Milestone Systems

XProtect® Smart Client 7.0

milestone

The Open Platform Company

Contents

Copyright, trademarks and disclaimer

Copyright

© 2012 Milestone Systems A/S.

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 reserve 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 surveillance system installation folder.

Target audience for this manual

This manual is aimed at users of the Milestone XProtect Smart Client.

This manual provides detailed descriptions of XProtect Smart Client installation, configuration, and use. It furthermore provides a number of targeted "how-to" examples, guiding users through completing common tasks in the XProtect Smart Client .

Note that depending on the type of Milestone surveillance system you connect to, depending on your user rights, and depending on your role in your organization, some features in the XProtect Smart Client may not be available to you. Ask your surveillance system administrator if in doubt.

Tip: If you know that your surveillance system administrator has already configured the necessary views for you, you may skip parts of this manual. After installing and logging in to your XProtect Smart Client, you can proceed straight to this manual's chapters about viewing live and recorded video. Consult your surveillance system administrator if in doubt.

Information for XProtect Analytics Users

If your organization uses the XProtect Analytics solution, which provides an intelligent yet highly intuitive solution for video content analysis tasks such as license plate recognition, perimeter protection, left objects detection, etc., it will be possible to view video together with analytics data in the XProtect Smart Client. Viewing of such analytics data in the XProtect Smart Client is not covered in this manual. If you require such information, please refer to the separate documentation for XProtect Analytics, available from www.milestonesys.com.

Information for XProtect Transact Users

If your organization uses the XProtect Transact add-on solution for handling loss prevention through video evidence combined with PoS or ATM transaction data, it will be possible to view video together with time-linked transaction data in the XProtect Smart Client. Viewing of such transaction data in the XProtect Smart Client is not covered in this manual. If you require such information, please refer to the separate documentation for XProtect Transact, available from www.milestonesys.com.

SC70-um-2(b1)-060912

First time use

Install the XProtect Smart Client

The XProtect Smart Client must be installed on your computer before you can use it. Typically, you download the XProtect Smart Client from the surveillance system server, then install it on your computer. Alternatively, your surveillance system administrator may ask you to install the XProtect Smart Client from a DVD.

Tip: To uninstall the XProtect Smart Client, follow the normal Windows procedure for uninstalling programs (see the Windows Help for more information).

Surveillance system administrators: For information on silent installation (when available), see the separate administrator's documentation for your surveillance system's server software.

- **Install from the surveillance server** (on page 12)

- **Install from a DVD** (on page 12)

Install from the surveillance server

1. Verify that your computer meets the XProtect Smart Client's minimum system requirements (on page 17).

2. Open an Internet Explorer browser (version 6.0 or later) and connect to the surveillance system server using the URL or IP address specified by your system administrator.

3. On the Welcome page, click **Language** and select your required language.

   Tip: You can easily change the language in the **Options** menu of the XProtect Smart Client. Under XProtect Smart Client **Installers**, click the relevant XProtect Smart Client link to start the installer.

4. If you receive a security warning (**Do you want to run or save this file?**, **Do you want to run this software?** or similar), accept this (by clicking **Run** or similar—the exact name depends on your browser version).

5. 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, such as XProtect Analytics or XProtect Transact, this path might not be valid anymore (see "Install from a DVD" on page 12).

Install from a DVD

1. Verify that your computer meets the XProtect Smart Client's minimum system requirements (on page 17).

2. Insert the surveillance system software DVD, select the required language, and then click **Install XProtect Smart Client.**

3. If you receive a security warning (**Do you want to run or save this file?**, **Do you want to run this software?** or similar), accept this (by clicking **Run** or similar—the exact name depends on your browser version).

4. The XProtect Smart Client **installation** wizard starts. In the wizard, follow the installation instructions.

MIP Plug-ins

Your XProtect Smart Client may contain a **MIP Plug-ins** pane. The pane is used for handling plug-in functionality, typically for third-party applications, for example an access control system or similar, which can be controlled through the XProtect Smart Client. If your **MIP Plug-ins** pane has no content, it is because your XProtect Smart Client has no plug-in functionality.

On some surveillance systems, you can add more types of content to views in your XProtect Smart Client. This may be the case if your organization uses add-on products for increasing the capabilities of its surveillance system.

Examples:

- XProtect Transact, which is used for tracking transactions from cash registers, ATMs, etc. linked with video recordings

- XProtect Analytics, which provides video content analysis tasks such as license plate recognition, perimeter protection, left-objects detection, etc.

The XProtect Smart Client plug-in for XProtect Analytics can only run on a 32-bit version of the XProtect Smart Client. The plug-in cannot run on a 64-bit installation. By default, in XProtect Smart Client versions **earlier than 4.0a**, the XProtect Smart Client is installed in:

```
C:\Program Files\Milestone\Milestone XProtect Smart Client\
```

and plug-ins for add-on products are installed in:

```
C:\Program Files\Milestone\Milestone XProtect Smart Client\plugin
```

By default, in XProtect Smart Client **version 4.0a and later**, the XProtect Smart Client is installed in:

```
C:\Program Files\Milestone\XProtect Smart Client\
```

and plug-ins for add-on products are installed in:

```
C:\Program Files\Milestone\XProtect Smart Client\plugin
```

The change to the default installation path means that if you have plug-ins for add-on products for XProtect Smart Client versions earlier than 4.0a, these plug-ins will not work with your new XProtect Smart Client because your new XProtect Smart Client will look for plug-ins at a different location.

If you want your new XProtect Smart Client to work with older plug-ins for add-on products, the solution is therefore either:

to copy the existing plug-ins from the old default installation path for plug-ins to the new default installation path for plug-ins

- or -

to change the XProtect Smart Client installation path to the old default, C:\Program Files\Milestone\Milestone XProtect Smart Client\, during the installation of your new XProtect Smart Client.

The log-in process

The Login window

The first time you log in, you need to determine whether any views exist. Views determine how video is displayed and are required in order to be able to use the 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 (see "The XProtect Smart Client window" on page 24).

Tip: 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 XProtect Smart Client installed and that you can restore views from your last log-in.

Server address

Type the URL or IP address of the surveillance system server, as specified by your surveillance system administrator. Internet connections may use different ports for different purposes; therefore, the URL or IP address may include a port number (example: http://123.123.123.123:80, where :80 indicates the port number). If you have logged in before, you can select your server from the Server address list.

Authentication

There are three possible methods of authentication (the process that verifies that you are who you claim to be):

Not all surveillance systems (see "Surveillance system differences" on page 32) support the use of all three authentication methods.

- **Windows authentication (current user)** with which you will be authenticated through your current Windows login, and do not have to specify any user name or password. This is the XProtect Smart Client 's default authentication method.

- **Windows authentication**, with which you will be authenticated through your Windows login, but you will need to type your Windows user name and password.

- **Basic authentication**, which can only be used when connecting to selected surveillance systems.

User Name

Only required if the authentication method **Windows authentication** or **Basic authentication** is selected. If using **Windows authentication**, type your Windows user name. If using **Basic authentication**, type the user name supplied by your surveillance system administrator. The user name is case-sensitive; there is a difference between typing, for example, "amanda" and "Amanda."

Password

Only required if the authentication method **Windows authentication** or **Basic authentication** is selected. If using **Windows authentication**, type your Windows password. If using **Basic authentication**, type the password supplied by your surveillance system administrator.

Remember password

Available when using **Windows authentication** or **Basic authentication**. Gives you the option of storing your password, in which case you just click **Connect** the next time you want to log in.

Security restrictions may apply. If in doubt, consult your surveillance system administrator.

Auto-login

Restores the default export settings assigned to your profile. If selected, you will automatically be logged in to the XProtect Smart Client with your credentials from your last log-in, when you log in to Windows. If using **Windows authentication**, you must select **Remember password** for the auto-login feature to be available.

Security restrictions may apply. If in doubt, consult your surveillance system administrator.

Log in and out

1. Open the XProtect Smart Client.

2. A splash screen appears for a few seconds while the XProtect Smart Client loads and then the XProtect Smart Client log-in dialog appears.
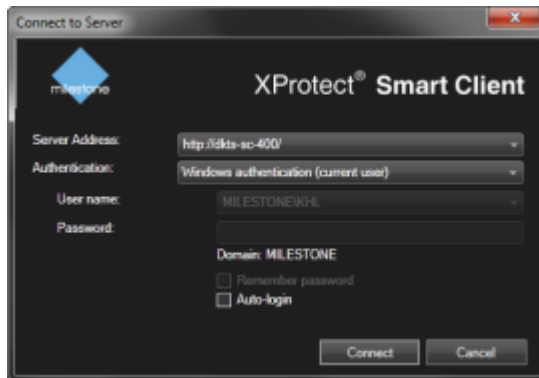
3. Specify your login information, and then click **Connect**.

   Tip: If a problem occurs during log-in, you will receive an error message (see "Troubleshooting" on page 15).

4. If you have logged in before, you can restore the views you last used. Depending on configuration, the XProtect Smart Client may ask you if you want to restore the view(s) you last used. Your options are:

   o **Main view:** If you select this, the view you last used in the XProtect Smart Client 's main window is restored.

   o **Detached views:** Only available when connecting to selected Milestone surveillance systems (see "Surveillance system differences" on page 32), and if you used views in detached windows in your last log-in (see Use Multiple windows for more information). Select this if you want to restore the views you last used in detached windows.

5. After a short wait, the XProtect Smart Client window opens.

6. To log out of the XProtect Smart Client, simply click the **Log Out** button in the XProtect Smart Client title bar.

Troubleshooting

If a problem or other issue occurs during login to the XProtect Smart Client, you will see one of the following error messages:

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...

Issue: You have tried to log in at a time when your user rights do not allow you to log in.

What to do: 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.

Issue: You currently have no access rights to any part of the XProtect Smart Client, and therefore you cannot log in.

What to do: Consult your surveillance system administrator, who will be able to change your access rights if required.

Failed to connect. Check the server address.

Issue: It was not possible to connect to the surveillance system server at the specified server address.

What to do: Verify that you have typed the correct server address. Note that the **http://** prefix as well as a port number is 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.

Issue: It was not possible to log in with the specified user name and/or password.

What to do: Verify that you have typed your user name correctly, then re-type your password to ensure it does not contain errors. User names as well as 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.

Issue: The maximum number of clients allowed to connect to the surveillance system server simultaneously has been reached.

What to do: 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.

New Client available. Upgrade is recommended/required. The new version can be downloaded from.

Issue: A new version of the XProtect Smart Client is available. This message is typically accompanied by information about whether an update is recommended or whether it is a requirement (for example because important new features will not work in your current XProtect Smart Client version). The message will typically also contain information about where to download the new version from.

What to do: Follow the advice given in the message. Consult your surveillance system administrator if in doubt.

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 32)—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 surveillance 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 32), 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/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.

System requirements

The following are **minimum** system requirements for running the XProtect Smart Client:

Operating System	Microsoft® Windows® XP Professional (32-bit or 64-bit), Windows Server 2003 (32-bit or 64-bit), Windows Server 2008 R1/R2 (32-bit or 64-bit), Windows Vista® Business (32-bit or 64-bit), Windows Vista Enterprise (32-bit or 64-bit), Windows Vista Ultimate (32-bit or 64-bit), Windows 7 Professional (32-bit or 64-bit), Windows 7 Enterprise (32-bit or 64-bit) or Windows 7 Ultimate (32-bit or 64 bit).
CPU	Intel® Core2™ Duo, minimum 2.4 GHz or higher (more powerful CPU recommended for XProtect Smart Clients running high number of cameras and multiple views and displays).
RAM	Minimum 1 GB (higher RAM recommended for XProtect Smart Clients running high number of cameras and multiple views and displays).
Network	Ethernet (100 Mbit or higher recommended).
Graphics Adapter	AGP or PCI-Express, minimum 1280ꞏ024, 16 bit colors.
Hard Disk Space	1 GB free.
Software	Microsoft .Net 4.0.
	DirectX 9.0 or newer.

Tip: To check which DirectX version is installed on a computer, click **Start**, select **Run...**, and type **dxdiag**. When you click **OK**, the **DirectX Diagnostic Tool** window will open; 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 http://www.microsoft.com/downloads/ (see http://www.microsoft.com/downloads/ - http://www.microsoft.com/downloads/).

The basics

What's new

If you have previously used the XProtect Smart Client, you may have noticed that the XProtect Smart Client has changed its appearance. You may also already have noticed one or more new features in the XProtect Smart Client.

Major changes

New streamlined interface

- New interface with dedicated tabs for the Sequence Explorer and Alarm Manager improves efficiency

- Choice of dark or light application themes allows you to optimize the XProtect Smart Client for your particular working environment

- Video overlaid pan-tilt-zoom (PTZ) button and a virtual joystick that works with all cameras that support joysticks give more intuitive PTZ control and make it easier to track moving objects

- If an alarm is triggered, the map automatically displays the corresponding alarm and camera locations, giving the operator instant visual and situational verification

Easy evidence creation

- Easy-to-use integrated video timeline with time navigation and playback controls allows you to drag and select a time interval for export, simplifying the video export process

- Advanced export options, including a digital signature, re-export disablement, bulk camera export, and direct export to optical media, resulting in faster video exports and more secure handling of evidence material

Minor changes

Copying views: you can copy views (see "Create and manage views" on page 40) or groups of views within the same client session.

Change map background: allows you to to update a map (see "Working with maps" on page 64) but keep all your cameras, and other elements in their relative positions on it.

Get to know the XProtect Smart Client

User rights determine the way you work

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**

- 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. Note that when connected to certain surveillance systems (see "Surveillance system differences" on page 32), 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.

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 your client. In such cases, you also need to know which plug-ins your XProtect Smart Client uses.

To view this information, click the **About** button on the XProtect Smart Client toolbar.

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. For example, XProtect Smart Client 6.0 is compatible with XProtect Enterprise 8.0, XProtect Enterprise 7.0, XProtect Corporate 4.0, and XProtect Corporate 3.1. However, an older version of the XProtect Smart Client is not compatible with the latest server version, for example, XProtect Smart Client 5.5 is not compatible with XProtect Enterprise 8.0.

The XProtect Smart Client plug-in for XProtect Analytics can only run on a 32-bit version of the XProtect Smart Client. The plug-in cannot run on a 64-bit installation. The main window

The main window

The XProtect Smart Client provides you with access to surveillance systems. The XProtect Smart Client must be installed locally on your computer.

In the XProtect Smart Client window (on page 24), you view live video on the **Live** tab of the XProtect Smart Client, and recorded video on the **Playback** tab. When you select the **Live** tab, your XProtect Smart Client connects to the surveillance system server, and displays live video from cameras in the selected view.

If your computer has more than one physical display attached, you can send individual views to separate windows (see "Multiple windows" on page 74) letting you watch more than one view at a time.

View live video
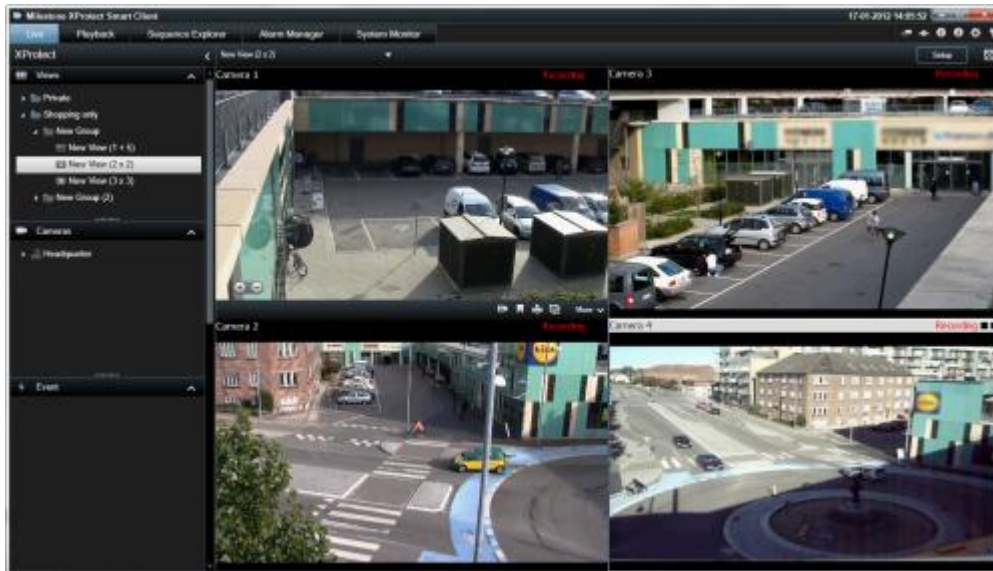
Example: **Live** tab displaying video from four cameras

The **Live** tab offers you numerous features, including audio (on page 54), carousels (on page 72), hotspots (on page 73), Matrix, camera shortcut menus, PTZ (Pan/Tilt/Zoom (see "PTZ and 360° lens images" on page 95)) control, digital zoom, events activation, output activation, quick playback, and more.

Even though you can see live video from a camera on the **Live** tab, the video stream from the camera is not necessarily being recorded. Video is normally recorded as defined by the surveillance system server. Typically, recording takes place according to a schedule (for example, every morning from 10.00 to 11.30) and/or whenever the surveillance system detects special events (for example, motion generated by a person entering a room, a sensor registering that a window is being opened, or manually activating an event in your XProtect Smart Client). Typically, you view recorded video on the **Playback** tab, but you can also view it on the **Live** tab (see "View recorded video" on page 21).

If title bars have been enabled in the camera properties (see "Cameras" on page 46) in setup mode, the title bar above the camera's image displays Recording if video is being recorded.

Tip: To maximize video from a particular position in a view, double-click the camera position. To return to normal view, simply double-click the camera position again.

You may notice that sometimes the camera is recording for short periods only. This is because the surveillance system server may have been configured to only record the video stream from a camera when there is motion, when a door is open, or similar, which can lead to many short periods of recordings.

You can therefore still select **Start Recording for # Minutes** even though the video stream from a camera is already being recorded; this way you can make sure that the video stream from the camera will be recorded without interruption for the specified number of minutes.

