Milestone Systems

XProtect® Professional 8.1

Administrator's Manual

milestone

The Open Platform Company

Contents

Copyright, trademarks and disclaimer

Trademarks

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

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

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

Disclaimer

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

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

Milestone Systems A/S 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.

XPP81-am-1(a2)-100912

Introduction

XProtect Professional overview

XProtect Professional is the right product for small to mid-sized installations that need robust single-server surveillance software with the full functionality of advanced management, flexible scheduling, fast searching and analysis. XProtect Professional supports up to 64 simultaneously with the widest choice of network video and computer hardware equipment.

XProtect Professional consists of a number of components, each targeted at specific tasks and user types:

Name	Description
Management Application	The main application used by surveillance system administrators for configuring the XProtect Professional surveillance system server, upon installation or whenever configuration adjustments are required, for example when adding new cameras or users to the system.
Recording Server service	A vital part of the surveillance system. Video streams are only transferred to XProtect Professional while the Recording Server service is running. The Recording Server service is automatically installed and runs in the background on the XProtect Professional surveillance system server. You can manage the service through the Management Application.
Event Server	Handles configuration of alarms and maps from all servers within XProtect XProtect ProfessionalXProtect Professional installations—including Master & Slave setups (see "Configure master and slave servers" on page 174)—throughout your organization. This enables monitoring and instant overview of alarms and possible technical problems within your systems. The event server is automatically installed on, and runs in the background of, the XProtect Professional surveillance system server.
Microsoft® SQL Server Express Database	The surveillance system's alarm data is stored in a SQL Server Express database. The SQL database is a lightweight, yet powerful, version of a full SQL server which is automatically installed on, and runs in the background of, your XProtect Professional surveillance system server.
Image Server service	Handles access to the surveillance system for users logging in with clients. The Image Server service is automatically installed and runs in the background on the XProtect Professional surveillance system server. You can manage the service through the Management Application.
Download Manager	Manage which XProtect Professional-related features your organization's users will be able to access from a targeted welcome page on the surveillance system server.

Name	Description
XProtect® Smart Client	Designed for Milestone XProtect surveillance systems, the XProtect Smart Client is a powerful, easy-to-use client application for the daily operations of security installations. A new, streamlined interface helps improve usability, making it easy to monitor installations of all sizes, manage security incidents and access and export live and recorded video. We recommend that you always use the latest version of the Smart Client to best use any possible new features and functions included in your XProtect Professional surveillance system.
XProtect® Mobile client	A free application designed by Milestone that allows you to view video from your XProtect Professional surveillance system from almost anywhere on your smartphone or tablet. You can also control outputs, such as opening and closing doors and switching lights on or off, allowing you to gain control and dynamically respond to incidents in the system.
XProtect® Web Client	A simplified web-based client application for XProtect surveillance systems for viewing, playing back and sharing video from most operating systems and web browsers. With no need to install additional software, you can monitor your XProtect system from any Internet-enabled computer or device.

Clients

Clients are applications used for viewing live and recorded video from the hardware devices set up in the Management Application.

XProtect Smart Client

About XProtect Smart Client

The XProtect Smart Client has many features and prepares for future integration of plugins, etc. The Smart Client must be installed on users' computers.

Surveillance system administrators manage clients' access to the surveillance system through the Management Application. Recordings viewed by clients are provided by the surveillance system's Image Server service. The service runs in the background on the surveillance system server. It does not require separate hardware.

To download a Smart Client, users connect to the surveillance system server which will present them with a welcome page. The welcome page will list the available clients and language versions. Surveillance system administrators use the Download Manager to control which clients and language versions should be available to users on the welcome page.

The Smart Client is unlicensed and can be freely downloaded and installed as many times as needed.

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 13)
- **Install from a DVD** (on page 14)

Install from the surveillance server

1. Verify that your computer meets the XProtect Smart Client's minimum system requirements.
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 14).

Install from a DVD

1. Verify that your computer meets the XProtect Smart Client's minimum system requirements.

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

```
C:\Program Files\Milestone\Milestone XProtect Professional\
```

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

```
C:\Program Files\Milestone\Milestone XProtect Professional\plugin
```

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

```
C:\Program Files\Milestone\XProtect Professional\
```

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

```
C:\Program Files\Milestone\XProtect Professional\plugin
```

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

If you want your new XProtect Professional 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 Professional installation path to the old default, C:\Program Files\Milestone\Milestone XProtect Professional\, during the installation of your new XProtect Professional.

Install silently

1. Locate the Smart Client installation program (.exe) file - **MilestoneXProtectSmart Client.exe** or **MilestoneXProtectSmart Client_x64.exe** for 32-bit and 64-bit versions respectively. You find the file in a subfolder under the folder **httpdocs**. The **httpdocs** folder is located under the folder in which your Milestone surveillance software is installed.

   The path is typically:
   C:\Program Files (x86)\Milestone\Milestone Surveillance\httpdocs\Smart Client Installer\[version number] [bit-version]\All Languages\en-US

   For example:
   C:\Program Files (x86)\Milestone\Milestone Surveillance\httpdocs\Smart Client Installer\6.0a (32-bit)\All Languages\en-US

2. Run a silent installation using one of the following two options:

a Run with default parameter settings:

To run a silent installation using the default values for all parameters, start a command prompt (cmd.exe) in the directory where the installation program is located and execute following command:

For XProtect Smart Client installation:

>MilestoneXProtectSmart Client.exe -–quiet

For XProtect Professional installation:

> MilestoneXProtectXProtect ProfessionalInstaller.exe --quiet

This will perform a quiet installation of the XProtect Smart Client/XProtect Professional using default values for parameters such as target directory etc. To change the default settings, please see next topic.

b Customize default parameters using an xml argument file as input:

In order to customize the default installation settings, an xml file with modified values must be provided as input. In order to generate the xml file with default values, open a command prompt in the directory where the installation program is located and execute following command:

For XProtect Smart Client:

> MilestoneXProtectSmart Client.exe --generateargsfile=args.xml For XProtect Professional:

> MilestoneXProtectXProtect ProfessionalInstaller.exe --generateargsfile=args.xml

Open the generated args.xml file, using for example Notepad.exe, and perform any changes needed. Then, in order to run silent installation using these modified values, execute following command in the same directory
For XProtect Smart Client:

>MilestoneXProtectSmart Client.exe --arguments=args.xml --quiet

For XProtect Professional:

> MilestoneXProtectXProtect ProfessionalInstaller.exe --arguments=args.xml --quiet

XProtect Mobile client

About XProtect Mobile client

XProtect® Mobile client is a mobile surveillance solution closely integrated with the rest of your XProtect surveillance setup. It runs on your Android tablet or smartphone or your Apple® device (tablet, smartphone or portable music player) and gives you access to cameras, views and other functionality set up in the Management Application.

In order to use XProtect Mobile client with XProtect Professional, you must add a Mobile server (see "About Mobile server" on page 184) to establish the connection between the XProtect Mobile client and XProtect Professional.

Install XProtect Mobile client

1. Access Google Play or App Store℠ on your device.
2. Search for and download the application XProtect Mobile.
3. Once the download of the application is completed, the XProtect Mobile client application is ready for use on your mobile device.

For detailed information about how to set up your XProtect Mobile client, visit the Milestone website at www.milestonesys.com.

XProtect Web Client

About XProtect Web Client

XProtect Web Client is a web-based and touch-enabled surveillance solution that provides users access to view live video, play back recorded video, print and export evidence, and more (access to features depend on individual user rights).

In order to use XProtect Web Client with XProtect Professional, you must add a Mobile server (see "About Mobile server" on page 184) to establish the connection between the XProtect Web Client and XProtect Professional.

Access XProtect Web Client

If you have an XProtect Mobile server (see "About Mobile server" on page 184) installed on your computer, you can use the XProtect® Web Client to access your cameras and views. Since you do not need to install XProtect Web Client, you can access it from the local computer on which you installed the XProtect Mobile server or any other computer you want to use for this purpose.

To access the XProtect Web Client:

1. Set up the XProtect Mobile server in the Management Application.
2. Open an Internet browser (Internet Explorer, Mozilla Firefox, Google Chrome, Opera, or Safari) or click **Open XProtect Web Client** in the Mobile Server Manager (see "About Mobile Server Manager" on page 190).
3. Type in the IP address and port of the server on which the XProtect Mobile server is running.

   Example: The XProtect Mobile server is installed on a server with the IP address 127.2.3.4 and is configured to accept HTTP connections on port 8081 and HTTPS connections on port 8082 (these port settings are the default settings of the installer).

   In the address bar of your browser, type: http://127.2.3.4:8081/XProtectMobile/Web/ or https://127.2.3.4:8082/XProtectMobile/Web/, depending on whether you want to use a standard HTTP connection or a secure HTTPS connection. You can now begin using the XProtect Web Client.
4. Add the address as a favorite in your browser for easy future access to the XProtect Web Client. If you use the XProtect Web Client on the local computer on which you installed the XProtect Mobile server, you can also use the desktop shortcut created by the installer. When you click the shortcut, this launches your default browser and opens the XProtect Web Client.

Clear your Internet browser's cache upon upgrade

Note that Internet browsers running the XProtect Web Client must have their cache cleared before a new version of the XProtect Web Client can be used. System administrators must ask their XProtect Web Client users to clear out their browser's cache upon upgrade or force this action remotely (this action can only be done in Internet Explorer in a domain).

Recording Server Manager

The Recording Server service is a vital part of the surveillance system. Video streams are only transferred to XProtect Professional while the Recording Server service is running. The Recording Server Manager informs you about the state of the Recording Server service. It also lets you manage the service.

In the notification area (the system tray), the Recording Server Manager's icon indicates whether the Recording Server service is running or not. Green indicates running (default), red indicates not running.

By right-clicking the icon, you can open the Management Application, start and stop the Recording Server service, view log files, and view version information.

A green icon in the notification area indicates that the Recording Server service is running.

A red icon in the notification area indicates that the Recording Server service has stopped.

Monitor System Status

By right-clicking the notification area's Recording Server icon and then selecting **Show System Status**, you get access to the **Status** window.

Tip: Alternatively, simply double-click the icon to open the **Status** window.

The **Status** window lets you view the status of the image server(s) and connected cameras. The status of each server/camera is indicated by a color:

- **Green** indicates that the server or camera is running correctly.
- **Gray** indicates that the **camera** (not the server) is not running. Typically, a camera will be indicated in gray in the following situations:
  - The camera is not online (as defined in the camera's online period schedule (see "Online period" on page 155)).
  - The Recording Server service has been stopped.
- **Red** indicates that the server or camera is not running. This may because it has been unplugged or due to a network or hardware error. Errors are listed in the Recording Server log file.

Place your mouse pointer over a camera in the status window to view details about the camera in question. The information appears as a pop-up and updates approximately every 10 seconds.

Name	Description
Resolution	The resolution of the camera.
FPS	The number of frames per second (frame rate) currently used by the camera. The number updates each time the camera has received 50 frames.
Resolution	The resolution of the camera.

Name	Description
Frame count	The number of frames received from the camera since the Recording Server service was last started.
Received KB	The number of kilobytes sent the by camera since the Recording Server service was last started.
Offline	Indicates the number of times the camera has been offline due to an error.

Download Manager

The Download Manager lets you manage which XProtect Professional-related features your organization's users can access from a targeted welcome page on the surveillance system server. You access the Download Manager from Windows' **Start** menu: Select **All Programs** > **Milestone XProtect Download Manager** > **Download Manager**.

Examples of user-accessible features

- **The Smart Client**. With a regular Internet Explorer browser, users connect to the surveillance server where they are presented with a welcome page. From the welcome page, users download the Smart Client software and install it on their computers.
- **Language packs**, which let users add additional language versions to their existing Smart Clients. Users download such language packs from the welcome page.
- **Various plug-ins**. Downloading such plug-ins can be relevant for users if your organization uses add-on products with the XProtect Professional system.

The welcome page

The welcome page has links to downloads of various features. It is available in a number of languages; users select their required language from a menu in the top right corner of the welcome page.

To view the welcome page, simply open an Internet Explorer browser (version 6.0 or later) and connect to the following address:

`http://[surveillance server IP address or hostname]`

If the Image Server service has been configured with a port number other than the default port 80 (you configure this as part of the server access properties), users must specify the port number as well, separated from the IP address or hostname by a colon:

`http://[surveillance server IP address or hostname]:[port number]`

The content of the welcome page is managed through the Download Manager; therefore the welcome page will often look different in different organizations.

Initial look

Immediately after you install XProtect Professional, the welcome page will provide access to a Smart Client in all languages. In addition, the Smart Client can be downloaded in 32- or 64-bit if you run a 64-bit operating system and in 32-bit if you run a 32-bit operating system.

This initial look of the welcome page is automatically provided through the Download Manager's default configuration—for more information, see **Default configuration of Download Manager** in the following.

Default configuration of Download Manager

The Download Manager has a default configuration. This ensures that your organization's users can access standard features without the surveillance system administrator having to set up anything.

The Download Manager configuration is represented in a tree structure.

Download Manager's Tree Structure Explained

- The **first level of the tree structure** simply indicates that you are working with a XProtect Professional system.
- The **second level** indicates that this is the default setup.
- The **third level** refers to the languages in which the welcome page is available. In the example, the welcome page is available in a dozen languages (English, Arabic, Danish, Dutch, French, and more).
- The **fourth level** refers to the features which are—or can be made—available to users. For example, these features could be limited to the Smart Client.
- The **fifth level** (**5**) refers to particular versions of each feature, for example, version 4.0, 32-bit, etc. which are—or can be made—available to users.
- The sixth **level** (**6**) refers to the language versions of the features which are—or can be made—available to users. For the Smart Client, which is only available with all languages embedded, the only option is **All Languages**.

The fact that only standard features are initially available helps reduce installation time and save space on the server. There is simply no need to have a feature or language version available on the server if nobody is going to use it.

You can, however, easily make more features and/or languages available as required. See **Making new features available** in the following for more information.

Making new features available

Making new features—plug-ins or special language versions—available to your organization's users involves two steps: first install the required features on the surveillance system server and then use the Download Manager to fine-tune which features you want available on the various versions of the welcome page.

Installing new features on the server

1. If the Download Manager is open, close it before installing new features on the server.

2. Download the relevant installation file(s) to to C:\Program Files\Milestone\Milestone Surveillance\[relevant subfolder, often **Installers** or relevant language folder]. Double-click the required installation (.exe) file.

3. When a new feature has been installed on the surveillance system server, you will see a confirmation dialog. If required, you can open the Download Manager from the dialog.

Making new features available through the Download Manager

When you have installed new features, by default they will be selected in the Download Manager, and immediately be available to users via the welcome page.

You can always show or hide features on the welcome page by selecting or clearing check boxes in the tree structure.

Tip: You can change the sequence in which features and languages are displayed on the welcome page by simply dragging items and dropping them in the required position.

Hiding and removing features

You can remove features in several ways:

- You can **hide features** from the welcome page by clearing check boxes in the Download Manager's tree structure. In that case, the features will still be installed on the surveillance system server, and by selecting check boxes in the tree structure you can quickly make the features available again.

- You can **remove features** which have previously been made available through the Download Manager. This will remove the installation of the features on the surveillance system server. The features will disappear from the Download Manager, but installation files for the features will be kept in the surveillance system server's **Installers** or relevant language folder, so you can re-install them later if required.

  1. In the Download Manager, click **Remove features...**

  2. In the **Remove Features** window, select the features you want to remove.

  3. Click **OK** and then click **Yes**.

Updates

Milestone Systems A/S regularly releases service updates for its products, offering improved functionality and support for new devices.

If you are a surveillance system administrator, we recommend that you check www.milestonesys.com for updates at regular intervals in order to make sure you are using the most recent version of your surveillance software.

Before you start

Minimum system requirements

Surveillance system server:

Name	Description
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*) • Windows 7 Ultimate (32-bit or 64-bit*).
CPU	Intel® Pentium® 4, 2.4 GHz or higher (CoreTM 2 recommended).
RAM	Minimum 2 GB (4 GB or more recommended).
Network	Ethernet (1 Gbit recommended).
Graphics adapter	AGP or PCI-Express, minimum 1024 x 768, 16-bit colors.
Hard disk type	E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster).
Hard disk space	Minimum 1 GB free hard disk space available, excluding space needed for recordings.
Software	• Microsoft .NET 4.0 Framework. • DirectX 9.0 or newer. • Windows Help (WinHlp32.exe) All can be downloaded from http:// www.microsoft.com/downloads/.

XProtect Smart Client

Name	Description
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*) • Windows 7 Ultimate (32-bit or 64-bit*).
CPU	Intel Core2™ Duo, minimum 2.4 GHz or higher (more powerful CPU recommended for Smart Clients running high number of cameras and multiple views and displays).
RAM	Minimum 1 GB (higher RAM recommended for 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 1024 x 768 (1280 x 1024 recommended), 16-bit colors.
Hard disk space	Minimum 1 GB free hard disk space available.
Software	• Microsoft .NET 4.0 Framework. • DirectX 9.0 or newer.

Administrator rights

When you install XProtect Professional, it is important that you have administrator rights on the computer that should run XProtect Professional. If you only have standard user rights, you cannot configure the surveillance system.

Important port numbers

XProtect Professional uses particular ports when communicating with other computers, cameras, etc.

Make sure that the following ports are open for data traffic on your network when you use XProtect Professional:

Name	Description
Port 20 and 21 (inbound and outbound)	Used for FTP traffic. FTP (File Transfer Protocol) is a standard for exchanging files across networks. FTP uses the TCP/IP standards for data transfer, and is often used for uploading or downloading files to and from servers.
Port 25 (inbound and outbound)	Used for SMTP traffic. SMTP (Simple Mail Transfer Protocol) is a standard for sending e-mail messages between servers. This port should be open since, depending on configuration, some cameras may send images to the surveillance system server via e-mail.
Port 80 (inbound and outbound)	Used for HTTP traffic between the surveillance server, cameras, and Smart Client, and the default communication port for the surveillance system's Image Server service.
Port 554 (inbound and outbound)	Used for RSTP traffic in connection with H.264 video streaming.
Port 1024 (outbound only)	Used for HTTP traffic between cameras and the surveillance server.
Port 1234 (inbound and outbound)	Used for event handling.
Port 1237 (inbound and outbound)	Used for communication with the XProtect Central add-on product (if used by your organization).
Port 22331 (inbound and outbound)	Used for communication with the Event Server service.

Your organization may also have selected to use any other port numbers, for example if you have changed the server access (on page 172) port from its default port number (80) to another port number.

Virus scanning information

Virus scanning uses a considerable amount of system resources on scanning all the data which is being archived or used by the Download Manager. The scanning process may temporarily lock each file it scans, which can further impact system performance negatively.

If allowed in your organization, you should therefore disable any virus scanning of affected areas (such as camera databases, etc.) on the XProtect Professional server as well as on any archiving destinations.

Time server recommended

All images are time-stamped by XProtect Professional upon reception, but since cameras are separate units which may have separate timing devices, power supplies, etc., camera time and XProtect Professional system time may not correspond fully, and this may occasionally lead to confusion.

If your cameras supports timestamps, we recommend that you auto-synchronize camera and system time through a time server for consistent synchronization.

For information about how to configure a time server, try searching www.microsoft.com (see http://www.microsoft.com/ - http://www.microsoft.com/) for **time server**, **time service**, or similar.

Install and upgrade

About installing surveillance server software or XProtect Smart Client silently

If you are a surveillance system administrator, you can deploy the XProtect Smart Client or XProtect Professional to users' computers by using tools such as Microsoft Systems Management Server (SMS). Such tools let you build up databases of hardware and software on local networks. You can then use the databases for distributing and installing software applications, such as the XProtect Smart Client, over local networks.

Install your surveillance server software

Do not install XProtect Professional on a mounted drive. A mounted drive is a drive that is attached to an empty folder on an NTFS (NT File System) volume, with a label or name instead of a drive letter. If you use mounted drives, critical system features may not work as intended. You will, for example, not receive any warnings if the system runs out of disk space.

Prerequisites: Shut down any existing surveillance software. If you are upgrading, read Upgrade from a previous version (on page 28) first.

1. Run the installation file. Depending on your security settings, you may receive one or more security warnings. Click the **Run** button if you receive a warning.
2. When the installation wizard starts, select language for the installer and then click **Continue**.
3. Select if you want to install a trial version of XProtect Professional or indicate the location of your license file.
4. Read and accept the license agreement, and indicate if you want to participate in the Milestone data collection program.
5. Select **Typical** or **Custom** installation. If you select **Custom** installation, you can select application language, which features to install and where to install them.
6. Let the installation wizard complete.

IMPORTANT: If you are installing on a Windows Server 2003 and installation fails, installing a Microsoft hotfix might solve the issue and allow you to complete your XProtect Professional installation. The Microsoft hotfix can be downloaded here:

http://www.microsoft.com/downloads/en/details.aspx?FamilyId=8EFFE1D9-7224-4586-BE2B-42C9AE5B9071&displaylang=en
http://www.microsoft.com/downloads/en/details.aspx?FamilyId=8EFFE1D9-7224-4586-BE2B-42C9AE5B9071&displaylang=en

When you have installed the hotfix, restart the XProtect Professional installation.

You can now begin to configure your XProtect Professional through its Management Application. See more under Get your system up and running (on page 31).

Install silently

1. Locate the Smart Client installation program (.exe) file - **MilestoneXProtectSmart Client.exe** or **MilestoneXProtectSmart Client_x64.exe** for 32-bit and 64-bit versions respectively. You find the file in a subfolder under the folder **httpdocs**. The **httpdocs** folder is located under the folder in which your Milestone surveillance software is installed.

   The path is typically:
   C:\Program Files (x86)\Milestone\Milestone Surveillance\httpdocs\Smart Client Installer\[version number] [bit-version]\All Languages\en-US

   For example:
   C:\Program Files (x86)\Milestone\Milestone Surveillance\httpdocs\Smart Client Installer\6.0a (32-bit)\All Languages\en-US

2. Run a silent installation using one of the following two options:

a Run with default parameter settings:

To run a silent installation using the default values for all parameters, start a command prompt (cmd.exe) in the directory where the installation program is located and execute following command:

For XProtect Smart Client installation:

>MilestoneXProtectSmart Client.exe -–quiet

For XProtect Professional installation:

> MilestoneXProtectXProtect ProfessionalInstaller.exe --quiet

This will perform a quiet installation of the XProtect Smart Client/XProtect Professional using default values for parameters such as target directory etc. To change the default settings, please see next topic.

b Customize default parameters using an xml argument file as input:

In order to customize the default installation settings, an xml file with modified values must be provided as input. In order to generate the xml file with default values, open a command prompt in the directory where the installation program is located and execute following command:

For XProtect Smart Client:

> MilestoneXProtectSmart Client.exe --generateargsfile=args.xml For XProtect Professional:

> MilestoneXProtectXProtect ProfessionalInstaller.exe --generateargsfile=args.xml

Open the generated args.xml file, using for example Notepad.exe, and perform any changes needed. Then, in order to run silent installation using these modified values, execute following command in the same directory
For XProtect Smart Client:

>MilestoneXProtectSmart Client.exe --arguments=args.xml --quiet

For XProtect Professional:

> MilestoneXProtectXProtect ProfessionalInstaller.exe --arguments=args.xml --quiet

Upgrade

About upgrading

When you upgrade from one product to a more advanced product, you get access to new functionality, but you can also expand the use of the functionality that were already available. Your settings from the previous product are transferred to the new product. This means that you will sometimes need to update the settings of your old product in order to make use of the expanded functionality.

For further information about the various differences between products, check the Milestone website at www.milestonesys.com.

Example: If you upgrade from XProtect Go to XProtect Professional, you should, among other things, be aware of:

- Smart Client: In XProtect Go, only one Smart Client can be connected at a time. When you upgrade, you get the possibility of connecting more Smart Clients. Since you come from XProtect Go, the Management Application is set to only allow one Smart Client connection at a time. You can change this setting **manually** in the Management Application. In general, you will gain the full use of Smart Client functionality when upgrading.

- Number of Cameras: XProtect Go allows you to use up to eight cameras at the same time, while XProtect Professional lets you use many more. The number of cameras added will be inherited by the upgraded product, but you must, of course, add any additional cameras to the Management Application yourself.

Upgrade from a previous version

You can upgrade your entire XProtect Professional system configuration from one XProtect Professional version to another. The following information applies if you upgrade from one XProtect Professional version to another and if you upgrade to XProtect Professional from a streamlined product in the XProtect product range.

Back up your current configuration

When you install the new version of XProtect Professional, it inherits the configuration from your previous version.

We recommend that you make regular backups of your server configuration as a disaster recovery measure. You should also do this when you upgrade your server. While it is rare that you lose your configuration (cameras, schedules, views, etc), it **can** happen under unfortunate circumstances. Fortunately, it takes only a minute to back up your existing configuration.

IMPORTANT: If you are upgrading from XProtect Professional 6.5 or earlier, you must back up your configuration before you upgrade.

The following describes backing up XProtect Professional 6.5 or earlier. If you need information about how to back up configuration for XProtect Professional7.0 or newer, see Back up system configuration (on page 200).

1. Create a folder called **Backup** on a network drive, or on removable media.
2. On the XProtect Professional server, open **My Computer**, and navigate to the XProtect Professional installation folder.
3. Copy the following files and folders into your **Backup** folder:
   - All configuration (.ini) files
   - All scheduling (.sch) files
   - The file **users.txt** (only present in a few installations)
   - Folders with a name ending with **...ViewGroup** and all their content

Note that some of the files/folders may not exist if upgrading from old software versions.

If you installed your XProtect Professional as a custom version to a non-default file-path, make a backup of your existing configuration and restore it to a new installation folder called **[relevant folder]\Milestone Surveillance**. When you run the installer, select **Custom** installation and when you are prompted for an installation folder, select the **[relevant folder]** created for restoring.

Remove the current version

You do not need to manually remove the old version of XProtect Professional before you install the new version. The old version is removed when you install the new version. Note, however, XProtect Basis+ versions earlier than 6.0 must be removed manually before installing the new version.

Video device drivers

Video device drivers are installed automatically during the initial installation of your XProtect Professional system. New versions of video device drivers, known as XProtect Device Pack, are released from time to time and made available for free on the Milestone website.

We recommend that you always use the latest version of video device drivers. When you update video device drivers, you can install the latest version on top of any version you may have installed.

IMPORTANT: When you install new video device drivers, your system cannot communicate with camera devices from the moment you begin the installation until the moment installation is complete and you have restarted the Recording Server service. Usually, the process takes no longer than a few minutes, but it is highly recommended that you perform the update at a time when you do not expect important incidents to take place.

1. On the XProtect Professional server on which you want to install the new video device drivers version, shut down any running surveillance software, including any running Recording Server service.
2. Run the XProtect Device Pack installation file and follow the wizard.
3. When the wizard is complete, remember to start the Recording Server service again.

If you use the Add Hardware Devices Wizard's Import from CSV File (on page 51) option, you must—if cameras and server are offline—specify a **HardwareDriverID** for each hardware device you want to add. To view a current list of IDs, view the release notes for the XProtect Device Pack used in your organization. Alternatively, visit the Milestone website for the latest information.

Removal

To remove the entire XProtect Professional surveillance system (that is the surveillance server software and related installation files, the video device drivers, the Download Manager and the Smart Client) from your server, follow the normal Windows procedure for uninstalling programs (see the Windows Help for more information).

Individual components, such as Smart Client and video device drivers, can also be removed individually using the normal Windows procedure for uninstalling programs.

If you remove your XProtect Professional surveillance system, your recordings will not be removed. They will remain on the server even after the server software has been removed. Likewise, the XProtect Professional configuration files will remain on the server. This allows you to reuse your configuration if you install XProtect Professional again at a later time.

Getting started

Get your system up and running

This checklist outlines the tasks typically involved when you set up a working XProtect Professional system. Note that although information is presented as a checklist, a completed checklist does not in itself guarantee that the system matches the exact needs of your organization. To make the system match the needs of your organization, it is highly recommended that you monitor and adjust the system once it is running.

For example, it is often a good idea to spend time on testing and adjusting the motion detection sensitivity settings for individual cameras under different physical conditions (day/night, windy/calm, etc.). Do this once the system is running. The setup of events and associated actions typically also depends on your organization's needs.

You can print and use this checklist as you go along.

Verify initial configuration of cameras and other hardware devices

Before doing anything on XProtect Professional, make sure the hardware devices (cameras, video encoders, etc.) that you want to use are correctly installed and configured with IP addresses, passwords, etc. as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the network and XProtect Professional.

