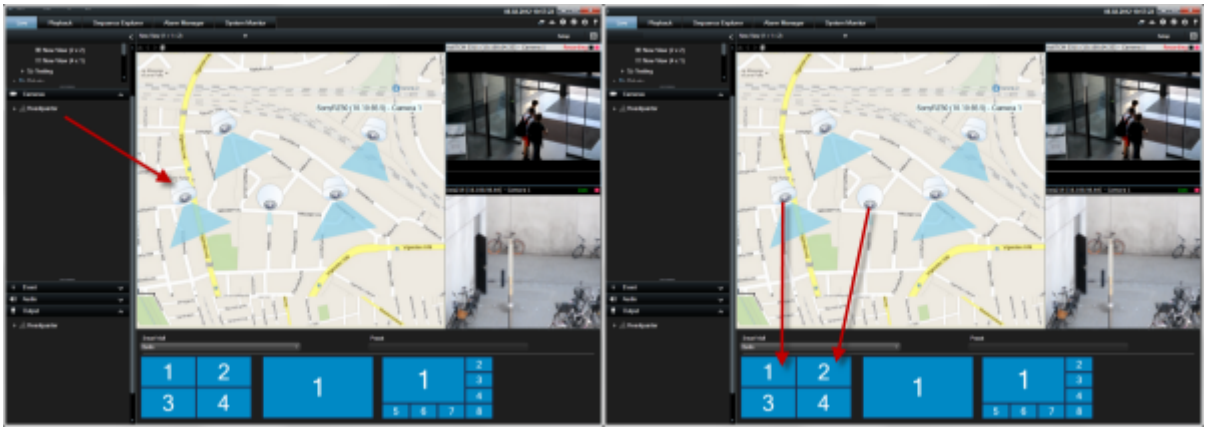
Steps:

1. Go to the view item that contains the map.
2. In the toolbar, click **More** > **Send to Smart Wall** and select the Smart Wall, monitor, and the tile where you want to display the map.
3. In the Smart Wall overview, click  and select a display option, for example **Primary Display**. For more information, see View XProtect Smart Wall content on page 228.

Drag camera from map to Smart Wall

If your view contains both a map with cameras and a Smart Wall, you can drag cameras from the map to the Smart Wall view item. For example, this is a good way to quickly share video when an alarm triggers.

> You can also drag cameras from maps in other displays, such as floating windows or secondary displays.



Displaying alarms on Smart Wall (explained)

You can share a prioritized overview of all alarms by adding the **Alarm List** to your Smart Wall. You can then double-click an alarm in the list to view and work with details about the alarm. For more information, see Viewing and editing details of an alarm on page 198.

You can also display an individual alarm on your Smart Wall with the following details:

- The time of day when the event triggered the alarm
- The name and video feed from the device that triggered the alarm, and all devices that are related to it
- You can view additional details and change some settings for the alarm by clicking the arrow in the upper right part of the position in the view. The details are as follows:
    - The person the alarm is assigned to, its priority, and the state of the alarm. You can change these if you want to
    - The source, or what triggered the alarm, such as when a camera detects motion or an analytics event occurs
    - Instructions on how to respond to the alarm
    - Activities. These are comments that users entered. Typically, they indicate decisions or actions related to the alarm. Additionally, when someone changes the details of the alarm, the system adds the changes to the list of activities
    - If you were recording video when the event occurred, you can view the video of the moment the alarm was triggered by clicking the **Playback** tab, and then **Go To Alarm Time**

For information about adding an individual alarm, see Display alarms on Smart Wall on page 236.

Display alarms on Smart Wall

When you have added the **Alarm List** to your Smart Wall, you can display the whole list or just individual alarms.

Requirements

You have added the **Alarm List** to your view. For more information, see Add alarms to views or Smart Wall on page 53.

Steps:

To display the whole alarm list on your Smart Wall:

1. Go the view item that contains the **Alarm List**.
2. In the toolbar, click **More** > **Send to Smart Wall** and select the Smart Wall, monitor, and the tile where you want to display the list.
3. In the Smart Wall overview, click  and select a display option, for example **Primary Display**. For more information, see View XProtect Smart Wall content on page 228.

To display an individual alarm on your Smart Wall.

1. Go the view item that contains the **Alarm List**.
2. Drag the alarm to the tile in your Smart Wall.
3. In the Smart Wall overview, click  and select a display option, for example **Primary Display**. For more information, see View XProtect Smart Wall content on page 228.

Stop displaying content on Smart Wall

You can stop displaying content on your Smart Wall, for example, when an incident is under control or the content is no longer relevant, in several ways.

> Other users can manually change the content on a Smart Wall, and the content can change according to a schedule or rules. This means that the content that you remove can reappear later. To permanently prevent content from displaying, contact your system administrator.

Remove the Smart Wall from a view:

1. On the **Views** pane, select the view that contains the Smart Wall.
2. Click **Setup**.
3. In the view item that contains the Smart Wall overview, click the  icon.