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.

Record video

Recording while watching live video is useful if you see something of interest.

Start recording

On the camera toolbar for the position in the view you want to record, select **Start recording for # Minutes**.

Alternatively, if available, click the overlay button, which appears when you move your mouse over the position in the view. Another quick way to start recording is to create a bookmark (click the bookmark icon ▮ on the camera toolbar)

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.

Tip: You can start recording the video stream from more than one camera simultaneously, although you must select them one by one. Note that the number of minutes you record may vary from camera to camera.

View recorded video

You view recorded video on the **Playback** tab of the XProtect Smart Client. When you select the **Playback** tab, the XProtect Smart Client will connect to the surveillance system server, and display recorded video from the cameras in the selected view. This way, you are able to play back recorded video. Note that particular user rights may be required in order to access the **Playback** tab, and that, depending on your user rights, access to browsing video from some cameras may be restricted.
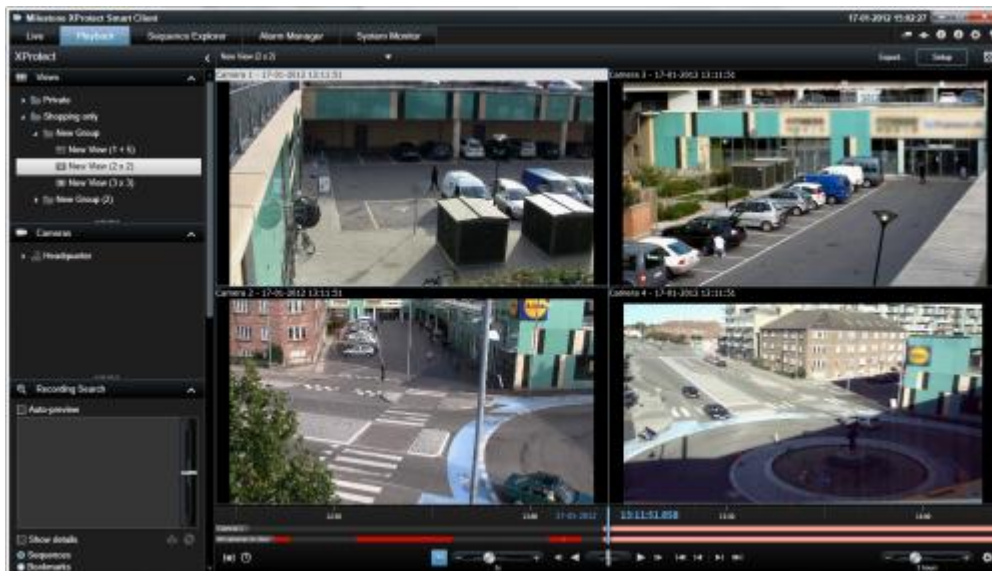
The **Playback** tab offers you numerous advanced features for browsing recorded video, including the timeline (see "Time navigation" on page 103), smart search (which lets you search for motion in selected areas of recordings from a particular camera), and two types of sequences browsing (either through a simple list with a preview option or through the Sequence Explorer (on page 100)'s thumbnail view of multiple sequences).

In addition to the video browsing features, the **Playback** tab also lets you listen to audio (when connected to selected Milestone surveillance systems only), use hotspots, use digital zoom (see "Digital zoom" on page 93), navigate 360° lens images, print images (see "Print evidence" on page 106), and export video evidence (see "Exporting evidence" on page 111) as AVIs (movie clips), JPEGs (still images) as well as XProtect format.

Tip: To maximize video from a particular position in a view, double-click the camera position. To return to normal view, simply double-click the camera position again.

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 **Options (see "Functions options" on page 85)** window).

You can use independent playback to view recorded video from the **Live** tab or to view video independently of the master time.

View recorded video using independent playback

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

1. Move your mouse across the camera that you want to view recorded video for. On the toolbar that appears, click the **Toggle Independent Playback** button.

    The independent playback timeline appears:
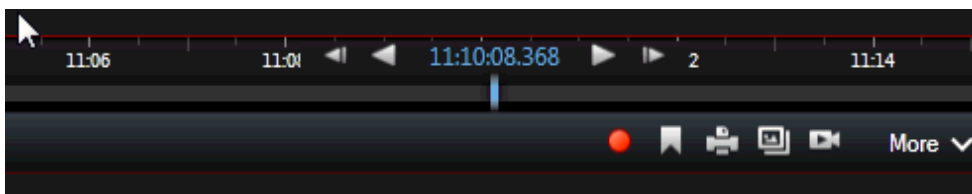
2. Drag the timeline (see "The timeline" on page 104) to select the time containing the video that you want to view.

3. If you want to view recorded video for the selected time on all the cameras in your view at once, click the

    red button on the toolbar. This displays the **Playback** tab with all cameras synchronized to the time you have selected.

Setup mode

*   To enter setup mode, on the XProtect Smart Client toolbar, click **Setup**.

In setup mode, the **Setup** button and panes (such as the **Properties (see "The Properties pane" on page 49)** pane) are highlighted in orange and different panes appear on the left side panel.
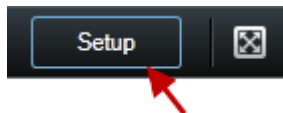
To return to the default view, click the **Setup** button again.

Select a view

You can select a view from the Views pane on the **Live** and **Playback** tab.

If neither the pane nor the shortcut is available, check the pane's availability in the Options (see "Panes options" on page 85) window.

If views have been assigned shortcut numbers (see "Create and manage views" on page 40), you will also be able to select a view by using keyboard shortcuts (see "Keyboard shortcuts" on page 26).

View in full screen

To view your XProtect Smart Client in full screen mode, on the XProtect Smart Client toolbar, click the **Full Screen** ☒ button (or press F11 on your keyboard).

When you change to full screen mode, the toolbars and panes are hidden. To display them, move your mouse to the top of the screen.

To return to the default view, press ESC or F11 on your keyboard.

Copy single images

You can copy single still images from selected cameras. Copied images can then be pasted (as bitmap images) into other applications, such as word processors, e-mail clients, etc. You can only copy a single image from one camera at a time.

On the camera toolbar, click the **Copy to Clipboard** icon to copy an image.

Get help

You can access the XProtect Smart Client help system by clicking the **Help** button in the XProtect Smart Client toolbar or by pressing F1 on your keyboard.

The help system is context-sensitive, which means it automatically displays a help topic relevant to the area you are working with. Help topic texts may contain various types of links, notably expanding drop-down links that display detailed information when you click them.

Tip: If you want to quickly collapse all texts from expanding drop-down links in a help topic, click the title of the topic on the **Contents** tab.

When you print a help topic, the topic is printed as you see it on your screen. Therefore, if a topic contains expanding drop-down links, click each required drop-down link to display the text in order for it to be included in your printout. This allows you to create targeted printouts, containing exactly the amount of information you want.

The XProtect Smart Client window
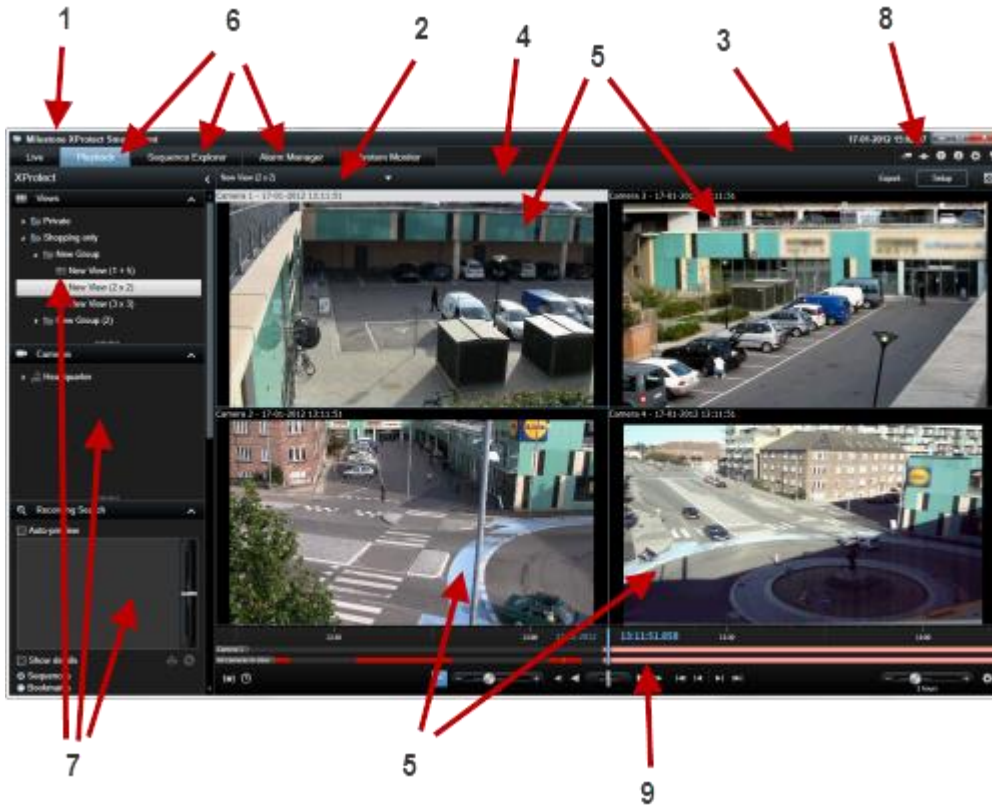
1. Title bar 2. Toolbar 3. Application toolbar

4. View 5. Position in a view 6. Tabs

7. Panes 8. Application buttons 9. Timeline

Panes

Panes give you access to the majority of the XProtect Smart Client features. The panes you see depend on your XProtect Smart Client configuration and on your task.

Panes can be minimized to save space and to give a better overview of the panes you use. Click the **Minimize/expand** icon ⌄ on the title bar of the pane to minimize or expand it.

Tabs

The XProtect Smart Client has the following main areas:

- The **Live** tab for viewing live video

- The **Playback** tab for viewing recorded video

- The **Sequence Explorer** tab for navigating video sequences and bookmarks

- The **Alarm Manager** tab for investigating incidents and alarms

- The **System Monitor** tab 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.

Views

About views

The way in which video is displayed in the XProtect Smart Client is called a view. A view can contain video from up to 100 cameras, depending on your surveillance system. Your XProtect Smart Client can handle an unlimited number of views, allowing you to switch between video from various groups of cameras. Each view's layout 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 (see "Private and shared views" on page 39).

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.

Your user settings, including information about your views, are stored centrally on the surveillance system server, so you can use your views, private as well as shared, on any computer that has a XProtect Smart Client installed, provided you log in with your own user name and password.

Example: XProtect Smart Client displaying a view with video from four different cameras (a 2x2 view)

Task buttons

These are on the XProtect Smart Client toolbar and depend on which tab you are on, for example, **Setup** is not available on all tabs. Examples of task buttons:

- **Setup:** click to enter setup mode (on page 22)

- **Export**: click to export video (see "Exporting evidence" on page 111)

- **Toggle full screen** : click to toggle between full screen (see "View in full screen" on page 23) and a smaller window that you can drag to the size you want.

Application Buttons
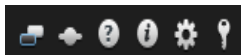
Application buttons in the toolbar let you select basic XProtect Smart Client actions. From left to right the buttons are:

- **Toggle Theme:** switch the XProtect Smart Client theme to dark or light

- **Connection Overview:** access to the **Connection Overview** (see "**View Server Status in Connection Overview**" on page 30) window.

- **Help:** access the help system (see "Get help" on page 23)

- **About:** view version number, etc.

- **Options:** configure XProtect Smart Client settings and behavior (see "XProtect Smart Client options" on page 83), joysticks, keyboard shortcuts, and language

- **Log Out:** log out (see "The log-in process" on page 13) of the XProtect Smart Client

Keyboard shortcuts

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

Tip: In addition to the standard keyboard shortcuts, you can assign your own custom shortcut key combinations (see "Keyboard options" on page 89) for particular actions in the XProtect Smart Client.

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

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.
/+<camera shortcut number>+ENTER	Change the camera displayed in the selected position in the view 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 used on your surveillance system. Camera shortcut numbers are defined on the server.
/+ENTER	Change the camera in the selected position in the view to the default camera for that position.
/+/+ENTER	Change the cameras displayed in all positions in the view to the default cameras for those positions.
*+<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 will be able to see them in the **Views** pane, where they will appear in parentheses before the views' names. View shortcut numbers are defined on the

Press these keys	To do this
	XProtect Smart Client 's Setup tab.
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.

Use an 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.

Tip: 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 (see "Scripting" on page 125) in the XProtect Smart Client.

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.ShowPlayback();">`

Tip: 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 (on page 125) 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:
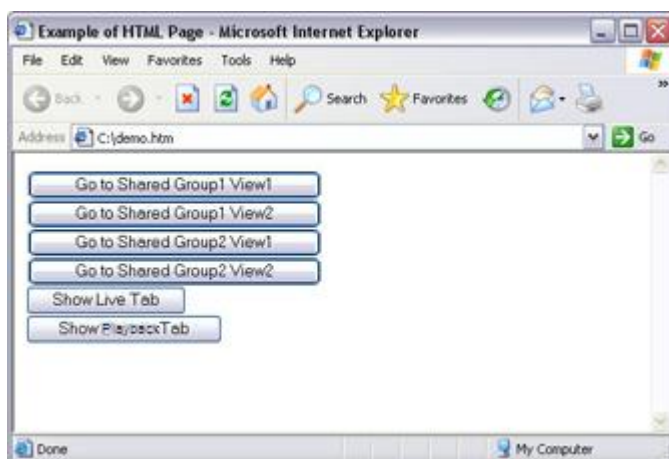
HTML page with buttons for navigating between views and tabs

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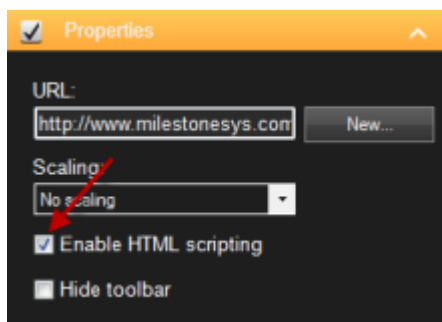
Selecting **Enable HTML scripting** ensures that the scripting required for the buttons to work is automatically inserted in the HTML page.

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:
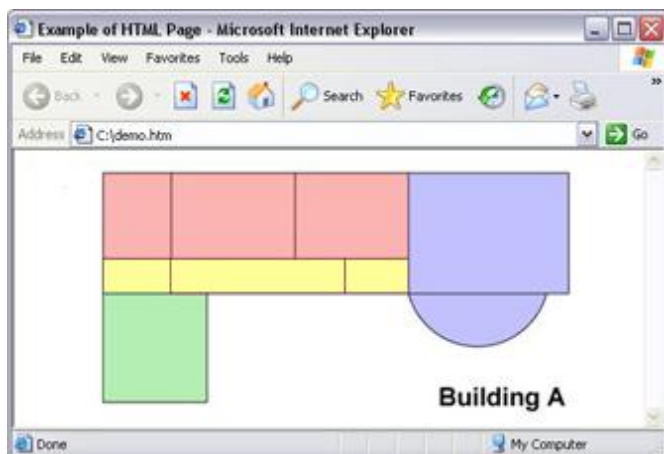
HTML page with image map for navigating between views

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 Clients. 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.

View Server Status in Connection Overview

The **Connection Overview** window lets you view the status of the surveillance servers your XProtect Smart Client is connected to. The dialog is useful if you are connected to a surveillance system that supports Milestone Federated Architecture (see "Surveillance system differences" on page 32). 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.

To view the **Connection Overview** window, click the **Connection Overview** button in the application toolbar:

Tip: If the button flashes red, one of more servers are unavailable.

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

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.

System Monitor tab

Use the <, > and home icons to navigate the System Monitor.

From here you can view system information and create reports on:

- **Management server:** shows data on **your management server**

- **Recording servers:** shows data on **any number of recording servers** in your surveillance setup, which can be viewed per:

  o **Disks**

  o **Storage**

  o **Network**

  o **Cameras**

- **Failover servers:** shows data on **any number of failover servers** in your surveillance setup

- **Additional servers:** shows data on **log servers, event servers etc**. in your surveillance setup

- **Cameras:** shows data **on any camera in any camera group** in your surveillance setup.

Each of these corresponds to a clickable, expandable area, most of which contains sub-areas. Each sub-area represents a server. When clicked, they provide relevant dynamic data on this server.

The **Cameras** bar however, contains a list of camera-groups to select from. Once a group is selected, you can select a specific camera and see dynamic data for it.

All servers display **CPU usage** and **available memory** information. Furthermore, recording servers also display **connection status** information.

Within each view, you can find a **History** link. Click it to view historic data and reports (to view reports on a camera, click the name of the camera). For each historic report, you can view data for the last 24 hours, 7 days or 30 days.

If you want to save and/or print reports, click the **Send to PDF** icon.

Milestone Federated Architecture™

If you run Milestone Federated Architecture™ (MFA) the **System Monitor** tab is divided into two parts. A left pane displaying a hierarchical tree-structure representing your federated architectural setup and on the right, a browser-based area with relevant system data for the selected MFA server.

Click any MFA server in the left-side pane to see its system data represented in the right-side area of the **System Monitor** tab.

If you move away from the tab or log out of the XProtect Smart Client and come back, the **System Monitor** tab will remember which server in your MFA is selected and continue to display system data from this server.

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

Surveillance system differences

The majority of the XProtect Smart Client features are available regardless of which type of Milestone surveillance system you connect to. However, a few features will work differently depending on the type of surveillance system your XProtect Smart Client is connected to. If in doubt, ask your surveillance system administrator about which type of Milestone surveillance system you connect to.

In general, we recommend 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 Enterprise surveillance system.

Connected to XProtect Corporate Surveillance System

The following lists refer to the latest version of XProtect; features **not** mentioned are fully available and no special conditions apply.