Register your XProtect Professional software

This step may not be required; your XProtect Professional vendor often takes care of the process for you.You must first register your software and next activate your licenses. See Manage licenses **(see "**About activating licenses**" on page 35).**

Install XProtect Professional

See Install surveillance server software **(see "**Install your surveillance server software**" on page 26).** If you are upgrading an existing version of XProtect Professional, see Upgrade from a previous version **(on page 28).**

Open the Management Application

See Access the Management Application**.**

Add hardware devices in XProtect Professional

XProtect Professional can quickly scan your network for relevant hardware devices (cameras, video encoders, etc.), and add them to your system. See Add hardware devices (see "The Add Hardware Devices wizard" on page 44).

Configure cameras in XProtect Professional

You can specify a wide variety of settings for each camera connected to your XProtect Professional system. Settings include video format, resolution, motion detection sensitivity, where to store and archive (see "About archiving" on page 143) recordings, any PTZ (Pan/Tilt/Zoom) preset positions, association with microphones , speakers etc. See About video and recording configuration (on page 77).

Configure events, input and output

If required, system events, for example based on input from sensors, can be used to automatically trigger actions in XProtect Professional. Examples of actions: starting or stopping recording on cameras, switching to a particular video frame rate, making PTZ cameras move to specific preset positions. Events can also be used to activate hardware output, such as lights or sirens. See Overview of events.

Configure scheduling

When do you want to archive? Do you want some cameras to transfer video to XProtect Professional at all times, and other cameras to transfer video only within specific periods of time, or when specific events occur? With the scheduling feature, you can specify this. You can also specify when you want to receive notifications from the system. See Configure general scheduling and archiving (on page 149) and Configure camera-specific schedules (on page 79).

Configure clients' access to XProtect Professional

A number of different client applications (see About clients) is included with XProtect Professional. You can specify whether you want clients to access the XProtect Professional server from the internet, how many clients you want to be able to connect simultaneously, etc. (see Configure server access (on page 171)).

Configure master/slave servers

This step is only required if you want to run several XProtect Professional servers together. A master/slave setup allows you to combine several XProtect Professional servers and thereby extend the number of cameras you can use beyond the maximum allowed number of cameras for a single server. In such a setup, clients will still have a single point of contact: they connect to the master server but also get access, transparently, to cameras and recordings on the slave servers. See Configure master and slave servers (on page 174).

Configure users

Now specify who should be able to access your XProtect Professional system, and how. Do you want password protection for the Management Application? Who should have client access, and with which rights? See Configure User Access wizard (on page 68), Add basic users (on page 177), Add user groups (on page 178) and Configure user and group rights (on page 179).

The above list represents the configuration steps that most administrators are likely to cover. Additional configuration is of course possible, for example if your organization wants to use the Matrix (see "Configure Matrix" on page 158)video sharing feature or similar.

Note that the behavior of the Management Application can be customized (see "Change/restore Management Application behavior" on page 41). Descriptions here are, however, always based on the Management Application's default behavior.

Use the built-in help system

To use the XProtect Professional built-in help system, click the **Help** button in the Management Application's toolbar. Alternatively, press the F1 key on your keyboard.

The help system opens in a separate window and allows you to easily switch between help and XProtect Professional itself. The help system is context-sensitive. This means that when you press F1 for help while you work in a particular XProtect Professional dialog, the help system displays help that matches that dialog.

Navigating the built-in help system

To navigate between the contents of the help system, use the help window's tabs: **Contents**, **Search**, and **Favorites,** or use the links inside the help topics.

- Contents Tab: Navigate the help system based on a tree structure. Many users are familiar with this type of navigation from, for example, Windows Explorer.
- Search Tab: Search for help topics that contain particular terms of interest. For example, you can search for the term **zoom** and every help topic that contains the term **zoom** is listed in the search results. When you double-click a help topic title in the search results list, the required topic opens.
- Favorites Tab: Build a list of your favorite help topics. Whenever you find a help topic of particular interest to you, add the topic to your favorites list. You can then access the topic with a single click—also if you close the help window and return to it later.

Help topics contain various types of links, notably so-called expanding drop-down links. When you click such a link, detailed information is displayed immediately below the link itself and the content of the topic expands. Expanding drop-down links help save space.

Tip: To quickly hide all texts from expanding drop-down links in a help topic, click the title of the topic on the help system's **Contents** tab.

Printing help topics

To print a help topic, navigate to the required topic and click the help window's **Print** button. A dialog box may ask you whether you wish to print the selected topic only or all topics under the selected heading; when this is the case, select **Print the selected topic** and then click **OK**.

Tip: When you print a help topic, it 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 to include it when you print. This allows you to create targeted printouts that contain exactly the amount of information you require.

Licenses

About licenses

When you purchase XProtect Professional, you also purchase a certain number of licenses for device channels. Device channels are typically cameras but could also be dedicated input/output boxes. One device channel license enables you to run one camera or one dedicated input/output box. You can use and define an unlimited number of microphones, , speakers inputs, and outputs.

When you have installed the various XProtect Professional components, configured the system, and added recording servers and cameras through the Management Application, the surveillance system initially runs on temporary licenses that need to be activated before a certain period ends. This is called the grace period.

If grace periods have expired on one or more of your devices and no licenses have been activated, recording servers and cameras do not send data to the surveillance system. We therefore recommend that you activate your licenses (see "About activating licenses" on page 35) before you make final adjustments to your system and its devices.

If you want to add—or have already added—more device channels than you currently have licenses for, you must buy additional licenses before the cameras can send data to your XProtect Professional system.

To get additional licenses for XProtect Professional, contact your vendor, or visit www.milestonesys.com to log into the software registration service center. When your license file (.lic) is updated, you can activate your licenses. See Manage licenses for more information on activating.

Tip: If short of licenses—until you get additional ones—you can disable some less important cameras to allow some of the new cameras to run instead. To disable or enable a camera, expand **Hardware Devices** in the Management Application's navigation pane. Then select the relevant hardware device, right-click the required camera, and then select **Enable** or **Disable**.

Which devices require a license?

About replacing cameras

You can replace a camera that is licensed in XProtect Professional and have the new camera activated and licensed instead. The total number of purchased device channels corresponds to the total number of cameras that can run on the surveillance system simultaneously. If you remove a camera from a recording server, you also free a license.

When you replace a camera, you must use the Management Application Replace Hardware Device wizard (see "About the Replace Hardware Device wizard" on page 71) to map all relevant databases of cameras, microphones, inputs, outputs, etc. Remember to activate the license once you are finished.

Overview of license information (on page 35)

About getting additional licenses

If you want to add—or have already added—more device channels than you currently have licenses for, you must buy additional licenses before the cameras can send data to your XProtect Professional system.

To get additional licenses for XProtect Professional, contact your vendor, or visit www.milestonesys.com to log into the software registration service center. When your license file (.lic) is updated, you can activate your licenses. See Manage licenses for more information on activating.

Overview of license information

You get an excellent overview of your XProtect Professional licenses from the Management Application's navigation pane. Expand **Advanced Configuration** and select **Hardware Devices**. This presents you with the **Hardware Device Summary** table.

Name	Description
Hardware Device Name	Hardware devices (typically cameras but could also be dedicated input/output boxes).
License	Licensing status of your hardware devices. Can be either **Licensed**, **[number of] day(s) grace, Trial,** or **Expired**.
Video Channels	Number of available video channels on your hardware devices.
Licensed Channels	Number of video channels on each of your hardware devices for which you have a license.
Speaker Channels	Number of available speaker channels on your hardware devices.
Microphone Channels	Number of available microphone channels on your hardware devices.
Address	http addresses of your hardware devices.
WWW	Links to http addresses of your hardware devices.
Port	Port used by your hardware devices.
Device Driver	Names of device drivers associated with your hardware devices.

You can activate licenses online or offline. On the Management Application's toolbar**,** click **File** and either **Activate License Online** or **Manage License Offline**.

Cameras (or dedicated input/output boxes) for which you are missing a license will not send data to the surveillance system. Cameras added after all available licenses are used are unavailable.

About activating licenses

When you purchase XProtect Professional, you receive a temporary license file (.lic) including a Software License Code (SLC). You must use this temporary license file when you install your system.

Also, in order to get your permanent license, you should register your SLC before you activate licenses.

When you have registered your SLC, you can activate your licenses in two ways: **online** or **offline**.

Tip: If the computer that runs the Management Application has internet access, use online activation.

You cannot activate more licenses than you have bought. If you have added more cameras than you have licenses for, you must buy additional licenses before you can activate them.

Tip: To get an overview of your licenses, go to the Management Application's navigation pane, expand **Advanced Configuration,** select **Hardware Devices** and view your **Hardware Device Summary** table.

In the following examples, it is assumed that XProtect Professional is installed with a temporary license (.lic) file.

About activating licenses after grace period

If the grace period is exceeded before activation, all cameras that are not activated within the given period become unavailable and cannot send data to the surveillance system.

If you exceed the grace period before you activate a license, the license is not lost. You can activate the license as usual.

Configuration, added cameras, and other settings are not removed from the Management Application if a license is activated too late.

Register SLC

If you do not have your SLC, contact your vendor.

1. Go to the Milestone website at www.milestonesys.com, and click the Software registration link in the menu.
2. Log in to the Software Registration Service Center with your user name (e-mail address) and password.

   Tip: If you have not used the Software Registration Service Center before, click the **New to the system?** link, and follow the instructions for registering yourself as a user, then log into the Software Registration Service Center by using your registered user name and password.
3. In the Software Registration Service Center, click the **Add SLC** link.
4. Type your SLC. Confirm that you want to add the SLC to your account, and then click **OK**.
5. Once your SLC has been added, click the **Main menu** link.
6. Click the **Logout** link to log out of the Software Registration Service Center.

   Tip: If you plan to use online activation when you activate your licenses, make sure you use the same user name (e-mail address) and password that you used when you registered the SLC.

Activate License - Online

Precondition

Add at least one device (see "The Add Hardware Devices wizard" on page 44) to your XProtect Professional system.

This starts the grace period of 30 days for the device in question. You must activate a license for the device before the end of the grace period.

Activate a license

On the Management Application's toolbar, click **File**, **Activate License Online**.

1. Specify how many licenses you want for each device, and then click **OK.**
2. Next:
   - If you are **an existing user**, enter your user name and password to log into the Software Registration Service Center.
   - If you are **a new user,** click the **Create new user...** link to set up a new user account in the Software Registration Service Center and then follow the registration procedure. If you have not yet registered your SLC, you must do so, see earlier.
3. When done, click **Activate**.
4. When your temporary license file (.lic) is successfully updated, click **Close**. Your license file (.lic) is now updated and permanent. Updates are visible in your Hardware Device Summary table.

Activate by using this process each time you add a new device.

If you receive an online activation error message

Under rare circumstances, you may receive one of the following error messages during online activation. Should you receive one, the following list of Problems and What to do will help you identify the problem:

- Unable to access license server, Error activating license, License not allowed, Feature not registered, Feature already in use, Failed to login.
  - Problem: Online activation was not possible, either due to a problem on the online activation server itself, a problem with your connection to the online activation server, or to a problem with the specified information (such as username or password).
  - What to do: Contact Milestone Support (support@milestonesys.com), who will investigate the issue for you. If activation has already taken place on another system, activation should not be necessary, as another system is already running with your activated licenses. If you believe that this is wrong, contact Milestone Support (support@milestonesys.com), who will investigate the issue for you.

Activate License - Offline

Precondition

Add at least one device (see "The Add Hardware Devices wizard" on page 44) to your XProtect Professional system.

This starts the grace period of 30 days for the device in question. You must activate a license for the device before the end of the grace period.

Step 1: Export license for activation (offline)

To export a license file with your currently added devices for activation, do the following:

1. On the Management Application's toolbar, click **File**, **Manage License Offline, Export License for Activation.**

2. Specify a file name and a location for the license request (.lrq) file (automatically generated by XProtect Professional). If your computer does not have internet access, use external, removable data storage.

3. If needed, move the external data storage with the .lrq file to a computer with internet access. Open an internet browser and go to Milestone's website at www.milestonesys.com. Select **Software Registration** from the top menu. If you have used the Software Registration Service Center before, log in with your e-mail and password. Otherwise, click **New to the System?** to create a new user account and register your SLC.

1. Under **Current SLCs**, select the SLC**.**

   2. In the menu for SLC properties, use the **Upload LRQ** function to upload the generated .lrq file.

4. Next, you receive the updated permanent license file (.lic) from Milestone via e-mail. Save it to a location accessible from the Management Application.

Step 2: Import license (offline)

When you have received your permanent license file (.lic) from Milestone via e-mail and saved it to a location accessible from the Management Application, you are ready to import it to your surveillance system.

Tip: The following procedure is also used for changing SLC/licenses.

1. On the Management Application's toolbar, click **File**, **Manage License Offline**, **Import License**, and select your saved .lic file to import it**.**

2. When the permanent license file is successfully imported, click **OK.**

Activate by using both step 1 and 2 in this process each time you add a new device.

Change SLC

If you need to change your SLC and you have received a new permanent license file (.lic) from Milestone via e-mail and saved it to a location accessible from the Management Application, you are ready to import it to your surveillance system.

1. On the Management Application's toolbar, click **File**, **Manage License Offline**, **Import License**, and select your saved .lic file to import it**.**

2. When the new permanent license file is successfully imported, click **OK.**

About replacing cameras

You can replace a camera that is licensed in XProtect Professional and have the new camera activated and licensed instead. The total number of purchased device channels corresponds to the total number of cameras that can run on the surveillance system simultaneously. If you remove a camera from a recording server, you also free a license.

When you replace a camera, you must use the Management Application Replace Hardware Device wizard (see "About the Replace Hardware Device wizard" on page 71) to map all relevant databases of cameras, microphones, inputs, outputs, etc. Remember to activate the license once you are finished.

Application settings

About privacy options

To help Milestone improve the usability and customer experience of XProtect Professional, you were presented with the option **Sign me up for the Customer Experience Improvement Program** during the installation of XProtect Professional.

- If you **declined**, **no software** contributing statistical information is included in your XProtect Professional installation.
- If you **accepted**, a cookie issuing a Global Unique IDentifier (GUID) is included as part of your XProtect Professional installation. As a result, XProtect Professional anonymously collects relevant information about your installation and operation of XProtect Professional at regular intervals. See the following for a detailed list of what is collected.

Also, if you accepted, a setting makes it possible to turn the collection of information off or on as needed.

What information is collected from XProtect Professional?

No personal information about the equipment (PC) XProtect Professional is installed on, or about any of the recordings you make.

This is collected:

- The country where the software is installed
- Hardware platform information, such as operating system version, Microsoft .NET framework version, CPU type, and memory size
- XProtect Professional version information
- Information about the number, and type of hardware devices (cameras) used with XProtect Professional
- Information on which XProtect Professional features are used, and how often they are used
- Information about which XProtect Professional menus and buttons are activated, and how often they are used
- Execution time for specific operations in your XProtect Professional installation
- Error reports and exceptions generated by your XProtect Professional installation.

When is information collected from XProtect Professional?

Information is only collected when the Management Application or Smart Client is active.

You can disable the automatic collection of information by either removing XProtect Professional or by disabling it using the Management Application (see earlier for details on how).

How does Milestone protect collected information?

Milestone is committed to protecting the security of the information collected from XProtect Professional installations.

Milestone has implemented security measures to help protect against the loss and misuse of data being collected.

The information is stored in a secure server environment that uses firewall and other advanced technologies to prevent interference or unauthorized access from outside intruders.

Disable information collection

1. In the Management Application toolbar, click **Help**, **Privacy Options**.
2. On the **Privacy Options** tab, clear the Yes, I would like to improve Milestone XProtect Professional information collection check box.
3. Click **OK**.

Change/restore Management Application behavior

You can change the way the Management Application behaves. For example, by default, the Management Application asks you to confirm many of your actions. If you feel this is not necessary, you can change the behavior of the Management Application so it will not ask you again.

1. In the Management Application's menu bar, select **Application Settings** > **Application Behavior...**
2. For each action, you can now select how the Management Application should behave. Examples:
   - When you attempt to delete a hardware device, should the Management Application ask you to confirm that you want to delete the hardware device, or should it delete the hardware device straight away without asking?
   - You can use a maximum of 64 cameras at a time on a single XProtect Professional server. If you add more than 64, should the Management Application warn you or not?

   Note that selectable behavior may vary, depending on the type of action.
3. Click **OK**.
4. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Tip: You can quickly restore default settings by clicking the button below the behavior list.

Change language

The Management Application is available in several languages. To change the language of the Management Application:

1. Go to the Management Application's menu bar and select **Application Settings** and then **Application Behavior**. In the dialog, click **Language**. This will display a drop down list that contains the available languages for the Management Application.
2. Select the relevant language that you want to switch to and then click **OK**.

The Management Application must be restarted for the change of language to take effect.

Analytics events settings

To change Analytic Events (see "Overview of events and output" on page 125) settings in the Management Application, go to the Management Application's menu bar and select **Application Settings** and then **Application Behavior**. In the dialog, click **Analytics Events Settings** and fill in the properties (see "Analytics event settings (for alarms) (properties)" on page 42).

Analytics event settings (for alarms) (properties)

Name	Description
Enabled	Lets you enable the analytics event feature
Port	Specify the port used by this service. Default port is 9090. Make sure that relevant VCA tool providers also use this port number. If you change the port number, make sure that VCA tool providers change their port number accordingly.
All network addresses or Specified network addresses	Specify whether events from all IP addresses/host names are accepted, or only events from IP addresses/host names specified in a list—see the following. In the **Address** list specify a list of trusted IP addresses/host names that you want this service to recognize. The list is used to filter incoming data so that only events from certain IP addresses/host names are allowed. Both Domain Name System (DNS) and IPv4 address formats can be used in the list. You have two ways of adding addresses to the list: either manually or by importing an external list of addresses. Manual entering: type the required IP address/host name in the address list. Repeat for each required address.
Import	Click the **Import...** button to browse for the required external list of addresses. To import an external list, the list must be saved in a .txt file format and each IP address or host name must appear on a separate line in the file. Windows' simple text editor Microsoft Notepad is an excellent tool for creating such .txt files.

Event Server settings

Event Server settings let you configure general settings for alarms and specify the following:

Name	Description
Keep closed alarms for	Specify the number of days for which to keep closed alarms, i.e. alarms in the states Closed, Ignore, and Reject. This is normally set to a low number, such as 3 days, but you can define any number up to 99999 days, server space permitting. The value 0 can be used to indicate keep closed alarms indefinitely, server space permitting.
Keep all other alarms for	Specify the number of days for which to keep all other alarms, i.e. alarms not in the states Closed, Ignore, and Reject. This is normally set to a somewhat higher number, such as 30 days, but you can define any number up to 99999 days, server space permitting. The value 0 can be used to indicate keep all other alarms indefinitely, server space permitting. IMPORTANT: Alarms often have associated video recordings. While the alarm information itself is stored on the event server, the associated video recordings are fetched from the relevant surveillance system server when users wish to view them. Therefore, if it is vital to have access to video recordings from all your alarms, make sure that video recordings from relevant cameras are stored on relevant surveillance system servers for at least as long as you intend to keep alarms on the event server.
Keep logs for	Specify the number of days for which to keep the Alarms log. Default is 30 days. The value of 0 will indicate keep log indefinitely (server space permitting).
Log server communication	Specify if you want to save a separate log of server communication in addition to the regular log for the number of days specified.

Wizards

The Add Hardware Devices wizard

You add cameras and other hardware devices, such as video encoders, to your XProtect Professional system through the **Add Hardware Devices...** wizard. If microphones or speakers are attached to a hardware device, they are automatically added as well.

You can use up to 64 cameras per XProtect Professional server. Note that, if required, it is possible to add more cameras than you are allowed to use. If you use video encoder devices on your system, bear in mind that many video encoder devices have more than one camera connected to them. For example, a fully used four-port video encoder will count as four cameras.

The wizard offers you four different ways of adding cameras:

Name	Description
Express (recommended)	Scans your network for relevant hardware devices, and helps you quickly add them to your system. To use the Express method, your XProtect Professional server and your cameras must be on the same layer 2 network, that is a network where all servers, cameras, etc. can communicate without the need for a router. See Add Hardware Devices wizard - Express (see "Express" on page 45).
Advanced	Scans your network for relevant hardware devices based on your specifications regarding required IP ranges, discovery methods, drivers, and device user names and passwords. See Add Hardware Devices wizard - Advanced (see "Advanced" on page 47).
Manual	Specify details about each hardware device separately. A good choice if you only want to add a few hardware devices, and you know their IP addresses, required user names and passwords, etc. See Add Hardware Devices wizard - Manual (see "Manual" on page 49).
Import from CSV file	Import data about cameras as comma-separated values from a file. An effective method if you are setting up several systems. See Add Hardware Devices Wizard - Import from CSV File (see "Import from CSV file" on page 51).

Express

The Express option scans your network for relevant hardware devices, and helps you quickly add them to your system. With the Express option, the wizard only scans for hardware devices supporting device discovery, and only on the part of your network (subnet) where the XProtect Professional server itself is located.

To use the Express method, **your XProtect Professional server and your cameras must be on the same layer 2 network**; that is a network where all servers, cameras, etc. can communicate without the need for a router. The reason for this is that device discovery relies on direct communication between the XProtect Professional server and the cameras. If you know that routers are used on your network, use the advanced (on page 47) or manual (on page 49) method instead.

When using the Express option, the wizard is divided into these pages:

- Hardware detection and verification (on page 45)
- Overview and names (on page 46)

What is device discovery? Device discovery is a method with which hardware devices make information about themselves available on the network. Based on such information, XProtect Professional can quickly recognize relevant hardware devices, such as cameras and video encoders, and include them in the scan.

Hardware detection and verification

The wizard automatically scans your network for hardware devices, and lists devices real-time as they are detected. All properties on a white background are editable, properties on a **light blue background** cannot be edited.

Wait until the scan is complete. If the scan takes very long, you can stop it with the **Stop Scan** button. The wizard will remember any devices detected up to that point.

When the scan is complete:

1. Go through the list of detected hardware devices to see if it contains unwanted devices. If it does, clear the check box in the **Use** column for each unwanted device.
2. If any hardware devices are missing from the list, verify that the missing hardware devices support device discovery, verify that they are working and connected to the same part of the network as the XProtect Professional server, then click the Rescan button. If hardware devices detected in the first scan cannot be detected in the second scan, the wizard will still remember them.
3. In the User name column, select or type the user name required to access the administrator account on each hardware device. The administrator account gives full access, and XProtect Professional is going to need that for each hardware device. Many organizations use the hardware device manufacturer's default user names for their hardware devices. If that is the case in your organization, select <default> (do not type a manufacturer's default user name as this can be a source of error; trust that XProtect Professional will know the manufacturer's default user name). Other typical user names, such as admin or root are also selectable from the list. If requiring a user name which is not on the list, simply type the required user name.

   Tip: User names you type yourself will subsequently be added to the list, so you can easily select them later.

4. In the Password column, specify the password required to access the administrator account on each hardware device. The administrator account gives full access, and XProtect Professional is going to need that for each hardware device. If the same password is used for all the hardware devices, use the Password field below the list, then click the Set on All button (which becomes available when you specify a password in the field).

   Tip: If you are in doubt about which user name/password to use, ask yourself: Have I previously used a web page to connect to the hardware device and view video? While I did this, was I also able to configure camera settings, such as resolution, etc.? If you can answer yes to both questions, you were probably using the hardware device's administrator account, in which case you will also know the user name/password. If still in doubt, look in the XProtect Device Pack release notes.

5. When you have specified a password for all hardware devices on the list (except unwanted devices), click Next. This will verify that all passwords are correct, and mark each device in the Verified column. If any hardware devices cannot be verified, make sure you have specified the correct passwords.

6. Click Next.The next wizard page provides you with an overview where you can select names for cameras, etc.

Overview and names

The wizard provides you with a detailed overview, listing each camera and microphone/speaker attached to the hardware devices. All properties on a white background are editable, properties on a light blue background cannot be edited.

- All cameras, etc. are by default enabled (selected in the **Enable** column). This means that they can communicate with XProtect Professional. If required, you can disable individual cameras or microphones/speaker, to prevent them from communicating with XProtect Professional.

- All cameras, etc. get automatically generated names based on their type plus a number (examples: Camera 1, Microphone 26). Such names are shown in the **Name** column. If required, you change names manually, or select another name format in the **Auto-generated name format** list.

Name	Description
Device type + number	The default name format. Example: Camera 1.
Custom text - Device type + number	Names will consist of a text of your choice (specified in the **Custom text** field) followed by a dash, type information and a number. Example: Airport Security - Camera 1
Address - Device type + number	Names will consist of the hardware device address followed by a dash, type information and a number. Example: 10.10.123.73 - Camera 1

Name	Description
Custom text - Address - Device type + number	Names will consist of a text of your choice (specified in the Custom text field) followed by a dash, then the hardware device address followed by a dash, type information and a number. Example: Airport Security - 10.10.123.73 - Camera 1
Hardware model - Device type + number	Names will consist of hardware device model information followed by a dash, type information and a number. Example: Axis P1311 - Camera 1
Hardware model - Custom text - Device type + number	Names will consist of hardware device model information followed by a dash, then a text of your choice (specified in the Custom text field), a dash, type information and a number. Example: Axis P1311 - Airport Security - Camera 1
Hardware model - Address - Device type + number	Names will consist of hardware device model information followed by a dash, then the hardware device address, a dash, type information and a number. Example: Axis P1311 - 10.10.123.73 - Camera 1

Tip: Need other name formats? Remember you can change names manually by overwriting all or parts of them in the **Name** column. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

When done, click **Finish**.

Advanced

The Advanced option scans your network for relevant hardware devices based on your specifications regarding required IP ranges, discovery methods, drivers, and device user names and passwords.

When using the Advanced option, the wizard is divided into these pages:

- Device discovery, IP ranges, drivers and authentication (see "IP ranges, drivers and authentication" on page 47)
- Detected and verified hardware devices (on page 49)
- Overview and names (on page 46)

IP ranges, drivers and authentication

All properties on a white background are editable, properties on a **light blue background** cannot be edited.

First specify which IP address ranges you want to scan. By default, the wizard suggests scanning the subnet on which the XProtect Professional server is located. To add additional ranges, or edit existing ones, click the **Add** or **Edit** button as required, then specify:

Name	Description
Start address	Specify the first IP address in the required range.

Name	Description
End address	Specify the last IP address in the required range. The start and end IP address may be identical, allowing you to only scan for a single hardware device.
Use TCP port scanning	If scanning for hardware devices which support TCP/HTTP—most devices do—keep the check box selected.
Perform scanning on port number(s)	Port number(s) on which to scan. If you want to scan on more than one port number, separate them by commas (example: 80,88,90). If you want to scan on a range of port numbers, separate the first and last port number in the range by a colon (example: 80:90 will scan on all ports from 80 up to and including 90). You can also combine individual port numbers and ranges (example: 77,80:90,97,99). Default is port 80. If your hardware devices are located behind a NAT-enabled router or a firewall, you may need to specify a different port number. When this is the case, also remember to configure the router/firewall so it maps the port and IP addresses used by the hardware devices.

Then select which drivers to use when scanning. By default, XProtect Professional will use all known drivers. If your organization only uses certain hardware device makes and/or models, you can achieve faster scanning by selecting only the drives required for those hardware devices. If that is the case, click **Select...**, then in the Select Drivers to Use for IP Scan, select the drivers you want to use when scanning.

Tip: The list of drivers is typically very long, and by default all drivers are selected. With the **Select All** and **Clear All** buttons, you can avoid having to select/clear all check boxes manually.

Next add user name/password combinations required to access the administrator account on each of your hardware devices. The administrator account gives full access, and XProtect Professional will need that for each hardware device.

User name	User name for the hardware device's administrator account. Many organizations use the hardware device manufacturer's default user names for their hardware devices. If that is the case in your organization, select <default> (do not type a manufacturer's default user name as this can be a source of error; trust that XProtect Professional will know the manufacturer's default user name). Other typical user names, such as admin or root are also selectable from the list. If you want a user name which is not on the list, simply type a new user name. **Tip:** User names you enter will subsequently be added to the list, so you can easily select them later.

Password	Password required to access the administrator account. A few hardware devices do not require user name/password for access; if such hardware devices are used in your organization, you can leave the field blank. **Tip:** If you are in doubt about which user name/password to use, ask yourself: Have I previously used a web page to connect to the hardware device and view video? While I did this, was I also able to configure camera settings, such as resolution, etc.? If you can answer yes to both questions, you were probably using the hardware device's administrator account, in which case you will also know the user name/password. If still in doubt, look in the XProtect Device Pack release notes.