> To add the Smart Wall again, follow the steps described in Add Smart Wall overview to view on page 46.

Stop displaying all content on a Smart Wall:

1. At the top of the Smart Wall overview for the monitor that you want to clear, click the  icon.
2. Select **Clear View**.

Remove content from a specific tile in the Smart Wall overview:

1. In the Smart Wall, right-click the tile that you want to clear.
2. Select **Remove from View**.

Send content from view to Smart Wall

You can send content from a view item to a Smart Wall overview. The steps required depend on whether your current view contains your Smart Wall overview.

1. If your current view does not contain your Smart Wall overview:
    1. On the view item toolbar, click **More** > **Send to Smart Wall**.
    2. Select the Smart Wall.
    3. Select the monitor.

4. Select the position on the monitor.

2. If your view contains your Smart Wall overview, drag a view item to a tile on your Smart Wall overview.

The way the view item is added depends on how your system administrator set up the element insertion method for the monitor. The content from the view item either replaces the content that the tile displayed, or pushes it to the next tile in the Smart Wall overview. For example, if you drag content to tile 1, the content of tile 1 is moved to tile 2, and so on.

Sharing smart map through Smart Wall

If you are using Smart Wall, you can send the smart map to the Smart Wall overview so that other people can view the smart map. The current zoom level, the location that you have navigated to, and the layers that are visible are also sent to the Smart Wall.

The next sections describe different ways of sharing the smart map.

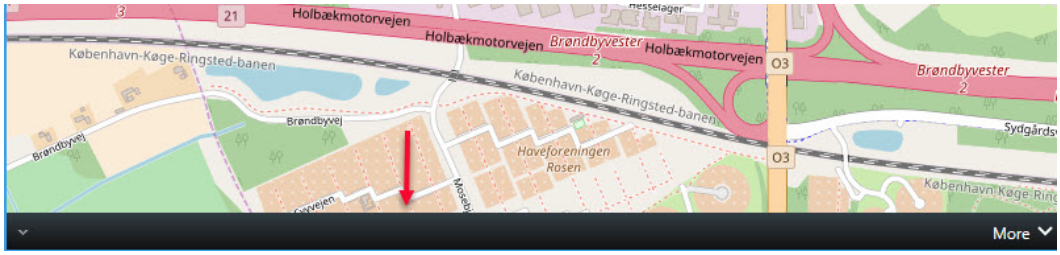
Send smart map to Smart Wall from the same view

If XProtect Smart Wall is set up in your system, you can share your smart map with others through Smart Wall. This topic describes how to do this if your view contains both a Smart Wall overview and a smart map.

If your view does not contain a Smart Wall overview, follow the steps described in Send smart map to Smart Wall when not in the view on page 239.

Steps:

1. Go to your view.
2. Navigate to the location on your smart map that you want to share.
3. At the bottom of the smart map view item, click the black bar and drag it into the view item that contains the Smart Wall overview.



4. Select the appropriate position inside the Smart Wall overview.
5. To verify that the smart map appears correctly on the Smart Wall, send the view to a floating window as described in View XProtect Smart Wall content on page 228.

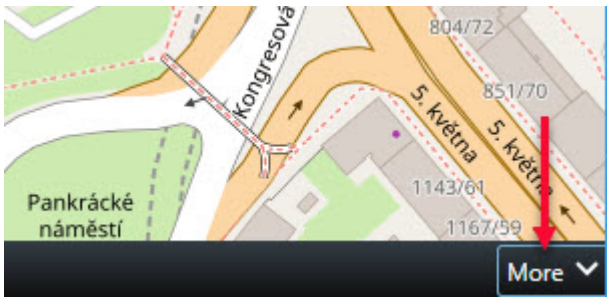
Send smart map to Smart Wall when not in the view

If XProtect Smart Wall is set up in your system, you can share your smart map with others through Smart Wall. This topic describes how to do this if your view contains both a Smart Wall overview and a smart map.

If your view does not contain a Smart Wall overview, follow the steps described in Send smart map to Smart Wall from the same view on page 238.

Steps:

1. Go to your view.
2. Navigate to the location on your smart map that you want to share.
3. At the bottom of the smart map view item, click the black bar and drag it into the view item that contains the Smart Wall overview.



4. Select the appropriate position inside the Smart Wall overview.
5. To verify that the smart map appears correctly on the Smart Wall, send the view to a floating window as described in View XProtect Smart Wall content on page 228.