Available

- **Login authentication methods:** Only Windows authentication (through Active Directory™ as well as through a local database on the surveillance system) is available; basic authentication cannot be used.

- **User rights:** When connected to XProtect Corporate, user rights can be very flexible indeed. User rights may thus vary depending on time of day, day of week, etc.

- **Shared view groups:** Shared view groups can be shared by all users, but often they are shared by selected users only. Shared view groups can be stored in more than one top-level folder. The folders can be visible for all users, but often they are visible to selected users only. Folders' names are determined by the surveillance system administrator. Users' ability to edit shared view groups is determined by their roles on the surveillance system.

- **Audio:** Fully available (provided microphones/speakers are available on surveillance system).

- **Milestone Federated Architecture:** Supported by XProtect Corporate. 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.

Available if Configured

- **Options controllable from the surveillance system server (Follow Server):** Settings in the XProtect Smart Client's Options dialog can be controlled from surveillance system server. Depending on server-side configuration, the XProtect Smart Client user may or may not be able to override such server-controlled settings.

- **Ability to use Matrix content in views:** Available, provided Matrix has been configured on the surveillance system, and the user has a role with necessary Matrix rights.

- **Ability to send video to Matrix recipients through XProtect Smart Client shortcut menu:** Available, provided Matrix has been configured on the surveillance system, and the user has a role with necessary Matrix rights.

- **Ability to connect to failover servers:** Available, if configured on the surveillance system. Failover servers can take over if recording servers become unavailable. You may experience a short break if viewing video when a failover server takes over from a recording server, or vice versa, because your views must be reloaded in your XProtect Smart Client.

- **Additional language packs:** Available if configured on the surveillance system.

- **Multicast stream support:** Available if configured on the surveillance system.

- **Map:** Available if configured on the surveillance system.

- **Smart Wall:** Available if installed and configured on the surveillance system.

Not Available

- **Default view:** Not available when connected to XProtect Corporate.

- **Event indicators on Live tab:** Not available when connected to XProtect Corporate.

- **Sound on event:** Not available when connected to XProtect Corporate.

- **Ability to manually start recording from Live tab:** Not available when connected to XProtect Corporate.

Surveillance system welcome pages, from which you can download the XProtect Smart Client, may look differently depending on the surveillance system version you connect to. Some versions provide extended features, such as the ability to view the welcome page in the language of your choice.

Connected to XProtect Enterprise Surveillance System

The following lists refer to the latest version of XProtect; features **not** mentioned are fully available and no special conditions apply.

Available

- **Login authentication methods:** Basic authentication as well as Windows authentication is available. Windows authentication can take place through Active Directory as well as through a local database on the surveillance system server.

- **Shared views:** Shared views are shared by all users. All shared views are always stored in a single top-level folder called **Shared**; the folder will be visible for all users. Users' ability to edit shared views is determined by their rights on the surveillance system.

- **Audio:** Two-way audio available. Only incoming audio (from microphones attached to cameras) is recorded and can be included when exporting evidence in the database format.

Available if Configured

- **Default view:** Available, provided surveillance system has at least one camera enabled.

- **Event indicators on Live tab:** Available, provided notifications on events have been configured on the surveillance system server.

- **Sound on event:** Available, provided notifications on events have been configured on the surveillance system server.

- **Ability to use Matrix content in views:** Available, provided Matrix has been configured on the surveillance system, and the user has a role with necessary Matrix rights.

- **Ability to send video to Matrix recipients through XProtect Smart Client shortcut menu:** Available, provided Matrix has been configured on the surveillance system.

- **Additional language packs:** Available if configured on the surveillance system.

- **Map:** Available if configured on the surveillance system.

- **Camera Navigator:** Available if configured on the surveillance system.

Not Available

- **Ability to connect to failover servers:** Not available when connected to XProtect Enterprise.

- **Bookmarks:** Not available when connected to XProtect Enterprise.

- **Options controllable from the surveillance system server (Follow Server):** Not available when connected to XProtect Enterprise.

- **Multicast stream support:** Not available when connected to XProtect Enterprise.

- **Smart Wall:** Not available when connected to XProtect Enterprise.

- **Milestone Federated Architecture :** Not supported by XProtect Enterprise.

Surveillance system welcome pages, from which you can download the XProtect Smart Client, may look differently depending on the surveillance system version you connect to. Some versions provide extended features, such as the ability to view the welcome page in the language of your choice.

Connected to XProtect Professional Surveillance System

The following lists refer to the latest version of XProtect; features **not** mentioned are fully available and no special conditions apply.

Available

- **Login authentication methods:** Basic authentication as well as Windows authentication is available, but Windows authentication can only take place against a local database on the surveillance system server, not against Active Directory.

- **Shared views:** Shared views are shared by all users. All shared views are always stored in a single top-level folder called **Shared**; the folder is visible to all users. Users' ability to edit shared views is determined by their rights on the surveillance system.

Available if Configured

- **Default view:** Available, provided surveillance system has at least one camera enabled.

- **Audio:** Two-way audio available. Only incoming audio (from microphones attached to cameras) is recorded and can be included when exporting evidence in the database format.

- **Event indicators on Live tab:** Available, provided notifications on events have been configured on the surveillance system server.

- **Sound on event:** Available, provided notifications on events have been configured on the surveillance system server.

- **Ability to use Matrix content in views:** Available, provided Matrix has been configured on the surveillance system, and the user has a role with necessary Matrix rights.

- Ability to send video to Matrix recipients through XProtect Smart Client shortcut menu: Available, provided Matrix has been configured on the surveillance system.

- **Additional language packs:** Available if configured on the surveillance system.

Not Available

- **Bookmarks:** Not available when connected to XProtect Professional.

- **Ability to connect to failover servers:** Not available when connected to XProtect Professional.

- **Options controllable from the surveillance system server (Follow Server):** Not available when connected to XProtect Professional.

- **Ability to connect to cameras from multiple surveillance system servers:** Not available when connected to XProtect Professional.

- **Multicast stream support:** Not available when connected to XProtect Professional.

- **Smart Wall:** Not available when connected to XProtect Professional.

- **Milestone Federated Architecture :** Not supported by XProtect Professional.

- **Map:** Not supported by XProtect Professional.

- **Camera Navigator:** Not supported by XProtect Professional.

Surveillance system welcome pages, from which you can download the XProtect Smart Client, may look differently depending on the surveillance system version you connect to. Some versions provide extended features, such as the ability to view the welcome page in the language of your choice.

Connected to XProtect Express Surveillance System

The following lists refer to the latest version of XProtect; features **not** mentioned are fully available and no special conditions apply.

Available

- **Login authentication methods:** Basic authentication as well as Windows authentication is available, but Windows authentication can only take place against a local database on the surveillance system server, not against Active Directory.

- **Shared views:** Shared views are shared by all users. All shared views are always stored in a single top-level folder called **Shared**; the folder will be visible for all users. Users' ability to edit shared views is determined by their rights on the surveillance system.

- **Audio:** One-way (incoming) audio available. Only incoming audio (from microphones attached to cameras) is recorded and can be included when exporting evidence in the database format.

Available if Configured

- **Default view:** Available, provided surveillance system has at least one camera enabled.

- **Event indicators on Live tab:** Available, provided notifications on events have been configured on the surveillance system server.

- **Sound on event:** Available, provided notifications on events have been configured on the surveillance system server.

- **Additional language packs:** Available if configured on the surveillance system.

Not Available

- **Ability to connect to cameras from multiple surveillance system servers:** Not available when connected to XProtect Express.

- **Options controllable from surveillance system server ("Follow Server"):** Not available when connected to XProtect Express.

- **Multiple windows:** Not available when connected to XProtect Express.

- **Bookmarks:** Not available when connected to XProtect Express.

- **Patrolling PTZ (Pan/Tilt/Zoom) cameras:** Not available when connected to XProtect Express.

- **Ability to use Matrix content in views:** Not available when connected to XProtect Express.

- **Ability to send video to Matrix recipients through XProtect Smart Client shortcut menu:** Not available when connected to XProtect Express.

- **Ability to connect to failover servers:** Not available when connected to XProtect Express.

- **Multicast stream support:** Not available when connected to XProtect Express.

- **Map:** Not available when connected to XProtect Express.

- **Camera Navigator:** Not available when connected to XProtect Express.

- **Smart Search on Playback tab:** Not available when connected to XProtect Express.

- **Alarm handling:** Not available when connected to XProtect Express.

- **Smart Wall:** Not available when connected to XProtect Express.

- **Milestone Federated Architecture :** Not supported by XProtect Express.

Surveillance system welcome pages, from which you can download the XProtect Smart Client, may look differently depending on the surveillance system version you connect to. Some versions provide extended features, such as the ability to view the welcome page in the language of your choice.

Connected to XProtect Essential Surveillance System

The following lists refer to the latest version of XProtect; features **not** mentioned are fully available and no special conditions apply.

Available

- **Login authentication methods:** Basic authentication as well as Windows authentication is available, but Windows authentication can only take place against a local database on the surveillance system server, not against Active Directory.

- **Shared views:** Shared views are shared by all users. All shared views are always stored in a single top-level folder called **Shared**; the folder will be visible for all users. Users' ability to edit shared views is determined by their rights on the surveillance system.

- **Audio:** One-way (incoming) audio available. Only incoming audio (from microphones attached to cameras) is recorded and can be included when exporting evidence in the database format.

Available if Configured

- **Default view:** Available, provided surveillance system has at least one camera enabled.

- **Event indicators on Live tab:** Available, provided notifications on events have been configured on the surveillance system server.

- **Sound on event:** Available, provided notifications on events have been configured on the surveillance system server.

- **Additional language packs:** Available if configured on the surveillance system.

Not Available

- **Ability to connect to cameras from multiple surveillance system servers:** Not available when connected to XProtect Essential.

- **Options controllable from the surveillance system server (Follow Server):** Not available when connected to XProtect Essential.

- **Multiple windows:** Not available when connected to XProtect Essential.

- **Bookmarks:** Not available when connected to XProtect Essential.

- **Patrolling PTZ (Pan/Tilt/Zoom) cameras:** Not available when connected to XProtect Essential.

- **Ability to use Matrix content in views:** Not available when connected to XProtect Essential.

- **Ability to send video to Matrix recipients through XProtect Smart Client shortcut menu:** Not available when connected to XProtect Essential.

- **Ability to connect to failover servers:** Not available when connected to XProtect Essential.

- **Multicast stream support:** Not available when connected to XProtect Essential.

- **Map:** Not available when connected to XProtect Essential.

- **Camera Navigator:** Not available when connected to XProtect Essential.

- **Smart Search on Playback tab:** Not available when connected to XProtect Essential.

- **Alarm handling:** Not available when connected to XProtect Essential.

- **Smart Wall:** Not available when connected to XProtect Essential.

- **Milestone Federated Architecture :** Not supported by XProtect Essential.

Surveillance system welcome pages, from which you can download the XProtect Smart Client, may look differently depending on the surveillance system version you connect to. Some versions provide extended features, such as the ability to view the welcome page in the language of your choice.

Connected to XProtect Go Surveillance System

The following lists refer to the latest version of XProtect; features **not** mentioned are fully available and no special conditions apply.

Available

- **Login authentication methods:** Basic authentication as well as Windows authentication is available, but Windows authentication can only take place against a local database on the surveillance system server, not against Active Directory.

- **Shared views:** Shared views are shared by all users. All shared views are always stored in a single top-level folder called **Shared**; the folder will be visible for all users. Users' ability to edit shared views is determined by their rights on the surveillance system.

Milestone XProtect® Smart Client 7.0

- **Audio:** One-way (incoming) audio available. Only incoming audio (from microphones attached to cameras) is recorded and can be included when exporting evidence in the database format.

Available if Configured

- **Default view:** Available, provided surveillance system has at least one camera enabled.

- **Event indicators on Live tab:** Available, provided notifications on events have been configured on the surveillance system server.

- **Sound on event:** Available, provided notifications on events have been configured on the surveillance system server.

- **Additional language packs:** Available if configured on the surveillance system.

Not Available

- **Options controllable from the surveillance system server (Follow Server):** Not available when connected to XProtect Go.

- **Ability to connect to cameras from multiple surveillance system servers:** Not available when connected to XProtect Go.

- **Multiple windows:** Not available when connected to XProtect Go.

- **Bookmarks:** Not available when connected to XProtect Go.

- **Patrolling PTZ (Pan/Tilt/Zoom) cameras:** Not available when connected to XProtect Go.

- **Export formats:** AVI only. Exported AVIs will prominently display manufacturer logo. JPEG and database export are not available when connected to XProtect Go.

- **Ability to use Matrix content in views:** Not available when connected to XProtect Go.

- **Ability to send video to Matrix recipients through XProtect Smart Client shortcut menu:** Not available when connected to XProtect Go.

- **Ability to connect to failover servers:** Not available when connected to XProtect Go.

- **Multicast stream support:** Not available when connected to XProtect Go.

- **Map:** Not available when connected to XProtect Go.

- **Camera Navigator:** Not available when connected to XProtect Go.

- **Smart Search on Playback tab:** Not available when connected to XProtect Go.

- **Alarm handling:** Not available when connected to XProtect Go.

- **Smart Wall:** Not available when connected to XProtect Go.

- **Milestone Federated Architecture :** Not supported by XProtect Go.

Defining your views

Views

About views

The way in which video is displayed in the XProtect Smart Client is called a view. A view can contain video from up to 100 cameras, depending on your surveillance system. Your XProtect Smart Client can handle an unlimited number of views, allowing you to switch between video from various groups of cameras. Each view's layout 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 (see "Private and shared views" on page 39).

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.

Your user settings, including information about your views, are stored centrally on the surveillance system server, so you can use your views, private as well as shared, on any computer that has a XProtect Smart Client installed, provided you log in with your own user name and password.

Example: XProtect Smart Client displaying a view with video from four different cameras (a 2x2 view)

Private and shared views

Views can be private or shared:

- **Private** views can only be accessed by the user who created them.

- **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 32), 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 surveillance system administrator may create and maintain a number of shared views, so users do not need to create their own views.

Create and manage views

Certain user rights are required in order to create 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. Consult your surveillance system administrator if in doubt.

To create a view, you must first have a group to add it to. You can either create a new view in an existing group or create a new group for the view. To create a view under a shared top-level folder, you must first create a group within this shared folder.

Tip: A group can contain an unlimited number of views. You can also create any number of subgroups if required.

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 a view

Not all users may have access to all cameras on the surveillance system and some of the features you include in your shared view may not be supported in earlier versions of the XProtect Smart Client. Therefore, 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.

1. In setup mode, in the **Views** pane, select the group in which you want to create the view.

2. Click the **Create New View** button:

3. Select a layout for your new view. You can select layouts for displaying up to 100 (10×10) cameras in a single view. Available layouts are grouped according to their aspect ratio (height/width relationship: 4:3 or 16:9), and according to whether they are optimized for regular content or content in portrait mode (where the height is greater than the width).

1	1 x 1
	1 + 1
	1 + 1*
	1 x 2
	1 + 2
	1 + 2*
	1 + 1 + 2
4	2 x 2
	4 x 1
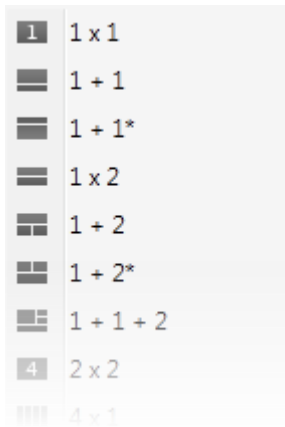
4. Enter a name for the view by overwriting the default **New View** name.

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" on page 26).

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.

Copy, rename, or delete a view or group

Important: 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.

   Tip: 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 rename it, 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**.

Important: Deleting a group will delete all views and any subgroups within the group as well.
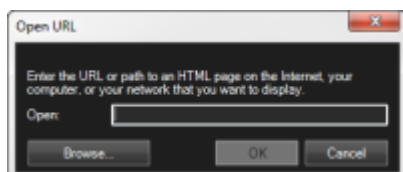
Add content to views

Add an HTML page to a view

HTML Pages can be used in views for a variety of purposes: company web pages, internet map services, collection of links, e-learning pages, and so on.

Example: A company web page inserted in a view

1. In setup mode, in the **System Overview** pane, click and drag the **HTML Page** item to the view.

2. The **Open URL** window opens.

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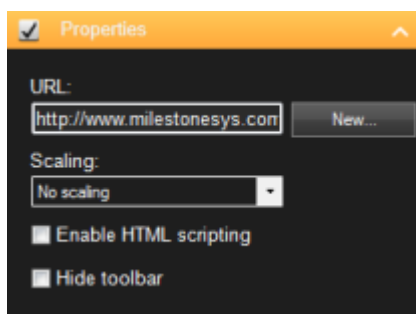
    - or -

    If the HTML page is stored locally on your computer, specify its location on your computer (example: C:\myfiles\mywebpage.htm), or click **Browse...** to browse for the required HTML page.

4. Click **OK**.

Once an HTML page is added to a view, you can change its properties:

1. In setup mode, select the imported HTML page in the view. In the **Properties** pane, change the necessary properties.

    o   **URL:** Click **New** to specify a new URL or location of the HTML page.

    o   **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, e.g. 1280×1024, text on the HTML page will appear relatively small, and a considerable amount of content will be visible without the need for scrolling. With a low scaling value, e.g. 320×200, text on the HTML page will appear relatively large, and a relatively small amount of content can be displayed without the need for scrolling.

    o   **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 Use an HTML Page for Navigation (on page 27)).

        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.

    o   **Hide toolbar:** By default, a simple navigation bar is inserted above each imported HTML page. The navigation bar has four buttons; from left to right the buttons are **Back**, **Forward**, **Refresh** and **Home**:

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

When an imported HTML page contains links, we recommend that the links have the `target='blank'` attribute (example: `<a href=" otherwebpage.htm" target="blank">Link</a>`). This makes the links open in separate windows, which will help you avoid losing view of the XProtect Smart Client window when a link opens a web page in the same browser as the XProtect Smart Client .