Click to add user a name/password combination.

When ready, click **Next**.

Detected and verified hardware devices

The wizard automatically scans your network for hardware devices, and lists devices real-time as they are detected. All properties on a white background are editable, properties on a **light blue background** cannot be edited.

Wait until the scan is complete. If the scan takes very long, you can stop it with the **Stop Scan** button; the wizard will remember any devices detected up to that point.

When the scan is complete:

1. Go through the list of detected hardware devices to see if it contains unwanted devices. If it does, clear the check box in the **Use** column for each unwanted device.
2. If any hardware devices are missing from the list, verify that the missing hardware devices are working and that they are located within the specified IP address ranges, then click the **Rescan** button. If hardware devices detected in the first scan cannot be detected in the second scan, the wizard will still remember them.
3. For all detected hardware devices, XProtect Professional has verified that user names/passwords are correct, and marked each device in the **Verified** column. If any hardware devices could not be verified, make sure you have specified the correct user names/passwords.
4. Click Next.The next wizard page provides you with an overview where you can select names for cameras, etc.

Manual

The Manual option lets you specify details about each hardware device separately. A good choice if you only want to add a few hardware devices, and you know their IP addresses, required user names and passwords, etc.

When using the Manual option, the wizard is divided into these pages:

- Hardware device information, driver selection and verification (see "Information, driver selection and verification" on page 50)
- Overview and names (on page 46)

Information, driver selection and verification

Specify information about each hardware device you want to add. All properties on a white background are editable, properties on a light blue background cannot be edited.

Name	Description
Use	Indicates that you want to include the hardware device in the scan. To begin with, leave the box cleared. Provided XProtect Professional can find a suitable driver for the hardware device, the **Use** box will automatically be selected later.
Address	IP address or host name of the hardware device.
Port	Port number on which to scan. The default is port 80. If a hardware device is located behind a NAT-enabled router or a firewall, you may need to specify a different port number. When this is the case, also remember to configure the router/firewall so it maps the port and IP address used by the hardware device.
User name	User name for the hardware device's administrator account. Many organizations use the hardware device manufacturer's default user names for their hardware devices. If that is the case in your organization, select <default> (do not type a manufacturer's default user name as this can be a source of error; trust that XProtect Professional will know the manufacturer's default user name). Other typical user names, such as admin or root are also selectable from the list. If you want a user name which is not on the list, simply type a new user name. **Tip:** User names you enter will subsequently be added to the list, so you can easily select them later.
Password	Password required to access the administrator account. A few hardware devices do not require user name/password for access; if such hardware devices are used in your organization, you can leave the field blank. **Tip:** If you are in doubt about which user name/password to use, ask yourself: Have I previously used a web page to connect to the hardware device and view video? While I did this, was I also able to configure camera settings, such as resolution, etc.? If you can answer yes to both questions, you were probably using the hardware device's administrator account, in which case you will also know the user name/password. If still in doubt, look in the XProtect Device Pack release notes.
Hardware Driver	Driver to use with the hardware device. If the Auto-detect option is selected, the hardware the XProtect Professional can find the relevant driver automatically.

Name	Description
Verified	Indicates whether access to the hardware device has been verified. Hardware devices for which you have specified correct address, port, user name and password will be verified immediately if you use the auto-detect method. If you select drivers manually, access will be verified once you click Next. **Tip:** To save time, when using the **Auto-detect** feature, you can enter information about other devices while the auto-detection is in progress.

Import from CSV file

This option lets you import data about hardware devices and cameras as comma-separated values (CSV) (see "CSV file format and requirements" on page 52) from a file; a highly effective method if setting up several similar systems.

First select whether cameras and the XProtect Professional server is online (that is having working network connections) or offline.

Then point to the CSV file, and click **Next**.

Add Hardware Devices wizard - Import from CSV File - example of CSV file

The following is an example of a CSV file for use when cameras and server are **online**. It includes the mandatory parameters **HardwareAddress** and **HardwarePort** as well as the optional parameters **HardwarePassword** and **CameraName**.

Note that some of the hardware devices in the example have more than one camera attached. In the example, we therefore use four versions of the **CameraName** parameter (**CameraName1**, **CameraName2**, etc.). Had all the hardware devices only had one camera attached each, we would only have needed **CameraName1**. See Add Hardware Devices Wizard - Import from CSV File (see "Import from CSV file" on page 51) for detailed descriptions of all mandatory and optional parameters.

```
HardwareAddress;HardwarePort;HardwarePassword;CameraName1;CameraName2
;CameraName3;CameraName4

192.168.200.220;80;T0P53cr3T;Reception;;;

192.168.200.221;80;tOpSeCrEt;Staircase A;Fire Exit;Staircase B;Lobby

192.168.200.222;80;TOP53CR3T;Car Park East;;;

192.168.200.223;80;topZKRID;Car Park West;;;

192.168.200.224;80;TopsEcreT;Street Exit;Street Entrance;Station
Exit;Station Entrance

192.168.200.225;80;tercespot;Production Level 2;;;

192.168.200.226;80;TOpsECreT;Production Level 3;;;

192.168.200.227;80;top$!cr!t;Storage Room;;;

192.168.200.228;80;ttooppssecrett;Canteen;;;
```

```
192.168.200.229;80;ecsotpert;Admin Office;;;
192.168.200.230;80;SECRETtop;Annex;;;
192.168.200.231;80;optescter;VIP Parking;;;
192.168.200.232;80;scteropte;Workshop;;;
192.168.200.233;80;scopetetr;Alleyway;;;
192.168.200.234;80;optescter;Demo Room;;;
192.168.200.235;80;oPtEscEr;Meeting Room 1;Meeting Room 2;Meeting
Room3;Meeting Room 4
```

CSV file format and requirements

The CSV file must have a header line (determining what each value on the subsequent lines is about), and subsequent lines must each contain information about one hardware device only.A minimum of information is always required for each hardware device:

Name	Description
HardwareOldMacAddress	The MAC address of the hardware device used in the template configuration. Required format: 12 hex characters without spaces or six groups of two hex characters separated with dashes (-) or colons (:).
HardwreNewMacAddress	The MAC address of the new hardware device to be used in the real configuration. Required format: 12 hex characters without spaces or six groups of two hex characters separated with dashes (-) or colons (:).
HardwareAddress	IP address of the hardware device.
HardwareUsername	User name for hardware device's administrator account. In the extremely rare cases where a particular user name has previously been required for a device, but you now want the user name to be <blank>, you cannot use the CSV file to specify <blank>. The reason is that no information is interpreted as "leave the user name as it currently is." If you need the new user name to be <blank>, you should not change it through the CCV file. Instead, change it as part of the hardware device's network, device type and license properties after you have imported the other changes through the CSV file.

Name	Description
HardwarePassword	Password for hardware device's administrator account. In the extremely rare cases where a particular password has previously been required for a device, but you now want the password to be <blank>, you cannot use the CSV file to specify <blank>. The reason is that no information is interpreted as "œleave the password as it currently is." If you need the new password to be <blank>, you should not change it through the CSV file. Instead, change it as part of the hardware device's network, device type and license properties after you have imported the other changes through the CSV file.
HardwareDeviceName	Name of the hardware device. Name must unique, and must not contain any of the following special characters: **< > & ' " \ / : * ? | [ ]**
HardwareDriverID	If cameras and server are offline—specify a **HardwareDriverID** for each hardware device you want to add. Example: **ACTi ACD-2100 105** indicates that you should use **105** as the ID if adding an ACTi ACD-2100 hardware device.
CameraName[number]	Name of the camera. Must appear as CameraName1, CameraName2, etc. in the header line since a hardware device can potentially have more than one camera attached. Names must be unique, and must not contain any of the following special characters: **< > & ' " \ / : * ? | [ ]**
CameraShortcut[number]	Number for keyboard shortcut access to the camera in the Smart Client. Must appear as CameraShortcut1, CameraShortcut2, etc. in the header line since a hardware device can potentially have more than one camera attached**.** A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits.
GenerateNewCameraGuid[optional number]	Lets you specify whether to generate a new GUID for a camera; this is especially relevant if using a cloned configuration (see "Export and import management application configuration" on page 204) as your template, since all GUIDs are removed from cloned configurations. If specified as, for example, **GenerateNewCameraGuid1**, information relates to a specific camera, otherwise to all cameras attached to the hardware device. Any character means "yes, generate a new GUID."•
PreBufferLength[optional number]	Required length (in seconds) of pre-recording. If specified as, for example, **PreBufferLength1**, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
PostBufferLength[optional number]	Required length (in seconds) of post-recording. If specified as, for example, **PostBufferLength1**, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
RecordingPath[optional number]	Path to the folder in which a camera's database should be stored. If specified as, for example, **RecordingPath1**, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

Name	Description
ArchivePath[optional number]	Path to the folder in which the camera's archived (see "About archiving" on page 143) recordings should be stored. Remember that an archiving path is only relevant if not using dynamic paths for archiving (see "Dynamic path selection" on page 86). If specified as, for example, **ArchivePath1**, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
OldRecordingsNewPath[optional number]	Lets you specify what to do with old recordings in case **RecordingPath** or **ArchivePath** have been changed. If this parameter is not specified, default behavior is **Leave** (see the following). If specified as, for example, **OldRecordingsNewPath1**, information relates to a specific camera, otherwise to all cameras attached to the hardware device. Valid options are: **Delete** (deletes old recordings), **Leave** (leaves old recordings for offline investigation but unavailable for online system), or **Move** (moves old recordings to archive).
OldRecordingsNewMac[optional number]	Lets you specify what to do with old recordings in case a new MAC address has been specified for the hardware device. If this parameter is not specified, default behavior is Leave (see the following). If specified as, for example, OldrecordingsNewMac1, information relates to a specific camera, otherwise to all cameras attached to the hardware device. Valid options are: Delete (deletes old recordings), Leave (leaves old recordings for offline investigation but unavailable for online system), or Inherit (renames all old recording folders according to the new MAC address, thus making them available for the online system).
RetentionTime[optional number]	Required retention time (in minutes). Remember that retention time is the total of recording time plus archiving time. If specified as, for example, **RetentionTime1**, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
MjpegLiveFrameRate[optional number]	Required MJPEG live frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If specified as, for example, **MjpegLiveFrameRate1**, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
MotionSensitivity[optional number]	A value between 0-256; corresponds to using the **Sensitivity** slider when configuring motion detection settings in the Management Application. If specified as, for example, **MotionSensitivity1**, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
MjpegRecordingFrameRate[optional number]	Required MJPEG recording frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If you need to specify a value which includes a decimal separator, use the full stop character (example: 7.62). If specified as, for example, **MjpegRecordingFrameRate1**, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

Name	Description
MotionDetectionThreshold[optional number]	A value between 0-10000; corresponds to using the **Motion** slider when configuring motion detection settings in the Management Application. If specified as, for example, **MotionDetectionThreshold1**, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
MotionDetectionInterval[optional number]	Lets you specify how often motion detection analysis should be carried out on video from the camera. Specified in milliseconds. The interval is applied regardless of the camera's frame rate settings. If specified as, for example, **MotionDetectionInterval1**, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
ServerName	Name with which the XProtect Professional will appear when listed in clients. Name must be unique, and must not contain any of the following special characters: **< > & ' " \ / : * ? | [ ]**
ServerPort	Port number to use for communication between the XProtect Professional server and clients.
OnlineVerification	If this parameter is used, all online hardware devices found using **HardwareOldMacAddress** are updated. All other hardware devices are not updated. Any character means "yes, use online verification.

Existing configuration parameters that are not specified in CSV file will remain unchanged. If a parameter value for an individual camera in the CSV file is empty, the existing parameter value will remain unchanged on that camera.

Most system integrators store hardware device information in spreadsheets like Microsoft Excel, from which they can save the information as comma-separated values in a CSV file. These examples show hardware information in Excel (**1**) and when exported to a CSV file (**2**); note the header lines:

Whichever method is used, the following applies:

- The first line of the CSV file must contain the headers, and subsequent lines must contain information about one hardware device each
- Separators can be commas, semicolons or tabs, but cannot be mixed
- All lines must contain valid values—pay special attention to the fact that camera names, user names, etc. must be unique, and must not contain any of the following special characters: **< > & ' " \ / : * ? | [ ]**
- There is no fixed order of values, and optional parameters can be omitted entirely
- Boolean fields are considered true unless set to 0, false or no
- Lines containing only separators are ignored
- Empty lines are ignored

Even though the CSV file format is generally ASCII only, Unicode identifiers are allowed; **even without Unicode identifiers, the entire file or even individual characters are allowed to be Unicode strings**

If you need to include separator characters in a value—for example if a camera name is Reception; Camera 1—you can encapsulate the value in quotes to indicate that the separator should not be interpreted as separating values in the file. Such quote-encapsulated values are interpreted as they appear. If a separator, a quote or a space is needed in a value, the whole value has to be encapsulated in quotes. Leading and trailing spaces outside the quote-encapsulated value are removed, while spaces inside the quote-encapsulated value are maintained. No characters (except spaces) are allowed outside the quote-encapsulated value. A double quote inside a quote-encapsulated value is interpreted as a single quote. Nested quotes (quotes inside quotes) are not allowed.

Some examples (using semicolon as the separator):

- "camera"; is interpreted as camera
- "cam;""era"; is interpreted as cam;"era
- """camera"""; is interpreted as "camera"
- ""; is interpreted as an empty string
- ...; " cam"" era " ;... is interpreted as **|** cam" era **|** (where the character **|** is not part of the interpretation but only used to show the start and end of the interpretation)
- ""camera; is not valid as there are characters outside the quote-encapsulated value
- "cam" "era"; is not valid as the two quotes are separated with a space and quotes cannot be nested
- "cam"er"a"; is not valid as you cannot nest quotes
- cam"era"; is not valid as there are characters outside the quotes

The Configure Video and Recording wizard

The **Configure Video and Recording** wizard helps you quickly configure your cameras' video and recording properties.

Pages in this wizard:

Video settings and preview

Video settings typically let you control bandwidth, brightness, compression, contrast, resolution, rotation, etc.

All properties on a white background are editable, properties on a **light blue** background cannot be edited.

Use the list in the left side of the wizard window to select a camera and adjust its video settings. Then select the next camera and adjust its settings, and so on. Video settings are to a large extent camera-specific, and must therefore be configured individually for each camera.

Click **Open Settings Dialog** to configure the camera's settings in a separate dialog.

When you change video settings, they are applied immediately. This means that—for most cameras—you are immediately able to see the effect of your settings in a preview image. However, it also means that you cannot undo your changes by exiting the wizard.

For cameras set to use the video formats MPEG or H.264, you are typically able to select which live frame rate to use for the camera.

Video settings may feature an **Include Date and Time** setting. If set to **Yes**, date and time from the camera will be included in video. Note, however, that cameras are separate units which may have separate timing devices, power supplies, etc. Camera time and XProtect Professional system time may therefore not correspond fully, and this may occasionally lead to confusion. As all frames are time-stamped by XProtect Professional upon reception, and exact date and time information for each image is already known, it is recommended that the setting is set to **No**.

Tip: For consistent time synchronization, you may—if supported by the camera—automatically synchronize camera and system time through a time server.

Online schedule

Specify when each camera should be online. An online camera is a camera that transfers video to the XProtect Professional server for live viewing and further processing. The fact that a camera is online will not in itself mean that video from the camera is recorded (recording settings are configured on one of the wizard's next pages).

All properties on a white background are editable, properties on a **light blue** background cannot be edited.

By default, cameras added to XProtect Professional will automatically be online (**Always on**), and you will only need to modify their online schedules if you require cameras to be online only at specific times or events. Note, however, that this default may be changed as part of the scheduling options (on page 153).

For each camera, you are initially able to select between two online schedules:

- **Always on:** The camera is always online.
- **Always off:** The camera is never online.

If these two options are too simple for your needs, use the **Create / Edit...** button to specify online schedules according to your needs, and then select these schedules for your cameras. This way, you can specify whether cameras should be online within specific periods of time, or whether they should start and stop transferring video when specific events occur within specific periods of time.

The **template** can help you configure similar properties quickly. For example, if you have 20 cameras and you want a particular frame rate on all of them, you can simply enter it once in the template, and then apply the template to the 20 cameras.

Name	Description
Apply Template	Select which cameras you want to apply the template for. You then use one of the two **Set** buttons to actually apply the template. **Tip:** To select all cameras in the list, click the **Select All** button.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Apply template on selected cameras	Lets you apply the value from the template to selected cameras.

Live and recording settings Motion-JPEG cameras

This wizard page only appears if one or more of your cameras use the MJPEG video format.

Specify which frame rates to use for each camera. You can also select pre- and post-recording, allowing you to store recordings from periods preceding and following detected motion and/or specified events.

All properties on a white background are editable, properties on a **light blue** background cannot be edited.

Name	Description
Frame Rate	Required average frame rate for video from the camera. Select number of frames, then select the time unit interval (second, minute or hour).
Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

Name	Description
Record on	Lets you select under which conditions video from the camera should be recorded: • **Always:** Record whenever the camera is enabled (see "General" on page 100) and scheduled to be online (see "Online period" on page 155) (the latter allows for time-based recording). • **Never**: Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera. • **Motion Detection**: Select this to record video in which motion (see "Motion detection & exclude regions" on page 110) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected. • **Event**: Select this to record video when an event occurs and until another event occurs. Use of recording on event requires that events have been defined, and that you select start and stop events. **Tip:** If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields. • **Motion Detection & Event**: Select this to record video in which motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.
Pre-recording	You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column. **How does pre- and post-recording work?** XProtect Professional receives video in a continuous stream from the camera whenever the camera is enabled and scheduled to be online. This is what lets you view live video, but it also means that XProtect Professional can easily store received video for a number of seconds in its memory (a.k.a. buffering). If it turns out that the buffered video is needed for pre- or post-recording, it is automatically appended to the recording. If not, it is simply discarded.

Name	Description
Seconds [of pre-recording]	Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving (see "About archiving" on page 143) times. That can be problematic since pre-recording does not work well during archiving.
Post-recording	You can store recordings from periods following detected motion and/or stop events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.
Seconds [of post-recording]	Specify the number of seconds for which you want to record video from after recording stop conditions (that is motion or stop event) are met. Usually, only some seconds of post-recording is required, but you can specify up to 65535 seconds of post-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long post-recording time, you can potentially run into a scenario where your post-recording time spans scheduled or unscheduled archiving times. That can be problematic since post-recording does not work well during archiving.

The **template** can help you configure similar properties quickly. For example, if you have 20 cameras and you want a particular frame rate on all of them, you can simply enter it once in the template, and then apply the template to the 20 cameras.

Name	Description
Apply Template	Select which cameras you want to apply the template for. You then use one of the two **Set** buttons to actually apply the template. **Tip:** To select all cameras in the list, click the **Select All** button.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Apply template on selected cameras	Lets you apply the value from the template to selected cameras.

Live and recording settings MPEG cameras

This wizard page only appears if one or more of your cameras use the MPEG video format.

Specify which frame rate to use for each camera, and whether to record all frames or keyframes only. You can also select pre- and post-recording, allowing you to store recordings from periods preceding and following detected motion and/or specified events.

Note that all of the properties can also be specified individually for each camera.

Name	Description
Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Record Keyframe Only	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. Select the check box if you only want to record keyframes.
Record on	Lets you select under which conditions video from the camera should be recorded: • **Always:** Record whenever the camera is enabled (see "General" on page 100) and scheduled to be online (see "Online period" on page 155) (the latter allows for time-based recording). • **Never**: Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera. • **Motion Detection**: Select this to record video in which motion (see "Motion detection & exclude regions" on page 110) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected. • **Event**: Select this to record video when an event occurs and until another event occurs. Use of recording on event requires that events have been defined, and that you select start and stop events. **Tip:** If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields. • **Motion Detection & Event**: Select this to record video in which motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.

Name	Description
Pre-recording	You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column. **How does pre- and post-recording work?** XProtect Professional receives video in a continuous stream from the camera whenever the camera is enabled and scheduled to be online. This is what lets you view live video, but it also means that XProtect Professional can easily store received video for a number of seconds in its memory (a.k.a. buffering). If it turns out that the buffered video is needed for pre- or post-recording, it is automatically appended to the recording. If not, it is simply discarded.
Seconds [of pre-recording]	Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving (see "About archiving" on page 143) times. That can be problematic since pre-recording does not work well during archiving.
Post-recording	You can store recordings from periods following detected motion and/or stop events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.
Seconds [of post-recording]	Specify the number of seconds for which you want to record video from after recording stop conditions (that is motion or stop event) are met. Usually, only some seconds of post-recording is required, but you can specify up to 65535 seconds of post-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long post-recording time, you can potentially run into a scenario where your post-recording time spans scheduled or unscheduled archiving times. That can be problematic since post-recording does not work well during archiving.

The **template** can help you configure similar properties quickly. For example, if you have 20 cameras and you want a particular frame rate on all of them, you can simply enter it once in the template, and then apply the template to the 20 cameras.

Name	Description
Apply Template	Select which cameras you want to apply the template for. You then use one of the two **Set** buttons to actually apply the template. **Tip:** To select all cameras in the list, click the **Select All** button.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Apply template on selected cameras	Lets you apply the value from the template to selected cameras.

Drive selection

Specify which drives you want to store cameras' recordings on. You can specify separate drives/paths for recording and archiving (see "About archiving" on page 143).

All properties on a white background are editable, properties on a **light blue** background cannot be edited.

Name	Description
Drive	Letter representing the drive in question, for example C:.
Purpose	Select what you want to use the drive for: **Not in use:** Do not use the drive. **Recording:** Only available if the drive is a local drive on the XProtect Professional server. Network drives cannot be used for recording. Use the drive for storing recordings in the regular database for XProtect Professional. **Archiving:** Use the drive for archiving. For archiving, it is generally a good idea to use a drive which has plenty of space. With dynamic path selection for archives (see description in the following), you do not have to worry about drive space. **Rec. & Archiving:** Only available if the drive is a local drive on the XProtect Professional server. Network drives cannot be used for recording. Use the drive for storing recordings in the regular database for XProtect Professional as well as for archiving.
Recording Path	Path to the folder in which the camera's database should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to a folder on a **local** drive. You cannot specify a path to a network drive. If you use a network drive, it is not be possible to save recordings if the network drive becomes unavailable. If you change the recording path, and you have existing recordings at the old location, you are asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them. **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.

Name	Description
Archiving Path	Only editable if not using dynamic paths for archiving (see "About archiving" on page 143). Path to the folder in which the camera's archived recordings should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can specify a path to a local or network drive. If you change the archiving path, and there are existing archived recordings at the old location, you will be asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if you move archived recordings, XProtect Professional will also archive what is currently in the camera database. In case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.
Total Size	Total size of the drive.
Free Space	Amount of unused space left on the drive.
Dynamic path selection for archives	If using this option (highly recommended), you should select a number of different local drives for archiving. If the path containing the XProtect Professional database is on one of the drives you have selected for archiving, XProtect Professional will always try to archive to that drive first. If not, XProtect Professional automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive. Which drive has the most available space may change during the archiving process, and archiving may therefore happen to several archiving drives during the same process. This fact will have no impact on how users find and view archived recordings.
Network Drive	Lets you add a network drive to the list of drives. First specify the network drive, then click **Add** (the button becomes available when you specify a network drive) . Note that network drives cannot be used for recording, only for archiving.
Archiving Times	Specify when you want XProtect Professional to automatically move recordings to your archiving path(s). You can specify up to 24 archiving times per day, with minimum one hour between each one. Select the hour, minute and second values and click the **up** and **down** buttons to increase or decrease values, or simply overwrite the selected value, and then click **Add**. The more you expect to record, the more often you should archive.

Recording and archiving settings

Select recording and archiving (see "About archiving" on page 143) paths for each individual camera.

All properties on a white background are editable, properties on a **light blue** background cannot be edited.

Name	Description
Recording Path	Path to the folder in which the camera's database should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to a folder on a **local** drive. You cannot specify a path to a network drive. If you use a network drive, it is not be possible to save recordings if the network drive becomes unavailable. If you change the recording path, and you have existing recordings at the old location, you are asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them. **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.
Archiving Path	Only editable if not using dynamic paths for archiving (see "About archiving" on page 143). Path to the folder in which the camera's archived recordings should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can specify a path to a local or network drive. If you change the archiving path, and there are existing archived recordings at the old location, you will be asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if you move archived recordings, XProtect Professional will also archive what is currently in the camera database. In case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.
Retention Time	Total amount of time for which you want to keep recordings from the camera (that is recordings in the camera's database as well as any archived recordings). Default is 30 days. Note that the retention time covers the **total** amount of time you want to keep recordings for. In earlier XProtect Professional versions, time limits were specified separately for the database and archives.

The **template** can help you configure similar properties quickly. For example, if you have 20 cameras and you want a particular frame rate on all of them, you can simply enter it once in the template, and then apply the template to the 20 cameras.

Name	Description
Apply Template	Select which cameras you want to apply the template for. You then use one of the two **Set** buttons to actually apply the template. **Tip:** To select all cameras in the list, click the **Select All** button.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.

Name	Description
Apply template on selected cameras	Lets you apply the value from the template to selected cameras.

Adjust Motion Detection wizard

The Adjust Motion Detection wizard helps you quickly configure your cameras' motion detection properties.

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, we recommended stopping (see "Start and stop services" on page 184) the Recording Server service when configuring such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 213).

Pages in this wizard:

Exclude regions

Exclude regions let you disable motion detection in specific areas of cameras' views. Disabling motion detection in certain areas may help you avoid detection of irrelevant motion, for example if a camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background.

Cameras that do not support multiple simultaneous video streams will not be able to connect to the surveillance server and the Management Application at the same time; therefore it is recommended to stop (see "Start and stop services" on page 184) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 213).

For each camera for which exclude regions are relevant, use the list in the left side of the wizard window to select the camera and define its exclude regions. Exclude regions are camera-specific, and must therefore be configured individually for each camera on which they are required.

When you have selected a camera, you will see a preview from the camera. You define regions to exclude in the preview, which is divided into small sections by a grid.

- To make the grid visible, select the Show Grid check box.
- To define exclude regions, drag the mouse pointer over the required areas in the preview while pressing the mouse button down. Left mouse button selects a grid section; right mouse button clears a grid section. Selected areas are highlighted in blue.

Tip: With the **Include All** button, you can quickly select all grid sections in the preview. This can be advantageous if you want to disable motion detection in most areas of the preview, in which case you can clear the few sections in which you do not want to disable motion detection. With the **Exclude All** button you can quickly deselect them all.

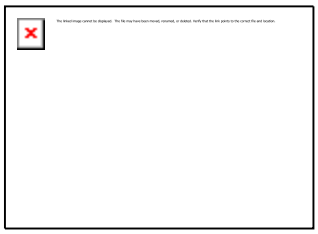
Motion Detection

Motion detection is a key element in most surveillance systems. Depending on your configuration, motion detection settings may determine when video is recorded (saved on the surveillance system server), when notifications are sent, when output (a light or siren) is triggered, etc.

It is important to find the best possible motion detection settings for each camera to avoid unnecessary recordings, notifications, etc. Depending on the physical location of your cameras, it is a good idea to test settings under different physical conditions (day/night, windy/calm weather, etc.).

Cameras that do not support multiple simultaneous video streams will not be able to connect to the surveillance server and the Management Application at the same time; therefore it is recommended to stop (see "Start and stop services" on page 184) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 213).

You can configure motion detection settings for each camera, or for several cameras at once. Use the list in the left pane of the wizard window to select cameras. To select several cameras at a time, press CTRL or SHIFT while selecting. When you select a camera, you will see a preview from that camera. If you select several cameras, you will see a preview from the last camera you select. A green area in the preview indicates motion.



Name	Description
Sensitivity	Adjust the **Sensitivity** slider so that irrelevant background noise is filtered out, and only real motion is shown in green. Alternatively, specify a value between 0 and 256 in the field next to the slider to control the sensitivity setting. The slider determines how much each pixel must change before it is regarded as motion. With a high sensitivity, very little change in a pixel is required before it is regarded as motion. The more you drag the slider to the left, the more of the preview becomes green. This is because with high sensitivity, even the slightest pixel change is regarded as motion.