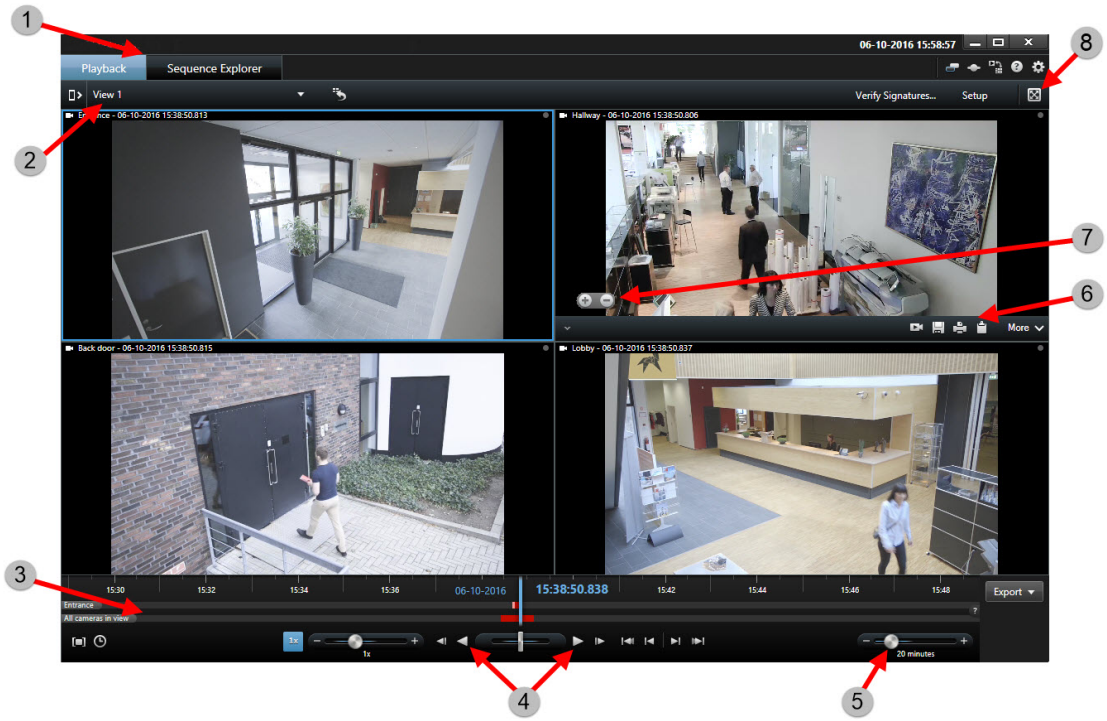
Working with XProtect Smart Client – Player

The XProtect Smart Client – Player lets you view exported video where the format **XProtect** was selected during the export.

XProtect Smart Client – Player (explained)

The XProtect Smart Client – Player is a version of the XProtect Smart Client that can be included with exported video data, letting the recipient view the exported files without having surveillance software installed. An 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 the 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



1 The **Playback** and **Sequence Explorer** tabs (see Searching for video sequences on page 151). The features on the **Playback** tab are limited compared to those in XProtect Smart Client. For information about the **Playback** tab in XProtect Smart Client, see Playback tab (advanced mode) overview on page 137.

2 The current view. See Views (explained) on page 138.

3 The timeline. See Timeline (explained) on page 147.

4 Play back the recorded video. See Time navigation controls (explained) on page 148.

5 Change the timeline span.

6 Copy or print still image.

7 Zoom in or out.

8 Switch to full screen.

Verifying the authenticity of video evidence

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 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 Smart Client – Player, you can compare the export signature with the one that was created during the export.

If - during the comparison - 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 **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**

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.

Digital signatures are available only for XProtect Expert and XProtect Corporate.

Verify digital signatures

If you are reviewing video evidence in 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.

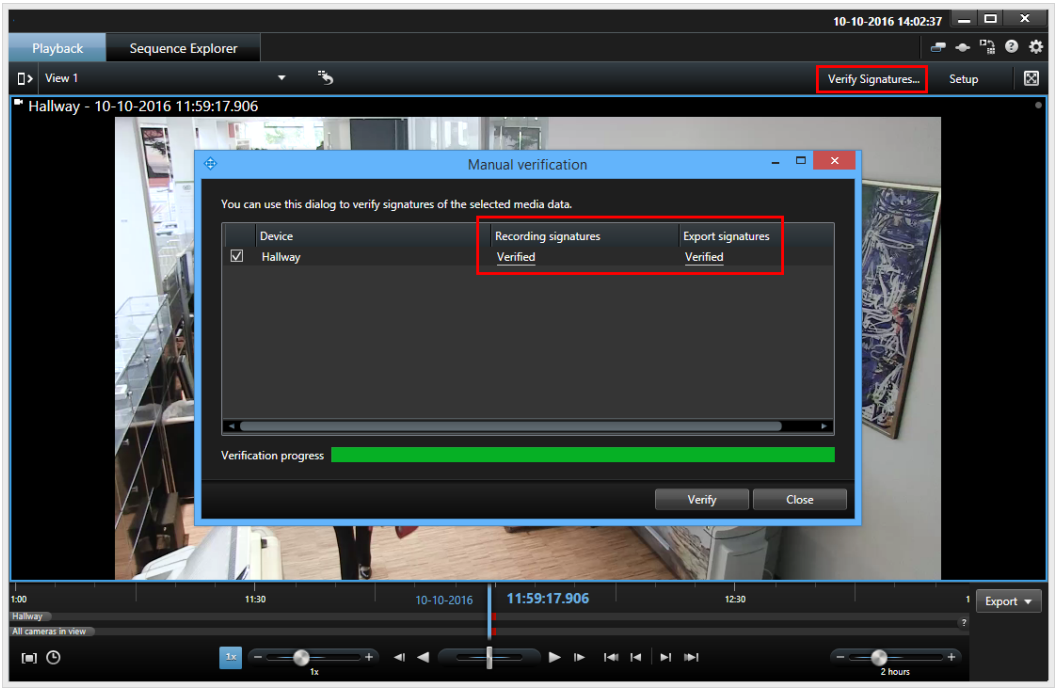
> Digital signing does not work for XProtect Smart Client 2017 R1 or earlier versions that logs into a 2017 R2 or newer system and the export will not succeed.