Add a static image to a view

Static images can be used in views for company logos, for including photos of wanted persons, and so on.

- In setup mode, in the **System Overview** pane, drag the **Image** link to the required position in the view and select the static image file.

When you add an image to a view, the proportions of the image are not kept. If you want to ensure that the image is displayed without distortion, in the **Properties** pane for images, select the **Maintain image aspect ratio** check box.

Tip: If you include floor plans or maps in a view, consider the Map feature (see "Maps" on page 57). The Map feature is available when connected to certain surveillance systems (see "Surveillance system differences" on page 32) only.

Add on 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.

Tip: In addition to activating speakers, events, etc., you can also use overlay buttons for activating many camera features, such as focus, iris, auxiliary commands, which you were in previous XProtect Smart Client versions only able to activate through custom keyboard shortcuts.

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. If you want 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 press ENTER. The text scales to the largest possible size on the button.

Send video between views

You can send video from a selected camera position to another single-camera position in an open view, including any views you may have open in floating windows or on secondary displays. This feature is not available for hotspots (on page 73), carousels (on page 72), or Matrix (on page 77) positions.

Send video between views

- On the camera toolbar, click **More > Send Camera**, 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.

You can also send video content to separate windows (see "Multiple windows" on page 74) or displays.

Switch cameras in views

You can temporarily change the cameras that are displayed in a view. However, this feature is for provisionally switching cameras; it does not permanently change the view. If you want to permanently change the content of a view (see "Add a camera to a view" on page 46), you must be in setup mode.

You cannot switch cameras if the view contains a hotspot (see "Hotspots" on page 73), carousel (see "Carousels" on page 72), or Matrix (on page 77) content. If used from the **Cameras** pane, the feature works with Smart Wall (on page 78) positions as well.

Switch a camera in a view temporarily

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 32)—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 (see "The XProtect Smart Client window" on page 24) video, overlay buttons are not included in the export.

Cameras

Some of the following features are only available in certain surveillance systems (see "Surveillance system differences" on page 32).

Add a camera to a view

Add a camera to a view

1.   In setup mode, select the view you want to add a camera to.

2.   In the **Overview** pane, expand **Cameras**, then 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 will—provided a connection can be established—appear in the selected position. If a connection cannot be established, just the camera name will be displayed.

   Tip: If parts of images are black, it is because privacy masks (on page 99) are in use.

You can specify the camera properties (such as quality, frame rate, etc.) in the **Properties** pane (see "The Properties pane" on page 49).

Repeat for each camera required in the view.

Tip: If you want to add multiple cameras to a view in one go (for example all of the cameras from a camera folder under a server), simply drag the folder to the view. This automatically adds all the folder's cameras in the view from the selected position onwards. Make sure a sufficient number of positions are available in the view.

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

Camera names and colored indicators

If configured (in setup mode, in the Properties pane (see "The Properties pane" on page 49)), the camera title bar displays the name of the camera. When video is displayed from the **Playback** tab, the bar shows the date and time of the displayed video. When you select a camera in a view, the camera title bar changes color.

The camera title bar displays **Live** when live video is displayed, **Recording** if video from the camera in question is being recorded, and **Stopped** if there is no camera feed and live viewing is not possible. 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. If all cameras display **Stopped**, connection to the surveillance system server may be lost.

Each title bar displays up to three colored indicators:

The title bar and indicators can be configured (see "Application options" on page 84) in the **Options** window.

- **Event indicator** (the yellow indicator   ): Lights up when specific events occur—defined by the surveillance system administrator. Click inside the image to reset the event indicator. The indicator may appear black if event indication has not been specified for the camera, or if no specified events have occurred.

  Note: This feature is only available in certain surveillance systems (see "Surveillance system differences" on page 32) and requires that notifications on events have been configured on the server.

- **Motion indicator** (the red indicator ▪): Lights up when motion is detected. Click inside the image to reset the motion indicator. This indicator may appear black if no motion has been detected.

- **Video indicator** (the flashing green indicator ▪): Changes every time a new image is received from the camera. This indicator can be turned off.

Tip: Event (▪) and motion (▪) indications can be accompanied by sound notifications (see "Handling sound notifications" on page 53).

Virtual joystick and PTZ overlay button

If your views include 360° cameras or lenses, or PTZ devices (see "PTZ and 360º lens images" on page 95), 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.
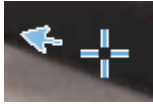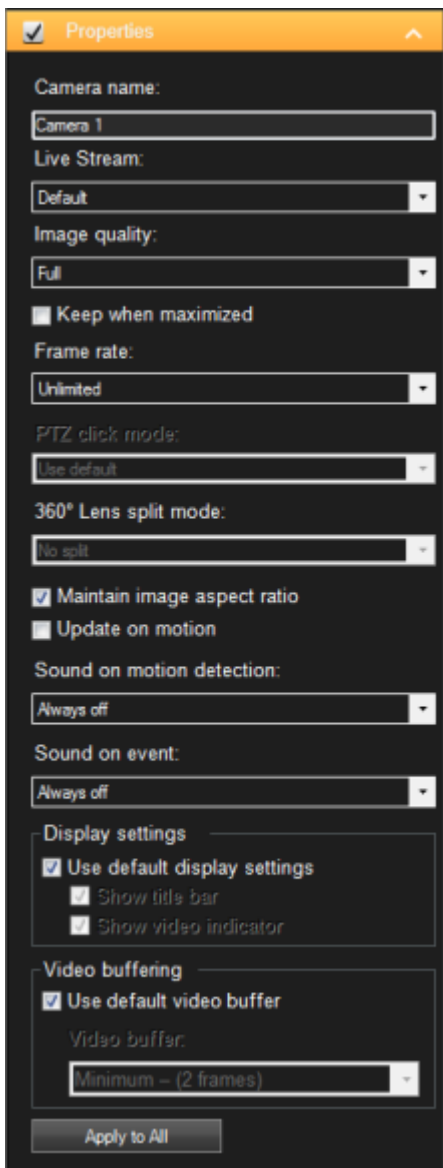

The virtual joystick

PTZ overlay

Tip: 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.

The Properties pane

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

Settings

Name	Description
Camera name	Displays the name of the selected camera. The field is read-only.
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.
	Tip: You can quickly reduce the bandwidth usage for all cameras in the view by reducing the image quality for a single camera, then clicking the **Apply To All** button.
Keep when maximized	When you view live or recorded video, you can double-click a particular 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 affects the quality of your video.

Name	Description
360° Lens split mode	Available only if the selected camera is a 360° lens camera. 360° lens technology allows the creation and viewing of 360° panoramic images. The XProtect Smart Client supports up to four different viewpoints from a single 360° lens camera. The **360° lens 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 (not available on all 360° lens cameras). When viewed on any of the XProtect Smart Client's tabs, the 360° lens camera will appear as specified, with either one or four viewpoints from the same image. **Tip:** When viewing different viewpoints from a 360° lens camera on the **Live** or **Playback** tabs, you can navigate each viewpoint independently by clicking inside each viewpoint, or by using the **More** menu on the 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.
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.

Name	Description
Sound on event	This feature is only available with certain surveillance systems; see Surveillance System Differences (on page 32).
	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.
Display settings	**Use default display settings:** Use default settings, as defined in the **Options** dialog, 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 (on page 47).
	Note: 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 video indicator: Requires that **Show title bar** is selected. Displays a flashing green ■ indicator in the title bar when displayed on the **Live** tab. The indicator changes state every time a new image is received from the camera, an effect which makes it easy to see that video is live. Often, it is evident from the video itself that it is live, but the video indicator can be advantageous at times when not much is happening in the camera's area of view.

Name	Description
Video buffering	This part of the **Properties** pane may not be visible. To view it, go to the **Options** window's (see "XProtect Smart Client options" on page 83) **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 PTZ (Pan/Tilt/Zoom) 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 2 frames to 2 seconds.
Apply to All	The **Apply to All** button lets you quickly apply the camera settings for the selected camera to all cameras in the view.

Keyboard shortcuts and overlay buttons

Depending on your surveillance system (see "Surveillance system differences" on page 32), you can assign custom keyboard shortcuts (see "XProtect Smart Client options" on page 83) and overlay buttons (see "Views" on page 39) to trigger auxiliary commands (commands defined by the camera) to the camera positions in the view. Auxiliary commands differ from camera to camera; for details, see the documentation for the camera.

Handling sound notifications

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

  - and/or -

- events (on page 119) 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 (on page 73), carousels (on page 72), or Matrix (on page 77) 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 can be perceived by the viewer 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\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.

Audio

Support for specific audio features may vary from system to system (see "Surveillance system differences" on page 32). 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.

About audio

The XProtect Smart Client supports both incoming and outgoing audio. You can listen to live recordings from microphones attached to cameras as well as 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 and/or speakers attached. When you select a camera or view, the corresponding microphone and/or speaker is also selected by default.

Tip: If your views contain maps, these maps may contain microphones and/or speakers. When this is the case, 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.

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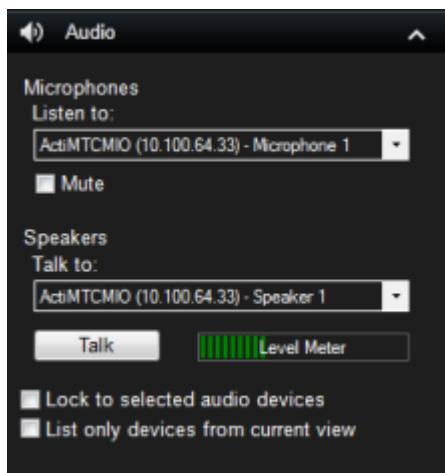
Tip: You can listen to recorded audio independently of the views/cameras you are watching. You must specify a time in the **Playback** tab's navigation feature to determine what recorded audio to hear.

Audio settings

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.

Name	Description
Lock to selected audio devices	When you select a camera or view, the corresponding microphone and/or speaker is also selected by default. However, if you want audio for a specific camera regardless of the ones you are viewing, you can select **Lock to selected audio devices**. **Example**: You need to listen and talk to a crime victim through microphones and speakers attached to camera A, but you also urgently need to view cameras X, Y and Z, some of which are displayed in different positions in the view. By selecting **Lock to selected audio devices**, you can communicate with the victim on camera A while viewing the other cameras at the same time.
List only devices from current view	If your surveillance system contains large numbers of microphones and/or speakers, the lists from which you select microphones and speakers in the Audio pane can be very long. To avoid this, you can limit the lists to only contain microphones and speakers relevant to your current view by selecting **List only devices from current view**. Note that in this context, **current view** also includes any views you have open as floating views and on primary and secondary displays (see "Multiple windows" on page 74).

Talking to an audience

IMPORTANT: 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 32).

There are three ways of talking to audiences through speakers attached to cameras, either by using the **Audio** pane, by using overlay buttons, or by using speaker functionality on maps.

Talk through speakers

1. On the Live tab, in the Audio pane, under Speakers, select the relevant speakers from the Talk to: list. See Audio settings (see "The Audio pane" on page 55) for specific information about speaker settings.

    Tip: If your surveillance system has speakers attached to multiple cameras (and you have the necessary rights), you can talk through all the speakers simultaneously by selecting All speakers.

    Alternatively, if a position in a view has an overlay button or a map with speaker elements, you can click these.

2. Click and hold down the Talk button while you talk. Keeping the button depressed when you speak gives you full control over what is actually transmitted through the speakers.

Frequently asked questions: audio

Why is the Speakers list not available?

Some surveillance systems do not support two-way audio; see Surveillance system differences (on page 32).

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; see Surveillance system differences (on page 32).

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.

Maps

Introduction to maps

The map feature is only available for selected surveillance systems (see "Surveillance system differences" on page 32). A map position does not display live video, a map is always a still image.

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 typically contain elements representing cameras, microphones, and so on. You can view recorded video from cameras in a preview window when you move your mouse over a camera icon on the map. Also note that status information in playback mode is **not** based on recorded data, but retrieved from the elements' current status, as displayed in live mode.
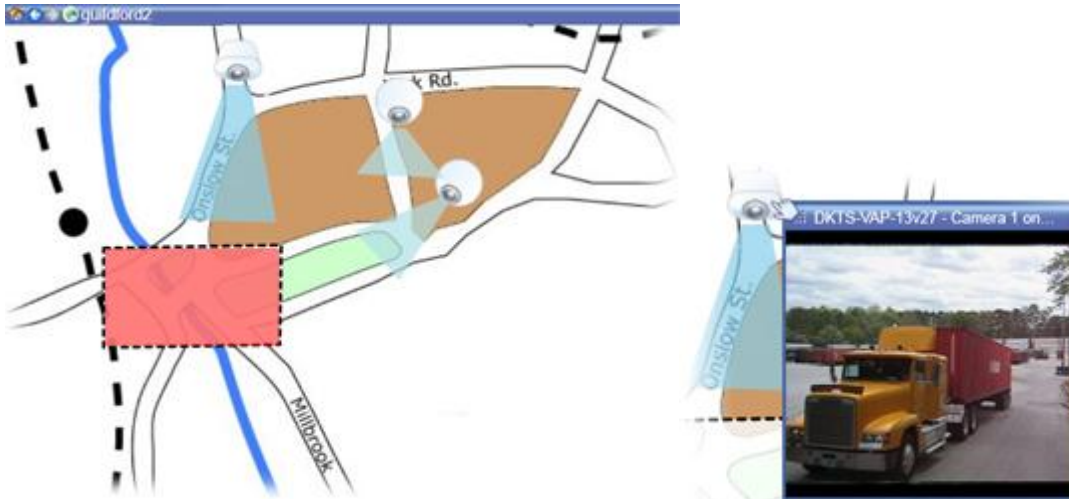
Map with camera elements and hot zone

Tip: 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.

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" on page 73). 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" on page 116) 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" on page 116) 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.
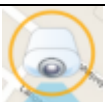
A hot zone can point to a map that you do not have access rights to and the XProtect Smart Client will inform you about this. Because user rights can be time-based, you might not be able to access a map that you could previously. This can be because you do not have access during certain hours of the 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.

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.

	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 display color is always purple and cannot be changed.
	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

1. In setup mode, select the map. Right-click the map and select **Status Visualization**.
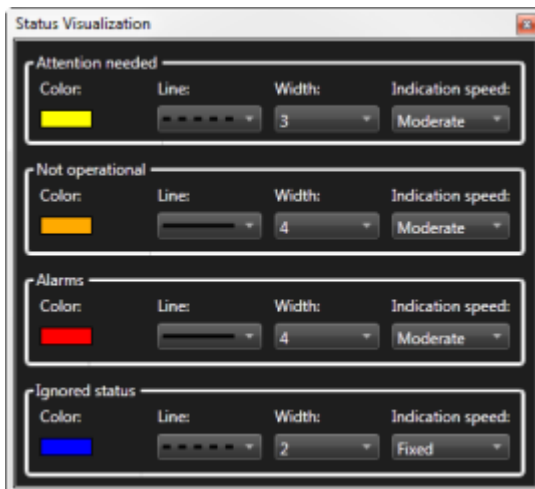
2. In the **Status Visualization** window, click the **Color** box to launch the **Color Selection** tool, and select a color for the status visualization line, then click the **Color** box again to fill the **Color** box with the selected color.

3. Select a line format from the **Line** list.

4. Select line thickness from the **Width** list.

5. To define how fast the status visualization flashes, select a speed from the **Indication Speed** list.

6. In the **Properties** pane, select **Status Visualization** to enable showing status visualization in live mode.

Tip: The status visualization applies to all maps, you do not need to define the status visualization appearance for each individual map.

Your status visualization settings may take some time to load and display correctly if you connect to a very large surveillance system with many maps. On complex systems, it can take 30 seconds or longer to correctly update status visualization.

Map settings

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

Map settings

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.
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. **Tip:** 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" on page 47), 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 "Status visualization" on page 59) 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.

The toolbox

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

	Camera	Selecting either **Camera**, **Server**, **Microphone**, **Speaker**, **Event** or **Output** opens the **Element Selector** with a list of cameras, servers, microphones, speakers, events, or output, allowing you to place these elements on the map.
	Server	
	Microphone	
	Speaker	
	Event	
	Output	
	Hot Zone	Activates the hot zone drawing tool, allowing you to place hot zones on the map.
	Text	Opens the text tool, allowing you to place editable text boxes on the map.
	Plug-in	Opens the **Element Selector** with a list of plug-ins (if used in your organization), allowing you to place a plug-in element on the map.
	Color Picker	Opens the color selection tool, and activates the color picker, allowing you to use a color already existing on the map.
	Color Fill	Opens the color selection tool, allowing you to change the color of texts, backgrounds, hot zones, etc.
	Selector	Activates the selector tool, allowing you to select elements on the map and pan and zoom the map.
	Map Overview	Opens the **Map Overview**, allowing you to navigate between different maps.

The right-click menu

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

The right-click commands

The content of the shortcut menu differs depending on which map element you right-click. Different features are available from shortcut menus when maps are viewed in setup mode.

- **Remove [...]:** Lets you remove the selected element or map.

- **Center Map Here:** Centers the map around the clicked position

- **Zoom In**

- **Zoom Out**

- **Zoom to Standard Size:** Zooms the map to the standard size it was set up with

- **Home:** Lets you quickly jump to your home map

- **Back:** Lets you quickly return to the previous map

- **Forward:** Lets you quickly go to a map you have viewed earlier in this session

- **(From a PTZ camera preset) Go to Preset [preset]:** Lets you direct the camera to an predefined preset.

- **(From a camera) Live Preview:** Lets you see a live preview from the selected camera.

- **(From a camera) View Zone:** Lets you toggle on and off a fixed camera's view zone that shows the camera's angle of view.

The shortcut menu that appears when you right-click the map also displays other features, such as **Home Map Setup**, **Toolbox**, **Map Overview**, **Element Selector**, **Font Selection**, **Color Selection**, and **Status Visualization**.

Shortcut menus for individual elements (see "How elements interact with maps" on page 58) may have other content.