Name	Description
Motion	Adjust the **Motion** slider so that motion detection is only triggered by the required level of motion. The selected motion level is indicated by the black vertical line in the **Level** bar above the sliders. The black vertical line serves as a threshold. When motion is above (to the right of) the selected level, the bar changes color from green to red, indicating a positive motion detection. Alternatively, specify a value between 0 and 10000 in the field on the left to control the motion setting. The more you drag the slider to the left, the more positive motion detections you see because less change will be needed to trigger a positive motion detection. The number of positive motion detections may also affect the amount of video you record, the amount of notifications you receive, etc.
Keyframe Only	If you want motion detection to take place only on keyframes of the video stream to reduce the system resources used on motion detection, select **Keyframe only**.
Detection interval	Specify how often motion detection analysis is carried out on video from the camera. The default is every 240 milliseconds (close to once a quarter of a second). The interval is applied regardless of your cameras' frame rate settings. Adjusting this setting can help lower the amount of system resources used on motion detection.
Detection resolution	Specify whether the full image or a selected percentage of the image should be analyzed. For example, by specifying 25%, every fourth pixel is analyzed instead of all pixels, reducing the system resources used but also offering less accurate motion detection.

Configure User Access wizard

The Configure User Access wizard helps you quickly configure clients' access to the XProtect Professional server as well as which users should be able to use clients. The access summary at the end of the wizard lists the cameras your users have access to.

When you use the wizard, all users you add will have access to all cameras, including any new cameras added at a later stage. You can however, specify access settings, users and user rights (see "Configure user and group rights" on page 179) separately. see Configure server access (on page 171). You cannot add users to groups (see "Add user groups" on page 178) through the wizard.

Pages in this wizard:

Server access settings

Name	Description
Server name	Name of the XProtect Professional server as it will appear in clients. Client users with rights to configure their clients will see the name of the server when they create views in their clients.
Local port	Port number to use for communication between clients and the surveillance server. The default port number is 80; you can change the port number if port 80 is used for other purposes in your organization.
Character encoding/Language	Select required language/character set. Example: If the surveillance server runs a Japanese version of Windows, select Japanese. Provided access clients also use a Japanese version of Windows, this will ensure that the correct language and character encoding is used in clients' communication with the server.
Internet access	Select if you want the server to be accessible from the internet through a router or firewall. If you select this option, you must also specify the public (“outside”) IP address and port number in the following fields. When using public access, the router or firewall must be configured so requests sent to the public IP address and port are forwarded to the local (“inside”) IP address and port of the XProtect Professional server.
Internet address	Lets you specify a public IP address or hostname for use when the XProtect Professional server should be available from the internet.
Internet port	Specify a port number for use when the XProtect Professional should be available from the Internet. The default port number is 80. You can change the port number if needed.

Basic & Windows Users

You can add client users in two ways, which may be combined.

- Basic user: create a dedicated surveillance system user account with basic user name and password authentication for each individual user. To add a basic user, specify required user name and password, and click the **Add Basic User** button. Repeat as required.
- Windows user: import users defined locally on the server and authenticate them based on their Windows login. This generally provides better security, and is the recommended method.

The users must have been defined as local PC users on the server. Simple file sharing must be disabled on the server. Depending on your operative system, this can be done in different ways.

- Windows 7: click the Windows logo and type **file sharing** in the search results window and press **Enter**. Under **File and Printer Sharing**, make sure that **Turn off file and printer sharing** is selected. Under **Public Folder Sharing**, make sure that **Turn off public folder sharing** is cleared.

- Windows Vista: click **Start** > **Control Panel**. Under **Network and Internet**, select **Set up file sharing**. The **Network and Sharing Center** window appears. Under **Sharing and Discovery**, set the option for file sharing to **Off** by clicking the down arrow next to **File Sharing** and select the radio button to **Turn off file sharing**. Click **Apply** and continue through the warning messages.
- Windows XP: click **Start** > **My Computer**. In the **My Computer** window, select **Tools** and in the top menu, select **Folder Options**. A new **Folder Options** window opens. Click on the **View** tab and scroll down to find **Use simple file sharing (recommended)**. Clear the box to disable file sharing. Click **OK**.

Add Windows users the following way:

1. Click **Add Windows User...** to open the S**elect Users or Groups** dialog.

   Note that you will only be able to make selections from the local computer, even if you click the **Locations...** button.

2. In **Enter the object names to select,** enter the required user name(s), then use the **Check Names** feature to verify that they are recognized. If you enter several user names, separate each name with a semicolon. Example: **Brian; Hannah; Karen; Wayne.**

3. When done, click **OK**.

When a user who has been added from a local database logs in with a client, the user should not specify any server name, PC name, or IP address as part of the user name. Example of a correctly specified user name: USER001, not: PC001/USER001. The user should of course still specify a password and any required server information.

Configure User Access wizard: access summary

The access summary simply lists which cameras your users will have access to. When using the wizard, all users you have added will have access all to cameras, including any new cameras added at a later stage. You can, however, limit individual users' access to cameras by changing their individual rights (see "Configure user and group rights" on page 179).

Advanced configuration

Hardware devices

About hardware devices

You add cameras and other hardware devices, such as video encoders, to your XProtect Professional system through the **Add Hardware Devices...** wizard (see "The Add Hardware Devices wizard" on page 44). If microphones or speakers are attached to a hardware device, they are automatically added as well.

About the Replace Hardware Device wizard

The Replace Hardware Device wizard helps you replace a hardware device that you have previously added to and configured on your surveillance system. To open the Replace Hardware Device wizard, right-click the device that you want to replace and select **Replace Hardware Device**.

The wizard is divided into these pages:

- New hardware device information (on page 71)
- Database action (see "Camera and database action" on page 72)

New hardware device information

Specify details about the new hardware device:

Name	Description
Address	IP address or host name of the hardware device.
Port	Port number on which to scan. The default is port 80. If a hardware device is located behind a NAT-enabled router or a firewall, you may need to specify a different port number. When this is the case, also remember to configure the router/firewall so it maps the port and IP address used by the hardware device.
User name	User name for the hardware device's administrator account. Many organizations use the hardware device manufacturer's default user names for their hardware devices. If that is the case in your organization, select <default> (do not type a manufacturer's default user name as this can be a source of error; trust that XProtect Professional will know the manufacturer's default user name). Other typical user names, such as admin or root are also selectable from the list. If you want a user name which is not on the list, simply type a new user name. **Tip:** User names you enter will subsequently be added to the list, so you can easily select them later.

Name	Description
Password	Password required to access the administrator account. A few hardware devices do not require user name/password for access; if such hardware devices are used in your organization, you can leave the field blank. **Tip:** If you are in doubt about which user name/password to use, ask yourself: Have I previously used a web page to connect to the hardware device and view video? While I did this, was I also able to configure camera settings, such as resolution, etc.? If you can answer yes to both questions, you were probably using the hardware device's administrator account, in which case you will also know the user name/password. If still in doubt, look in the XProtect Device Pack release notes.

To specify which device driver to use for the new hardware device, you can:

- Select the video device driver in the **Hardware device type** list, and then click **Auto-detect/Verify Hardware Device Type** to verify that the driver matches the hardware device.

  - or -

- Click **Auto-detect/Verify Hardware Device Type** to automatically detect and verify the right driver.

When the right driver is found, the **Serial number (MAC address)** field will display the MAC address of the new hardware device.

When done, click **Next**.

Camera and database action

The last page of the Replace Hardware wizard lets you decide what to do with the camera and the database containing recordings from the camera attached to the old hardware device. For multi-camera devices such as video encoders, you must decide what to do for each video channel on the new hardware device.

The table in the left side of the wizard page lists available video channels on the new hardware device. For a regular single-camera hardware device, there will only be one video channel. For video encoders, there will typically be several video channels.

1. For each video channel, use the table's **Inherit** column to select which camera from the old hardware device should be inherited by the new hardware device.

2. Then decide what to do with camera databases. You have three options:

   - **Inherit existing database(s):** The cameras you selected to be inherited by the new hardware device will inherit camera names, recordings databases as well as any archives from the old hardware device. Databases and archives (see "About archiving" on page 143) will be renamed to reflect the new hardware device's MAC address and video channels. The rights (see "Configure user and group rights" on page 179) of users with access to the inherited cameras are automatically updated so they can view both old and new recordings. Users will basically not notice the hardware device replacement since camera names will remain the same.

- **Delete the existing database(s):** The databases of the cameras you selected to be inherited by the new hardware device will be deleted. New databases will be created for future recordings, but it will not be possible to view recordings from before the hardware replacement.
- **Leave the existing database(s):** The databases of the cameras you selected to be inherited by the new hardware device will not be deleted. New databases will be created for future recordings, but even though the old databases still exist on the XProtect Professional server it will not be possible to view recordings from before the hardware replacement. Should you later want to delete the old databases, deletion must take place manually.

3. If the new hardware device has fewer video channels than the old hardware device, it will not be possible for the new hardware device to inherit all cameras from the old hardware device. When that is the case, you will be asked what to do with the databases of cameras that could not be inherited by the new hardware device. You have two options:
   - **Delete the databases for the cameras that are not inherited:** The databases of the cameras that could not be inherited by the new hardware devices will be deleted. It will not be possible to view recordings from before the hardware replacement. New databases will of course be created for future recordings by the new hardware devices.
   - **Leave the databases for the cameras that are not inherited:** The databases of the cameras that could not be inherited by the new hardware devices will not be deleted. Even though the old databases still exist on the XProtect Professional server it will not be possible to view recordings from before the hardware replacement. Should you later want to delete the old databases, deletion must take place manually. New databases will of course be created for future recordings by the new hardware devices.
4. Click **Finish**.

   When ready, restart (see "Start and stop services" on page 184) the Recording Server service. The hardware replacement will not be evident in clients until you restart the Recording Server service.

About dedicated input/output devices

You can add a number of dedicated input/output (I/O) hardware devices to XProtect Professional (see Add hardware devices (see "The Add Hardware Devices wizard" on page 44)). For information about which I/O hardware devices are supported, see the release notes.

When you add I/O hardware devices, input on them can be used for generating events in XProtect Professional, and events in XProtect Professional can be used for activating output on the I/O hardware devices. This means that you can use I/O hardware devices in your events-based system setup in the same way as a camera.

With certain I/O hardware devices it is necessary for the surveillance system to regularly check the state of the hardware devices' input ports to detect whether input has been received. Such state checking at regular intervals is called **polling**. The interval between state checks, called a **polling frequency**, is specified as part of the general ports & polling properties (see "Ports and polling" on page 133). For such I/O hardware devices, the polling frequency should be set to the lowest possible value (one tenth of a second between state checks). For information about which I/O hardware devices require polling, see the release notes.

Configure hardware devices

Once you have added hardware devices (see "The Add Hardware Devices wizard" on page 44), you can specify/edit device-specific properties, such as the IP address, which video channels to use, which COM ports to use for controlling attached PTZ (Pan/Tilt/Zoom) cameras, whether to use 360° lens technology, etc.

1. In the Management Application's navigation pane, expand **Advanced Configuration**, expand **Hardware Devices**, right-click the required hardware device, and select Properties.
2. Specify Name & Video channels, Network, Device type and license (see "Network, device type, and license" on page 75), PTZ device (on page 76), and 360° Lens (see "Fisheye" on page 113) properties as required.
3. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Delete hardware devices

IMPORTANT: If you delete a hardware device you will not only delete all cameras , speakers and microphones attached to the hardware device. You will also delete any recordings from cameras on the hardware device.

1. In the Management Application's navigation pane, expand **Advanced Configuration**, expand **Hardware Devices**, right-click the hardware device you want to delete, and select **Delete Hardware device**.
2. Confirm that you want to delete the hardware device and all its recordings.
3. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.
4. Restart (see "Start and stop services" on page 184) the Recording Server service.

If deleting a hardware device is not the right thing to do, consider disabling the individual cameras , speakers or microphones connected to the hardware device:

1. In the Management Application's navigation pane, expand **Advanced Configuration**, expand **Hardware Devices**, and expand the hardware device in question.
2. Right-click the camera or microphone or speaker that you want to disable, and select **Disable**.
3. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.
4. Restart (see "Start and stop services" on page 184) the Recording Server service.

Replace hardware devices

If required, you can replace a hardware device—which you have previously added to and configured on your surveillance system—with a new one. This can typically be relevant if you replace a physical camera on your network.

- Open the Replace Hardware Device wizard (see "About the Replace Hardware Device wizard" on page 71), which helps you through the entire replacement process on the surveillance system server, including:
  - Detecting the new hardware device
  - Specifying license for the new hardware device
  - Deciding what to do with existing recordings from the old hardware device

Hardware properties

Properties in this window:

Hardware name and video channels

When you configure hardware devices (on page 74), specify the following properties:

Name	Description
Hardware name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
Video channel # enabled	Enable/disable each of the selected hardware device's video channels. Many hardware devices only have a single video channel, in which case only one channel will be listed. Other hardware devices—typically video encoder devices—have several video channels.

If some of the channels are unavailable, this is because you are not licensed to use all of a video encoder device's channels. Example: You have a video encoder device with four channels, but your license for the device only allows you to use two of them. In that case, you can only have two channels enabled at a time; the two other channels will be disabled. Note that you are free to select which two channels you want to enable. Contact your Milestone vendor if you need to change your number of licenses.

Network, device type, and license

When you configure hardware devices (on page 74), specify the following properties:

Name	Description
Address	IP address or host name of the hardware device.

Name	Description
HTTP Port	Port to use for HTTP communication with the hardware device. Default is port 80. To use the default port, select Use default HTTP port.
FTP port	• Port to use for FTP communication with the hardware device. Default port is port 21.To use the default port, select U**se default FTP port**.
User name	Only required when **Server requires login** is selected. Specify the user name required for using the SMTP server.
User name	User name for the hardware device's administrator account. Many organizations use the hardware device manufacturer's default user names for their hardware devices. If that is the case in your organization, select <default> (do not type a manufacturer's default user name as this can be a source of error; trust that XProtect Professional will know the manufacturer's default user name). Other typical user names, such as admin or root are also selectable from the list. If you want a user name which is not on the list, simply type a new user name. **Tip:** User names you enter will subsequently be added to the list, so you can easily select them later.
Password	Password for the hardware device's administrator account, a.k.a. the root password.
Hardware type	Read-only field displaying the type of video device driver used for communication with the hardware device.
Serial number (MAC address)	Read-only field displaying the serial number of device. The serial number is usually identical to the 12-character hexadecimal MAC address of the hardware device (example: 0123456789AF).
License information	The current license status for the hardware.
Replace Hardware Device	Opens a wizard (see "About the Replace Hardware Device wizard" on page 71), with which you—if required—can replace the selected hardware device with another one. This can typically be relevant if you replace a physical camera on your network. The wizard helps you take all relevant issues into account: for example, deciding what to do with recordings from cameras attached to the old hardware device, etc.

PTZ device

The PTZ Device tab is only available if you configure (see "Configure hardware devices" on page 74) video encoder hardware devices on which the use of PTZ (Pan/Tilt/Zoom) cameras is possible:

Name	Description
Connected cameras have Pan/tilt/Zoom capabilities	Select check box if any of the cameras attached to the video encoder device is a PTZ camera.

Name	Description
PTZ type on COM#	If a PTZ camera is controlled through the COM port (a.k.a. serial port) in question, select the required option. Options are device-specific, depending on which PTZ protocols are used by the device in question. If no PTZ cameras are controlled through the COM port in question, select None. Some of the options concern absolute and relative positioning. What is that? Absolute positioning is when the PTZ camera is controlled based on a single fixed position, against which all other positions are measured. Relative positioning is when the PTZ camera is controlled relative to its current position.

The table in the lower half of the dialog contains a row for each video channel on the hardware device. First row from the top corresponds to video channel 1, second row from the top corresponds to video channel 2, etc.

Name	Description
Name	Name of the camera attached to the video channel in question.
Type	Select whether the camera on the selected camera channel is fixed or moveable: • **Fixed**: Camera is a regular camera mounted in a fixed position • **Moveable**: Camera is a PTZ camera
Port	Available only if **Moveable** is selected in the **Type** column. Select which COM port on the video encoder to use for controlling the PTZ camera.
Port Address	Available only if **Moveable** is selected in the **Type** column. Lets you specify port address of the camera. The port address will normally be 1. If using daisy chained PTZ cameras, the port address will identify each of them, and you should verify your settings with those recommended in the documentation for the camera.

Cameras and storage information

About video and recording configuration

Once you have added hardware devices and attached cameras, you can configure video and recording settings in three ways:

- **Wizard-driven:** Guided configuration which lets you specify video, recording and archiving settings for all your cameras. See Configure Video and Recording wizard and Adjust Motion Detection wizard.

- **General:** Specify video, recording and shared settings (such as dynamic archiving paths and whether audio should be recorded or not) for all your cameras.
    - In the Management Application navigation pane, expand Advanced Configuration, right-click Cameras and Storage Information, and select Properties.
- **Camera-specific:** Specify video, recording and camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for each individual camera.
    - In the Management Application navigation pane, expand Advanced Configuration, and expand Cameras and Storage Information, right-click the required camera, and select Properties.

About database resizing

In case recordings for a camera get bigger than expected, or the available drive space is suddenly reduced in another way, an advanced database resizing procedure will automatically take place:

If archives (see "About archiving" on page 143) are present on the same drive as the camera's database, the oldest archive for all cameras archived on that drive will be moved to another drive (moving archives is only possible if you use dynamic archiving (see "Dynamic path selection" on page 86), with which you can archive to several different drives) or—if moving is not possible—deleted.

If no archives are present on the drive containing the camera's database, the size of all camera databases on the drive will be reduced by deleting a percentage of their oldest recordings, temporarily limiting the size of all databases.

When the Recording Server service (see "About services" on page 183) is restarted upon such database resizing, the original database sizes will be used. You should therefore make sure that the drive size problem is solved.

Should the database resizing procedure take place, you will be informed on-screen in the Smart Client, in log files, and (if set up) through an e-mail and/or SMS notification.

About motion detection settings

Motion detection settings are linked to the Recording properties (see "Recording" on page 105) settings for the camera. Motion detection is enabled as default. Disabling it will improve CPU and RAM performance of your XProtect Professional system, but will—depending on your system settings—also affect your motion detection, event and alarm management. In the following two tables, You can see the differences between enabling (table 1) and disabling (table 2) built-in motion detection for a camera.

Enabled motion detection

Recording properties setting	Recordings	Motion-based events	Non-motion based events	Sequences
Always	Yes	Yes	Yes	Yes
Never	No	Yes	Yes	No
Built-in Motion Detection	Yes	Yes	Yes	Yes

Recording properties setting	Recordings	Motion-based events	Non-motion based events	Sequences
Built-in Motion Detection & Event or Event only	Yes	Yes	Yes	Yes

Disabled motion detection

Camera's recording settings	Recordings	Motion-based events	Non-motion based events	Sequences
Always	Yes	No	Yes	No
Never	No	No	Yes	No
Built-in Motion Detection	No	No	Yes	No
Built-in Motion Detection & Event or Event only	Yes (depending on settings)	No	Yes (depending on settings)	No

About motion detection and PTZ cameras

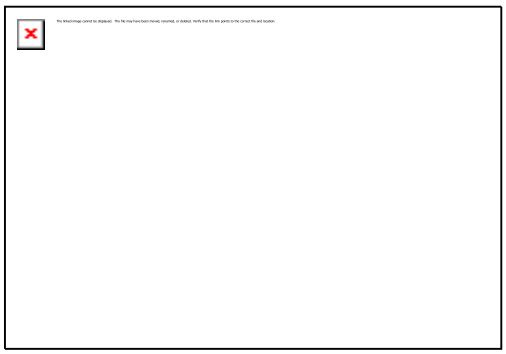
Motion detection generally works the same way for PTZ (Pan/Tilt/Zoom) cameras as it does for regular cameras. However:

- It is not possible to configure motion detection separately for each of a PTZ camera's preset positions.
- In order to activate unwanted recordings, notifications, etc., motion detection is automatically disabled while a PTZ camera moves between two preset positions. After a number of seconds, the so-called transition time, specified as part of the PTZ camera's PTZ patrolling properties (see "PTZ patrolling" on page 117), motion detection is automatically enabled again.

Configure camera-specific schedules

If you base your schedule profile—or parts of it—on events within periods of time, remember to select **Start event** and **Stop event** from the lists below the calendar section.

Tip: If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields.



The fact that a camera transfers video to XProtect Professional does not necessarily mean that video from the camera is recorded. Recording is configured separately; see Configure video and recording (see "About video and recording configuration" on page 77).

For each camera, you can create schedule profiles based on:

Online periods

- Periods of time (example: Mondays from 08.30 until 17.45), shown in pink: 
- Events within periods of time (example: from Event A occurs until Event B occurs Mondays from 08.30 until 17.45), shown in yellow: 

  The two options can be combined  , but they cannot overlap in time.

Speedup

- Periods of time (example: Mondays from 08.30 until 17.45), shown in olive green: 

E-mail notification

- Periods of time (example: Mondays from 08.30 until 17.45), shown in blue: 

SMS notification

- Periods of time (example: Mondays from 08.30 until 17.45), shown in green: 

PTZ patrolling

- Periods of time (example: Mondays from 08.30 until 17.45), shown in red: 
- If use of one patrolling profile is followed immediately by use of another, run your mouse pointer over the red bar to see which patrolling profile applies when.

XProtect Professional comes with two simple schedule profiles, **Always on** and **Always off,** which cannot be edited or deleted. If these do not meet your needs, you can create any number of

customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required.

1. In the **Schedule Profiles** list, select **Add new...**.
2. In the **Add Profile** dialog, enter a name for the profile. Names must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
3. In the top right corner of the dialog, select **Set camera to start/stop on time** (to base subsequent settings on periods of time) or **Set camera to start/stop on event** (to base subsequent settings on events within periods of time).

   Tip: You can combine the two, so you may return to this step in order to toggle between the two options.
4. In the calendar section, place your mouse pointer at a required start point, then hold down the left mouse button, drag the mouse pointer and release at the required end point.
   - You specify each day separately.
   - You specify time in increments of five minutes. XProtect Professional helps you by showing the time over which your mouse pointer is positioned.

If you base your schedule profile—or parts of it—on events within periods of time, remember to select **Start event** and **Stop event** from the lists below the calendar section.

- **Tip:** If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields.
- To delete an unwanted part of a schedule profile, right-click it and select **Delete**.
- To quickly fill or clear an entire day, double-click the name of the day.
- As an alternative to dragging inside the calendar section, use the **Start time**, **End time** and **Day** fields, then the **Change Period** or **Set Period** button as required. When using the **Start time** and **End time** fields, remember that time is specified in increments of five minutes. You cannot specify a period shorter than five minutes, and you can only use times like 12:00, 12.05, 12:10, 12:15, etc. If you specify a time outside of the five-minute intervals, such as 12:13, you will get an error message.

Configure when cameras should do what

Use the scheduling feature to configure when:

- Cameras should be online (that is transfer video to XProtect Professional)
- Cameras should use speedup (that is use a higher than normal frame rate)
- You want to receive any e-mail and/or SMS notifications regarding cameras
- PTZ cameras should patrol, and according to which patrolling profile

- Archiving should take place

See Configure general scheduling and archiving (on page 149) and Configure camera-specific schedules (on page 79).

Configure motion detection

Do the following:

1. In the Management Application navigation pane, expand **Advanced Configuration**, expand **Cameras and Storage Information**, right-click the required camera, and select **Properties**.
2. In the **Camera Properties** window, select the **Recording Properties** tab, and select the relevant settings (see "About motion detection settings" on page 78).
3. Select the **Motion Detection** tab.

   If there are any areas that should be excluded from motion detection (for example if the camera covers an area where a tree is swaying in the wind), you can exclude that area (see "Exclude regions" on page 66) by selecting it with your mouse.
4. Fill in the relevant properties (see "Motion detection & exclude regions" on page 110).

   There are some differences in motion-detection behavior for PTZ cameras (see "About motion detection and PTZ cameras" on page 79).
5. Click OK.

Disable or delete cameras

All cameras are by default enabled. This means that video from the cameras can be transferred to XProtect Professional provided that the cameras are scheduled to be online (see "Online period" on page 155).

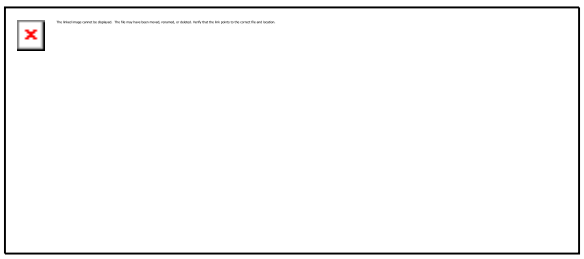
To **disable** a camera:

1. In the Management Application's navigation pane, expand **Advanced Configuration**, expand **Cameras and Storage Information**, double-click the camera you want to disable, and clear the **Enabled** box.
2. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

To **delete** a camera, you have to delete the hardware device (see "Delete hardware devices" on page 74). If you delete the hardware device, you also delete any attached microphones and speakers. If you do not want this, consider disabling the camera instead.

Move PTZ type 1 and 3 to required positions

For PTZ types 1 and 3, you can move the PTZ camera to required positions in several different ways:



1. Click the required position in the camera preview (if supported by the camera).
2. Use the sliders located near the camera preview to move the PTZ camera along each of its axes: the X-axis (for panning left/right), the Y-axis (for tilting up/down), and the Z-axis (for zooming in and out; to zoom in, move the slider towards **Tele;** to zoom out, move the slider towards **Wide**).
3. Use the navigation buttons:

 Moves the PTZ camera up and to the left

 Moves the PTZ camera up

 Moves the PTZ camera up and to the right

 Moves the PTZ camera to the left

 Moves the PTZ camera to its home position (that is default position)

 Moves the PTZ camera to the right

 Moves the PTZ camera down and to the left

 Moves the PTZ camera down

 Moves the PTZ camera down and to the right

 Zooms out (one zoom level per click)

 Zooms in (one zoom level per click)

Recording and storage properties

Properties in this window:

Recording and archiving paths

When you configure video and recording (see "About video and recording configuration" on page 77), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the properties can also be specified individually for each camera.

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. You then use one of the two **Set** buttons to actually apply the template. **Tip:** To select all cameras in the list, click the **Select All** button.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

Name	Description
Shortcut	Users of the Smart Client can take advantage of keyboard shortcuts, some of which let the users toggle between viewing different cameras. Such shortcuts include numbers which are used to identify each camera. Shortcut numbers must be unique for each camera. A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits. Examples of correct camera shortcut numbers: 3, 12345678. Examples of incorrect camera shortcut numbers: Cam#3, 123456789. More information about using the keyboard shortcuts is available in the separate documentation for the Smart Client.
Recording Path	Path to the folder in which the camera's database should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to a folder on a **local** drive. You cannot specify a path to a network drive. If you use a network drive, it is not be possible to save recordings if the network drive becomes unavailable. If you change the recording path, and you have existing recordings at the old location, you are asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them. **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.
Archiving Path	Only editable if not using dynamic paths for archiving (see "About archiving" on page 143). Path to the folder in which the camera's archived recordings should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can specify a path to a local or network drive. If you change the archiving path, and there are existing archived recordings at the old location, you will be asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if you move archived recordings, XProtect Professional will also archive what is currently in the camera database. In case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.
Retention Time	Total amount of time for which you want to keep recordings from the camera (that is recordings in the camera's database as well as any archived recordings). Default is 30 days. Note that the retention time covers the **total** amount of time you want to keep recordings for. In earlier XProtect Professional versions, time limits were specified separately for the database and archives.

Name	Description
Camera	Click the **Open** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras. **Tip:** To select more than one value press CTRL while selecting.
Set all template values on selected cameras	Apply all values from the template to selected cameras.

Dynamic path selection

When you configure video and recording (see "About video and recording configuration" on page 77), you can specify certain properties for many cameras in one go. In the case of Dynamic Path Selection, it is because the properties are shared by all cameras.

With dynamic archiving (see "About archiving" on page 143) paths, you specify a number of different archiving paths, usually across several drives. If the path containing the XProtect Professional database is on one of the drives you have selected for archiving, XProtect Professional will always try to archive to that drive first. If not, XProtect Professional automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive. Which drive has the most available space may change during the archiving process, and archiving may therefore happen to several archiving drives during the same process. This fact will have no impact on how users find and view archived recordings.

Dynamic archiving paths are general for all your cameras; you cannot configure dynamic archiving paths for individual cameras.

All properties on a white background are editable, properties on a light blue background cannot be edited.

Name	Description
Enable dynamic path selection archives	Enables the use of dynamic path selection, allowing you to select which paths you want to use. The list of selectable paths initially represents all drives on the server, both local and mapped drives. You can add further paths with the **New path** feature below the list.
Use	Select particular paths for use as dynamic archiving paths. You can also select a previously manually added path for removal (see description of **Remove** button in the following).
Drive	Letter representing the drive in question, for example C:.
Path	Path to where you save the files, for example C:\ or \\OurServer\OurFolder\OurSubfolder\.
Drive Size	Total size of the drive.
Free Space	Amount of unused space left on the drive.