Requirements

- In Management Client, signing has been turned on for the recording server
- In XProtect Smart Client, during the export process, the **XProtect format** and **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. You can use this wizard to open a database and add it to your project, for example, if you want to view an archived database or previously exported material. The **Open Database** wizard also repairs corrupted databases automatically.

Steps:

1. Click the Setup button in the upper-right corner. The panes in 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 Verifying the authenticity of video evidence on page 241.

Working with XProtect Access

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 on the Live tab (explained)

On the **Live** tab, 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 150).

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. On the **Live** tab, 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 (see Monitor doors via maps) 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 (see Switch to or from live update mode of the Events list on page 246).
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 on the **Live** tab, 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 type 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 244).

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 type 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 106).

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 106).

Working with XProtect LPR

LPR on the Live tab (explained)

On the **Live** tab, 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 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 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 for previewing video associated with individual LPR events. Below the preview, information about the license plate appears together with details from the license plate match list it is associated with.

You can filter the event list according to the period, country module, LPR camera, or license plate match list. Use the **Search** field to search for a particular license plate number. By default, this list shows LPR events from the last hour.

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

You can make updates to the existing match lists by using the **License Plate 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 number, country module, time of the event and the match list that triggered the event.

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 (see Filtering LPR events (explained) on page 251) or use the **Search** 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.

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
- **License plate match list**: Select one or more license plate lists to view only LPR events generated by those lists

You can combine the filters, for example, for a particular country module on a certain date.

You can also use the **Search** 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 license plate match lists

You can add and delete license plates from license plate match lists.

1. On the **LPR** tab, at the top right of the window, click **License Plate Match Lists** to open the **License Plate Match Lists** dialog box.
2. In **Select license plate match list**, select the list you want to edit.
3. To add a license plate, click **Add**. Enter relevant information and click **OK**.
4. To edit an existing license plate, you can use the search function to find the relevant license plate.
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, you can use the search function to find the relevant license plate.
8. Select multiple rows if needed and click **Delete**.
9. Click **Close**.

Alternatively, you can add a license plate to a license plate match list by right-clicking an unlisted LPR event and select **Add to list**. You can also remove a license plate by selecting the relevant LPR event, and on the right, below the preview, click the **Remove from list** icon.

Import or export license plate match lists

You can import a file with a list of license plates that you want to use in a license plate 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 license plate match list:
    1. On the **LPR** tab, at the top right of the window, click **License Plate Match Lists** to open the **License Plate 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 license plate 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 108
- Alarms list must be in Event mode (see View LPR recognitions on page 253)

In general, read the sections about alarm management for more details on XProtect Smart Client functionality.

View LPR recognitions

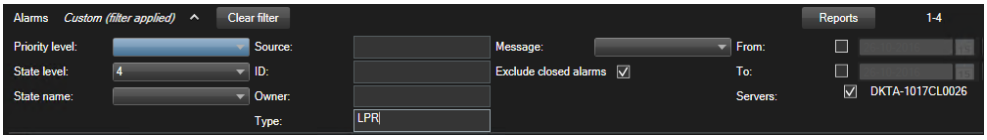
You can view LPR recognitions in the alarm list. If you select events as the data source, all recognitions are displayed. If you select alarms as the data source, only the recognitions associated with an alarm are displayed.

Requirements

To use the **Type** field referred to in the steps below, the field must be enabled in Management Client or Management Application 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. 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. 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.

Working with XProtect Transact

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
Live	On the **Live** tab, you can observe live 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.

Tab	Description
Playback	On the **Playback** tab, you can browse past 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 video previewer, the receipt is displayed.