In addition to the common right-click menu items, the right-click menus of events and output also feature **Select Icon Type,** which lets you select whether the event icon or output should be displayed as a lamp, a door, a gate or a switch. Changing the event/output icon to something more adequate to the actual event/output helps end users more quickly get an overview of the actual contents of the map.

To display status details, right-click the required element and select **Status Details**. **S**tatus details are displayed in a separate, floating window.

The Map Overview window

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.

Note that content in the **Map Overview** may take some time to load if you are connected to a very large surveillance system with many maps.

Working with maps

If you are connected to a surveillance system that supports Milestone Federated Architecture, note that you can only add maps from the surveillance system server you logged in to. 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. See Surveillance System Differences (on page 32) for information about which surveillance systems support Milestone Federated Architecture.

- Add a map to a view (on page 65)

- Change background of a map (on page 65)

- Remove the map (on page 65)

- View status details (on page 69)

- Zoom and auto maximize (on page 69)

Working with elements on a map:

- Add or remove an element (on page 65)

- Add a hot zone to a map (on page 66)

- Change the appearance of map elements (on page 67)

- Add/edit text on a map (on page 68)

Add a map to a view

You can add existing maps or create new ones.

1. In setup mode, in the **System Overview** pane, drag the **Map** item to the required position in the view.

2. 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 could have one or more sub-maps and all related sub-map(s) with all added elements will automatically be included.

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

   Tip: If you leave the **Name** field blank and click **Browse...**, the **Name** field will automatically be filled out with the image file name when you select an image file.

4. Click **Browse...** to browse for the image file to be used as a map.

5. Click **Open** to select image file.

6. Click **OK**.

Change 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 or remove an element

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.

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

Removing elements

To remove an element, right-click the unwanted element (camera, hot zone, server, event, output, microphone, or speaker) and select Remove [element].

Move elements

To move an element, click and drag it to a new position on the map.

Rotate elements

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.

Tip: 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 "The toolbox" on page 62).**

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.

   Tip: 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 32), for technical and performance reasons, a maximum of 20 hot zones on a single map can point to maps from other surveillance system servers than the one to which you are logged in. There is no such limit for hot zones pointing to maps belonging on the server to which you are logged in. 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.

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 s**etup** 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.

   Tip: 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.
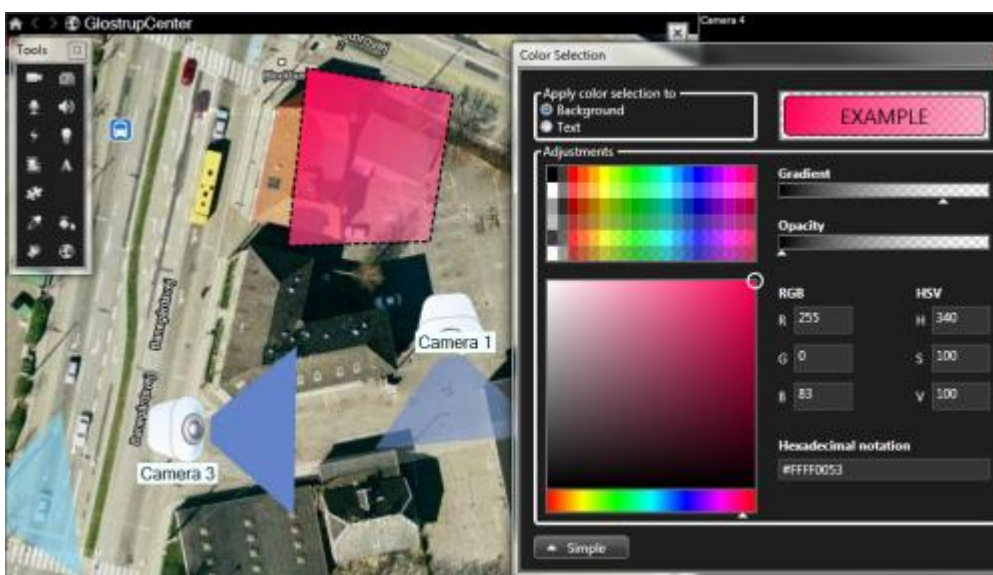
Adjusting Opacity

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.

Use the color slider to select the main color shade, then drag the color circle to select the required tone.

- or -

Type the hexadecimal color code in the **Hexadecimal notation** field.

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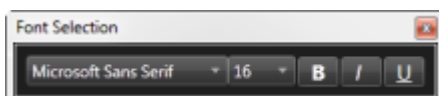
Tip: You can always edit your text settings; click the required text box and select the text tool from the toolbox, then change the text settings for the selected text box.

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.

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

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

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**. **S**tatus 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.

Tip: 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.
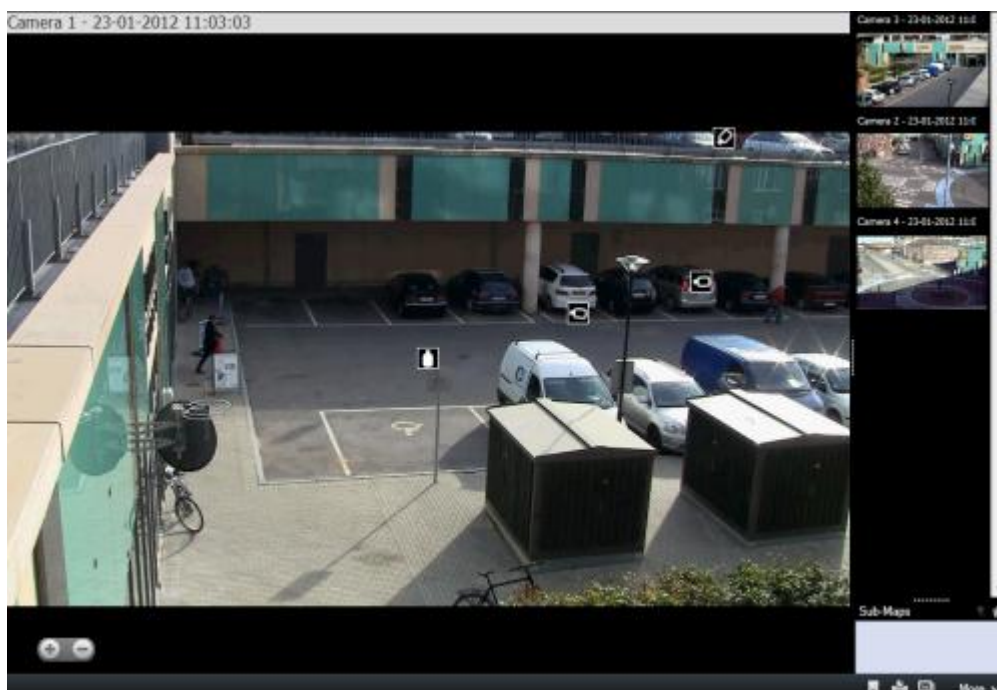
The Camera Navigator

This feature is only available for selected surveillance systems; see Surveillance System Differences (on page 32).

About the camera navigator

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.

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.

Camera navigator settings

In the **Properties (see "The Properties pane" on page 49)** 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.
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. Note that the more cameras that you preview, the more of your system resources they will take up.

Using the camera navigator

Before you can use the camera navigator, you must set up a map (see "Add a map to a view" on page 65) and add cameras to it. When you have added the camera navigator to a view, you can define properties (see "Camera navigator settings" on page 71) for how you want the camera navigator to display the views.

Add the camera navigator to a view

1. In setup mode, set up a new view.

    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. In the **System Overview** pane, select and drag the **Camera Navigator** onto your view.

3. In the **Select Home Map and Camera** window that appears, 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**.

Carousels

About carousels

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 a thin green border.

360° lens cameras cannot be included in a carousel.

Thin green border indicates 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.

Place your mouse over the carousel toolbar to access the carousel buttons that let you copy the current carousel image to your clipboard, pause the carousel, or change the carousel's rotation direction.

Example: A carousel has been configured to display camera A, then camera B, then camera C, and so on. By changing the direction, you can make the carousel display camera C, then camera B, then camera A, and so on.

Add a carousel to a view

Add a carousel to a view

1. In setup mode, in the **System Overview** pane, click and drag the **Carousel** item to the position in the view.

2. In the **Carousel Setup** window, on the left, click to expand the servers and then click to select the camera you want to include in the carousel. Click Add. Repeat for each camera you want to include in the carousel.

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

3. To determine the sequence the cameras appear in the carousel, in the **Selected cameras** list, select the camera and move up or down .

4. Enter the number of seconds each camera appears in the carousel, either with a common default or individually for each camera.

5. Click **OK** to close the **Carousel Setup** window.

    If you want to adjust your carousel settings, click **Setup**, and in the **Properties** pane on the left, click **Carousel Setup** to open the **Carousel Setup** window and make the necessary changes to your settings.

Carousel properties

In the **Properties** (see "**The Properties pane**" on page 49) 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.

Hotspots

About hotspots

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.

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

*   It is surrounded by a thin orange border

Thin orange border indicates hotspot

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**.

Add a hotspot to a view

Add a hotspot to a view

1. In setup mode, in the **System Overview** pane, click and drag the **Hotspot** item to the required position in the view.

   Tip: Note that the position now displays a thin orange border to indicate that it is a hotspot.
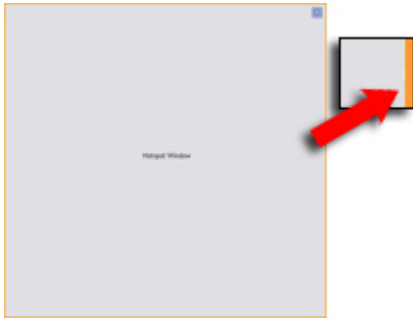
2. Specify the properties for the hotspot (see "Hotspot properties" on page 74) in the **Properties** pane. To save bandwidth, you can specify a low image quality for the other positions in your view and a high quality for the hotspot.

Hotspot properties

In the **Properties** (see "**The Properties pane**" on page 49) 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.

Multiple windows

This feature is only available for selected surveillance systems (see "Surveillance system differences" on page 32).

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.

You can send a 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. The separate full-screen window will only show the selected view, none of the **Live** or **Playback** tab's other features, and it can only show one view at a time.

- A secondary display to show the view in a full-screen window on another physical display (if available). The other physical display will only show the selected view, none of the **Live** or **Playback** tab's other features, and it can only show one view at a time.

- A floating window to show the view in a small separate window on your main display. The floating window will only show the selected view, none of the **Live** or **Playback** tab's other features. A floating window can only show one view at a time, but you can use any number of floating windows. You are able to change the size of a floating window to suit your needs.

You can also send a camera to a floating window. You can only display one camera at a time in a floating window, but you can use any number of floating windows, and you can change the size of each window.

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.

Primary display

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

Secondary display

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

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

Use multiple windows

Send a view between displays

1. In the **Views** pane, right-click the relevant view (or in the **Cameras** pane, the camera in the view).

2. Click **Send View To** and then select where you want your view to display.
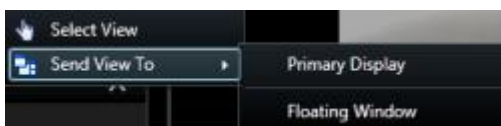
If more secondary displays are available, they will be numbered.

3. To close a separate view window, click the **Close** button in the right corner of the window:

If a view is sent to Primary Display or a Secondary Display the title bar is hidden. To display the title bar and get access to the Close button, move your mouse to the top of the view.

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: 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 properties (on page 73).

Matrix

The ability to add Matrix content to views is only available when connecting to selected surveillance systems (see "Surveillance system differences" on page 32). Matrix is only available if Matrix has been configured on your surveillance system, and you have the required user rights.

About Matrix

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.

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 the 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.

View Matrix content

A Matrix position has a thin blue border. You can maximize a Matrix by double-clicking it.

Thin blue border indicates Matrix

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, etc. You can change this ranking in setup mode (see "Matrix properties" on page 78), see Matrix settings.

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, of course, play back this video using the **Playback** tab's various navigation features.

Matrix properties

In setup mode, in the **Properties** (see "**The Properties pane**" on page 49) pane, you can specify the settings for Matrix positions.

Matrix settings

Add Matrix to a view

Add Matrix content to a view

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 (see "Matrix properties" on page 78).

    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.

Send video to a Matrix recipient

You cannot send video to a hotspot (see "Hotspots" on page 73) or carousel (see "Carousels" on page 72).

Manually send video to a Matrix recipient

1. Select the view.

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

Smart Wall

Smart Wall introduction

This is an add-on product. It is only available for selected surveillance systems (see "Surveillance system differences" on page 32). Your user rights may restrict your access to certain features.

A Smart Wall lets you easily manage collections of wall-mounted monitors (monitor walls or video walls), often used by command centers, city surveillance operators, traffic control centers, and so on. A Smart Wall on a shared monitor provides an excellent overview. You can quickly share important video from your view to your organization's Smart Wall by dragging your entire view (or a camera from a map) directly onto the Smart Wall display.

Example of a Smart Wall setup

Events defined on the server can also trigger that one or more cameras are shown on the Smart Wall. For example, if a door is opened, the Smart Wall can be configured to display the nearest cameras. You do not need to set up or configure a Smart Wall, it is available from the **Live** and **Playback** tabs (depending on your user rights).

View Smart Wall content

You can view Smart Wall content on all the **Live** and **Playback** tabs. However, the Smart Wall monitor only displays live video even if you are viewing recorded video in your XProtect Smart Client. Similarly, if you drag XProtect Smart Client views or cameras from maps onto a graphical representation of a Smart Wall, the actual Smart Wall monitors will also only display live video and not recorded video.

In the **Views** pane, expand **Smart Walls**, expand the required Smart Wall folder, then select the relevant monitor.

User rights may in some cases prevent one or more cameras from being displayed on Smart Walls or in your XProtect Smart Client.

Tip: If your organization uses Smart Wall, your XProtect Smart Client views may contain positions in the view with graphical representations of Smart Walls. Such positions have a number of advantages, such as the ability quickly to display important video on your organization's Smart Walls by dragging entire XProtect Smart Client views, or single cameras from maps, directly onto the graphical representations of Smart Walls.

Add Smart Wall content to views

In setup mode, you can add Smart Wall content to your views.

Add a Smart Wall to a view

1. Select a new or existing view. Wide layouts are especially suitable for displaying Smart Wall content.

Tip: The bottom of the 1+1+2 view ⊞ provides a wide position ideal for displaying Smart Wall content. The 1×3 view ☰ is capable of graphically representing three different Smart Walls at the same time.

2. In the **System Overview** pane, drag the **Smart Wall** link to the relevant position in the view.

3. The position in the view now contains a graphical representation of the Smart Wall.

   If your organization has more than one Smart Wall, select the relevant Smart Wall from the Smart Wall menu that appears at the top of the graphical representation.

   If the relevant Smart Wall has several presets (predefined settings determining which cameras are displayed as well as how content is structured on each monitor in the Smart Wall), select the relevant preset in the **Presets** menu:

   The Smart Wall and **Preset** menus will also appear on the **Live** and **Playback** tabs, so users can subsequently select different Smart Walls and/or presets if required.

   If the **Preset** menu is blank after your have made a selection, your selection is applied, but the preset may have been changed manually by other users or automatically by predefined rules on the surveillance system.

Drag cameras onto a Smart Wall

You can quickly display relevant cameras on your Smart Walls by dragging (click and hold down the mouse button) the camera from the **Live** tab's **Cameras** pane directly onto a monitor in the graphical representation of a Smart Wall.

If your organization uses the Map feature, you can display relevant cameras on your organizations' Smart Walls by dragging the cameras from the map onto the graphical representation of the Smart Wall. You can also drag cameras from maps in other views, such as floating views or views on secondary displays.
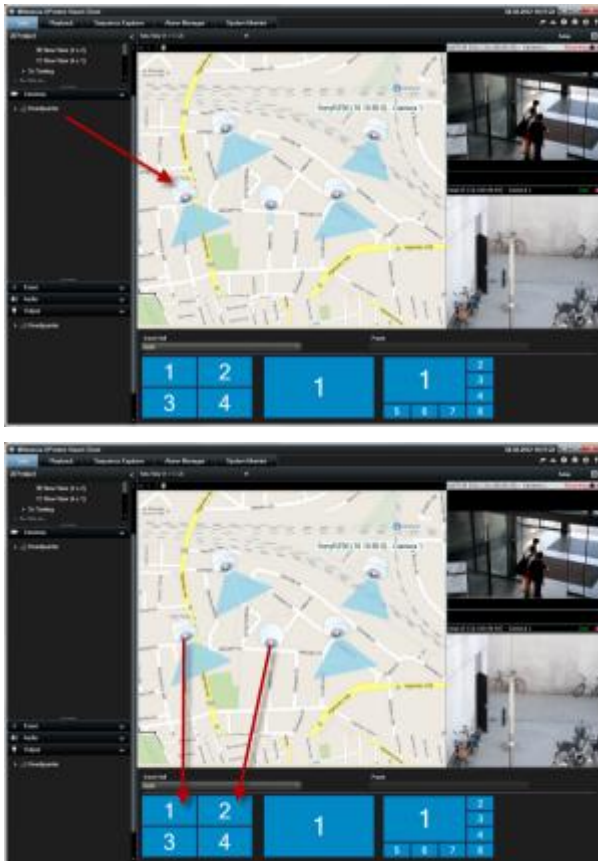
In the **Cameras** pane, the list of cameras is grouped by server . If a server is listed with a red icon it is unavailable, in which case you will not be able to select cameras from that server.

Send Video from a view to a Smart Wall

On the camera toolbar, click **More** > **Send to Smart Wall**, select the Smart Wall, select the monitor, and then select the position on the monitor.
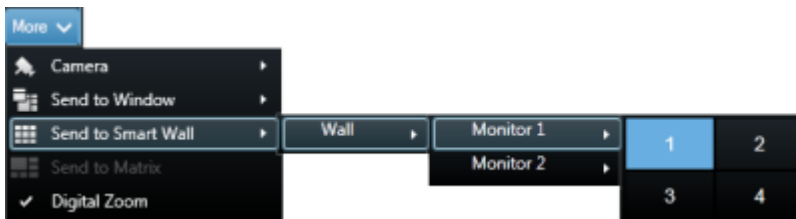
Send video from a Smart Wall to a view

Just as you can send video between views in the XProtect Smart Client (see "Send video between views" on page 44), you can also send video from individual monitors in a Smart Wall to views in your XProtect Smart Client.