Name	Description
New path	Specify a new path, and add it to the list using the Add button. Paths must be reachable by the surveillance system server, and you must specify the path using the UNC (Universal Naming Convention) format, example: \\server\volume\directory\. When the new path is added, you can select it for use as a dynamic archiving path.
Add	Add the path specified in the **New path** field to the list.
Remove	Remove a selected path—which has previously been manually added—from the list. You cannot remove any of the initially listed paths, not even when they are selected.

Video recording

When you configure video and recording (see "About video and recording configuration" on page 77), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

In XProtect Professional, the term **recording** means **saving video and, if applicable, audio from a camera in the camera's database on the surveillance system server**. Video/audio is often saved only when there is a reason to do so, for example as long as motion is detected, when an event occurs and until another event occurs, or within a certain period of time.

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the Video Recording properties can also be specified individually for each camera (see "Recording" on page 105).

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. You then use one of the two **Set** buttons to actually apply the template. **Tip:** To select all cameras in the list, click the **Select All** button.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

Name	Description
Record on	Lets you select under which conditions video from the camera should be recorded: • **Always:** Record whenever the camera is enabled (see "General" on page 100) and scheduled to be online (see "Online period" on page 155) (the latter allows for time-based recording). • **Never**: Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera. • **Motion Detection**: Select this to record video in which motion (see "Motion detection & exclude regions" on page 110) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected. • **Event**: Select this to record video when an event occurs and until another event occurs. Use of recording on event requires that events have been defined, and that you select start and stop events. **Tip:** If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields. • **Motion Detection & Event**: Select this to record video in which motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.
Start Event	Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).
Stop Event	Select required stop event. Recording will end when the stop event occurs (or later if using post-recording; see the following).
Pre-recording	You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column. **How does pre- and post-recording work?** XProtect Professional receives video in a continuous stream from the camera whenever the camera is enabled and scheduled to be online. This is what lets you view live video, but it also means that XProtect Professional can easily store received video for a number of seconds in its memory (a.k.a. buffering). If it turns out that the buffered video is needed for pre- or post-recording, it is automatically appended to the recording. If not, it is simply discarded.

Name	Description
Seconds [of pre-recording]	Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving (see "About archiving" on page 143) times. That can be problematic since pre-recording does not work well during archiving.
Post-recording	You can store recordings from periods following detected motion and/or stop events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.
Seconds [of post-recording]	Specify the number of seconds for which you want to record video from after recording stop conditions (that is motion or stop event) are met. Usually, only some seconds of post-recording is required, but you can specify up to 65535 seconds of post-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long post-recording time, you can potentially run into a scenario where your post-recording time spans scheduled or unscheduled archiving times. That can be problematic since post-recording does not work well during archiving.
Camera	Click the **Open** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras. **Tip:** To select more than one value press CTRL while selecting.
Set all template values on selected cameras	Apply all values from the template to selected cameras.

Properties in this window:

If the camera uses the MJPEG video format

With MJPEG, you can define frame rates for regular as well as speedup modes. If the camera offers dual stream, you can also enable this:

Regular frame rate mode:

Name	Description
Frame Rate	Required average frame rate for video from the camera. Select number of frames, then select the time unit interval (second, minute or hour).
Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

Speedup frame rate mode:

Name	Description
Enable speedup frame rate	The speedup feature lets you use a higher than normal frame rate if motion is detected and/or an event occurs. When you enable speedup, further columns for specifying speedup details become available.
Frame Rate	Speedup frame rate for viewing video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.
Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode. If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.
On motion	Select this check box to use the speedup frame rates when motion is detected. The camera will return to the normal frame rates two seconds after the last motion is detected.

Name	Description
On event	Select this check box to use the speedup frame rates when an event occurs and until another event occurs. Use of speedup on event requires that events have been defined, and that you select start and stop events in the neighboring lists. **Tip:** If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields.
Start Event	Select required start event. The camera will begin using the speedup frame rates when the start event occurs.
Stop Event	Select required stop event. The camera will return to the normal frame rates when the stop event occurs.

Tip: Speedup does not necessarily have to be based on motion- or events, you can also use scheduling (see "Speedup" on page 156) to configure speedup based on particular periods of time. If you prefer such time-based speedup, you should still enable the use of speedup by selecting the **Enable speedup** check box.

Dual stream:

This feature is only available on cameras supporting dual stream.

Name	Description
Enable dedicated live stream	This additional stream feature lets you use the alternative stream of the camera. It enables two independent streams to the recording server—a stream for live viewing and another stream for recording purposes, with different resolution, encoding, and frame rate.
Stream	Select the type of the live stream. Stream settings for viewing live video and for recording video may very well be different in order to get the best result.
Resolution	Select the resolution of the camera.
FPS	Select the camera's live frame rate per second (FPS)

Why are there three different places where I can configure frame rates for video? The first, Live frame rate, is for the regular recording stream. The second, Live frame rate, is for when speeding up recordings in connection with motion detection or similar. And the third, FPS, is for the additional stream used for live viewing.

If the camera uses the MPEG video format

With MPEG, you can define frame rate and other settings:

Name	Description
Frame rate per second	Frame rate for viewing live and recorded video from the camera. Select number of frames per second.

Name	Description
Record keyframes only	Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change. This helps greatly reducing the size of MPEG files. Select the check box if you only want to record keyframes. Note that you can specify exceptions if motion is detected or events occur (see the following).
Record all frames on motion	Allows you to make exceptions if you have selected to record keyframes only. Select this check box to record all frames when motion is detected. Two seconds after the last motion **is detected**, the camera will return to recording keyframes only**.**
Record all frames on event	Allows you to make exceptions if you have selected to record keyframes only. Select this check box to record all frames when an event occurs and until another event occurs. Use of this feature requires that events have been defined, and that you select start and stop events in the neighboring lists. **Tip:** If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields.
Start Event	**Use when recording on Event or Motion Detection & Event.** Select required start event. The camera will begin recording all frames when the start event occurs.
Stop Event	Select required stop event. The camera will again only recording keyframes when the stop event occurs.

Dual stream:

This feature is only available on cameras supporting dual stream.

Name	Description
Enable dedicated live stream	This additional stream feature lets you use the alternative stream of the camera. It enables two independent streams to the recording server—a stream for live viewing and another stream for recording purposes, with different resolution, encoding, and frame rate.
Stream	Select the type of the live stream. Stream settings for viewing live video and for recording video may very well be different in order to get the best result.
Resolution	Select the resolution of the camera.
FPS	Select the camera's live frame rate per second (FPS)

Manual recording

When you configure video and recording (see "About video and recording configuration" on page 77), you can specify certain properties for many cameras in one go. In the case of Manual recording, it is because the properties are shared by all cameras.

When manual recording is enabled, Smart Client users with the necessary rights (see "Configure user and group rights" on page 179) can manually start recording if they see something of interest while viewing live video from a camera which is not already recording.

If enabled, manual recording can take place even if recording for individual cameras (see "Recording" on page 105) is set to **Never** or **Conditionally**.

When started from the Smart Client, such user-driven recording will always take place for a fixed time, for example for five minutes.

Name	Description
Enable manual recording	Select check box to enable manual recording and specify further details.
Default duration of manual recording	Period of time (in seconds) during which user-driven recording will take place. Default duration is 300 seconds, corresponding to five minutes.
Maximum duration of manual recording	Maximum allowed period of time for user-driven recording. This maximum is not relevant in connection with manual recording started from the Smart Client, since such manual recording will always take place for a fixed time. In some installations it is, however, also possible to combine manual recording with third-party applications if integrating these with XProtect Professional through an API or similar, and in such cases specifying a maximum duration may be relevant. If you are simply using manual recording in connection with the Smart Client, disregard this property.

Frame rate - MJPEG

When you configure video and recording (see "About video and recording configuration" on page 77), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the Frame Rate - MJPEG properties can also be specified individually for each camera (see "Recording" on page 105) using MJPEG.

Properties in this window:

Template and common properties

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. You then use one of the two **Set** buttons to actually apply the template. **Tip:** To select all cameras in the list, click the **Select All** button.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras. **Tip:** To select more than one value press CTRL while selecting.
Set all template values on selected cameras	Apply all values from the template to selected cameras.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

Regular frame rate properties

Name	Description
Frame Rate	Required average frame rate for video from the camera. Select number of frames, then select the time unit interval (second, minute or hour).
Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.
Time Unit	Select required unit for live and recording frame rates (per second, minute, or hour). Note that you can only select time bases that let you speed up frame rates. Example: If you have specified 15 frames per **second** in normal mode, you cannot specify 16 frames per **minute** or **hour** in speedup mode.

Name	Description
Camera	Click the **Open** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.

Speedup frame rate properties

Name	Description
Enable Speedup	The speedup feature lets you use a higher than normal frame rate if motion is detected and/or an event occurs. When you enable speedup, further columns for specifying speedup details become available.
Frame Rate	Speedup frame rate for viewing video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.
Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode. If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.
Time Unit	Select required unit for live and recording frame rates (per second, minute, or hour). Note that you can only select time bases that let you speed up frame rates. Example: If you have specified 15 frames per **second** in normal mode, you cannot specify 16 frames per **minute** or **hour** in speedup mode.

Name	Description
Speedup On	• **Motion Detection**: Select this to speed up when motion (see "Motion detection & exclude regions" on page 110) is detected. Normal frame rates will be resumed immediately after the last motion **is detected.** • **Event:** Select this to speed up when an event occurs and until another event occurs. Use of speedup on event requires that events have been defined, and that you select start and stop events in the neighboring columns. **Tip:** If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields. • **Motion Detection & Event:** Select this to speed up when motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.
Schedule Only	Select this to speed up according to the camera's speedup schedule (see "Speedup" on page 156) only.
Start Event	Select required start event. The camera will begin using the speedup frame rates when the start event occurs.
Stop Event	Select required stop event. The camera will return to the normal frame rates when the stop event occurs.
Camera	Click the **Open** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.

Frame Rate - MPEG

When you configure video and recording (see "About video and recording configuration" on page 77), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the Frame Rate - MPEG properties can also be specified individually for each camera (see "Recording" on page 105) using MPEG.

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.

Name	Description
Apply Template	Select which cameras you want to apply the template for. You then use one of the two **Set** buttons to actually apply the template. **Tip:** To select all cameras in the list, click the **Select All** button.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
Dual Stream	Allows you to check if dual streaming is enabled on the camera(s). Note that the information is read-only. For cameras that support dual streaming, this can be enabled/disabled as part of individual cameras' Video (on page 101) properties.
Live FPS	Select the camera's live frame rate per second (FPS).
Record Keyframe Only	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. Select the check box if you only want to record keyframes.
Record All Frames on	Allows you to make exceptions if you have selected to record keyframes only. • **Motion Detection**: Select this to record all frames when motion is detected. Two seconds after the last motion (see "Motion detection & exclude regions" on page 110) is detected, the camera will return to recording keyframes only**.** • **Event**: Select this to record all frames when an event occurs and until another event occurs. Requires that events have been defined, and that you select start and stop events in the neighboring columns. **Tip:** If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields. • **Motion Detection & Event**: Select this to record all frames when motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns. • **Schedule only**: Select this to record all frames according to the camera's speedup schedule (see "Speedup" on page 156) only.
Start Event	**Use when recording on Event or Motion Detection & Event.** Select required start event. The camera will begin recording all frames when the start event occurs.
Stop Event	Select required stop event. The camera will again only recording keyframes when the stop event occurs.

Name	Description
Camera	Click the **Open** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras. **Tip:** To select more than one value press CTRL while selecting.
Set all template values on selected cameras	Apply all values from the template to selected cameras.

Audio recording

When you configure video and recording (see "About video and recording configuration" on page 77) for specific cameras, you can determine whether audio should be recorded or not. Your choice applies for all cameras on your XProtect Professional system.

Name	Description
Always	Always record audio on all applicable cameras.
Never	Never record audio on any cameras. Note that even though audio is never recorded, it is still be possible to listen to live audio in the Smart Client.

If you record audio, it is important that you note the following:

- Audio recording affects video storage capacity: Audio is recorded to the associated camera's database. Therefore, it is important to bear in mind that the database is likely to become full earlier if you record audio and video than if you only record video. The fact that the database becomes full is not in itself a problem since XProtect Professional automatically archives (see "About archiving" on page 143) data if the database becomes full. However, you may need additional archiving space if you record audio.
    - Example: If you use MPEG4, each one-second video GOP (Group Of Pictures) will be stored in one record in the database. Each second of audio will also be stored in one record in the database. This reduces the database's video storage capacity to half its capacity, because half of the database's records is used for storing audio. Consequently, the database runs full sooner, and automatic archiving takes place more often than if you were only recording video.
    - Example: If you use MJPEG, audio is stored in one record for every JPEG for as long as the audio block size does not exceed the time between the JPEGs. In extreme cases, this reduces the database's video storage capacity to half its capacity, because half of the database's records is used for storing audio. If you use very high frame rates, which means less time between each JPEG, a smaller portion of the database is used for storing audio records, and consequently a larger portion is available for storing video. The result is that the database runs full sooner, and automatic archiving takes place more often than if you were only recording video.

Above examples are simplified. The exact available video storage capacity also depends on GOP/JPEG and audio kilobyte size.

Audio selection

When you configure video and recording (see "About video and recording configuration" on page 77), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

With a default microphone and/or speaker selected for a camera, audio from the microphone and/or speaker will automatically be used when video from the camera is viewed. Note that all of the properties can also be specified individually for each camera.

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. You then use one of the two **Set** buttons to actually apply the template. **Tip:** To select all cameras in the list, click the **Select All** button.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
Default Microphone	Select required default microphone. **Tip:** Note that you can select microphones or speakers attached to another hardware device than the selected camera.
Default Speaker	Select required default speaker.
Camera	Click the **Open** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras. **Tip:** To select more than one value press CTRL while selecting.
Set all template values on selected cameras	Apply all values from the template to selected cameras.

Storage information

The storage information lets you view how much storage space you have on your XProtect Professional system—and, not least, how much of it is free:

Name	Description
Drive	Letter representing the drive in question, for example C:.
Path	Path to where you save the files, for example C:\ or \\OurServer\OurFolder\OurSubfolder\.
Usage	What the storage area is used for, for example recording or archiving.
Drive Size	Total size of the drive.
Video Data	Amount of video data on the drive.
Other Data	Amount of other data on the drive.
Free Space	Amount of unused space left on the drive.

Tip: To quickly view disk space usage in a pie chart format, select the line representing the drive you are interested in.

Camera properties

Properties in this window:

General

When you configure video and recording (see "About video and recording configuration" on page 77) for specific cameras, properties include:

Name	Description
Enabled	Cameras are by default enabled, meaning that provided they are scheduled to be online (see "Online period" on page 155), they are able to transfer video to XProtect Professional. If required, you can disable an individual camera, in which case no video/audio will be transferred from the camera source to XProtect Professional.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
Camera shortcut number	Users of the Smart Client can take advantage of keyboard shortcuts, some of which let the users toggle between viewing different cameras. Such shortcuts include numbers which are used to identify each camera. Shortcut numbers must be unique for each camera. A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits. Examples of correct camera shortcut numbers: 3, 12345678. Examples of incorrect camera shortcut numbers: Cam#3, 123456789. More information about using the keyboard shortcuts is available in the separate documentation for the Smart Client.

These properties are to a large extent camera-specific. Since such properties vary from camera to camera, descriptions in the following are for guidance only. If the selected camera is accessible, a live preview is displayed. Click the **Camera Settings...** button to open a separate window with properties for the selected camera.

The video properties typically let you control bandwidth, brightness, compression, contrast, resolution, rotation, etc. by overwriting existing values of selecting new ones. When you adjust video settings, you can—for most cameras—preview the effect of your settings in an image below the fields.

Video settings may feature an **Include Date and Time** setting. If set to **Yes**, date and time from the camera will be included in video. Note, however, that cameras are separate units which may have separate timing devices, power supplies, etc. Camera time and XProtect Professional system time may therefore not correspond fully, and this may occasionally lead to confusion. As all frames are time-stamped by XProtect Professional upon reception, and exact date and time information for each image is already known, it is recommended that the setting is set to **No**.

Tip: For consistent time synchronization, you may—if supported by the camera—automatically synchronize camera and system time through a time server.

Video

When you configure video and recording (see "About video and recording configuration" on page 77) for specific cameras, properties include:

If the camera uses MJPEG video format

With MJPEG, you can define frame rates for regular as well as speedup modes. If the camera offers dual stream, you can also enable this:

Regular frame rate mode:

Name	Description
Frame Rate	Required average frame rate for video from the camera. Select number of frames, then select the time unit interval (second, minute or hour).
Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

Speedup frame rate mode:

Name	Description
Enable speedup frame rate	The speedup feature lets you use a higher than normal frame rate if motion is detected and/or an event occurs. When you enable speedup, further columns for specifying speedup details become available.
Frame Rate	Speedup frame rate for viewing video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.
Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode. If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.
On motion	Select this check box to use the speedup frame rates when motion is detected. The camera will return to the normal frame rates two seconds after the last motion is detected.

Name	Description
On event	Select this check box to use the speedup frame rates when an event occurs and until another event occurs. Use of speedup on event requires that events have been defined, and that you select start and stop events in the neighboring lists. **Tip:** If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields.
Start Event	Select required start event. The camera will begin using the speedup frame rates when the start event occurs.
Stop Event	Select required stop event. The camera will return to the normal frame rates when the stop event occurs.

Tip: Speedup does not necessarily have to be based on motion- or events, you can also use scheduling (see "Speedup" on page 156) to configure speedup based on particular periods of time. If you prefer such time-based speedup, you should still enable the use of speedup by selecting the **Enable speedup** check box.

Dual stream:

This feature is only available on cameras supporting dual stream.

Name	Description
Enable dedicated live stream	This additional stream feature lets you use the alternative stream of the camera. It enables two independent streams to the recording server—a stream for live viewing and another stream for recording purposes, with different resolution, encoding, and frame rate.
Stream	Select the type of the live stream. Stream settings for viewing live video and for recording video may very well be different in order to get the best result.
Resolution	Select the resolution of the camera.
FPS	Select the camera's live frame rate per second (FPS)

Why are there three different places where I can configure frame rates for video? The first, Live frame rate, is for the regular recording stream. The second, Live frame rate, is for when speeding up recordings in connection with motion detection or similar. And the third, FPS, is for the additional stream used for live viewing.

If the camera uses MPEG video format

With MPEG, you can define frame rate and other settings:

Name	Description
Frame rate per second	Frame rate for viewing live and recorded video from the camera. Select number of frames per second.

Name	Description
Record keyframes only	Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change. This helps greatly reducing the size of MPEG files. Select the check box if you only want to record keyframes. Note that you can specify exceptions if motion is detected or events occur (see the following).
Record all frames on motion	Allows you to make exceptions if you have selected to record keyframes only. Select this check box to record all frames when motion is detected. Two seconds after the last motion **is detected**, the camera will return to recording keyframes only**.**
Record all frames on event	Allows you to make exceptions if you have selected to record keyframes only. Select this check box to record all frames when an event occurs and until another event occurs. Use of this feature requires that events have been defined, and that you select start and stop events in the neighboring lists. **Tip:** If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields.
Start Event	**Use when recording on Event or Motion Detection & Event.** Select required start event. The camera will begin recording all frames when the start event occurs.
Stop Event	Select required stop event. The camera will again only recording keyframes when the stop event occurs.

Dual stream:

This feature is only available on cameras supporting dual stream.

Name	Description
Enable dedicated live stream	This additional stream feature lets you use the alternative stream of the camera. It enables two independent streams to the recording server—a stream for live viewing and another stream for recording purposes, with different resolution, encoding, and frame rate.
Stream	Select the type of the live stream. Stream settings for viewing live video and for recording video may very well be different in order to get the best result.
Resolution	Select the resolution of the camera.
FPS	Select the camera's live frame rate per second (FPS)

Audio

When you configure video and recording (see "About video and recording configuration" on page 77) for specific cameras, properties include the possibility of selecting a default microphone and/or speaker for the camera.

With a default microphone and/or speaker selected for a camera, audio from the microphone and/or speaker will automatically be used when video from the camera is viewed.

If a microphone and/or a speaker is attached to the same hardware device as the camera, that microphone and/or speaker will be the camera's default microphone and/or speaker if you do not select otherwise.

Name	Description
Default Microphone	Select required default microphone. **Tip:** Note that you can select microphones or speakers attached to another hardware device than the selected camera.
Default Speaker	Select required default speaker.

The ability to select a default microphone and/or speaker for the camera requires that at least one microphone and/or speaker has been attached to a hardware device on the surveillance system.

Recording

In XProtect Professional, the term **recording** means **saving video and, if applicable, audio from a camera in the camera's database on the surveillance system server**. Video/audio is often saved only when there is a reason to do so, for example as long as motion is detected, when an event occurs and until another event occurs, or within a certain period of time.

When you configure video and recording (see "About video and recording configuration" on page 77) for specific cameras, recording properties include:

Name	Description
Always	Record whenever the camera is enabled (see "General" on page 100) and scheduled to be online (see "Online period" on page 155) (the latter allows for time-based recording).
Never	Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera.
Conditionally	Record when certain conditions are met. When you select this option, specify required conditions (see the following) which enables you to store recordings from periods preceding and following detected motion and/or specified events. Example: If you have defined that video should be stored when a door is opened, being able to see what happened immediately prior to the door being opened may also be important. Say you have specified that video should be stored conditionally on event, with a start event called **Door Opened** and a stop event called **Door Closed**. With three seconds of pre-recording, video will be recorded from three seconds before **Door Opened** occurs and until **Door Closed** occurs
Built-in motion detection	Select this check box to record video in which motion (see "Motion detection & exclude regions" on page 110) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.

Name	Description
On event	Select this check box to record video when an event occurs and until another event occurs. Use of recording on event requires that events have been defined, and that you select start and stop events in the neighboring lists. **Tip:** If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields.
Start Event	Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).
Stop Event	Select required stop event. Recording will end when the stop event occurs (or later if using post-recording; see the following).
Enable pre-recording	Available only when the option **Conditional** is selected. Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met.
Enable post-recording	Available only when the option **Conditional** is selected. Specify the number of seconds for which you want to record video after recording stop conditions (that is motion end or stop event) are met.

How does pre- and post-recording work? XProtect Professional receives video in a continuous stream from the camera whenever the camera is enabled and scheduled to be online. This is what lets you view live video, but it also means that XProtect Professional can easily store received video for a number of seconds in its memory (a.k.a. buffering). If it turns out that the buffered video is needed for pre- or post-recording, it is automatically appended to the recording. If not, it is simply discarded.

Note that manual recording (on page 92) may be enabled. With manual recording, Smart Client users with the necessary rights (see "Configure user and group rights" on page 179) can manually start recording if they see something of interest while viewing live video from a camera which is not already recording. If enabled, manual recording can take place even if recording for individual cameras is set to **Never** or **Conditionally**.

Recording and archiving paths

When you configure video and recording (see "About video and recording configuration" on page 77) for specific cameras, properties include:

Name	Description
Recording Path	Path to the folder in which the camera's database should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to a folder on a **local** drive. You cannot specify a path to a network drive. If you use a network drive, it is not be possible to save recordings if the network drive becomes unavailable. If you change the recording path, and you have existing recordings at the old location, you are asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them. **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.
Delete Database	Click button to delete all recordings in the database for the camera. Archived recordings will not be affected. **IMPORTANT:** Use with caution. All recordings in the database for the camera will be permanently deleted. As a security measure, you will be asked to confirm the deletion.
Archiving Path	Only editable if not using dynamic paths for archiving (see "About archiving" on page 143). Path to the folder in which the camera's archived recordings should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can specify a path to a local or network drive. If you change the archiving path, and there are existing archived recordings at the old location, you will be asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if you move archived recordings, XProtect Professional will also archive what is currently in the camera database. In case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.
Delete Archives	Click button to delete all archived recordings for the camera. Recordings in the camera's regular database will not be affected. The ability to delete is available regardless of whether you use a single archiving path or dynamic archiving paths. **MPORTANT:** Use with caution. All archived recordings for the camera will be permanently deleted. As a security measure, you will be asked to confirm the deletion.

Name	Description
Retention Time	Total amount of time for which you want to keep recordings from the camera (that is recordings in the camera's database as well as any archived recordings). Default is 30 days. Note that the retention time covers the **total** amount of time you want to keep recordings for. In earlier XProtect Professional versions, time limits were specified separately for the database and archives.
Database Repair Action	Select which action to take if the database becomes corrupted: • **Repair, scan, delete if fails**: Default action. If the database becomes corrupted, two different repair methods will be attempted: a fast repair and a thorough repair. If both repair methods fail, the contents of the database will be deleted. • **Repair, delete if fails**: If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be deleted. • **Repair, archive if fails**: If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be archived. • **Delete (no repair)**: If the database becomes corrupted, the contents of the database will be deleted. • **Archive (no repair)**: If the database becomes corrupted, the contents of the database will be archived. If you choose an action to repair a corrupt database, this corrupt database is closed while it is repaired. Instead, a new database is created to allow recordings to continue. **Why archive a corrupt database?** Provided the corrupt database has been archived, it can often be repaired by the Smart Client. So when you open the corrupt database in the Smart Client, the Smart Client will repair it automatically if at all possible. **Tip:** There are several things you can do to prevent that your databases become corrupt in the first place. See Protect recording databases from corruption (see "About protecting recording databases from corruption" on page 210).
Configure Dynamic Paths	With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. If the drive containing the camera's database is among the path you have selected for dynamic archiving, XProtect Professional will always try to archive to that path first. If not, XProtect Professional automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive. See also Dynamic path selection (on page 86).

Event notification

When you configure video and recording (see "About video and recording configuration" on page 77) for specific cameras, properties include event notification:

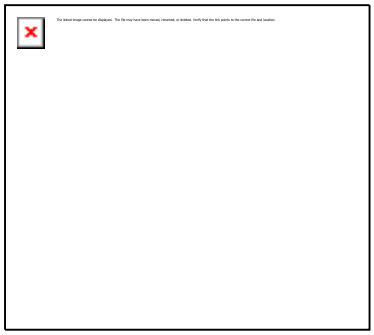
About event notifications

Event notification lets you inform Smart Client users that an event has occurred on the XProtect Professional system. Event notification can be valuable for client users, as they will be able to quickly detect that an event has occurred, even though their focus was perhaps on something else the moment the event occurred.

Tip: Even though event notification is configured separately for each camera, you can select between all events on your XProtect Professional system, regardless whether events are manual, generic, or originate on another hardware device than the camera itself.

In the Smart Client, event notification is given by a yellow indicator which lights up when a relevant event has taken place. An optional sound on event notification can furthermore be configured in the Smart Client itself.

In the clients, three differently colored indicators are available for each camera:



- The yellow event indicator. When event notification is used for a camera, the yellow indicator will light up when a relevant event has occurred.
- A red motion indicator; lights up when motion has been detected.
- An optional green video indicator; lights up when video is received from the camera.

In the Smart Client, all three indicators are in effect optional since the blue bar in which the indicators are displayed can be turned off in the Smart Client. If Smart Client users in your organization are going to rely on event notification, make sure they do not switch the blue bars off.

How to select required events

1. In the **Available events** list, select the required event. It is only possible to select one event at a time.

   Tip: If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields.

2. Click the **>>** button to copy the selected event to the **Selected Events** list.
3. Repeat for each required event.

If you later want to remove an event from the **Selected Events** list, simply select the event in question, and click the **<<** button.

Output

When you configure video and recording (see "About video and recording configuration" on page 77) for specific cameras, you can also associate a camera with particular hardware output (see "Add a hardware output" on page 127), for example the sounding of a siren or the switching on of lights.

Associated output can then be activated automatically when motion is detected in video from the camera, or manually when Smart Client users with the necessary rights (see "Configure user and group rights" on page 179) view live video from the camera.

1. In the **Available output** list, select the required output. It is only possible to select one output at a time.

   Tip: If you have not yet defined any suitable output, you can quickly do it: Use the **Configure Output** button, located below the other fields.

   Tip: Even though output is configured separately for each camera, you can select between all output on your XProtect Professional system, regardless whether output originates on another hardware device than the camera itself.

2. Click the **>>** button to copy the selected output to the:

   - **On manual activation** list, in which case the output will be available for manual activation in the Smart Client.

     - and/or -

   - **On motion detected** list, in which case the output will be activated when motion is detected in video from the camera.

   If required, the same output can appear on both lists.