Observe live transactions

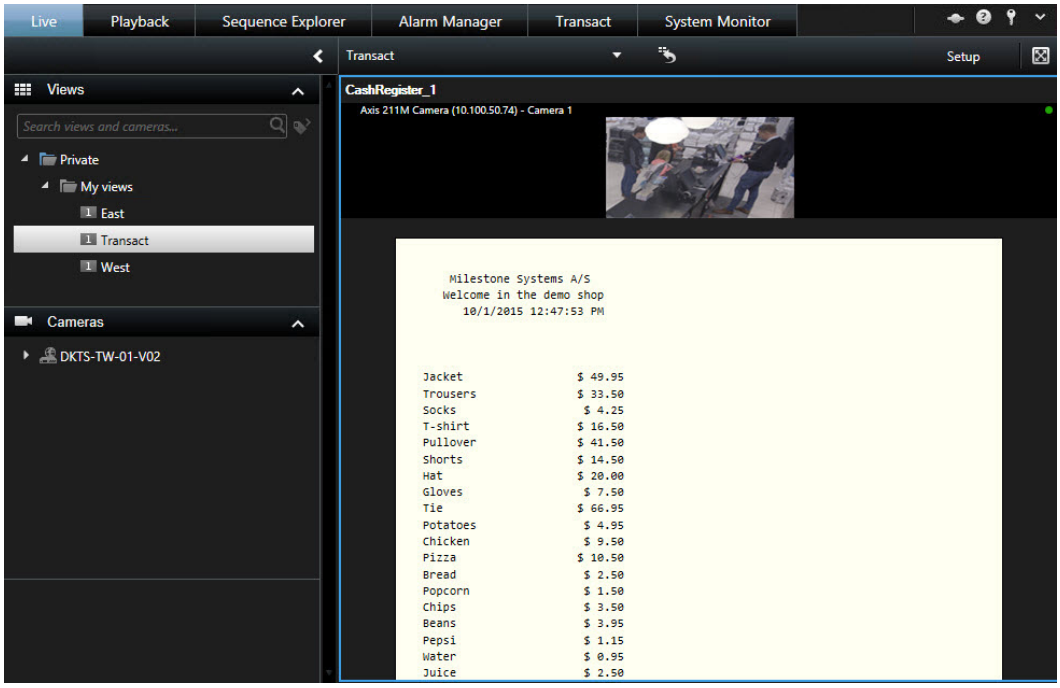
You can observe real time transactions in combination with live video surveillance from the cameras recording the transactions. For example, you may want to observe a cash register, the sales clerk, and the ongoing transactions.

Requirements

You have set up a view to display transactions. For more information, see Set up views for transactions on page 111.

Steps:

1. On the **Live** tab, 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 scrollbar allows you to view the part of the receipt that is hidden. If you try to access the scrollbar, the view item toolbar appears covering the scrollbar. To access the scrollbar, press and hold down **Ctrl** while moving the cursor into the view item area.

Investigating transactions

There a several tasks related to investigating your transactions. For example, you can view transactions in views in combination with other types of content, you can search and filter transactions, and you can view transaction alarms.

Investigate transactions in a view

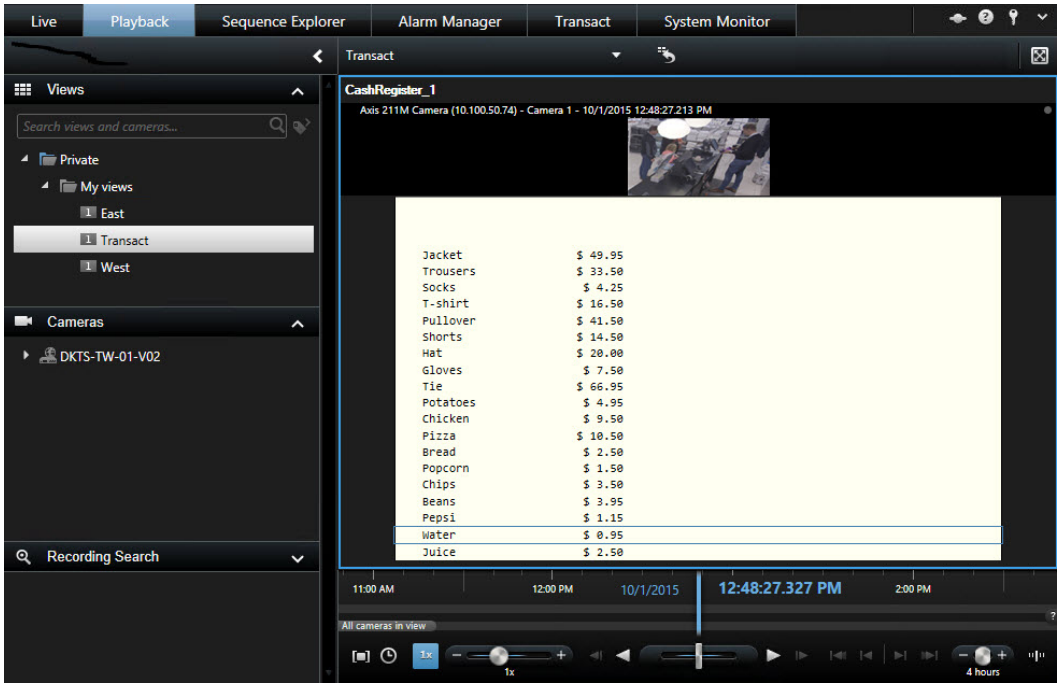
The simplest method of investigating transactions is to view transactions in a view, where the receipts roll over the screen in sync with the video recordings.