In the graphical representation of the Smart Wall, right-click the relevant monitor, select **Send View To**, and then select the destination (**Primary Display, Secondary Display**, or **Floating Window**).
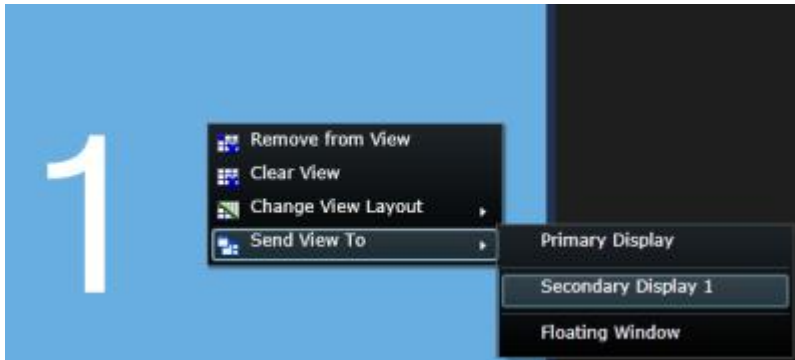
Change the layout of a Smart Wall monitor

There are several ways of changing the content and layout of monitors in a Smart Wall:

- You can send a camera from an existing XProtect Smart Client view, private as well as shared, to a Smart Wall. Right-click the camera in the view, select **Send to Smart Wall**, the Smart Wall, the monitor, and then the relevant position in the view.

- You can quickly display an existing view (private or shared) from your XProtect Smart Client on a monitor on a Smart Wall by dragging the view from the **Views** pane directly onto the monitor in the graphical representation of the Smart Wall.

- In the graphical representation of the Smart Wall, right-click the required monitor, select **Change View Layout**, select the display format (4:3 or 16.9), and then select the view layout.

- Select a different preset for the Smart Wall (note that this may affect all monitors in the Smart Wall).

Remove content from a Smart Wall

You can quickly remove video (the entire monitor content or individual positions in a view) displayed on Smart Wall monitors, for example, video containing sensitive information from the Smart Wall.

Remove the entire content of monitor

In the graphical representation of the Smart Wall, right-click the monitor and select **Clear View**. This will remove all video from the monitor while keeping the monitor's layout.

Remove video from a position in a view

In the graphical representation of the Smart Wall, right-click the position on the monitor and select **Remove from View**. This will remove video from the position in the view while keeping the monitor's other video content and layout.

What is displayed on a Smart Wall can be changed manually by other users or automatically by predefined rules on the surveillance system. Therefore, even though you can manually remove content from the Smart Wall, the content may reappear on the Smart Wall later. Contact your surveillance server administrator if certain content should be prevented from appearing on Smart Walls.

XProtect Smart Client options

The **Options** 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 XProtect Smart Client tabs.

Open the **Options** window by clicking the **Options** button in the application bar:

Application options

Application options 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 server's recommended settings. 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 "View in full screen" on page 23).
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 flashing green video indicator on the camera title bar. The indicator changes state every time a new image is received from the camera, which makes it easy to see that video is live. You can override this setting on individual cameras by adjusting camera properties (see "The Properties pane" on page 49) for the camera(s) in setup mode.
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" on page 47) signifying events, detected motion, and video. You can override this setting on individual cameras by adjusting camera properties (see "The Properties pane" on page 49) 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.

Name	Description
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 "The Properties pane" on page 49) 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 "The Properties pane" on page 49) for the camera(s) in setup mode.
Default PTZ click mode	Select a default PTZ click mode for your PTZ cameras. Options are click-to-center or virtual joystick.
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.

Panes options

The **Panes** options 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 32) 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 server's recommended settings. Certain settings may already be server-controlled, in which case configuration on the server decides whether you can override the settings.

Functions options

The **Functions** options 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 server's recommended settings. 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 signals from cameras, etc.
Live & Playback > Print	The ability to print from the **Live** and **Playback** tab. Note that enabling/disabling this option on the **Playback** tab will control whether or not the corresponding button is enabled on the **Sequence Explorer** tab.
Live & Playback > Bookmark overlay button & view position toolbar	Select whether you want to add quick or detailed bookmarks (on page 97) from the view position toolbar or through ready-made overlay buttons on the **Live** and/or the **Playback** tab. Note that enabling/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 32). Depending on your user rights, access to adding bookmarks from some cameras may be restricted. Note that you may be able to view bookmarks even though you may not be able to add them, and vice versa.
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).
Setup > Edit overlay buttons	The ability to add new or edit existing overlay buttons in setup mode. Note that in order to add overlay buttons, the **Setup** tab's **Overlay Buttons** pane must also be made available (you manage this on the **Options** dialog's **Panes** tab).
Setup > Edit video buffering	The ability to edit video buffering as part of the camera properties (see "Cameras" on page 46) in setup mode. Note that in order to edit video buffering, the **Setup** tab's **Properties** pane must also be made available (you manage this on the **Options** dialog's **Panes** tab).

Timeline options

The Timeline options 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 server's recommended settings. 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.
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 options

The Export options let you specify general export settings.

If available, the Follow Server column lets you specify that you want your XProtect Smart Client to follow the server's recommended settings. 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.
Privacy mask	Select whether or not privacy masks are available on export.
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.
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.

Joystick options

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 PTZ (Pan/Tilt/Zoom) configuration for the joystick is added automatically. However, the Joystick options let you customize the setup for all your XProtect Smart Client joysticks.

1. In the **Selected Joystick** list, select the joystick.

2. In the **Axis setup** section, specify settings for the available axes.

   With a joystick, you can typically navigate camera images three-dimensionally, along three axes: an X-axis (horizontal), a Y-axis (vertical), and a Z-axis (refers to the depth or zoom level).

   o **Invert:** By default, a PTZ camera moves to the right when you move the joystick to the right and moves up when you move the joystick towards you. If you want to change this to the opposite, select Invert.

   o **Absolute:** By default, joystick control takes place based on a relative positioning scheme and moving a joystick moves the joystick-controlled object based on the object's current position. If you want to use a fixed rather than a relative positioning scheme, select Absolute.

   o **Action:** Select the function for an axis: Camera PTZ Pan, Camera PTZ Tilt, Camera PTZ Zoom, or No action.

o **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 dark blue bar.

When previewing your selections, consider adjusting the joystick's dead zones. Dead zones determine how much the joystick handle is allowed to move before information is sent to the camera. Ideally, a joystick handle should be completely vertical when not used, but many joystick handles lean at a slight angle. Without a dead zone, the slight slant can cause cameras to move when it is not required.
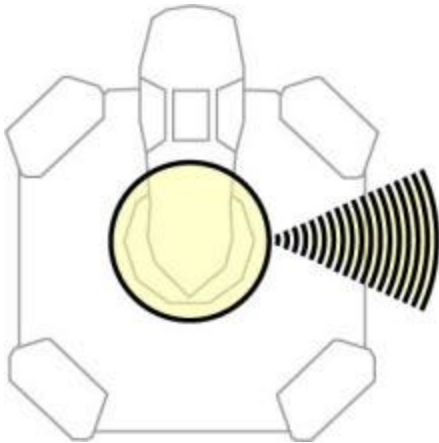
Example of dead zone: When you move the joystick handle outside the dead zone, the PTZ camera will begin to move. The further out you move the handle, the quicker the camera typically moves.

o **Pan/Tilt:** Lets you 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 preview to test the effect of your dead zone settings.

o **Zoom:** Lets you 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 preview to test the effect of your dead zone settings.

3. In the **Button setup** section, specify an action for each required joystick button. Select the actions in the **Action** column.

Tip: To verify that you are configuring the right button, press the corresponding button on the joystick. The relevant button will display in dark blue in the Preview column.

Joystick setup is tied to your computer

Unlike your views and custom keyboard settings, which are simply tied to your user login and can therefore be used on any computer with a XProtect Smart Client, your joystick setup is tied to your user login as well as to the computer on which you configured the joystick setup.

This means that your joystick setup will only work on the computer on which it has been configured. The reason for this is that different computers are likely to have different joysticks attached.

If you want to use a joystick with the XProtect Smart Client on more than one computer, you must configure the XProtect Smart Client's joystick setup on each computer.

Keyboard options

Keyboard options let you assign your own shortcut key combinations to particular actions in the XProtect Smart Client.

Tip: The XProtect Smart Client also features a small number of standard keyboard shortcuts (see "Keyboard shortcuts" on page 26), immediately ready for use.

1. On the **Keyboard** tab in the **Press shortcut key** field, enter the key combination you want to use.

   Custom key combinations must begin with CTRL or ALT. Example: CTRL+B (press and hold the CTRL key and then press the B key).

2. In the **Categories** list, select a command category and then select one of the associated commands.

   Tip: If you want all your views listed to allow you to create keyboard shortcuts for individual views, select the **Views.All** category.

   Some commands will 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.

3. In the **Use new shortcut in** list, select how you want the shortcut key combination to apply:

   o **Global:** On all of the XProtect Smart Client tabs.

   o **Playback mode:** Only on the **Playback** tab.

   o **Live mode:** Only on the **Live** tab.

   o **Setup mode**: Only in setup mode.

4. Click **Assign**. This adds your shortcut key combination to the **Assigned keys** list.

5. Click **OK**.

Tip: Your shortcut key combinations are kept as part of your user settings on the surveillance system server. This means that you will be able to use your shortcut key combinations 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.

Alarm options

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

Advanced options

The **Advanced** options let you customize advanced XProtect Smart Client options. If you are not familiar with the advanced options and how they work, just keep their default settings. If connected to certain types of surveillance systems (see "Surveillance system differences" on page 32), you will see a **Follow Server** column, which you can use for making your XProtect Smart Client follow the surveillance system server's recommended settings. 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.

Advanced options:

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—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%. |
| Time zone | Lets you specify 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. |

Language options

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.

Viewing

Digital zoom

About digital zoom

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 "Exporting evidence" on page 111), 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 evidence" on page 106) an image on which you have used digital zoom, the digitally zoomed area of the image will be printed.

Work with digital zoom

Use digital zoom

1. On the camera toolbar, click **More** > **Digital zoom** to enable it.

   Tip: 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.

   A small overview frame appears in the bottom right corner of the view, providing an overview of the full image when you zoom in on an area.

2. 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.

3. If you want 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.

4. 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.

5. Selecting a zoom level of **0%** lets you view the full image again.

Tip: If your mouse has a scroll wheel, you can also use the scroll wheel to control the zoom level. On many mice, clicking the scroll wheel or middle mouse button quickly lets you view the full image again.

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 PTZ (Pan/Tilt/Zoom) 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.

PTZ and 360º lens images

Use of 360º cameras is not supported by all surveillance systems and some 360° cameras are not supported by the 64-bit version of Microsoft Windows. Depending on your user rights, access to PTZ controls from some cameras may be restricted. PTZ features may be limited when connecting to selected surveillance systems; see Surveillance System Differences. (see "Surveillance system differences" on page 32)

360° lens images

If your views include 360° cameras or lenses, you can navigate 360° 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 360° 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.

The PTZ navigation buttons and the virtual joystick mouse pointer

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** for navigating 360° lens images but you can save a favorite position.

Define a favorite 360° lens position

You can only save positions for 360° lens cameras.

1. Navigate to the position in the 360° lens image that you want to save.

2. On the camera toolbar, click **More** > **Save 360° Lens Positions** to save the position.

3. When you want to return to the 360° lens position, on the camera toolbar, click **More** > **Load 360° Lens Positions.**

PTZ images

If your views contain PTZ (Pan/Tilt/Zoom) camera images, you can control the PTZ cameras using the overlay PTZ navigation button. In setup mode, in the **Properties** pane, you can define whether you want PTZ click mode for the position in the view to be default, click-to-center, or virtual joystick. Your XProtect Smart Client options (on page 83) define whether your default is virtual joystick or click-to-center.

Tip: You may be able to use a joystick for controlling your PTZ cameras. Joystick control can be customized (see "Joystick options" on page 87). Even though joystick and point-and-click control is supported for a large number of PTZ cameras, not all PTZ cameras may be controlled this way.

Many PTZ cameras can be controlled simply by pointing and clicking inside the images from the camera. If you see a set of cross hairs when placing your mouse pointer over the images from a PTZ camera, point-and-click control is supported for the camera.

Cross hairs indicate point-and-click control. For some cameras, cross hairs may look different.

For some cameras, cross hairs surrounded by a square may be displayed. 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.

Select a PTZ preset position

1. Selecting a preset position from the list of presets will make the PTZ camera move to the specified position. If preset positions have been defined for the selected PTZ camera, you can select them in the following way.On the **Live** tab, on the camera toolbar, click **More > PTZ Control > PTZ Presets**, and then the required preset position.

2. Selecting the preset position **Home** will move the camera to its default position.

Stop PTZ Patrolling

You can stop PTZ patrolling (a PTZ camera can continuously move between a number of preset positions according to a schedule).

Only stop PTZ patrolling when there is an important reason to do so; PTZ patrolling schedules are normally carefully planned to meet your organization's surveillance needs. On the **Live** tab, select the required view.

1. On the camera toolbar, click **More** > **PTZ Control** > **PTZ Presets** > **Stop PTZ Patrolling**.

2. To resume patrolling, either select the command again or close the view.

Bookmarks

About bookmarks

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 recorded video" on page 107) pane

- The Sequence Explorer (see "The Sequence Explorer tab" on page 100)

- The Timeline (see "Bookmarks in the timeline" on page 106)

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 recorded video" on page 107) pane or the **Sequence Explorer**).

- The bookmarked video no longer exists on the surveillance system.

The Bookmark window

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

Bookmark settings

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" on page 103) 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

A headline can contain a maximum of 50 characters.

Description

A description of the incident can contain a maximum of 10000 characters.

Add and edit bookmarks

You can add a bookmark by clicking the bookmark icon ◾ on the position in the view or an overlay button.

Add or edit a bookmark

1. Select the required camera in the view.

2. Click the bookmark icon ◾. If you have specified that you can add details in the **Options** (see "**Functions options**" on page 85) window, the Bookmark window appears where you can add a detailed description of the incident. The length of a bookmark clip is determined on the surveillance system server, but you can change this by dragging the timeline indicators.

   Tip: Do not worry if it takes you a while to enter the details for your bookmark; the XProtect Smart Client remembers your bookmarks until you click Save (unless it takes several days to create the bookmark and the video no longer exists on the surveillance system).

3. Click **OK**.

Manually activate output

If external output has been defined on your surveillance system, for example, switching on lights or sounding a siren, this can be activated from the **Live** tab. Note that, depending on your user rights, access to activating output may be restricted.

There are two ways of manually activating output, either by using the **Output** pane or by clicking the overlay button if this is available (if an overlay button is available, it appears when you move your mouse over the view).

On the **Live** tab, in the **Output** pane select the required output, and then click **Activate**. The list of selectable output is grouped by server 🖥 in some surveillance systems, while in others, they are grouped by cameras. If a server is listed with a red icon 🖥, it is unavailable, in which case you cannot activate output on that server.

If activation fails, a message appears.

Privacy masks

Privacy masks protect sensitive information by blocking out certain areas in a camera's angle of view. In the XProtect Smart Client, a privacy mask is displayed as a black area in video.For example, if a camera overlooks the windows of a resident's kitchen and living room, these windows can be blocked with privacy masks to ensure privacy.

You cannot remove privacy masks; they are defined entirely by the surveillance system administrator.

If privacy masks are used, they appear in all viewing contexts—also when you export (see "Exporting evidence" on page 111) video or print (see "Print evidence" on page 106) still images.

If you export video containing 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.

Investigating incidents

Sequence Explorer

The Sequence Explorer tab

The Sequence Explorer tab lets you navigate through thumbnail images from one or multiple cameras, so you can easily find relevant video and play this immediately.

The thumbnail views displays content chronologically from left to right, with the most recent thumbnails towards the bottom right part of the view:

You can adjust the size of the thumbnails by dragging the **Size Slider** below the thumbnail view:

The thumbnail images can relate to an individual selected camera or several selected cameras in a view. The fact that you can compare the thumbnail images side-by-side, while navigating in time by dragging the thumbnail view, enables you to look at large amounts of recorded video and identify the most relevant video, which you can then immediately play back.

To view video associated with a particular thumbnail, click the thumbnail. When you click a thumbnail, it becomes highlighted and (provided **Autoplay** is selected) the associated sequence is played back in the right side of the Sequence Explorer.
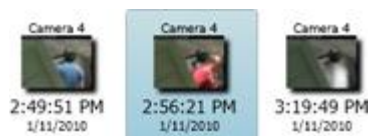
Tip: If you have clicked a thumbnail, and then navigated away from it by dragging the thumbnail view, you can quickly return to the selected thumbnail by clicking **Refresh**.

Define what you see

Before you can see any thumbnails, you must select the cameras that you want to see thumbnails for. Select either the **Time Interval**, **Sequence**, or **Bookmark** tab, and then select the cameras or views by clicking the include or exclude arrows to move them to the **Selected camera(s)** list. When you have made your selection, click **Refresh**.
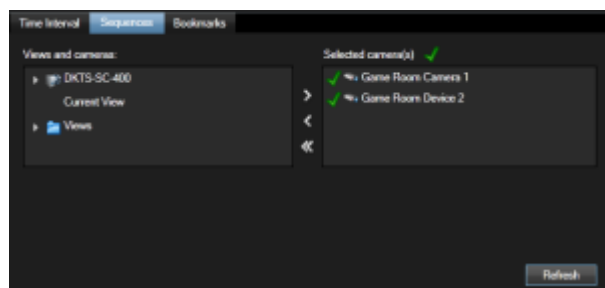
The list of selectable cameras is grouped by servers to which the cameras belong. If a server is listed with a red icon , it is unavailable, in which case you will not be able to select cameras from that server.