3. Repeat for each required output.

If you later want to remove an output from the one of the lists, select the output in question, and click the **<<** button.

Motion detection & exclude regions

When you configure video and recording (see "About video and recording configuration" on page 77) for specific cameras, adjusting motion detection is important because it may determine when video from the camera is recorded, when e-mail notifications are generated, when hardware output (such as lights or sirens) is activated, etc. Time spent on finding the best possible motion detection settings for each camera may help you later avoid unnecessary recordings, notifications, etc. Depending on the physical location of the camera, it may be a very good idea to test motion detection under different physical conditions (day/night, windy/calm weather, etc.).

Before you configure motion detection for a camera, you should configure the camera's video properties (see "General" on page 100), such as compression, resolution, etc.

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, we recommended stopping (see "Start and stop services" on page 184) the Recording Server service when configuring such devices

for motion detection and PTZ. See also View video from cameras in Management Application (on page 213).

Name	Description
Enable	Lets you enable or disable (see "About motion detection settings" on page 78) the built-in motion detection.
Show grid	Lets you toggle the grid on and off. Toggling the grid off may provide a less obscured view of the preview image; selection of areas which should be excluded from motion detection takes place the same way as when the grid is visible. When on, the preview image will be divided into small sections by a grid. To define areas which should be excluded from motion detection, drag the mouse over the areas in the preview image while pressing the mouse button down. Left mouse button selects a grid section; right mouse button clears a grid section. Selected areas are highlighted in blue.
Include All	Lets you quickly select all grid sections in the preview image. This can be useful if you want to exclude motion detection in most areas of the image, in which case you can simply clear the few sections in which you do not want to exclude motion detection.
Exclude All	Lets you quickly clear all grid sections in the preview image.
Sensitivity	Determines how much each pixel must change before it is regarded as motion. With a high sensitivity, very little change in a pixel is required before it is regarded as motion. Areas in which motion is detected are highlighted in green in the preview image. Select a slider position in which only detections you consider motion are highlighted. The more you drag the slider to the left, the more of the preview image becomes highlighted. This is because with a high sensitivity even the slightest change in a pixel will be regarded as motion. As an alternative to using the slider, you may specify a value between 0 and 256 in the field next to the slider to control the sensitivity setting.
Motion	Adjust the **Motion** slider so that motion detection is only triggered by the required level of motion. The selected motion level is indicated by the black vertical line in the **Level** bar above the sliders. The black vertical line serves as a threshold. When motion is above (to the right of) the selected level, the bar changes color from green to red, indicating a positive motion detection. Alternatively, specify a value between 0 and 10000 in the field on the left to control the motion setting. The more you drag the slider to the left, the more positive motion detections you see because less change will be needed to trigger a positive motion detection. The number of positive motion detections may also affect the amount of video you record, the amount of notifications you receive, etc.
Keyframe Only	If you want motion detection to take place only on keyframes of the video stream to reduce the system resources used on motion detection, select **Keyframe only**.

Name	Description
Detection interval	Specify how often motion detection analysis is carried out on video from the camera. The default is every 240 milliseconds (close to once a quarter of a second). The interval is applied regardless of your cameras' frame rate settings. Adjusting this setting can help lower the amount of system resources used on motion detection.
Detection resolution	Specify whether the full image or a selected percentage of the image should be analyzed. For example, by specifying 25%, every fourth pixel is analyzed instead of all pixels, reducing the system resources used but also offering less accurate motion detection.

Privacy masking

Ask yourself whether there are any areas of the camera image that must be masked from viewing. For example, if the camera points in a way so that it catches the window of a private building, the privacy of the residents must be respected. In that case, you can mask areas of the image by configuring the settings below.

Name	Description
Enable	Enable the **Privacy Masking** feature.
Show grid	Toggle the grid on and off. Toggling the grid off may provide a less obscured view of the preview image; selection of areas which should be excluded from privacy masking takes place the same way as when the grid is visible. When on, the preview image will be divided into small sections by a grid. To define areas which should be excluded from privacy masking, drag the mouse over the areas in the preview image while pressing the mouse button down. Left mouse button selects a grid section; right mouse button clears a grid section. Selected areas are highlighted in red.
Show privacy mask	Toggle the red area indicating privacy masking on and off. Toggling the red area off may provide a less obscured view of the preview image.
Clear	Clear the privacy masking.

360° lens

360° lens technology allows you to view 360° panoramic video through an advanced lens. If a camera is going to use 360° lens technology, you must enable the technology and, in some cases, enter a special license key.

Name	Description
Enable 360° lens	Select check box to enable use of the 360° lens technology and to be able to specify further properties.

Name	Description
Enable panomorph support	Select to enable panomorph support. Panomorph is an advanced technology can provide high resolution in zones of interest, while at the same time using fewer pixels than conventional fisheye solutions. In the list, also select whether the camera is located in the ceiling, on a wall or on ground level.
Immervision Enables® panomorph RPL number	When enabling the panomorph support functionality, you must also select a Registered Panomorph Lens (RPL) number from the **ImmerVision Enables® panomorph RPL number** list. This is to ensure identification and correct configuration of the lens used with the camera in question. The RPL number is usually found on the lens itself or on the box it came in. If you, at some point, want to add additional types of lenses, go to **File** and select **Import new lens types.** Locate the .xml file that contains information about the lens type and press **OK.** For details of ImmerVison, panomorph lenses, and RPLs, see http://www.immervision.com/en/home/index.php **(**http://www.immervision.com/en/home/index.php**).**
Enable fisheye support	Select to enable fisheye support. Fisheye technology uses a wide-angle lens to capture a hemispherical image, which can then be de-warped through configured fisheye settings (see "Fisheye" on page 113) for the camera in question.
License key	If required, enter your special fisheye license key and click OK, after which it will be possible to configure fisheye settings for camera(s) attached to the hardware device.

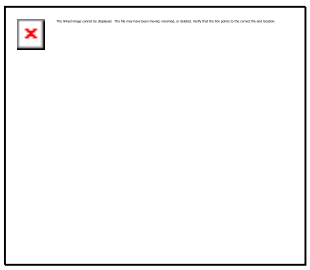
Do I need the special fisheye license key, and where do I get it? Contact your XProtect Professional vendor for further information.

Fisheye

When you configure video and recording (see "About video and recording configuration" on page 77) for specific cameras, fisheye properties may be available. Fisheye is a technology that allows viewing of 360-degree panoramic video through an advanced lens.

You will not see the fisheye properties until certain conditions are met: The camera must be either a dedicated fisheye camera or be equipped with a special fisheye lens. A special fisheye license key is also required; you enter the key when you configure the hardware device (see "Configure hardware devices" on page 74) to which the fisheye camera is attached.

You configure the camera's fisheye functionality by adjusting its fisheye view field, indicated by a green circle in the fisheye view, until the circle encloses the actual image area of the fisheye lens. Your settings are then used by the fisheye technology for converting the circular fisheye view into a flattened rectangular view.



Name	Description
Ceiling mount	If the camera is mounted on a ceiling, you can adjust properties to reflect this by selecting the check box.
Resolution	Resolution values are automatically displayed above the fisheye image. When using fisheye, resolution will automatically be set to the highest possible value.
X radius	Controls the horizontal (X) radius of the green circle. Move the slider to the left for a narrower circle, or to the right for a wider circle. Alternatively, specify a value between 0 and 800 in the field next to the slider. 0 corresponds to the slider's leftmost position, 800 corresponds to the slider's rightmost position.
Milestone Recording Server service	A vital part of the surveillance system. Video streams are only transferred to XProtect Professional while the Recording Server service is running.
X center	Controls the horizontal (X) position of the green circle. Move the slider to the left or right as required. Alternatively, specify a value between 0 and 800 in the field next to the slider.
Y center	Controls the vertical (Y) position of the green circle. Move the slider to the left in order to move the circle up, or to the right in order to move the circle down. Alternatively, specify a value between 0 and 800 in the field next to the slider.
Enable preview	Toggle between viewing the circular fisheye view and the flattened rectangular view resulting from your settings. When you preview the flattened view, the following navigation buttons become available for moving around within the flattened view.
Set as Home	Use after navigating to a suitable viewpoint using the navigation buttons. Sets the current viewpoint as home position (that is default position), so that when client users viewing the camera click their clients' **Home** button, their view of the camera changes to that position.

Button	Description
	Moves the flattened view up

Name	Description
	Moves the flattened view up and to the left
	Moves the flattened view up and to the right
	Moves the flattened view to the left
	Moves the flattened view to its home position (that is default position)
	Moves the flattened view to the right
	Moves the flattened view down and to the left
	Moves the flattened view down
	Moves the flattened view down and to the right
	Zooms out (one zoom level per click)
	Zooms in (one zoom level per click)

PTZ preset positions

PTZ-related properties are only available when you are dealing with a PTZ (Pan/Tilt/Zoom) camera. PTZ preset positions can be used for making the PTZ camera automatically go to a particular position when particular events occur, and when setting up PTZ patrolling profiles. Preset positions also become selectable in clients, allowing users with required rights (see "Configure user and group rights" on page 179) to move the PTZ camera between preset positions.

Names of preset positions must contain only the characters A-Z, a-z and the digits 0-9. If you import preset positions from cameras (see the following), verify that their names do not contain other characters. If they do, change the preset position names before you import them.

Restart services (see "Start and stop services" on page 184) after having made changes to PTZ settings.

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, we recommended stopping (see "Start and stop services" on page 184) the Recording Server service when configuring such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 213).

Name	Description
PTZ type	Your configuration options depend on the type of PTZ camera in question: • Type 1 (stored on server): You define preset positions by moving the camera using the controls (see "Move PTZ type 1 and 3 to required positions" on page 83) in the upper half of the window, then storing each required position on the XProtect Professional server. You can define up to 260 preset positions this way. • Type 2 (imported from camera): You import preset positions which have previously been defined and stored on the PTZ camera itself through the camera's own configuration interface. The number of allowed preset positions depends on the PTZ camera and driver used. • Type 3 (stored on camera): You define preset positions by moving the camera with the controls (see "Move PTZ type 1 and 3 to required positions" on page 83) in the upper half of the window, then storing each required position in the camera's own memory. You can define up to 260 preset positions this way. If preset positions have already been defined for the camera, you can simply import them for use with XProtect Professional.
Import / Refresh	Only available when you have selected PTZ type 2 or 3. Lets you import already defined preset positions from the camera's memory for use with XProtect Professional. If you have already imported preset positions this way, and preset positions have since then been added or changed on the camera, you can use this button to refresh the imported preset positions.
Add New	Only available when you have selected PTZ type 1. When you have move the camera to a required position using the controls in the upper half of the window, type a name for the position in the blank field, then click the button to add the position to the list of defined preset positions. Remember that names of preset positions must contain only the characters A-Z, a-z and the digits 0-9.
Set New Position	Only available when you have selected PTZ type 1 or 3. Lets you change an already defined preset position. In the list, select the preset position you want to change. Then move the camera to the new required position using the controls in the upper half of the window. Then click the button to overwrite the old position with the new one.

Name	Description
Delete	Only available when you have selected PTZ type 1 or 3. Lets you delete an already defined preset. In the list, select the preset position you want to delete, then click the button. Before you delete a preset position, make sure it is not used in PTZ patrolling or PTZ on event. Since the preset positions are stored on the camera, you can bring a deleted preset position back into XProtect Professional by clicking the **Import / refresh** button. If you bring back a preset position this way, and the preset position is to be used in PTZ patrolling or PTZ on event, you must manually configure PTZ patrolling and/or PTZ on event to use the preset position again.
Test	Lets you try out a preset position. In the list, select the preset position you want to test, then click the button to view the camera move to the selected position.
PTZ control wheel	Lets you move a preset position selected in the list up and down respectively. The selected preset position is moved one step per click. By moving preset positions up or down, you can control the sequence in which preset positions are presented in clients.

PTZ patrolling

PTZ-related properties are only available when you are dealing with a PTZ (Pan/Tilt/Zoom) camera. PTZ patrolling is the continuous movement of a PTZ camera between a number of preset positions (see "PTZ preset positions" on page 115). To use patrolling, you should normally have specified at least two preset positions for the PTZ camera in question.

To configure PTZ patrolling, you basically select a patrolling profile in the **Patrolling profiles** list, then specify required properties to define the exact behavior of the patrolling profile.

Tip: Although it is technically not patrolling, specifying a patrolling profile with only one preset position is possible. A patrolling profile with only one preset position can, when combined with scheduling, be useful in two cases: For moving a PTZ camera to a specific position at a specific time, and for moving a PTZ camera to a specific position upon manual control of the PTZ camera.

Restart services (see "Start and stop services" on page 184) after having made changes to PTZ settings. When you have defined your patrolling profiles, also remember to schedule (see "PTZ patrolling" on page 156) the use of patrolling profiles. Bear in mind that patrolling can be overridden if users (with the required rights (see "Configure user and group rights" on page 179)) manually operate PTZ cameras.

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, we recommended stopping (see "Start and stop services" on page 184) the Recording Server service when configuring such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 213).

Patrolling profiles

A PTZ camera may patrol according to several different patrolling profiles. For example, a PTZ camera in a supermarket may patrol according to one patrolling profile during opening hours, and according to another patrolling profile when the supermarket is closed. The **Patrolling profiles** list lets you select which patrolling profile to configure.

- Add New: Lets you add a new patrolling profile to the list. When you add a new patrolling profile, you can either give it a unique name, or reuse an existing name from another PTZ camera with PTZ patrolling.

  Using several identically named patrolling profiles can be advantageous when you later configure scheduling. Example: If you have configured patrolling profiles identically named Night Patrolling on 25 different cameras, you can schedule the use of Night Patrolling on all 25 cameras in one go, even though Night Patrolling covers individual preset positions on each of the 25 cameras.

- Delete: Lets you delete an existing patrolling profile. Note that the selected patrolling profile will be removed from the list without further warning.

There are already some patrolling profiles listed, why? Names of patrolling profile defined for other cameras can be reused. This allows you to use a single patrolling profile name across several PTZ cameras, and this can make scheduling (see "PTZ patrolling" on page 156) of PTZ patrolling much easier. Despite the fact that several PTZ cameras share a patrolling profile name, the movement between preset positions is of course individual for each camera.

Preset positions to use in a patrolling profile

Having selected a patrolling profile in the **Patrolling profiles** list, you can specify which of the PTZ camera's preset positions should be used for the selected patrolling scheme:

1. In the **Preset Positions** list, select the preset positions you want to use. A preset position can be used more than once in a patrol scheme, for example if the preset position covers an especially important location.

   Tip: By pressing the CTRL button on your keyboard while selecting from the **Preset Positions** list, you can select several or all of list's preset positions in one go.

2. Click the button to copy the selected preset positions to the **Patrolling list**.

3. The camera will move between preset positions in the sequence they appear in the **Patrolling list**, starting at the preset position listed first. If you want to change the sequence of preset positions in the **Preset Positions** list, select a preset position, and use the or buttons to move the selected preset position up or down in the list. The selected preset position is moved one step per click.

If you later want to remove a preset position from the Patrolling list, select the preset position in question, and click the button.

Wait and transition timing for a patrolling profile

ame	Description
Wait time (sec.)	Lets you specify the number of seconds for which the PTZ camera should stay at each preset position before it moves on to the next preset position. Default is 10 seconds. The wait time applies to all presets in the patrolling profile, that is the PTZ camera will stay at each preset position for the same number of seconds.
Transition time (sec.)	Transition time (sec.): Lets you specify the number of seconds required for the PTZ camera to move from one preset position to another. Default is five seconds. During this transition time, motion detection is automatically disabled, as irrelevant motion is otherwise likely to be detected while the camera moves between the preset positions. After the specified number of seconds, motion detection is automatically enabled again. The transition time applies to all presets in the patrolling profile. It is thus important that the camera is able to reach between any of the patrolling profile's preset positions within the number of seconds you specify. If not, false motion is likely to be detected. Bear in mind that it takes longer for the PTZ camera to move between positions that are located physically far apart (for example from an extreme left position to an extreme right position) than between positions that are located physically close together.

Tip: Note that wait time and transition time settings are tied to the selected patrolling profile. This allows you the flexibility of having different wait time and transition time settings for different patrolling profiles on the same camera.

PTZ scanning

PTZ scanning (continuous panning) is supported on a few PTZ cameras only.

- **PTZ scanning:** Only available if your camera supports PTZ scanning. Lets you enable PTZ scanning and select a PTZ scanning speed from the list below the check box.

Note that PTZ scanning only works for PTZ type 1 cameras (where preset positions are configured and stored on the XProtect Professional server). If the camera is a PTZ type 2 camera, and you import preset positions which have previously been defined and stored on the PTZ camera itself through the camera's own configuration interface, PTZ scanning will stop working. For more information about PTZ types, see PTZ preset positions (on page 115).

Pause PTZ patrolling

PTZ patrolling is automatically paused when the camera is operated manually as well as if PTZ on Event (on page 120) is used. PTZ patrolling can also be paused if motion is detected.

Tip: Note that pause settings are tied to the selected patrolling profile. This allows you the flexibility of having different pause settings for different patrolling profiles on the same camera.

Pause patrolling if motion is detected

To pause PTZ patrolling when motion is detected, so that the PTZ camera will remain at the position where motion was detected for a specified period of time, do the following:

1. Select the **Pause patrolling if motion is detected** check box.
2. Select whether the PTZ camera should resume patrolling:
   - After a certain number of seconds has passed since first detection of motion, regardless whether further motion is detected

     - or -

   - After a certain number of seconds has passed without further detection of motion
3. Specify the required number of seconds for the selected option (default is ten and five seconds respectively).

   Unless transition time (see the previous information under **Wait and Transition Timing ...**) is set to zero, motion detection is automatically disabled while the camera moves between preset positions, as irrelevant motion is otherwise likely to be detected while the camera moves between the preset positions.

Resume PTZ patrolling

PTZ patrolling is automatically paused when the camera is operated manually as well as if PTZ on Event is used. You can specify how many seconds should pass before the regular patrolling is resumed after a manual or event-based interruption. Default is 30 seconds.

Users of the Smart Client are—in addition to manual control—able to stop a selected PTZ camera's patrolling entirely. This takes place through a context menu in the Smart Client view. For Smart Client users, the number of seconds specified in the **Patrolling settings** section therefore only applies when users manually control a PTZ camera; not when users stop a PTZ camera's patrolling entirely. When Smart Client users stop a PTZ camera's patrolling entirely, the camera's patrolling will resume only when the Smart Client user selects to resume it.

PTZ on event

PTZ-related properties are only available when you are dealing with a PTZ (Pan/Tilt/Zoom) camera. When a PTZ camera supports preset positions (see "PTZ preset positions" on page 115), it is possible to make the PTZ camera automatically go to a particular preset position when a particular event occurs.

When associating events with preset positions on a PTZ camera, you can select between **all** events defined on your XProtect Professional system; you are not limited to selecting events defined on a particular hardware device.

1. In the **Events** list in the left side of the window, select the required event.

   Tip: If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields.

2. In the **PTZ Preset Position** list in the right side of the window, select the required preset position.

   For this purpose, you can only use an event once per PTZ camera. However, different events can be used for making the PTZ camera go to the same preset position. Example:

   - Event 1 makes the PTZ camera go to preset position A
   - Event 2 makes the PTZ camera go to preset position B

- Event 3 makes the PTZ camera go to preset position A

If later you want to end the association between a particular event and a particular preset position, clear the field containing the event.

After you have made the PTZ setting changes, restart services (see "Start and stop services" on page 184).

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, we recommended stopping (see "Start and stop services" on page 184) the Recording Server service when configuring such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 213).

Audio

About recording audio

If you record audio, it is important that you note the following:

- Only audio from microphones is recorded. Only incoming audio, that is audio recorded by microphones attached to hardware devices, is recorded. Outgoing audio, that is what operators say when they talk through speakers attached to hardware devices, is not recorded.
- Audio recording affects video storage capacity. Audio is recorded to the associated camera's database. Therefore, it is important to bear in mind that the database is likely to become full earlier if you record audio and video than if you only record video. The fact that the database becomes full is not in itself a problem since XProtect Professional automatically archives (see "About archiving" on page 143) data if the database becomes full. However, you may need additional archiving space if you record audio.
  - Example: If you use MPEG4, each one-second video GOP (Group Of Pictures) will be stored in one record in the database. Each second of audio will also be stored in one record in the database. This reduces the database's video storage capacity to half its capacity, because half of the database's records is used for storing audio. Consequently, the database runs full sooner, and automatic archiving takes place more often than if you were only recording video.
  - Example: If you use MJPEG, audio is stored in one record for every JPEG for as long as the audio block size does not exceed the time between the JPEGs. In extreme cases, this reduces the database's video storage capacity to half its capacity, because half of the database's records is used for storing audio. If you use very high frame rates, which means less time between each JPEG, a smaller portion of the database is used for storing audio records, and consequently a larger portion is available for storing video. The result is that the database runs full sooner, and automatic archiving takes place more often than if you were only recording video.

The above examples are simplified. The exact available video storage capacity also depends on GOP/JPEG and audio kilobyte size.

Speakers

About speakers

Speakers are attached to devices, and therefore also typically physically located next to cameras. They can typically transmit information to people near a camera. Operators, with the necessary rights, can talk through such speakers using their Smart Clients (provided the computer running the Smart Client has a microphone attached).

Example: An elevator is stuck. Through a camera mounted in the elevator, Smart Client operators can see that there is an elderly lady in the elevator. A microphone attached to the camera records that the lady says: “I am afraid; please help me out!” Through a speaker attached to the camera, operators can tell the lady that: “Help is on its way; you should be out in less than fifteen minutes.”

Show or hide microphone and/or speaker

If you have added more microphone and/or speaker to your XProtect Professional system than you need, you can hide the ones you do not need by right-clicking the relevant microphone and/or speaker and select **Hide**. If you need the hidden microphone again, you can right-click the overall microphone and/or speaker icon and select **Show Hidden Items**.

Speaker properties

When you configure video and recording (see "About video and recording configuration" on page 77) for specific cameras, you can determine when audio should be recorded or not. Your choice applies for all cameras on your XProtect Professional system.

Name	Description
Enabled	Speakers are by default enabled, meaning that they are able to transfer audio to XProtect Professional. If required, you can disable an individual speaker, in which case no audio will be transferred from the speaker to XProtect Professional.
Speaker name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

Microphones

About microphones

Microphones are attached to hardware devices, and therefore typically physically located next to cameras. They can typically record what people near a camera are saying. Operators, with the necessary rights, can then listen to these recordings through their Smart Clients (provided the computer running the Smart Client has speakers attached).

When you manage microphones in XProtect Professional, you can always manage the microphones attached to cameras; **not** microphones attached to Smart Client operators' computers.

If you have added more microphones and speakers to your XProtect Professional system than you need, you can hide the ones you do not need by right-clicking the relevant microphone and/or speaker and select **Hide**. If you need the hidden microphone again, you can right-click the overall microphone and/or speaker icon and select **Show Hidden Items**.

Configure microphones or speakers

1. In the Management Application's navigation pane, expand **Advanced Configuration**, expand **Hardware Devices**, and expand the hardware device to which the relevant microphones or speakers is attached.
2. Right-click the required microphones or speakers, and select **Properties**.
3. Specify properties (see "Speaker properties" on page 122) as required.

Configuration of microphones or speakers in XProtect Professional is very basic. Settings such as volume, etc. are controlled on the microphones or speakers units themselves.

Show or hide microphone and/or speaker

If you have added more microphone and/or speaker to your XProtect Professional system than you need, you can hide the ones you do not need by right-clicking the relevant microphone and/or speaker and select **Hide**. If you need the hidden microphone again, you can right-click the overall microphone and/or speaker icon and select **Show Hidden Items**.

Microphone properties

When you configure video and recording (see "About video and recording configuration" on page 77) for specific cameras, you can determine when audio should be recorded or not. Your choice applies for all cameras on your XProtect Professional system.

Microphone properties

Enabled	Microphones/speaker are by default enabled, meaning that they are able to transfer audio to XProtect Professional. If required, you can disable an individual microphone/speaker, in which case no audio will be transferred from the microphone/speaker to XProtect Professional.
Microphone/speaker name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

On some hardware devices, audio can also be enabled/disabled on the hardware device itself, typically through the hardware device's own configuration web page. If audio on a hardware device does not work after enabling it in the Management Application, you should verify whether the problem may be due to audio being disabled on the hardware device itself.

Recording settings

Name	Description
Always	Always record audio on all applicable cameras.
Follow video	Record audio only when video is recorded.
Never	Never record audio on any cameras. Note that even though audio is never recorded, it is still be possible to listen to live audio in the Smart Client.

Events and output

About input and output

Hardware input, such as door sensors, can be attached to input ports on hardware devices. Input from such external hardware input units can be used for generating events in XProtect Professional.

Hardware output units can be attached to output ports on many hardware devices, allowing you to activate lights, sirens, and more from XProtect Professional. Such hardware output can be activated automatically by events, or manually from clients.

Before you specify use of hardware input and hardware output units on a hardware device, verify that sensor operation is recognized by the hardware device. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the XProtect Professional release notes to verify that input and output controlled operations are supported for the hardware device and firmware used.

You do not have to configure hardware input units separately, any hardware input units connected to hardware devices are automatically detected when you add the hardware devices to XProtect Professional. The same goes for hardware output, but hardware output does require some simple configuration in XProtect Professional.

If you want to **configure hardware output** and **automatically trigger output when events occur**, so that, for example, lights are switched on when a door is opened or when motion is detected in video, see Add a hardware output (on page 127) and Configure hardware output on event (on page 130).

About events and output

Events and output of various types can be used for automatically triggering actions in XProtect Professional. Examples of actions: starting or stopping recording on cameras, switching to a particular video frame rate, triggering e-mail and/or SMS notifications, making PTZ cameras move to specific preset positions, etc. Events can also be used for activating hardware output.

You can also configure events and output to generate alarms (see "About alarms" on page 192).

Events can be divided in to:

- **Internal events (system-related):** for example, motion, server responding/not responding, archiving problems, lack of disk space, etc.

- **External events (integrated):** for example, MIP plug-in events.

Overview of events and output

Types of events:

Name	Description
Analytics events:	Analytics events can be used as alarms and integrated seamlessly with the Alarms feature (see "About alarms" on page 192). Analytics events (see "Overview of events and output" on page 125) are typically data received from external third-party video content analysis (VCA) (see "VCA" on page 222) providers. An example of a VCA-based system could be an access control system.
Hardware input events:	Hardware input, such as door sensors, can be attached to input ports on hardware devices. Input from such external hardware input units can be used for generating events in XProtect Professional. Events based on input from hardware input units attached to hardware devices are called hardware input events. Some hardware devices have their own capabilities for detecting motion, for detecting moving and/or static objects, etc. (configured in the hardware devices' own software; typically by accessing a browser-based configuration interface on the hardware device's IP address). When this is the case, XProtect Professional considers such detections as input from the hardware, and you can use such detections as input events as well. Lastly, hardware input events can be based on XProtect Professional detecting motion in video from a camera, based on motion detection settings in XProtect Professional. This type of hardware input events is also called system motion detection events or VMD (Video Motion Detection) events. In earlier XProtect Professional versions, VMD events were an event type of their own; now they are simply considered a type of hardware input event.
Hardware output:	Hardware output units can be attached to output ports on many hardware devices, allowing you to activate lights, sirens, and more from XProtect Professional. Such hardware output can be activated automatically by events, or manually from clients.

Name	Description
Manual events:	Events may be generated manually by the users selecting them in their clients. These events are called manual events. Manual events can be of the type **Global events** or **Timer events:** Global events apply to all hardware whereas timer events are separate events, triggered by the hardware input event, manual event or generic event under which they are defined. Timer events occur a specified number of seconds or minutes after the event, under which they are defined, has occurred. Timer events may be used for a wide variety of purposes, typically for stopping previously triggered actions. **Example:** A camera starts recording based on a hardware input event, for example when a door is opened; a timer event stops the recording after 15 seconds.
Generic events:	Input may also be received in the form of TCP or UDP data packages, which can be analyzed by XProtect Professional, and—if they match specified criteria—used to generate events. Such events are called generic events.
Output control on event:	Hardware output can be activated automatically when events occur. For example, when a door is opened (hardware input event), lights are switched on (hardware output). When configuring the output control, you can select between all output and events defined in XProtect Professional. You are not limited to selecting output or events defined on particular hardware devices. You can use a single event for activating more than one output.

Before you configure events of any type, **configure general event handling**, such as which ports XProtect Professional should use for event data. Normally, you can just use the default values, but it is a good idea to verify that your organization is not already using the ports for other purposes. See Configure general event handling (on page 130).