Requirements

You have set up a view to display transactions. For more information, see Set up views for transactions on page 111.

Steps:

1. Click the **Playback** tab.
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.



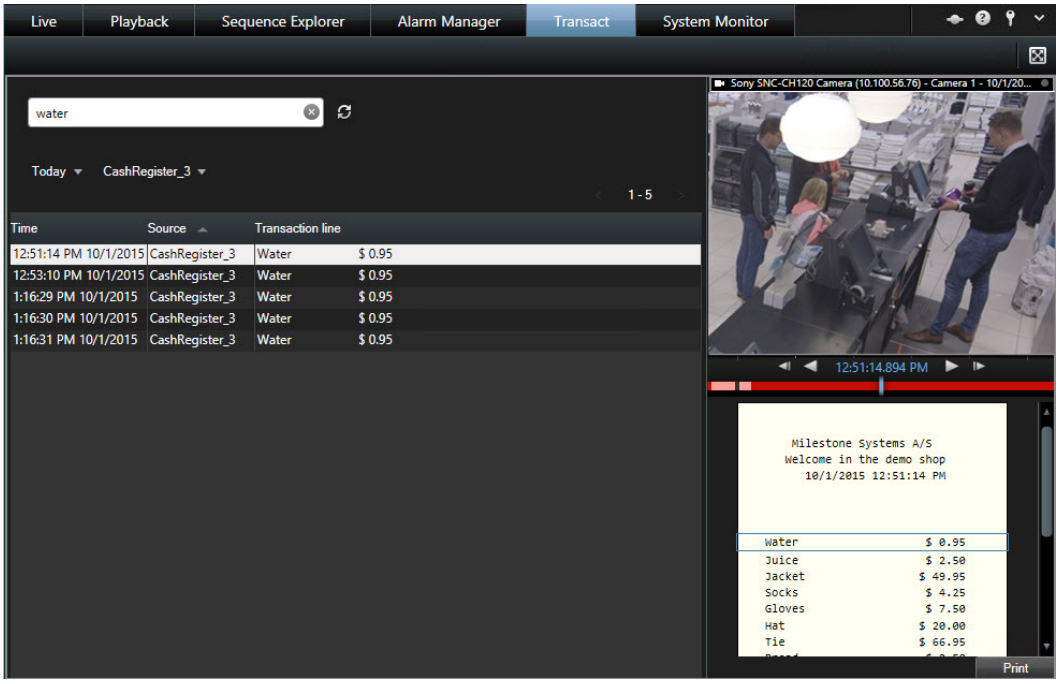
3. To browse the video sequences in backward mode, drag the time line to the right.
4. To browse the video sequences in forward mode, drag the time line to the left.
5. Use the  or  buttons to play the video in backward or forward play mode.

If the transaction view item is narrower than the receipt, a horizontal scrollbar allows you to view the part of the receipt that is hidden. If you try to access the scrollbar, the view item toolbar appears covering the scrollbar. To access the scrollbar, press and hold down **Ctrl** while moving the cursor into the view item area.

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  buttons to start the video in backward play or forward play mode.

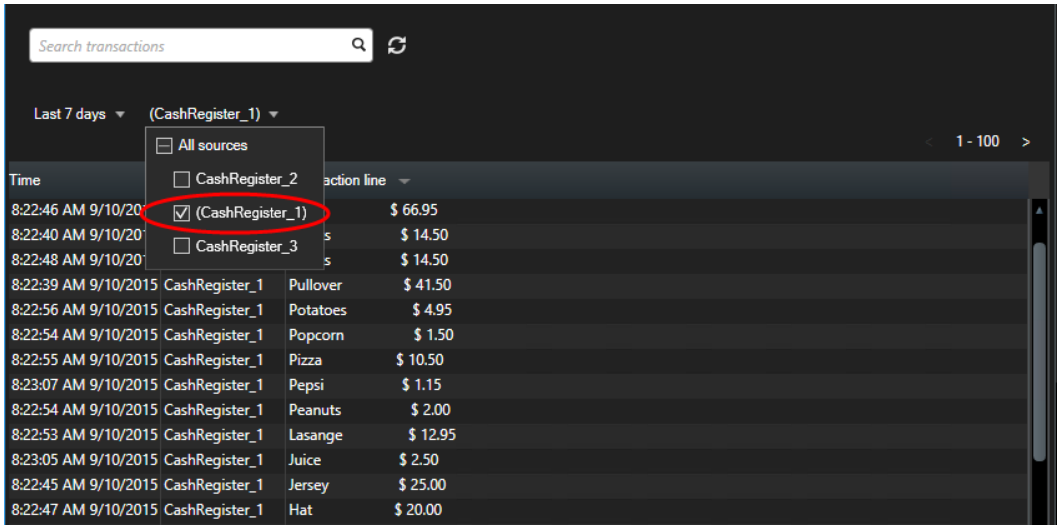
By default, transaction data is stored for 30 days, but depending on the configuration, data can be stored up to 1000 days.