The **Selected camera(s)** list shows the status of the selected cameras:

 A green check mark indicates that everything is fine.

 A yellow X indicates that the loading of some sequences and bookmarks was unsuccessful.

 A red warning X indicates that there are no recorded sequences and/or bookmarks, or that loading was unsuccessful.

Time intervals

The **Time Interval** tab lets you display thumbnails for specific intervals of time. For example, one thumbnail for every 30 seconds. You specify the required interval in the field on the tab.

You can specify the required interval in hours, minutes, and seconds (HH-MM-SS). Intervals can be up to 24 hours long. You cannot use the field to navigate to a particular point in time, you can only use it to specify intervals.

Sequences

The **Sequences** tab lets you display a thumbnail for each recorded video sequence. Because sequence length may vary, some thumbnails may represent short sequences while others may represent very long sequences. Sequences often begin some seconds before a motion detection or event occurs and end some seconds after. This buffer allows you to see what happened immediately before and after an incident; the buffer length is determined by the surveillance system administrator

Bookmarks

The bookmark feature is only available when connecting to selected surveillance systems; see Surveillance System Differences (on page 32). Depending on your user rights, access to viewing bookmarks from some cameras may be restricted. Note that you may be able to view bookmarks even though you may not be able to add them, and vice versa.

The **Bookmarks** tab lets you display a thumbnail for each available bookmark (see "Bookmarks" on page 97). Since the length of the video sequences associated with the bookmarks may vary, some thumbnails may represent bookmarks with short sequences while other thumbnails may represent bookmarks with very long sequences.

Tip: When you place your mouse over a thumbnail, details about the bookmark will be displayed in a pop-up window.

To the right of the preview you can see details about the selected bookmark. Depending on your user rights, you may be able to edit, delete, print, or export the bookmark:

- o To edit a bookmark's time settings, headline or description, click

- o To delete an irrelevant bookmark, click

When you delete a bookmark, the bookmark will be deleted not only from the thumbnail view but from the entire surveillance system. You will be asked to confirm that you really want to delete the selected bookmark.

The timeline

The timeline on the Sequence Explorer (see "The timeline" on page 104) lets you navigate through video content.

Navigating sequences

You have several options for navigating the thumbnails.

Click and drag

Click and drag the thumbnail views to the left (backward in time) or right (forward in time) inside the thumbnail view.

The sequence slider

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

Date and time

Click the **Calendar** icon below the thumbnails to access a calendar where you can specify a date and time. Click Go To to see thumbnails for this time.
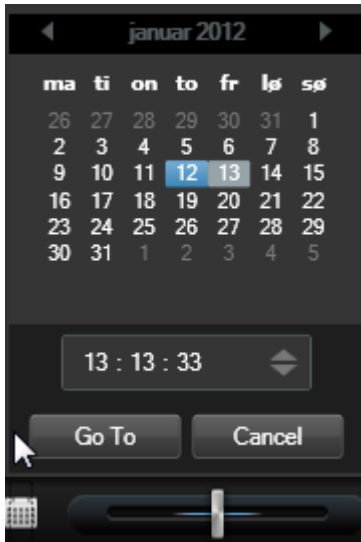
Tip: In the calendar, a blue background indicates the selected date, while a gray background indicates the current date.

Thumbnail Image with Yellow X

Depending on your navigation method, you may occasionally see placeholder thumbnails with yellow Xs if there is no recorded image from a specific point in time:

These appear when the Sequence Explorer cannot retrieve a proper thumbnail image, 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, since such deviating thumbnail images could otherwise cause confusion

On the Sequence Explorer's **Time Interval** tab, a placeholder thumbnail appears if the retrieved thumbnail image 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 image is at 12:00:33. If there are no recording sequences that cover this interval, no attempt to retrieve a thumbnail will be made and the next thumbnail will be from the next interval (12:00:30-12:01:00). If however, there are recording sequences that cover this interval, a placeholder thumbnail will appear instead.

On the Sequence Explorer's **Sequences** and **Bookmarks** tabs, a placeholder thumbnail appears if the retrieved thumbnail image is more than three seconds off compared with the requested time, i.e. 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.

Time navigation

The timeline buttons and controls

1: Playback Date

2: Timeline Time

3: Playback Time

4: Time Selection Mode

5: Set Start/End Time

6: Playback Speed and Playback Speed Slider

Play buttons:

7: Previous Image

8: Play Backward

9: Playback Slider

10: Play Forward

11: Next Image

Navigation buttons:

12: First Sequence

13: Previous Sequence

14: Next Sequence

15: Last Sequence

16: Time Span Slider

17: Timeline Options

The timeline

The timeline displays an overview of periods with recordings from all cameras displayed in your current view. The timeline is displayed on the **Playbac**k and **Sequence Explorer** tabs, in independent playback mode, and when you add or edit bookmarks.

Two timelines are displayed in the timeline area (see "The timeline buttons and controls" on page 104). 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.

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 zoom the range of the timeline so it increases or decreases the units of time, 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. The **Timeline time** is indicated by a blue vertical line.

Playback date and time

The area in the upper part of the timeline shows the playback time and date of the recordings in blue The playback 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. When this is the case, 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.

Date and time navigation

Click the **Playback Date** or **Playback Time** to open the **Go to** window, where you can select the date and time that you want to go to. Double-clicking anywhere on the timeline moves it to that particular time.

Time selection

Click **Set Start/End Time** 🕐 to jump to a specific point in time, by specifying the date and time. Clicking **Time selection mode** 🔲 lets you select a period of time by dragging the start and end time indicators on the timeline (typically when you are exporting video (see "Exporting evidence" on page 111)). Click again to see the timeline with no time selected.

Playback Speed

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.

Play buttons

Use the playback buttons to play back recordings:

◀ⅼ	**Previous image:** Moves to the image just before the one currently viewed
◀	**Play backward in time**
▶	**Play forward in time**
ⅼ▶	**Next image:** Moves to the image just after the one currently viewed

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.

❚❚	**Pause**

Tip: Quickly dragging the **Playback Slider** to the left also pauses playback.

Navigation buttons

Use the navigation buttons **to** navigate through recording sequences.

ⅼ◀	**First sequence:** Moves to the first image in the database for the selected camera

	Previous sequence: Moves to the first image in the previous sequence
	Next sequence: Moves to the first image in the following sequence
	Last sequence: Moves to the last image in the database for the selected camera

Time span

The time span slider lets you specify the time span of playback, independent playback, and sequences (for example, 1 hour, 2 hours, or up to 4 weeks) of your recordings in the timeline.

Bookmarks in the timeline

Bookmarks in the timeline are indicated with a blue bookmark icon: . To view the bookmarked video, place your mouse over the icon.

Print 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, in which you can include notes about the recorded incident.
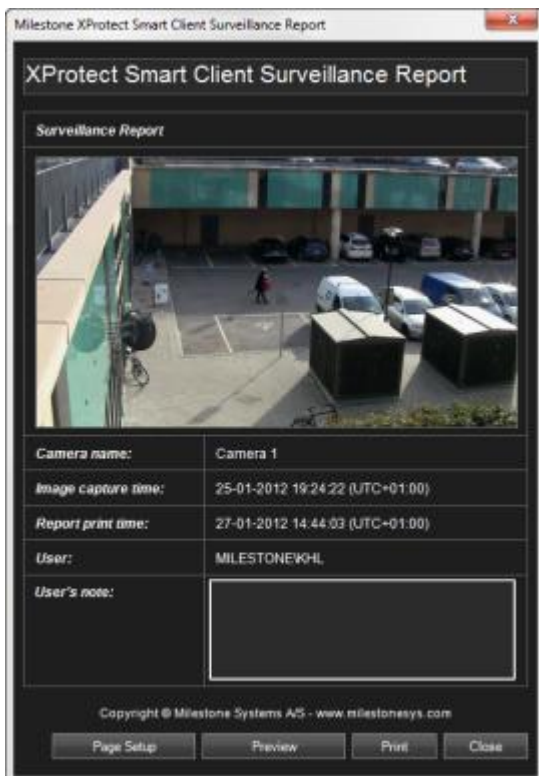
You can also print information about alarms (on page 116) if your organization uses the alarm handling features.

To print a surveillance report

1. Select the relevant camera, view, or bookmark that you want to print as part of a surveillance report.

2. Browse to the relevant time or sequence.

3. Move your mouse over the image and in the menu that appears on the camera's toolbar, click the **Print** icon 🖶. If you want to print a bookmark, on the **Sequence Explorer** tab, in the preview toolbar for the bookmark, click the **Print** icon 🖶.

    The **Surveillance Report** appears displaying a preview of the image as well as information about:

    o   Camera name

    o   Image capture time

    o   Print time

    o   Name of the user

    For bookmarks:

    o   the bookmark ID

    o   time details

    o   bookmark headline

    o   bookmark description (if available).

    In **User's Note:**, you can include a description of the incident.

    Tip: If you used digital zoom on the image, only the area on which you have zoomed in will be printed.

    Optional: If you want to change or verify paper size, source and orientation for the printout, in the **Surveillance Report** window, click **Page Setup** to open the **Page Setup** window.

    When ready, click **OK** to return to the XProtect Smart Client **Surveillance Report** window. If you want to preview the report, click **Preview**.

4. Click **Print** to print the image and associated details.

Search recorded video

You can search recorded video using the Sequence Explorer, the **Recording Search** pane, or **Smart Search** pane.

On the **Playback** tab, you can use the **Recording Search** pane to quickly search for recorded sequences or bookmarks for a single selected camera or for all cameras in a view. Alternatively, you can use the **Smart Search** pane to search for motion in one or more selected areas of recordings from a particular camera.

Smart search cannot be used for video from 360° lens cameras. Depending on your user rights, access to smart search may be restricted.

Search using the Recording Search pane

1. On the **Playback** tab, in the **Recording Search** pane, select either **Sequences** or **Bookmarks**.

2. For bookmarks, select the search criteria you are interested in, for example, time, your bookmarks only, or content from the bookmark's Bookmark ID, Headline and Description fields (see "Add and edit bookmarks" on page 98).

3. Select whether you want the search to include only the selected camera or all cameras in the view.

4. Click **Search**. This will retrieve a list of results. The sequence closest to the time you have selected for the view appears in the middle of the list. Sequences or bookmarks from before the time you have selected appear above, and ones from after, below. Each sequence is listed with camera information, date, and time. Selecting a sequence in the list moves all video in the view to the time of the selected sequence.

5. 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).

6. To quickly preview the video when you place your mouse over the bookmark or sequence in the list, select **Auto-preview**.

7. 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. For more information, see Add and edit bookmarks, Print evidence (on page 106) and Exporting (see "Exporting evidence" on page 111).

Search using the Smart Search pane

1. On the **Playback** tab, in the **Smart Search** pane, under Search area, select **Show grid** .

2. Select the camera in the view. A blue grid overlay appears.
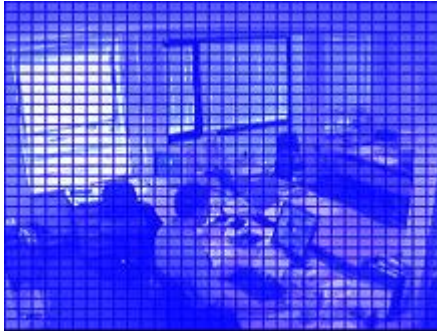
Tip: For a better view, double-click the image to enlarge it.

3. Click and drag inside the image to select the area in which you want to use smart search. You can select more than one area.

    The areas you select will become visible through the blue overlay. The blue overlay indicates the areas that are excluded from the smart search.
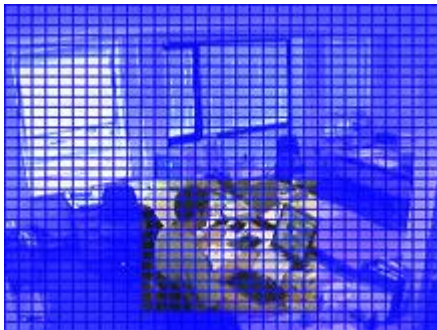
You can toggle between including or excluding the areas that you select by clicking **Include** or **Exclude** options. Alternatively you can invert your selection to include or exclude everything you have selected. With the **Smart Search** pane's **Include** and **Exclude** options, you can toggle between including/excluding areas when you drag.

Example of inverted selection

Tip: As an alternative to clicking **Invert**, press the SHIFT key while clicking/dragging to select an area.

4. Click **Save** to save your search area settings.

    Tip: If you want to experiment with further changes to the search area, you can return to your saved search area settings by clicking **Load**.

5. In the **Sensitivity** list, select the search sensitivity, and in the **Interval** list, select the image interval. If you select **All images**, all images will be analyzed. If you select e.g. 10 seconds, only one image per ten seconds of recordings will be analyzed. Selecting a long interval will greatly reduce the search time. However, with a long interval, the search may not find motion sequences that are shorter than the specified interval.

6. Click the **Next** (to move forward in time) or **Previous** (to move back in time) to search through sequences with motion detected in the selected areas.

    When a sequence with motion inside the selected area(s) is found, it is displayed with the motion highlighted.
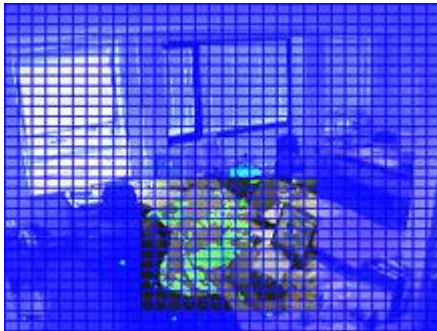
    Tip: The **Playback** tab's **timeline displays** the corresponding time information.

7. If required, click the **Next** or **Previous** to continue the smart search.

Exporting evidence

The Export window

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

With the XProtect Smart Client you can quickly export recorded evidence in movie clip, audio, still images, or in the XProtect format. The format and settings you choose are stored and displayed next time you export.

General export settings

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.
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 will be created automatically. **Media burner** - Select a burner. The media burner you need to have installed is the Image Mastering API (IMAPI-v2) from Microsoft, which is installed by default on most computers. If your computer does not have IMAPI-v2 installed, you can download and install it from the Microsoft website.
Selection	This contains the items you have selected to include in your export, but you can add or remove items, for example, cameras. You can include items from the current view in your XProtect Smart Client window, from all views you have access to (including Smart Wall views) and all cameras and audio you have access to.
Privacy mask	Click to set a privacy mask on the camera. This covers the area that you select in a black area of solid color, so those parts of the image are not viewable. You cannot remove existing privacy masks, you can only add new ones.

XProtect format

Export in the XProtect format is available when connected to selected surveillance systems (see "Surveillance system differences" on page 32) only. Depending on your user rights, access to exporting evidence from some or all cameras may be restricted.

XProtect format settings

Name	Description
Include XProtect Smart Client – Player	Select to include the XProtect XProtect Smart Client – Player application with the exported video. The XProtect format can only be viewed with the XProtect Smart Client.

Name	Description
Prevent re-export	Select that you do not want to allow the video 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.
Include digital signature	Select to include a digital signature to your exported database. Depending on your surveillance system settings, the data 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 signatures" on page 124) 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 data has been tampered with.

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

If a privacy mask has been added, no digital signatures for the recording server will be included 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. |
Keep view layout	Select to keep the view layout from the current view that you are exporting from.
Optimize view layout	Select to optimize the layout to squared views of up to 25 positions in the view.
Comments	Click to open the **Add Comments to Export** window, where you can add comments to individual cameras or to the project s a whole. You can also choose to include a project comment (not individual camera comments) by default to subsequent exports.

Media player format

The media player format allows you to export a standard video clip and/or audio clip that can be viewed and/or listened to from computers that have a standard codec/media player installed.

Media player settings

Name	Description
Codec	A video codec is a particular compression/decompression technology used when generating video files. Your choice of codec will affect the quality and size of the AVI file. The list contains the video codecs available on your PC. You can change the codec, but we recommend that you keep the default codec settings, unless you have a good reason to change these.
Include timestamps	Select if you want to add the date and time from the surveillance system to the exported images. The timestamp will be displayed at the top of the exported video.
Reduce frame rate	Select to reduce the frame rate for the export; every second image will be included, yet still play back in real-time.
Video texts	Click to open the **Video Texts** window where you can create pre- and post-texts for the AVI file. These texts will be added to all cameras for the export and displayed as still images before (**Pre-slides**) and/or after (**Post-slides**) the video.
Still images and audio	If you want to export single video frames, you can export these as still images.

Still images and audio

If you want to export single video frames, you can export these as still images.

Still image settings

Name	Description
Include timestamps	Select if you want to add the date and time from the surveillance system to the exported images. The timestamp will be displayed at the top of the exported video.

Export evidence

Export a video clip, audio, or still image

1. On the Playback tab, in the timeline, click the **Time Selection Mode** button to select the start and end time (see "Time selection" on page 105) of the sequence you want to export.

2. On the XProtect Smart Client toolbar, click **Export**.

    If any additional items to the one you have selected contain relevant video or data, you can select to include these in the export by selecting the check box on the right of the title bar for each position in the view. You can also change this selection in the **Export** window.

3. In the **Export name** field, enter a name for the exported video. If you do not enter a name here, the program automatically creates a name with the current date and time.

4. Specify a path and/or media burner for the destination of the exported file.

5. Click the relevant tab to select one of the following formats to export to:

o   **XProtect format.** Export in a Milestone XProtect database format, with the option of including the XProtect Smart Client – Player, to let your recipients view exported video. This format can only be viewed in the XProtect Smart Client – Player application.

o   **Media player format.** Exports in a format that can be played from most computers.

o   **Still images.** Export as a still image for each frame for the selected period.

6.   Specify the necessary settings (see "The Export window" on page 111) for the format you have chosen.

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

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 audio recorded by microphones in the export. Export in the database format is only available if connected to selected surveillance systems; see Surveillance System Differences (on page 32). 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" on page 97) 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.

Can I export digitally zoomed images?