Before you specify use of hardware input and hardware output units on a hardware device, verify that sensor operation is recognized by the hardware device. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the XProtect Professional release notes to verify that input and output controlled operations are supported for the hardware device and firmware used.

You do not have to configure hardware input units separately, any hardware input units connected to hardware devices are automatically detected when you add the hardware devices to XProtect Professional. The same goes for hardware output, but hardware output does require some simple configuration in XProtect Professional.

If you want to **configure hardware output** and **automatically trigger output when events occur**, so that, for example, lights are switched on when a door is opened or when motion is detected in video, see Add a hardware output (on page 127) and Configure hardware output on event (on page 130).

When you are ready to **configure events**, see Add a hardware input event (on page 127), Add a generic event (on page 129), and Add a manual event (on page 128). If you want to use timer events with your other events, see Add a timer event (on page 129).

Add an analytics event

To add an analytics event, do the following:

1. In the Management Application's navigation pane, expand **Events and Output**, right-click **Analytics Events** and select **Create New**.
2. Specify required properties (see "Analytics event" on page 133).
3. Click **OK**.
4. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Add a hardware input event

With hardware input events, you can turn input received from input units attached to hardware devices into events in XProtect Professional.

Before you specify input for a hardware device, verify that sensor operation is recognized by the hardware device. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the release notes to verify that input-controlled operation is supported for the hardware device and firmware used.

To add and/or configure a hardware input event, do the following:

1. In the Management Application navigation pane, expand **Advanced Configuration,** then expand **Events and Output.** Right-click **Hardware Input Events** and select **Enable New Input Event**.
2. In the **Hardware Input Event Properties** window's list of hardware devices, expand the required hardware device to see a list of pre-defined hardware input.
3. Select the required types of input to use them as events. The types of input often vary from camera to camera. If motion detection (see "Motion detection & exclude regions" on page 110) is enabled in XProtect Professional for the camera in question, note the input type **System Motion Detection**, which lets you turn detected motion in the camera's video stream into an event. In earlier XProtect Professional versions, this was known as a VMD event.

   Note that some types of input are mutually exclusive. When you select one type of input, you may therefore note that other types of input become unavailable for selection.
4. For each selected type of input, select required properties (see "Hardware input event" on page 135). When ready, click **OK**, or click the **Add button** to add a timer event (on page 129) to the event you have just created.
5. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Add a hardware output

With hardware output, you can add external output units, such as lights, sirens, door openers, etc., to your XProtect Professional system. Once added, output can be activated automatically by events or detected motion, or manually by client users.

Before you specify output, verify that sensor operation is recognized by the hardware device with which you are going to use the output. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the release notes to verify that output-controlled operation is supported for the hardware device and firmware used.

To add a hardware output event, do the following:

1. In the Management Application navigation pane, expand **Advanced Configuration,** then expand **Events and Output.** Right-click **Hardware Output** and select **Add New Output**.
2. In the **Hardware Output Properties** window's list of hardware devices, select the required hardware device, and click the **Add** button below the list.
3. Specify required properties (see "Hardware input event" on page 135).
4. Click **OK**.
5. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

For information about how to configure automatic activation of hardware output when events occur, see Configure hardware output on event (on page 130). You configure output for manual activation in clients as well as for automatic activation on detected motion individually for each camera (see "Output" on page 110).

Add a manual event

With manual events, your users with required rights (see "Configure user and group rights" on page 179) can trigger events manually from their clients. Manual events can be global (shared by all cameras) or tied to a particular camera (only available when the camera is selected). You can use manual events for a wide variety of purposes, for example:

- As start and stop events for use when scheduling cameras' online periods (see "Online period" on page 155). For example, you can make a camera start or stop transferring video to the surveillance system based on a manual event.
- As start and stop events for controlling other camera settings. For example, you can make a camera use a higher frame rate based on a manual event or you can use a manual event for triggering PTZ on event (on page 120).
- For triggering output. Particular output can be associated (see "Configure hardware output on event" on page 130) with manual events.
- For triggering event-based e-mail and/or SMS notifications.
- In combinations. For example, a manual event could make a camera start transferring video to the surveillance system while an output is triggered and an e-mail notification is sent to relevant people.

To add a manual event, do the following:

1. In the Management Application navigation pane, expand **Advanced Configuration,** then expand **Events and Output.** Right-click **Manual Events** and select **Add New Manual Event**
2. In the list in the left side of the **Manual Event Properties**, select global or a camera as required.

3. Click the **add** button and specify required properties (see "Hardware input event" on page 135). When ready, click **OK**, or click the **Add** button again to add a timer event (on page 129) to the event you have just created.

4. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Add a generic event

XProtect Professional can analyze received TCP and/or UDP data packages, and automatically trigger events when specified criteria are met. This way, you can easily integrate your XProtect Professional surveillance system with a very wide range of external sources, for example access control systems and alarm systems and more. Events based on the analysis of received TCP and/or UDP packets are called generic events.

1. In the Management Application navigation pane, expand **Advanced Configuration**, then expand **Events and Output**. Right-click **Generic Events** and select **Add New Generic Event**.

2. In the Generic Event Properties window, click the **Add** button, and specify required properties (see "Generic event" on page 138). When ready, click **OK**, or click the **Add** button to add a timer event to the event you have just created.

3. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Generate alarms based on analytics events

Generating alarms based on analytics events is normally a three-step process:

1. Enable the analytics events feature and set up its security. A list of allowed addresses can be used to control who can send event data to the system and on which port the server listens.

2. Create the analytics event, possibly with a description of the event, and test it.

3. Use the analytics event as the source of an alarm definition (see "Alarms definition" on page 195).

As indicated, to use VCA-based events (see "VCA" on page 222), most often a third-party VCA tool is required for supplying data to XProtect Professional. Which VCA tool to use is entirely up to you, as long as the data supplied by the tool adheres to the applied formatting rules described in the Milestone Analytics Events Developers Manual. Contact Milestone for more details.

Add a timer event

Timer events are separate events, triggered by the type of event under which they are defined. Timer events occur a specified number of seconds or minutes after the event under which they are defined has occurred. Timer events may be used for a wide variety of purposes, typically for stopping previously triggered actions. Examples:

- A camera starts recording based on a hardware input event, for example when a door is opened; a timer event stops the recording after 15 seconds

- Lights are switched on and a camera starts recording based on a manual event; a timer event stops the recording after one minute, and another timer event switches the lights off after two minutes

To add a timer event, select any event you have previously configured, click the **Add** button, and specify required properties (see "Timer event" on page 138). XProtect Professional comes with two simple schedule profiles, **Always on** and **Always off,** which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Tip: You can add as many timer events as required under an event. This way, you can, for example, make one timer event trigger something 10 seconds after the main event, another timer event trigger something else 30 seconds after the main event, and a third timer event trigger something else 2 minutes after the main event.

Configure hardware output on event

Once you have added hardware output (see "Add a hardware output" on page 127), such as lights, sirens, door openers, etc., you can associate the hardware output with events. This way, particular hardware output can be activated automatically when events occur. Example: When a door is opened (hardware input event), lights are switched on (hardware output).

When making the associations, you can select between **all** output and events defined on your XProtect Professional server; you are not limited to selecting output or events defined on particular hardware devices.

1. In the Management Application's navigation pane, expand **Advanced Configuration,** then expand **Events and Output.** Right-click **Output Control on Event** and select **Properties**.
2. Fill in the relevant properties (see "Output control on event (Events and Output-specific properties)" on page 142).
3. Click **OK**.
4. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

You can use a single event for activating more than one output.

You cannot delete associations, but you can change your selections or select **None** in both columns as required.

Tip: If you have not yet defined any suitable event or output, you can quickly do it: Use the **Configure events** list and/or **Configure Output...** button, located below the list of associations.

Configure general event handling

Before configuring events of any type, configure general event handling, such as which ports XProtect Professional should use for event data. Normally, you can just use the default values, but it is a good idea to verify that your organization is not already using the ports for other purposes.

1. In the Management Application's navigation pane, expand **Advanced Configuration**, right-click **Events and Output**, and select **Properties.**

2. Specify required properties (see "Ports and polling" on page 133). XProtect Professional comes with two simple schedule profiles, **Always on** and **Always off,** which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required.

3. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Test a generic event

If you have added a generic event, a quick and easy way to test your generic event is to first set up an event notification and then use Telnet to send a small amount of data which will trigger the generic event and in turn the event notification.

For this example, we have created a generic event called **Video**. Our generic event specifies that if the term **video** appears in a received TCP data package, the generic event should be triggered. Your generic event may be different, but you can still use the principles outlined in the following:

1. In the Management Application navigation pane, expand **Advanced Configurations**, then expand **Cameras and Storage Information**, right-click a camera to which you have access in the Smart Client, and select **Properties**.

2. Select **Event Notification** and select the required generic event. XProtect Professional comes with two simple schedule profiles, **Always on** and **Always off,** which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required.

   Make sure that your generic event is the **only** event appearing in the **Selected Events** list while you are performing the test, otherwise you cannot be sure that it is your generic event which triggers the event notification. Once you are done testing, you can move any temporarily removed events back to the **Selected Events** list.

3. Save your configuration changes by clicking the **Save Configuration** button in the Management Application toolbar.

4. Make sure the Recording Server service is running. Also make sure that the camera for which you just configured the event notification is displayed in your Smart Client, and that you have camera title bars enabled in your Smart Client so that you can see the yellow event indicator.

5. In Windows' **Start** menu, select **Run...**, and type the following in the **Open** field:

   - If you are performing the test on the XProtect Professional server itself:

     telnet localhost 1234

   - **If you are performing the test from a remote computer:** Substitute **localhost** with the IP address of the XProtect Professional server. Example: If the IP address of the XProtect Professional server is 123.123.123.123, type:

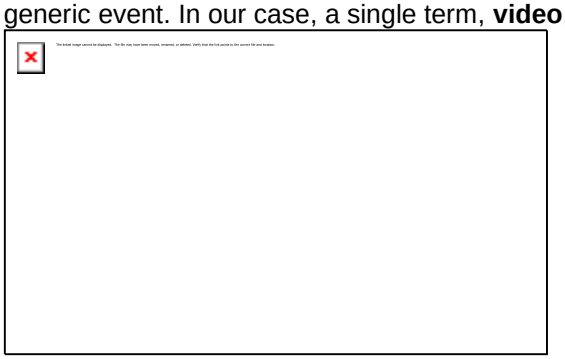
     ```
     telnet 123.123.123.123 1234
     ```

   This will open a **Telnet** window.

   In the above examples, the number **1234** indicates the port on which the XProtect Professional server listens for generic events. Port 1234 is the default port for this purpose, but it is possible

to change this by specifying another port number as part of the general event handling configuration (see "Configure general event handling" on page 130). If the alert and generic event port number has been changed on your system, type your system's alert and generic event port number instead of **1234**.

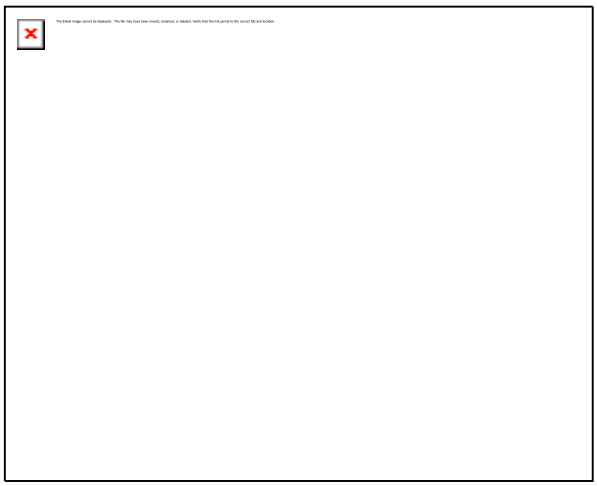
6. In the **Telnet** window, type the terms (so-called **event substring**) required to trigger your generic event. In our case, a single term, **video**, is required:



While you type in the Telnet window, you may experience so-called echo. This is the server repeating some or all of the characters it receives. It will not have any impact as long as you are sure you type the required characters.

7. Close the **Telnet** window. It is important that you close the window, since your input is not sent to the surveillance system until you close the window.

8. Go to your Smart Client. If the yellow event indicator lights up for the required camera, your generic event works as intended.:



What is Telnet? Telnet is a terminal emulation program used on TCP/IP networks. With Telnet, you can connect to a server from a computer on the network, and execute commands through Telnet as if you were entering them directly on the server. Windows includes a client for use with Telnet.

General event properties

Ports and polling

The **General Event Properties** window lets you specify network settings to be used in connection with event handling.

Name	Description
Alert and generic event port	Specify port number to use for handling events , including generic events. Default port is port 1234.
SMTP event port	Specify port number to use for sending event information from hardware devices to XProtect Professional via SMTP. Default port is port 25.
FTP event port	Port to use for FTP communication with the hardware device. Default port is port 21.
Polling interval [1/10] second	For a small number of hardware devices, primarily dedicated input/output devices (see "About dedicated input/output devices" on page 73), it is necessary for XProtect Professional to regularly check the state of the hardware devices' input ports in order to detect input. Such state checking at regular intervals is called polling. You can specify (in tenths of a second) the interval between state checks. Default value is 10 tenths of a second (that is one second). For dedicated input/output devices, it is highly recommended that the polling frequency is set to the lowest possible value (one tenth of a second between state checks). For information about which hardware devices require polling, see the release note.

Events and output properties

Properties in this window:

Analytics event

When you configure analytics events (see "Add an analytics event" on page 127), specify the following:

Name	Description
Name	Type a name for the event.
Description	Enter a description (optional).
Test Event	Test the validity of the event by clicking this button (optional). **Tip:** You can carry out this test at any step of the analytics event creation/editing process and as many times as you wish.

When you click **Test Event**, a window opens which goes through a number of conditions that must be met for analytics events to work. The window consists of two tabs: **Tasks** and **Errors**.

The **Tasks** tab lists the conditions that are tested and mark them failed: or success: The **Errors** tab shows a list of errors corresponding to any failed conditions.

Remember to save any changes made during the test.

When done, check the presence of your test event in the Smart Client's **Alarm list**. Sort by type **Test Alarm** to make your test event appear at the top of the **Alarm list**. See the Smart Client documentation for more details.

Conditions	Description	Error messages and solutions
Changes saved	If the event is new, is it saved? Or if there are changes to the event name, are these changes saved?	**Save changes before testing analytics event.** Solution/Explanation: Save changes.
Analytics Events enabled	Is the Analytics Event feature enabled?	**Analytics events have not been enabled.** Solution/Explanation: Enable the Analytics Events feature.
Address allowed	Is the IP address/host name of the machine sending the event(s) allowed (listed on the analytics events address list)?	**The local host name must be added as allowed address for the Analytics Event service.** Solution/Explanation: Add your machine to the analytics events address list (of allowed IP addresses/host names). **Error resolving the local host name.** Solution/Explanation: The IP address/host name of the machine cannot be found or is invalid.
Analytics event used in alarm definition	Is the analytics event used actively in any alarm definitions?	**Analytics event is not used in any alarm definition.** Solution/Explanation: Use the analytics event in an alarm definition.
Send analytics event	Did sending a test event to the Event Server succeed?	See table below.

Error messages and solutions for the condition **Send analytics event**:

Error messages	Solution/Explanation
Event Server not found.	Unable to find the Event Server service on the list of registered services.
Error connecting to Event Server.	Unable to connect to the Event Server service on the defined port (most likely due to network problems, the Event Server service being stopped or similar).
Error sending analytics event.	Connection to the Event Server service established but event cannot be sent (most likely due to network problems, for example time out).
Error receiving response from Event Server.	Event sent to Event Server but no reply received (most likely due to network problems or port being busy (see the Event Server log, typically located at ProgramData\Milestone\XProtect Event Server\logs\—can be opened in Microsoft Notepad or similar tool)).
Analytics event unknown by Event Server.	The Event Server service does not know the event most likely due to the event—or changes to the event—not having been saved.
Invalid analytics event received by Event Server.	Event format is somehow incorrect.
Sender unauthorized by Event Server.	Most likely your machine is not on the list of allowed IP addresses/host names.
Internal error in Event Server.	An Event Server error. Open the Event Server log in Microsoft Notepad or similar tool. The log is typically located at ProgramData\Milestone\XProtect Event Server\logs\
Invalid response received from Event Server.	Response is invalid. Possibly due to port being busy or network problems Open the Event Server log in Microsoft Notepad or similar tool. The log is typically located at ProgramData\Milestone\XProtect Event Server\logs\
Unknown response from Event Server.	Response is valid but not understood. Possibly due to port being busy or network problems. Open the Event Server log in Microsoft Notepad or similar tool. The log is typically located at ProgramData\Milestone\XProtect Event Server\logs\
Unexpected error.	Please contact your system provider Milestone Support (support@milestonesys.com) for help.

Hardware input event

When you add hardware input events (see "Add a hardware input event" on page 127), some properties depend on the selected type of input:

Name	Description
Enable	Select check box to use selected type of input as an event in XProtect Professional, and specify further properties.

Name	Description
Event name	Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]** Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Images from camera	Only relevant if using pre- and post-alarm images, a feature available for selected cameras only; it enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. Pre- and post-alarm images should not be confused the pre- and post-recording feature (see "Recording" on page 105) particular to XProtect Professional. Lets you select which camera you want to receive pre- and/or post-alarm images from.
Number of pre-alarm images	Only relevant if using pre-alarm images, a feature available for selected cameras only. Specify required number of pre-alarm images. Allowed number may differ from camera to camera; allowed range is displayed to the right of the field.
Frames per second	Only relevant if using pre-alarm images, a feature available for selected cameras only. Specify required frame rate. Used in combination with the Number of pre-alarm images field, this field indirectly allows you to control how long before the event you want to receive pre-alarm images from.
Send e-mail if this event occurs	Only available if e-mail notification (see "Configure e-mail notifications" on page 165) is enabled. Select if XProtect Professional should automatically send an e-mail when the event occurs. Recipients are defined as part of the e-mail notification configuration. When using e-mail notifications, also bear in mind individual cameras' scheduling (see "E-mail notification" on page 156).
Attach image from camera	Only available if e-mail notification (see "Configure e-mail notifications" on page 165) is enabled. Select to include an image—recorded at the time the event is triggered—in the e-mail notification, then select the required camera in the list next to the check box.
Send SMS if this event occurs	Only available if SMS notification (see "Configure SMS notifications" on page 168) is enabled. Select if XProtect Professional should automatically send an SMS when the event occurs. Recipients are defined as part of the SMS notification configuration. When using SMS notifications, also bear in mind individual cameras' scheduling (see "SMS notification" on page 156).
Delete	Delete a selected event.
Add	When a specific hardware input event is selected, clicking Add will add a timer event (on page 129) to the selected hardware input event.

Hardware output

When you add hardware output (see "Add a hardware output" on page 127), specify the following properties:

Name	Description
Output name	Specify a name. If you are going to make the hardware output available for manual activation in clients, this is the name that client users will see. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]** Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Output connected to	Select which of the hardware device's output ports the output is connected to. Many hardware devices only have a single output port; in that case simply select **Output 1**.
Keep output for	Lets you specify the amount of time for which the output should be applied. Specify the required amount of time in either 1/10 seconds or seconds. Some hardware devices are only able to apply output for a relatively short time, for example for up to five seconds. Refer to the documentation for the hardware device in question for exact information.

Tip: To verify that your hardware output works, click the **Test Output** button.

Manual event

When you add manual events (see "Add a manual event" on page 128), specify the following properties:

Name	Description
[List of defined global events and cameras]	Contains a Global node and a list of all defined cameras. You can configure as many manual events as required, no matter whether they are global or camera-specific. A + sign next to the Global node indicates that one or more global manual events have already been configured. A + sign next to a camera indicates that one or more manual events have already been configured for that camera.
Event name	Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]** Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.

Name	Description
Send e-mail if this event occurs	Only available if e-mail notification (see "Configure e-mail notifications" on page 165) is enabled. Select if XProtect Professional should automatically send an e-mail when the event occurs. Recipients are defined as part of the e-mail notification configuration. When using e-mail notifications, also bear in mind individual cameras' scheduling (see "E-mail notification" on page 156).
Attach image from camera	Only available if e-mail notification (see "Configure e-mail notifications" on page 165) is enabled. Select to include an image—recorded at the time the event is triggered—in the e-mail notification, then select the required camera in the list next to the check box.
Send SMS if this event occurs	Only available if SMS notification (see "Configure SMS notifications" on page 168) is enabled. Select if XProtect Professional should automatically send an SMS when the event occurs. Recipients are defined as part of the SMS notification configuration. When using SMS notifications, also bear in mind individual cameras' scheduling (see "SMS notification" on page 156).
Delete	Delete a selected event.
Add	Add a new event. When **Global** or a specific camera is selected, clicking **Add** will add a new manual event. When a specific manual event is selected, clicking **Add** will add a timer event (on page 129) to the selected manual event.

Timer event

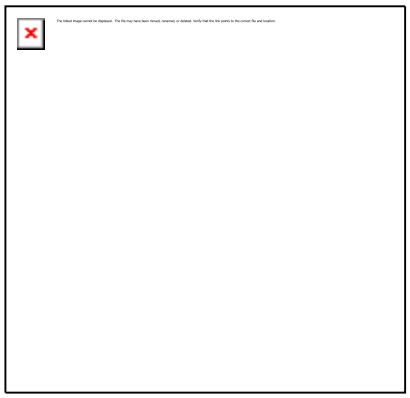
When you add timer events (see "Add a timer event" on page 129), specify the following properties:

Name	Description
Timer event name	Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]** Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Timer event occurs after	Specify the amount of time that should pass between the main event occurring and the timer event (in seconds or minutes).

Generic event

When you add generic events (see "Test a generic event" on page 131), specify the following properties:

Name	Description
Event name	Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]** Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Event port	Read-only field displaying the port number on which XProtect Professional listens for generic events (default is port 1234). The port number can be changed as part of the general event handling configuration (see "Configure general event handling" on page 130).
Event substring	Lets you specify the individual items for which XProtect Professional should look out for when analyzing data packages. Specify one or more terms, then click the Add button to add the specified term(s) to the Event message expression field, the content of which will be used for the actual analysis. Examples: • **Single term:** User001 (when added to the Event message expression field, the term will appear as "User001") • **Several terms as one item:** User001 Door053 Sunday (when added to the Event message expression field, the terms will appear as " User001 Door053 Sunday") When you add several terms as one item (appearing as, for example, " User001 Door053 Sunday" in the Event message expression field), everything between the quotation marks must appear together in the package, in the specified sequence, in order to match your criterion. If the terms must appear in the package, but not necessarily in any exact sequence, add the terms one by one (that is so they will appear as "User001" "Door053" "Sunday" in the Event message expression field). **Tip:** It is OK for TCP and UDP packages used for generic events to contain special characters, such as @, #, +, 敷~, etc. within the text string to be analyzed.

Name	Description
Event message expression	Displays the string which will be used for the actual package analysis. The field is not directly editable. However, you can position the cursor inside the field in order to determine where a new item should be included when you click the Add button or one of the parenthesis or operator buttons described in the following. Likewise, you can position the cursor inside the field in order to determine where an item should be removed when clicking the Remove button: The item immediately to the left of the cursor will be removed when you click the Remove button. • **(:** Lets you add a start parenthesis character to the Event message expression field. Parentheses can be used to ensure that related terms are processed together as a logical unit; in other words, they can be used to force a certain processing order in the analysis. Example: If using ("User001" OR "Door053") AND "Sunday", the two terms inside the parenthesis will be processed first, then the result will be combined with the last part of the string. In other words, XProtect Professional will first look for any packages containing either of the terms User001 or Door053, then it will take the results and run through them in order to see which packages also contain the term Sunday. • **):** Lets you add an end parenthesis character to the Event message expression field. • **AND:** Lets you add an AND operator to the Event message expression field. With an AND operator, you specify that the terms on both sides of the AND operator must be present. Example: If using User001 AND Door053 AND Sunday, the term User001 as well as the term Door053 as well as the term Sunday must be present in order for the criterion to be met. It is not enough for only one or two of the terms to be present. As a rule of thumb, the more terms you combine with AND, the fewer results you will retrieve:  Combinations with AND yields few results (indicated in red) • **OR:** Lets you add an OR operator to the Event message expression field. With an OR operator, you specify that either one or another term must be present. Example: If using User001 OR Door053 OR Sunday, the term User001 or the term Door053 or the term Sunday must be present in order for the criterion to be met. The criterion is satisfied even if only one of the terms is present. As a rule of thumb, the more terms you combine with OR, the more results you will retrieve:

Name	Description
Event priority	The same data package may be analyzed for different events. The ability to assign a priority to each event lets you manage which event should be triggered if a received package matches the criteria for several events. The priority must be specified as a number between 0 (lowest priority) and 1000 (highest priority). When XProtect Professional receives a TCP and/or UDP package, analysis of the packet will start with analysis for the event with the highest priority. This way, when a package matches the criteria for several events, only the event with the highest priority will be triggered. If a package matches the criteria for several events with an identical priority, for example two events with a priority of 999, all events with the priority in question will be triggered.
Event protocol	Select which protocol XProtect Professional should listen for in order to detect the event: • **Any:** Listen for, and analyze, packages using TCP as well as UDP protocol. • **TCP:** Listen for, and analyze, packages using TCP protocol only. • **UDP:** Listen for, and analyze, packages using UDP protocol only.
Event rule type	Select how particular XProtect Professional should be when analyzing received data packages: • **Search:** In order for the event to occur, the received package must contain the message specified in the Event message expression field, but may also have more content. Example: If you have specified that the received package should contain the terms "User001" and "Door053", the event will be triggered if the received package contains the terms "User001" and "Door053" and "Sunday" since your two required terms are contained in the received package. • **Match:** In order for the event to occur, the received package must contain exactly the message specified in the Event message expression field, and nothing else.
Send e-mail if this event occurs	Only available if e-mail notification (see "Configure e-mail notifications" on page 165) is enabled. Select if XProtect Professional should automatically send an e-mail when the event occurs. Recipients are defined as part of the e-mail notification configuration. When using e-mail notifications, also bear in mind individual cameras' scheduling (see "E-mail notification" on page 156).
Attach image from camera	Only available if e-mail notification (see "Configure e-mail notifications" on page 165) is enabled. Select to include an image—recorded at the time the event is triggered—in the e-mail notification, then select the required camera in the list next to the check box.

Name	Description
Send SMS if this event occurs	Only available if SMS notification (see "Configure SMS notifications" on page 168) is enabled. Select if XProtect Professional should automatically send an SMS when the event occurs. Recipients are defined as part of the SMS notification configuration. When using SMS notifications, also bear in mind individual cameras' scheduling (see "SMS notification" on page 156).
Delete	Delete a selected event.
Add	Add a new event. When the **Generic Events** node is selected, clicking **Add** will add a new generic event. When a specific generic event is selected, clicking **Add** will add a timer event (on page 129) to the selected generic event.

Output control on event (Events and Output-specific properties)

When you add output controls on events (see "Configure hardware output on event" on page 130), specify the following properties:

Name	Description
Event	Select the required event.
Output	Select the required output event.

Scheduling and archiving

About scheduling

The scheduling feature lets you specify:

- When you want to archive (see "About archiving" on page 143)
- That some cameras transfer video to XProtect Professional at all times
- That some cameras transfer video only within specific periods of time or when specific events occur
- When you want to receive notifications from the system

You can set up general scheduling properties for all your cameras or individual properties per camera. You can set up when:

- One or more cameras should be online (that is transfer video to XProtect Professional)

- One of more cameras should use speedup (that is use a higher than normal frame rate)
- You want to receive any e-mail and/or SMS notifications regarding one or more cameras.
- Archiving takes place.
- PTZ cameras should patrol, and according to which patrolling profile

About archiving

Archiving is an integrated and automated feature in XProtect Professional with which recordings are moved to free up space for new recordings. By default, recordings are stored in the XProtect Professional database for each camera. The database for each camera is capable of containing a maximum of 600,000 records or 40 GB. XProtect Professional automatically archives (see "About archiving" on page 143) recordings if a camera's database becomes full. Consequently, having sufficient archiving space is important.

You do not have to do anything to enable archiving. It runs in the background and is automatically enabled and carried out from the moment XProtect Professional is installed. The most recent recordings are saved on a local storage in order to prevent network-related problems in the saving process.

The default settings for XProtect Professional is to perform archiving once a day, or if your database becomes full. You can change the settings (see "Archiving" on page 154) for when and how often archiving takes place in the Management Application. You can also schedule archiving (see "About archiving schedules" on page 149) up to 24 times a day, with a minimum of one hour between each one. This way, you can proactively archive recordings, so databases will never become full. Basically, the more you expect to record, the more often you should archive.