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 in backward or forward play mode.

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

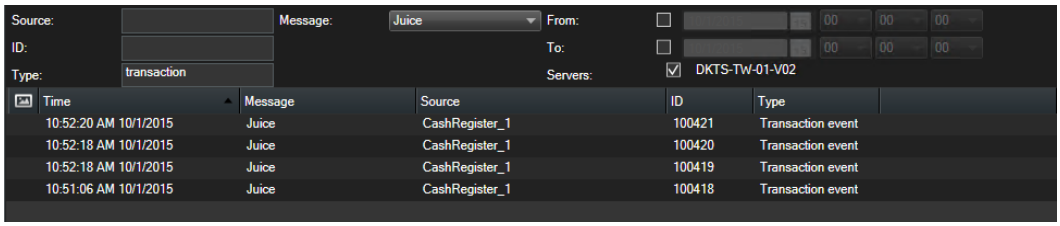
You can investigate transaction events, for example by identifying transactions where a specific item has been purchased. Investigating a transaction event involves viewing the details about the event in the alarm list and the associated video recordings.

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 type "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 video previewer.

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:

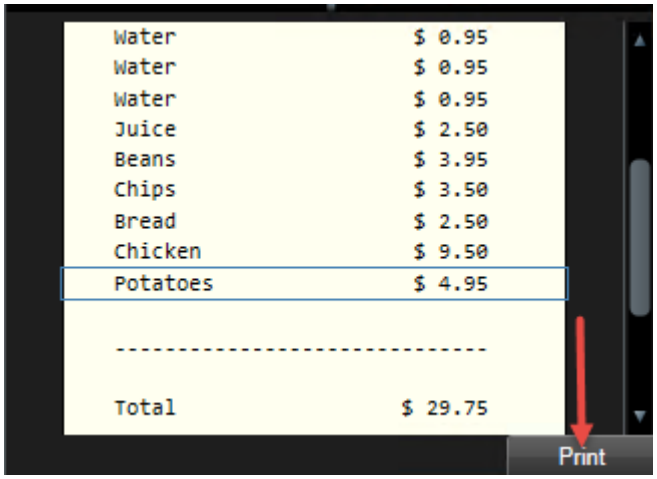
1. Click the **Alarm Manager** tab.
2. Click the **Setup** button in the upper right corner to enter the setup mode.
3. Expand the **Properties** pane.
4. In the **Data Source** list, select **Alarm** and click **Setup** again to exit the setup mode. The most recent alarms are displayed at the top.
5. To view only the alarms triggered by transaction events, expand the **Filter** section and type "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 video previewer.

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 Investigate transactions using search and filters on page 257.



3. Click **Print** below the transaction to print it. A Windows dialog box appears.
4. Select the required printer and click **OK**.

Troubleshooting

Logging in (troubleshooting)

These are error messages that you may encounter while trying to log in to XProtect Smart Client:

Your user rights do not allow you to log in at this point in time. User rights may vary depending on time of day, day of week, etc...

You have tried to log in at a time when your user rights do not allow you to log in. To resolve this issue:

Wait until you are permitted to log in. Consult your surveillance system administrator if in doubt about your user rights.

You do not have access to any part of the application. Contact the system administrator.

You currently have no access rights to any part of the XProtect Smart Client, and therefore you cannot log in. To resolve this issue:

Consult your surveillance system administrator, who will be able to change your access rights if required.

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 rights. 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 rights to do so. To resolve this issue:

Ask your system administrator to check that you have the necessary rights to authorize other users or ask someone else with sufficient rights to authorize the user.

Failed to connect. Check the server address.

It was not possible to connect to the surveillance system server at the specified server address. To resolve this issue:

Verify that you have typed the correct server address. The http:// prefix and port number are required as part of the server address (example: http://123.123.123.123:80, where :80 indicates the port number). Consult your surveillance 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 typed your user name correctly, then re-type your password to ensure it does not contain errors. User names and passwords are case sensitive. For example, there may be a difference between typing **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 surveillance system administrator, who may be able to extend the number of simultaneously connected clients.

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 surveillance system is mistakenly used without any modification on another surveillance system. This can cause different cameras to "fight" over the same identity, and that can in turn block your XProtect Smart Client's access to the surveillance system. If you see such a message, you cannot correct the problem. Instead, contact your surveillance system administrator, who will be able to handle the issue.

Some messages will appear in an orange ribbon above your views:

You no longer have permission to do this

Occurs if your time-dependent user rights 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 21), your user rights 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 21), your rights 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.

Exporting (troubleshooting)

I have received an export, but I cannot run the SmartClient-Player.exe file

If you get an error message when double-clicking the **SmartClient-Player.exe** file, the export may have been created on a computer with a 64 bit Windows operating system, and you are using a 32 bit operating system.