Yes. If you used digital zoom prior to exporting, you will, when exporting in the media player or still image formats, be able to export the regular images or the digitally zoomed images. When exporting in the XProtect format, making this selection is not necessary because recipients will be able to use digital zoom on the exported recordings.

Can I export 360° 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). You can export 2×2 or split 360° lens views.

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 32), 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 a privacy mask has been added, no digital signatures for the recording server will be included 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 select to **prevent your recipients from re-exporting** (see "XProtect format" on page 111) the material, to **protect the exported evidence with a password** (see "XProtect format" on page 111), and to **add a signature** (see "XProtect format" on page 111) to the exported material.

Events and alarms

Alarms

About alarms

The Alarm and Map features are only available when connected to certain types of surveillance system (see "Surveillance system differences" on page 32). Particular user rights may be required to use the features described in the following.

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.

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 121).

The Alarm Manager tab

The alarm preview

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.

Alarm preview settings

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..

Name	Description
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.

The Alarm list

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. 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 view recorded video from the camera(s) associated with the alarm or event, select the alarm or event in the list to display it in the **Alarm** preview.

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.
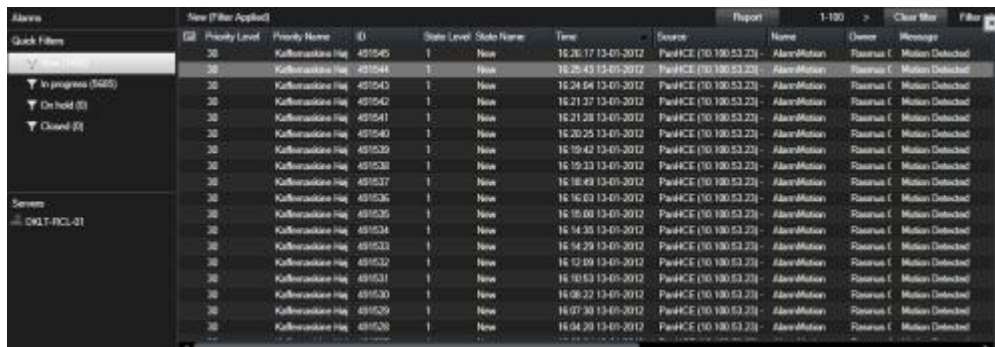
Tip: You can select multiple alarms or events in one go, in which case video from up to 16 cameras associated with the selected alarms or events will be displayed in the alarm preview position.

To allow for optimum performance, the list by default displays a maximum of 100 alarms or events at a time. To browse to the previous/next alarms or events, simply use the buttons in the top right part of the alarm list position.
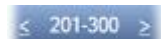
In setup mode, you can select whether or not you want to see the alarms or events grouped by servers in a navigation tree and how many alarms or events you want the list to display at a time. This is also where you specify whether you want the alarm list to display alarms or events.

Alarm List settings

Filters

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** column. The **Filters** pane, lets you filter according to certain criteria (see "Filter alarms" on page 118). Initially, all alarms will be in the New state, but once an alarm is being handled, its state is updated.

Servers

On the left side of the alarm list, alarms are grouped by the surveillance system server they 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. Each item is clickable, allowing you to quickly filter the alarm list by server, all priorities, high priority, etc.

The number displayed for each item represents the number of alarms with the relevant priority or state. Note, however, that the number shown for servers only represents the number of alarms in the New state. If a server is listed with a red icon , it is unavailable, in which case you will not be able to view alarms from that server. Alarms can be one of the following priorities: **High** , **Medium** , or **Low** . You can see the priority of each alarm in the alarm list's first column. To quickly view all alarms with a certain priority, select the required priority in the tree structure in the left side of the alarm list.

Failure to connect

If your XProtect Smart Client loses connection to the Event Server, the surveillance system server component dealing with alarms, the alarm list will notify you of this by switching the color of its top bar from blue to red . This is important since you will not be able to receive new alarms as long as the connection is broken. Loss of connection can, for example, happen because of network problems; contact your surveillance system administrator if the problem persists. As soon as the connection is re-established, the top bar will switch back to blue again.

dkts-vap-13v27 - Failed to connect to Event Server

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; you can click an element on a map to see only alarms associated with that element, you can click a predefined filter in the Filter pane, or you can define your own custom filters.

- To filter the alarm list's content, in the **Alarm List** toolbar, click **Filter** to open the **Filter** pane above the alarm list. 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.

You can combine filters (for example, for a location on a certain date). When you apply a filter, the filter section will change background color from blue to orange . To return to the unfiltered alarm list, click the **Clear filter** link in the Alarm List toolbar.

Tip: In fields where you type your filtering criteria, typing the first few characters of the required name, location or similar is often enough.

Having entered filtering criteria, note that the alarm list will not be updated until you move the insertion point to another filter field.

Tip: 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.

- To sort the alarm list's content, in the **Alarm** list, click the button at the top of the column.

Alarms on maps

If your alarm handling view contains one or more map (see "Maps" on page 57) 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.

Tip: 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.
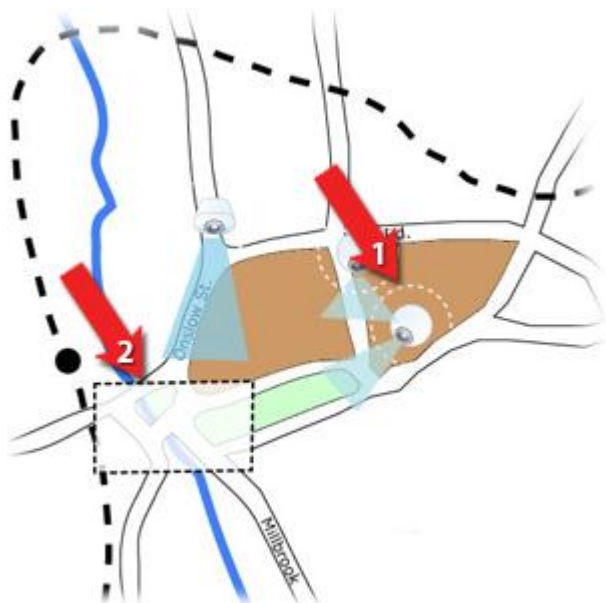
To return to an alarm list mode where you can see alarms from more than just the one element, click the required server, priority or state in the alarm list.

Events

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, XProtect Analytics, 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 an event

- On the **Live** tab, in the **Event** pane, select the relevant event and click **Activate**.

The list of selectable events is grouped by server, and the camera/device with which the event is associated. 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.

Alternatively, if available for the camera, click the overlay button that appears when you move your mouse over the image.

There is no confirmation once you have activated an output.

Working with alarms

From the alarm list, you are able to acknowledge alarms, edit details of alarms, or print reports with information about alarms.

- View and edit details of an alarm (on page 120)

- Acknowledge an alarm (on page 121)

- Disable an alarm (on page 121)

- Ignore an alarm (on page 121)

- Print a report with alarm information (on page 121)

- View alarm reports (on page 121)

- Alarm filtering (see "Filter alarms" on page 118)

View and edit details of an alarm

Double click on an alarm to open the window for the alarm. The window shows a preview of the alarm incident and live video. You can manage the alarm in the following way:

- **State**: Lets you change the state of the alarm. Typically, you would change 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 if required. The person to whom you assign the alarm will then become the owner of the alarm, and will be listed in the alarm list's **Owner** column.

- **Comment**: Write comments and remarks, which will be added to the alarm history. Comments typically relate to the actions you have taken. Examples: "Suspect detained by Security," "Suspect handed over to Police," "False alarm," etc.

- **Alarm History**: The alarm history is a summary of 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 alarm history. To view the alarm history, click the ⌄ button in the bottom left side of the edit dialog.

Depending on surveillance system server configuration, the alarm history may contain instructions about what to do when handling the alarm. When that is the case, the alarm history is automatically displayed when you edit the alarm.

- **Print**: Lets you print a report with information about the alarm, including the alarm history and, if available, a still image from the time of the alarm.

Acknowledge an alarm

To record that you have received an alarm, and that you will do something about it, right-click the alarm and select **Acknowledge**. This will change the state of the alarm from **New** to **In progress**. You can only acknowledge new alarms.

Tip: You can acknowledge multiple alarms simultaneously; press and hold down the CTRL key, and then selecting the alarms you want to acknowledge.

Disable an alarm

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 an alarm

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.

Print a report with alarm information

From the alarm list, 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, right-click the alarm in question and select **Print**. You cannot use the print feature if you have selected multiple alarms in the alarm list.

View alarm reports

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

  o   Category

  o   State

  o   Priority

- o Reasons for closing

- o Site

- o 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.

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; you can click an element on a map to see only alarms associated with that element, you can click a predefined filter in the Filter pane, or you can define your own custom filters.

- • To filter the alarm list's content, in the **Alarm List** toolbar, click **Filter** to open the **Filter** pane above the alarm list. 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.

You can combine filters (for example, for a location on a certain date). When you apply a filter, the filter section will change background color from blue ▮ to orange ▮. To return to the unfiltered alarm list, click the **Clear filter** link in the Alarm List toolbar.

Tip: In fields where you type your filtering criteria, typing the first few characters of the required name, location or similar is often enough.

Having entered filtering criteria, note that the alarm list will not be updated until you move the insertion point to another filter field.

Tip: 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.

- • To sort the alarm list's content, in the **Alarm** list, click the 🔽 button at the top of the column.

The XProtect Smart Client – Player

About the XProtect Smart Client – Player

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. You can use the XProtect Smart Client – Player to view video and archives and to repair corrupted databases. The application has many of the features of the XProtect Smart Client and looks similar.

Work with views in the XProtect Smart Client – Player

You create and manage views by clicking **Setup** on the   XProtect Smart Client – Player toolbar.

The Project pane

A project in the XProtect Smart Client – Player is a collection of files that are created when video is exported in database format from the XProtect Smart Client. Click **Setup** to make changes to a view or your application settings and save these to your project.

Your user settings, including information about your views, are stored as part of a project.

Passwords

You can assign passwords to a project, for example, so 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 by clicking the New Project button , and then clicking the Open Database button to start the Open Database wizard and add the relevant devices.

The Views Pane

In the **Views** pane you can add, create, edit, or delete views. For more information on what you can do with views, see Views (on page 39).

The Overview Pane

The **Overview** pane displays the cameras, microphones, speakers, HTML, images, and other plug-ins, for example, XProtect Transact, that are assigned to the project.

Click **Open Database** , to open the **Open Database wizard**. You can rename and delete devices from a project by clicking Rename or Delete .

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

Link Audio

You can link audio to a device by clicking **Link Audio to Camera** 🖉 to have associated audio automatically selected when you view recorded video for a particular camera.

Open Database wizard

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. To start the Open Database wizard, on the XProtect Smart Client toolbar, click Setup, and in the Overview pane, click Open Database: 📥.

WARNING: Do not attempt to open a live database—this can damage your system.

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**.

You can also see whether or not the database contains signatures. You can verify the database when it is added to the project (see the following section).

If the database you are trying to open is corrupted, the wizard can repair it.

Verify signatures

If the exported material you are viewing has a signature assigned to it, you can verify this manually. On the XProtect Smart Client – Player toolbar, click the **Verify Signatures** button to open the **Manual verification** window. Here you can see the devices and whether they have been modified (tampered with) on the recording server and/or after the export process. A database can be verified, partially verified (if some of the files have not had signatures attached), or not signed. Click **Verify** to start the verification process, in which all the files are checked and verified.

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

If a privacy mask has been added, no digital signatures for the recording server will be included 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.

Scripting

Scripting

For system administrators and advanced users it is possible to create function calls in the XProtect Smart Client. Note that the use of scripting will require some familiarity with programming.

View a list of function calls

To view a list of the more than 100 available function calls in the XProtect Smart Client:

1. In setup mode, drag the **System Overview** pane's **HTML Page** link to a position in a view.

    Tip: Preferably use a 1×1 view; this will give you the best possible overview of the list's content.
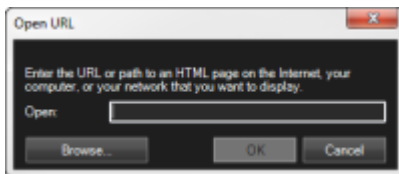
2. In the **Open URL** window, in **Open**, type **about:script** and click **OK**.

    This displays a list of function calls. Each function call is listed with a short description of its purpose. You can try out many of the function calls directly from the list.

Startup scripting

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; see Surveillance System Differences (on page 32).

Parameters

You can use the following parameters:

ServerAddress

Refers to the URL of the server to which the XProtect Smart Client connects (if connecting to an XProtect Corporate system, this is the URL of the Management Server; if connecting to an XProtect Enterprise, an XProtect Professional, an XProtect Express, or an XProtect Essential system, it is the URL of the Image Server).

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

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

The XProtect Smart Client's 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 (see "Scripting" on page 125)) 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'
```

Glossary of terms

Symbols & Numeric

360° Lens

A lens that allows the creation and viewing of 360º panoramic images.

A

Alarm

Incident defined on surveillance system to trigger an alarm in the Smart Client. Triggered alarms will, if your organization uses the feature, be displayed in views containing alarm lists and/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 Smart Client 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.

Carousel

A particular position for viewing video from several cameras, one after the other, in a Smart Client view (on page 132).

Codec

A technology for compressing and decompressing audio and video data, for example in an exported AVI (on page 128) file.

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 (on page 131) 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

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 (on page 129) (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 (on page 130), the standard uses so-called 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 the Smart Client should be capable of using considerable resources on de-compressing H.264 video when it receives it from the surveillance system.

Hexadecimal

A numeral system with a base of 16, meaning that it uses 16 distinct symbols. Here used for defining color nuances in the map view's color tool.

Host

A computer connected to a TCP/IP network. A host has its own IP address, but may—depending on network configuration—furthermore have a name (host name) in order to make it easily identifiable.

Host Name

A name by which a particular computer on a network is identified. Host names are often easier to remember than IP addresses (see "IP Address" on page 130).

Hotspot

A particular position for viewing magnified and/or high quality camera images in a Smart Client view (on page 132).

HTML

Hyper Text Markup Language; a common format used when creating web pages.

HTML Page

A document, such as a web page, created using Hyper Text Markup Language (HTML (on page 129)). HTML pages, for example an organization's website, can be included in Smart Client views (see "View" on page 132).

HTTP

HyperText Transfer Protocol, a standard for exchanging files across the internet. HTTP is the standard used for formatting and transmission of data on the world wide web.

I

I/O

Short for Input/Output.

I-Frame

Short name for intraframe. Used in the MPEG (on page 130) 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.

IP

Internet Protocol; a protocol (i.e. standard) specifying the format and addressing scheme used for sending data packets across networks. IP is often combined with another protocol, TCP (Transmission Control 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.

IP Address

Internet Protocol address; the identifier for a computer or device on a network. Used by the TCP/IP protocol for routing data traffic to the intended destination. An IP address consists of four numbers, each between 0 and 256, separated by full stops (example: 192.168.212.2).

IPIX

A technology that allows creation and viewing of 360° panoramic images.

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 (on page 130), 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 (on page 129).

M

MAC Address

Media Access Control address, a 12-character hexadecimal number uniquely identifying each device on a network.

Map

1) 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 (on page 132).

Matrix

Product integrated into selected surveillance systems, enabling control of live camera views on remote computers for distributed viewing. Computers on which Matrix-triggered video can be viewed are commonly known as Matrix recipients (see "Matrix Recipient" on page 130).

Matrix Recipient

Computer on which Matrix-triggered video can be viewed.

Monitor

An individual monitor in a Smart Wall (a.k.a. monitor wall or video wall).

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

Output

Data going out of a computer. On IP surveillance systems, output is frequently used for activating devices such as gates, sirens, strobe lights, etc.

Overlay Button

Button appearing as a layer upon the video when you move your mouse cursor over individual camera positions in views on the **Live** tab. With overlay buttons it is possible to activate speakers, events, output, move PTZ (on page 131) cameras, start recording, clear signals from cameras, etc.

P

Pane

Small groups of buttons, fields, etc. located in the left side of the Smart Client window. Panes have a sky blue background, and give you access to the majority of the Smart Client 's features. Exactly which panes you will see depends on your Smart Client 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.

P-Frame

Short name for predictive frame. The MPEG (on page 130) standard for digital video compression uses P-frames together with I-frames (see "I-Frame" on page 129). 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.

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 a Smart Wall (a.k.a. monitor wall or video wall).

Private View

A Smart Client view (on page 132) which is only visible by the user who created it.

PTZ

Pan/Tilt/Zoom; a highly movable and flexible type of camera.

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 the Smart Client.

Sequence Explorer

Key feature in the Smart Client: The Sequence Explorer lists thumbnail images representing recorded sequences from an individual camera or

all cameras in a view. The fact that you are able to 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.

Shared View

A Smart Client view (on page 132) shared by several users.

Smart WallSolution for managing collections of wall-mounted monitors (a.k.a. monitor walls or video walls), often used by command centers, city surveillance operators, traffic control centers, etc.

SMS

Systems Management Server, a Microsoft tool which lets system administrators build up databases of hardware and software on local networks. The databases can then—among other things—be used for distributing and installing software applications over local networks.

Speakers

In the Smart Client context: Loudspeakers attached to a camera device, allowing Smart Client users to talk to audiences at the physical location of a camera.

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.

Transact

Product available as an add-on to surveillance systems. With Transact, it is possible to combine video with time-linked PoS or ATM transaction data.

U

URL

Uniform Resource Locator; an address of a resource on the world wide web. The first part of a URL specifies which protocol (i.e. data communication standard) to use when accessing the resource, whereas the second part of the URL specifies the domain or IP address at which the resource is located. Example: http://www.myorganization.org.

V

View

A collection of video from one or more cameras, presented together in the 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.

X

X-Axis

The horizontal axis in a coordinate system.

Y

Y-Axis

The vertical axis in a coordinate system.

Z

Z-Axis

The spatial axis in a coordinate system. When using joysticks, the Z-axis typically refers to the depth (zoom) level.

Index

About Milestone Systems

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

www.milestonesys.com.