To resolve the issue, try one or more of the following:

- Open the **SmartClient-Player.exe** file on a 64-bit Windows computer.
- Open the export with a 32-bit version of XProtect Smart Client. To do this, follow these steps:
  1. Open this link: https://www.milestonesys.com/downloads/.
  2. Select **Product**, for example XProtect Corporate, **Version**, and **Language**.
  3. Click **XProtect Smart Client 32-bit** to download the application.
  4. When installed, go to the export folder and open the **Client Files** folder.
  5. Double-click the **Exported Project.scp** file. The XProtect Smart Client – Player should open, and you can play back the video.
- Ask the person who provided the export to create a new export using a 32-bit XProtect Smart Client.
- Ask the person who provided the export to create a new export using a different export format, for example AVI or MKV.

If this did not help you, please contact support.

Smart map (troubleshooting)

My camera does not appear on the smart map

If there are one or more cameras that should, but do not appear on the smart map, then likely the cameras have not been positioned. To resolve this issue, do one of the following:

- Drag the cameras onto the smart map from the camera hierarchy. This requires that editing of cameras is enabled on your user profile
- Ask you system administrator to set the GPS position of the cameras in the camera properties in Management Client

XProtect Smart Wall (troubleshooting)

Some of the solutions will require help from your system administrator.

My monitors do not display the layout that I specified for my Smart Wall

Typically, this occurs because your system administrator did not activate the preset for the monitor. Ask your system administrator to verify that the preset is active in Management Client.

My camera is not part of a preset. Why isn't it removed when I activate the preset?

This can be because the **Empty preset item** setting is not selected for the preset. Ask your system administrator to verify the setting for the preset in Management Client.

I cannot drag an item, for example a camera, to a view. When I click the item, nothing happens

This is a known issue in Microsoft Windows that can also occur in XProtect Smart Wall. The workaround is press ESC one time, and the drag functionality should work again.

When I drag an image from a view to my Smart Wall, it isn't displayed.

You probably did not embed the image in the view, and the computer that is running the Smart Wall cannot access the image file. To ensure that everyone can see an image, it's a good idea to embed it in the view. For more information, see Displaying content on Smart Wall on page 230.

My Smart Wall monitors are displayed on top of each other

When your system administrator added monitors to your Smart Wall, he or she did not define the layout of the monitors. When your administrator adds monitors, the system automatically stacks them in the layout in the order in which they were added. Your administrator must then arrange them according to your needs.

I cannot drag an image from Windows Explorer to my Smart Wall monitor. The cursor does not change to the Allow Drop icon

This occurs when your Smart Client is not running under the same user profile as Windows Explorer. For example, you are running Smart Client under the Local administrator user profile, but you are running Windows Explorer as a Standard user. To resolve this issue, ensure that both programs are running under the same user profile.

I have added the Alarm List to a view item, but I cannot use the scroll bar to view details

This is a known issue in XProtect Smart Wall. To use the scrollbar, position the pointer outside the view item, and then press and hold the CTRL key. This prevents the view item's toolbar from covering the scrollbar. You can now move the pointer into the view item and use the scrollbar.

XProtect Transact (troubleshooting)

The error messages in this topic are related to the event server. If you encounter one of these errors, Milestone suggests that you contact your system administrator.

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.

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.

If the error is an internal server or database error, the error is registered in one of the server logs.

Upgrade

Upgrading XProtect Smart Client

During log-in, if you are using an older version of XProtect Smart Client than the server that you are connecting to, a message informs you that a newer version of the XProtect Smart Client is available, including where to download the application. Milestone recommends that you download the newer version.

If XProtect Smart Client is newer than the server that you are connecting to, certain features may not be available.

Glossary

A

access control
A security system that controls the entering of persons, vehicles or others into a building or area.

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

camera navigator
A feature that allows you to see all your cameras in relation to each other, for example, as they are laid out according to a floor plan. Using the Camera Navigator, you can navigate from one camera to the next from a single view.

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.

codec
A technology for compressing and decompressing audio and video data, for example in an exported AVI file.

custom overlay
A user-defined, graphic element that users can add to a smart map, for example to illustrate a floorplan 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.

F

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.

H

H.264
A compression standard for digital video. Like MPEG, the standard uses lossy compression as it stores 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. Together with a very large degree of compression, this helps greatly reduce the size of video in the H.264 format. The very large degree of compression in H.264, however, can use considerable resources on the devices involved in the data communication. For example, the computer running XProtect Smart Client should be able to use considerable resources on decompressing H.264 video when it receives it from the surveillance system.

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.

JPG
See JPEG.

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".

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 camera positions in views on the Live tab. 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 on the Live tab or recorded video on the Playback tab.

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.

preset
A predefined layout for an individual monitor in XProtect Smart Client.

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.

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 cameras, 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 with which you can easily and quickly find video with motion in one or more selected areas of recordings from a particular camera.

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/.