You can also change the retention time, which is the total amount of time you want to keep recordings from a camera (recordings in the camera's database as well as any archived recordings) under the properties of the individual camera.

XProtect Professional automatically archives recordings if a camera's database becomes full. You only specify **one** time limit (the retention time) as part of the general Recording and Archiving paths (on page 84) properties. Note that retention time will determine when archiving takes place. Retention time is the **total** amount of time for which you want to keep recordings from a camera (that is recordings in the camera's database **as well as** any archived recordings).

Backup of archives

Creating backups based on the content of camera databases is not recommended as it may cause sharing violations or other malfunctions. Instead, create backups based on the content of archives. If you have not specified separate archiving locations for separate cameras, you could back up the default local archiving directory, **Archives**.

Important: When you schedule a backup, make sure the backup job does not overlap with any scheduled archiving times.

If archiving fails

Under rare circumstances, archiving may fail, for example due to network problems. However, in XProtect Professional this does not pose a threat. XProtect Professional creates a new database and continues archiving in this new database. You can work with—and view—both this new database and the old one like any other databases.

About archiving locations

The default archiving folder (see "Configure default file paths" on page 212) (C:\MediaDatabase) is located on the XProtect Professional server. You can change the default archiving folder to any other location locally, or select a location on a network drive to use as the default archiving folder. In the archiving folder, separate subfolders for storing archives for each camera are automatically created. These subfolders are named after the MAC address of the hardware device to which the camera is connected.

Because you can keep archives spanning many days of recordings and archiving may take place several times per day, further subfolders, named with the archiving date and time, are also automatically created.

The subfolders are named according to the following structure:

```
...\Archives\CameraMACAddress_VideoEncoderChannel\DateAndTime
```

If the video encoder does not have several channels, the video encoder channel will always be _1 (example: 00408c51e181_1).

Example: an archiving at 23.15 on 31st December 2012 for a camera with the MAC address 00408c51e181 attached to channel 2 would be stored:

```
C:\MediaDatabase\Archives\00408c51e181_2\2012-12-31-23-15
```

Before configuring archiving (see "About archiving" on page 143) locations, consider whether you want to use static or dynamic archiving paths:

- **Static** archiving paths mean that for a particular camera, archiving will take place to a particular location, and to that location only. Static archiving paths are in principle individual for each camera, but they do not have to be unique: several cameras can easily use the same path if required.

  You can configure static archiving paths for individual cameras, or as part of the general Recording and archiving paths properties.

  - **Individual cameras:** In the Management Application's navigation pane, expand **Advanced Configuration**, expand **Cameras and Storage Information**, double-click the required camera, select **Recording & Archiving Paths**, and specify required properties (see "Recording and archiving paths" on page 106).
  - **General Recording and Archiving Paths:** In the Management Application 's navigation pane, expand **Advanced Configuration**, double-click **Cameras and Storage Information**, and specify required properties (see "Recording and archiving paths" on page 84).

  Tip: If several cameras should use the same path, use the general Recording & Archiving Paths properties. There you get a template feature which lets you specify shared archiving locations in just a few clicks.

- **Dynamic** archiving paths allow greater flexibility, and are highly recommended. With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. If the path containing the camera database to be archived is on one of the drives you have selected for dynamic archiving, XProtect Professional will always try to archive to that drive first. If not, XProtect Professional automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive. This fact will have no impact on how users find and view archived recordings.

Dynamic archiving paths are general for all your cameras; you cannot configure dynamic archiving paths for individual cameras.

To configure archiving paths: In the Management Application's navigation pane, expand **Advanced Configuration**, double-click **Cameras and Storage Information**, select **Dynamic Path Selection - Archives**, and specify required properties (see "Dynamic path selection" on page 86).

If you configure your cameras through the Configure video and recording wizard (see "The Configure Video and Recording wizard" on page 56), the wizard also lets you configure archiving paths.

About archiving to other locations

When you archive to other locations than the default archiving directory, XProtect Professional will first temporarily store the archive in the local default archiving directory, then immediately move the archive to the archiving location you have specified.

Archiving directly to a network drive can mean that archiving time varies depending on the available bandwidth on the network. First storing the archive locally, then moving it speeds up the archiving procedure, and reduces delays in case of network problems.

If you archive to a network drive, the regular camera database can only be stored on a local drive attached directly to the XProtect Professional server.

About dynamic archive paths

With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. Using dynamic paths is recommended and is the default setting when you configure cameras through the Configure video & recording wizard (see "About video and recording configuration" on page 77).

If the path containing the camera's database is on one of the drives you have selected for dynamic archiving, XProtect Professional will always try to archive to that drive first. If not, XProtect Professional automatically archives to the archiving drive with the most available space at any time, provided a camera database is not using that drive.

The drive that has the most available space may change during the archiving process, and archiving may therefore happen to several archiving drives during the same process. This will have no impact on how users find and view archived recordings.

Dynamic archiving paths are general for all your cameras; you cannot configure dynamic archiving paths for individual cameras.

When deciding which drives to use for dynamic archiving, consider the pros and cons in the following examples (in which we assume that the default archiving path (see "Configure default file paths" on page 212) is on drive C:—drive letters are examples only, different drive letters may of course be used in your organization):

- **Camera records to drive C: and archives to drive C:**

  If the path containing the camera's database is on one of the drives you have selected for dynamic archiving, XProtect Professional will always try to archive to that drive first. Archiving will take place quickly, but may also fill up the drive with data fairly quickly.

- **Camera records to drive C: and archives to drive D:**

  Recordings and archives are on separate drives. Archiving takes place less quickly. XProtect Professional will first temporarily store the archive in the local default archiving directory on C:,

then immediately move the archive to the archiving location on D:. Therefore, sufficient space to accommodate the temporary archive is required on C:.

- **Camera 1 records to drive C: and archives to drive D: while Camera 2 records to drive D: and archives to drive C:**

  Avoid this. One camera's archiving may take up space required for another camera's recordings. In the above example, Camera 1's archiving to D: may result in no recording space for camera 2 on D:. The rule is: "Do not cross recording and archiving drives."•

If you use several surveillance servers in a master/slave setup, each surveillance server must archive to its own mapped location in order for archiving to work. If you attempt to archive to the same mapped location for all the servers, archiving will fail.

If you use several surveillance servers in a master/slave setup, each surveillance server must archive to its own mapped location in order for archiving to work. If you attempt to archive to the same mapped location for all the servers, archiving will fail.

About archiving audio

If an audio source (for example, a microphone) is enabled on a hardware device, audio recordings are archived together with video recordings from the camera attached to the hardware device. If the hardware device is a video encoder with several channels, audio is archived with the camera on channel 1.

When an audio source is enabled, audio is recorded to the associated camera's database. This will affect the database's capacity for storing video. You may, therefore, want to use scheduled archiving more frequently if recording audio and video than if only recording video.

Storage capacity required for archiving

The storage capacity required for archiving depends entirely on the amount of recordings you plan to keep, and on how long you want to keep them (retention time). Some organizations want to keep archived recordings from a large number of cameras for several months or years. Other organizations may only want to archive recordings from one or two cameras, and they may want to keep their archives for much shorter periods of time.

You should always first consider the storage capacity of the **local** drive containing the default archiving directory to which archived recordings are always moved, even though they may immediately after be moved to an archiving location on another drive. Basically, the capacity of the local drive should be at least twice the size required for storing the databases of all cameras.

When you archive, XProtect Professional automatically checks that space required for the data to be archived plus 1 GB of free disk space per camera is available at the archiving location. If not, the archive location's oldest data from the camera in question will be deleted until there is sufficient free space for the new data to be archived.

When you estimate storage capacity required for archiving, consider your organization's needs, then plan for worst case rather than best case scenarios.

You cannot archive to external drives, only to local drives on the XProtect Professional server.

Tip: The Storage Calculator, found in the Support section of the Milestone website, can help you determine the storage capacity required for your surveillance system.

Automatic response if running out of disk space

If XProtect Professional runs of disk space while archiving, you can set up an automatic response. Two scenarios can occur, depending on whether the camera database drive is different from, or identical to, the archiving drive:

Different drives: Automatic archiving if database drive runs out of disk space

In case the XProtect Professional server is running out of disk space, and the archiving drive is **different from** the camera database drive, and archiving has not taken place within the last hour, archiving will automatically begin in an attempt to free up disk space. This will happen regardless of any archiving schedules. The server is considered to be running out of disk space if:

- there is less than 10% disk space left, and the available disk space goes below 30 GB plus 1.5 GB per camera
- the available disk space goes below 150 MB plus 20 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 350 MB (150 MB plus 20 MB for each of the ten cameras))

The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 10% disk space left.

On the archiving drive, XProtect Professional automatically checks that the space required for data from a camera to be archived plus 1 GB of free disk space per camera is available. If not, the archive drive's oldest data from the camera in question will be deleted until there is sufficient free space for the new data to be archived.

IMPORTANT: You will lose the archive data being deleted.

Same drive: Automatic moving or deletion of archives if drive runs out of disk space

If the XProtect Professional server is running out of disk space, and the archiving drive is identical to the camera database drive, XProtect Professional will automatically do the following in an attempt to free up disk space:

1. First, the program will attempt to move archives (moving archives is only possible if you use dynamic archiving, with which you can archive to several different drives). This will happen if:
   - there is less than 15% disk space left, and the available disk space goes below 40 GB plus 2 GB per camera

     - or -
   - the available disk space goes below 225 MB plus 30 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 525 MB (225 MB plus 30 MB for each of the ten cameras))

   The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 15% disk space left.
2. If moving archives is not possible, XProtect Professional will attempt to delete the oldest archives. This will happen if:
   - there is less than 10% disk space left, and the available disk space goes below 30 GB plus 1.5 GB per camera

- or -

- the available disk space goes below 150 MB plus 20 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 350 MB (150 MB plus 20 MB for each of the ten cameras))

The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 10% disk space left.

IMPORTANT: You will lose data from the archives being deleted.

3. Ultimately, if there are no archives to delete, XProtect Professional will attempt to resize camera databases by deleting their oldest recordings. This will happen if:

- there is less than 5% disk space left, and the available disk space goes below 20 GB plus 1 GB per camera

- or -

- the available disk space goes below 75 MB plus 10 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 175 MB (75 MB plus 10 MB for each of the ten cameras))

The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 5% disk space left.

IMPORTANT: You will lose the data deleted as part of the database resizing process.

When the recording server is restarted upon such database resizing, the original database sizes will be used. You should therefore make sure the drive size problem is solved, or adjust camera database sizes to reflect the altered drive size.

Tip: Should the database resizing procedure take place, you will be informed on-screen in the Smart Client, in log files, and (if set up) through an e-mail and/or SMS notification.

1. First, XProtect Professional will attempt to delete archives. This will happen if:

- there is less than per camera

- or -

- the available disk space goes below 150 MB plus 20 MB per camera

The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 10% disk space left.

IMPORTANT: You will lose data from the archives being deleted.

1. Ultimately, if there are no archives to delete, XProtect Professional will attempt to resize camera databases. This will happen if:

- there is less than 5% disk space left, and the available disk space goes below 20 GB plus 1 GB per camera

- or -

- the available disk space goes below 75 MB plus 10 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 175 MB (75 MB plus 10 MB for each of the ten cameras))

The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 5% disk space left.

IMPORTANT: You will lose the data deleted as part of the database resizing process.

When the recording server is restarted upon such database resizing, the original database sizes will be used. You should therefore make sure the drive size problem is solved, or adjust camera database sizes to reflect the altered drive size.

Tip: Should the database resizing procedure take place, you will be informed on-screen in the Smart Client, in log files, and (if set up) through an e-mail notification.

About archiving schedules

There are two ways in which to configure archiving schedules:

- While you configure your cameras through the Configure Video and Recording wizard (see "The Configure Video and Recording wizard" on page 56), in which case you configure your archiving schedule on the wizard's **Drive selection** page.
- As part of the general Scheduling and Archiving properties: In the Management Application's navigation pane, expand **Advanced Configuration**, right-click **Scheduling and Archiving**, select **Properties**, select **Archiving** in the dialog, and specify required properties.

View archived recordings

You can view archived recordings via the Smart Client. Use, for example, all of the Smart Client's advanced features (video browsing, and export) for archived recordings.

Stored archives

For archived recordings stored on a local or network drive, you use the Smart Client playback features to find and view the relevant recordings, just like you would with recordings stored in a camera's regular database.

Exported archives

For exported archives, for example archives stored on a CD, you use the Smart Client. See the Smart Client documentation for more information.

Configure general scheduling and archiving

Do the following:

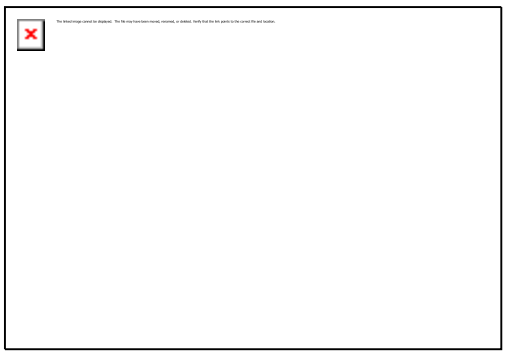
1. In the Management Application navigation pane, expand **Advanced Configuration**, right-click **Scheduling and Archiving**, and select **Properties**.
2. Specify properties as required for Scheduling all cameras (on page 152), Scheduling options (on page 153), and Archiving.
3. XProtect Professional comes with two simple schedule profiles, **Always on** and **Always off,** which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required.
4. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

When archiving, disable any virus scanning (see "Virus scanning information" on page 24) of camera databases and archiving locations.

Configure camera-specific schedules

If you base your schedule profile—or parts of it—on events within periods of time, remember to select **Start event** and **Stop event** from the lists below the calendar section.

Tip: If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields.



The fact that a camera transfers video to XProtect Professional does not necessarily mean that video from the camera is recorded. Recording is configured separately; see Configure video and recording (see "About video and recording configuration" on page 77).

For each camera, you can create schedule profiles based on:

Online periods

- Periods of time (example: Mondays from 08.30 until 17.45), shown in pink: 
- Events within periods of time (example: from Event A occurs until Event B occurs Mondays from 08.30 until 17.45), shown in yellow: 

  The two options can be combined  , but they cannot overlap in time.

Speedup

- Periods of time (example: Mondays from 08.30 until 17.45), shown in olive green: 

E-mail notification

- Periods of time (example: Mondays from 08.30 until 17.45), shown in blue: 

SMS notification

- Periods of time (example: Mondays from 08.30 until 17.45), shown in green: 

PTZ patrolling

- Periods of time (example: Mondays from 08.30 until 17.45), shown in red: 

- If use of one patrolling profile is followed immediately by use of another, run your mouse pointer over the red bar to see which patrolling profile applies when.

XProtect Professional comes with two simple schedule profiles, **Always on** and **Always off,** which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required.

1. In the **Schedule Profiles** list, select **Add new...**.
2. In the **Add Profile** dialog, enter a name for the profile. Names must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
3. In the top right corner of the dialog, select **Set camera to start/stop on time** (to base subsequent settings on periods of time) or **Set camera to start/stop on event** (to base subsequent settings on events within periods of time).

   Tip: You can combine the two, so you may return to this step in order to toggle between the two options.
4. In the calendar section, place your mouse pointer at a required start point, then hold down the left mouse button, drag the mouse pointer and release at the required end point.
   - You specify each day separately.
   - You specify time in increments of five minutes. XProtect Professional helps you by showing the time over which your mouse pointer is positioned.

If you base your schedule profile—or parts of it—on events within periods of time, remember to select **Start event** and **Stop event** from the lists below the calendar section.

- **Tip:** If you have not yet defined any suitable events, you can quickly do it: Use the **Configure events** list, located below the other fields.
- To delete an unwanted part of a schedule profile, right-click it and select **Delete**.
- To quickly fill or clear an entire day, double-click the name of the day.
- As an alternative to dragging inside the calendar section, use the **Start time**, **End time** and **Day** fields, then the **Change Period** or **Set Period** button as required. When using the **Start time** and **End time** fields, remember that time is specified in increments of five minutes. You cannot specify a period shorter than five minutes, and you can only use times like 12:00, 12.05, 12:10, 12:15, etc. If you specify a time outside of the five-minute intervals, such as 12:13, you will get an error message.

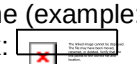
General scheduling properties

Properties in this window:

Scheduling all cameras

When you configure general scheduling and archiving (see "Configure general scheduling and archiving" on page 149), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that the properties **Online Period**, **Speedup**, **E-mail Notification**, **SMS Notification**, and **PTZ Patrolling** can also be specified individually for each camera.

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. You then use one of the two **Set** buttons to actually apply the template. **Tip:** To select all cameras in the list, click the **Select All** button.
Camera	The name as it appears in the Management Application as well as in clients.
Online	Select the required profile (for example **Always on**) for the online schedule (see "Configure camera-specific schedules" on page 79) for the camera(s) in question. You specify a camera's online periods by creating schedule profiles based on: • Periods of time (example: Mondays from 08.30 until 17.45), shown in pink:  • Events within periods of time (example: from Event A occurs until Event B occurs Mondays from 08.30 until 17.45), shown in yellow:  The two options can be combined  ; but they cannot overlap in time.

Name	Description
E-mail	Select the required profile for the e-mail notification schedule (see "E-mail notification" on page 156) for the camera(s) in question. You specify a camera's e-mail notification periods by creating schedule profiles based on periods of time (example: Mondays from 08.30 until 17.45), shown in blue: 
SMS	Select the required profile for the SMS notification schedule (see "SMS notification" on page 156) for the camera(s) in question. You specify a camera's SMS notification periods by creating schedule profiles based on periods of time (example: Mondays from 08.30 until 17.45), shown in green: 
PTZ Patrolling	Only available for PTZ (Pan/Tilt/Zoom) cameras with patrolling, the continuous movement of a PTZ camera between a number of preset positions. Lets you select the required profile for the PTZ patrolling schedule (see "PTZ patrolling" on page 156) for the camera(s) in question. You specify a camera's patrolling schedule based on patrolling profiles within particular periods of time (example: Mondays from 08.30 until 17.45), shown in red: 
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras. **Tip:** To select more than one value press CTRL while selecting.
New schedule profile	Create a new schedule profile of any type by clicking the **Create...** button.

Scheduling options

When you configure general scheduling and archiving (see "Configure general scheduling and archiving" on page 149), you can specify certain properties for many cameras in one go. In the case of Scheduling Options, it is because the properties are shared by all cameras.

Name	Description
Start cameras on client requests	Cameras may be offline, for example because they have reached the end of an online recording schedule (see "Online period" on page 155), in which case client users will not be able to view live video from the cameras. However, if you select **Start cameras on client requests**, client users will be able to view live video from the camera outside online schedule—but without recording (technically: force the camera to be online outside its online schedule). You must select **Enable recording when started on client request** (see the following), if you want recording to take place.

Name	Description
Enable recording when started on client request	Enable recording on the camera when **Start cameras on client requests** (see the previous) is also selected. If a user does not have access to manual recording (see "Camera access" on page 181), selecting **Enable recording when started on client request**, will **not** enable the user to do manual recording.
Schedule profile for new cameras	Select which online schedule profile to use as default for cameras you subsequently add to your XProtect Professional system. Note that your selection only applies for the online schedule, not for any other schedules. Default selection is **Always on**, meaning that new cameras will always be online, that is transferring video to the XProtect Professional server for live viewing and further processing.
Maximum delay between reconnect attempts	Control the aggressiveness of reconnection attempts. If XProtect Professional loses the connection to a camera, it will by default attempt to re-establish the connection after ten seconds. In some environments, for example if using vehicle-mounted cameras through wireless connections, camera connections may frequently be lost, and you may want to change the aggressiveness of such reconnection attempts.

You can view live and even record video from a camera outside its online recording schedule. To do this, you select the **Start cameras on client requests** and, if needed, the **Enable recording when started on client request** options in the following when setting up your scheduling properties for the camera in question.

Archiving

XProtect Professional automatically archives (see "About archiving" on page 143) recordings if a camera's database becomes full (in earlier versions, this was an option configured individually for each camera).

Name	Description
Archiving Times	Specify when you want XProtect Professional to automatically move recordings to your archiving path(s). You can specify up to 24 archiving times per day, with minimum one hour between each one. Select the hour, minute and second values and click the **up** and **down** buttons to increase or decrease values, or simply overwrite the selected value, and then click **Add**. The more you expect to record, the more often you should archive.
Send e-mail on archiving failure	If selected, XProtect Professional will automatically send an e-mail to selected recipients if archiving fails. This requires that the e-mail notification (on page 156) feature is enabled. Recipients are defined as part of the e-mail notification properties.
Send SMS on archiving failure	If selected, XProtect Professional will automatically send an SMS (mobile phone text message) to selected recipients if archiving fails. This requires that the SMS notification (on page 156) feature is enabled. Recipients are defined as part of the SMS notification properties (see "SMS properties" on page 168).

Camera-specific scheduling properties

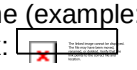
Properties in this window:

Online period

When you configure scheduling (see "Configure camera-specific schedules" on page 79) for specific cameras, your **Online Period** settings are probably the most important, since they determine when each camera should transfer video to XProtect Professional.

By default, cameras added to XProtect Professional will automatically be online, and you will only need to modify the online period settings if you require cameras to be online only at specific times or events. Note, however, that this default may be changed as part of the general scheduling options (see "Scheduling options" on page 153), in which case subsequently added cameras will not automatically be online.

The fact that a camera transfers video to XProtect Professional does not necessarily mean that video from the camera is recorded. Recording is configured separately; see Configure video and recording (see "About video and recording configuration" on page 77).

Name	Description
Online	Select the required profile (for example **Always on**) for the online schedule (see "Configure camera-specific schedules" on page 79) for the camera(s) in question. You specify a camera's online periods by creating schedule profiles based on: • Periods of time (example: Mondays from 08.30 until 17.45), shown in pink:  • Events within periods of time (example: from Event A occurs until Event B occurs Mondays from 08.30 until 17.45), shown in yellow:  The two options can be combined  ; but they cannot overlap in time.

Is it possible to view live and even record video from a camera outside its online recording schedule? Yes, you select the Start cameras on client requests (see "Scheduling options" on page 153) and, if needed, the Enable recording when started on client request **(see "Scheduling options" on page 153)** options when setting up your scheduling properties for the camera in question.

Speedup

Speedup may also take place based on events, but that is configured elsewhere: See Frame rate - MJPEG (General recording and storage properties) (see "Frame rate - MJPEG" on page 93) and Video (Camera-specific properties) (see "Video" on page 101).

Name	Description
Speedup	For specific MJPEG cameras, specify speedup periods. Before you can define this type of schedule, speedup must be enabled (see "Frame rate - MJPEG" on page 93). You specify a camera's speedup periods by creating schedule profiles based on periods of time (example: Mondays from 08.30 until 17.45), shown in olive green: 

E-mail notification

When you configure scheduling (see "Configure camera-specific schedules" on page 79) for specific cameras, you can specify e-mail notification (see "Configure e-mail notifications" on page 165) periods. Before you can define this type of schedule, e-mail notification must be enabled (see "E-mail properties" on page 166).

Name	Description
E-mail	Select the required profile for the e-mail notification schedule (see "E-mail notification" on page 156) for the camera(s) in question. You specify a camera's e-mail notification periods by creating schedule profiles based on periods of time (example: Mondays from 08.30 until 17.45), shown in blue: 

SMS notification

When you configure scheduling (see "Configure camera-specific schedules" on page 79) for specific cameras, you can specify SMS notification (see "Configure SMS notifications" on page 168) periods. Before you can define this type of schedule, SMS notification must be enabled (see "SMS properties" on page 168).

Name	Description
SMS	Select the required profile for the SMS notification schedule (see "SMS notification" on page 156) for the camera(s) in question. You specify a camera's SMS notification periods by creating schedule profiles based on periods of time (example: Mondays from 08.30 until 17.45), shown in green: 

PTZ patrolling

When you configure scheduling (see "Configure camera-specific schedules" on page 79) for PTZ (Pan/Tilt/Zoom) cameras capable of patrolling (see "PTZ patrolling" on page 117), you can specify

which patrolling profiles to use at specific times. Before you can define this type of schedule, patrolling must be configured for the cameras in question.

Name	Description
PTZ Patrolling	Only available for PTZ (Pan/Tilt/Zoom) cameras with patrolling, the continuous movement of a PTZ camera between a number of preset positions. Lets you select the required profile for the PTZ patrolling schedule (see "PTZ patrolling" on page 156) for the camera(s) in question. You specify a camera's patrolling schedule based on patrolling profiles within particular periods of time (example: Mondays from 08.30 until 17.45), shown in red: 

Use of one patrolling profile may be followed immediately by use of another (example: use the Daytime patrolling profile Mondays from 08.30 until 17.45, then the Evening patrolling profile Mondays from 17.45 until 23.00). Use of two patrolling profiles cannot overlap.

Unlike other types of scheduling, there are no ready-made **Always on** and **Always off** schedule profiles for PTZ patrolling. You can create any number of customized schedule profiles for each camera. When you create a customized schedule profile (see "Configure camera-specific schedules" on page 79) for one camera, you can reuse it with other cameras if required.

Matrix

About Matrix video sharing

The Matrix feature allows distributed viewing of live video from any camera to any Matrix recipient on a network operating with XProtect Professional. A computer on which Matrix-triggered video can be viewed is known as a Matrix recipient. In order to become a Matrix recipient, the computer must have the multi-purpose Smart Client installed.

For more information about Matrix recipients refer to the Smart Client User's Manual, available on the XProtect Professional software DVD as well as from www.milestonesys.com. Also, once installed, the Smart Client has its own built-in help system.

There are two ways in which Matrix-triggered video can appear on a Matrix recipient:

- **Manual triggering**: Another user wants to share important video, and sends it from a Smart Client—or from a custom-made web page—to the required Matrix recipient.
- **Automatic triggering**: Video is sent to the required Matrix recipient automatically when a predefined event occurs; for example when a door sensor detects that a door is opened, or when the surveillance system detects motion in the video from a camera.

About Matrix recipients

A computer on which Matrix-triggered video can be viewed is known as a Matrix recipient. In order to become a Matrix recipient, the computer must have the multi-purpose Smart Client installed.

For more information about Matrix recipients refer to the Smart Client User's Manual, available on the XProtect Professional software DVD as well as from www.milestonesys.com. Also, once installed, the Smart Client has its own built-in help system.

There are two ways in which Matrix-triggered video can appear on a Matrix recipient:

- **Manual triggering**: Another user wants to share important video, and sends it from a Smart Client—or from a custom-made web page—to the required Matrix recipient.
- **Automatic triggering**: Video is sent to the required Matrix recipient automatically when a predefined event occurs, for example when a door sensor detects that a door is opened, or when the surveillance system detects motion in the video from a camera.

Configure Matrix

1. In the Management Application's Navigation pane, expand **Advanced Configuration**, right-click **Matrix** and select **Properties**.
2. Enable the use of Matrix by selecting the **Enable Matrix** check box.
3. Specify required properties (see "Matrix recipients" on page 158), or, for automatically triggered video sharing, select **Matrix Event Control** and configure Matrix Event Control properties (see "Matrix event control" on page 160).When ready, click **OK.**
4. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Configure Matrix for video sharing

1. In the Management Application's Navigation pane, expand **Advanced Configuration**, right-click **Matrix** and select **Properties**.
2. Enable the use of Matrix by selecting the **Enable Matrix** check box.
3. Specify required properties (see "Matrix recipients" on page 158), or, for automatically triggered video sharing, select **Matrix Event Control** and configure Matrix Event Control properties (see "Matrix event control" on page 160).When ready, click **OK.**
4. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Matrix properties

Properties in this window:

Matrix recipients

The **Matrix Recipients** tab is used for enabling Matrix functionality and for defining on which computers to display Matrix-triggered live video. A computer on which Matrix-triggered video can be displayed is known as a Matrix recipient. Being able to view Matrix-triggered video requires that a Smart Client is installed on the user's computer.

Name	Description
Enable Matrix	Select check box to enable Matrix functionality.
[List of Defined Matrix recipients]	Lists any already defined Matrix recipients, that is computers on which Matrix-triggered video can be displayed. To change the properties of an already defined Matrix recipient, select the required Matrix recipient, make the changes in the fields below the list, then click the Update button. To remove a Matrix recipient from the list, select the unwanted Matrix recipient, then click the **Delete** button.
Delete	Available only when you have selected a Matrix recipient in the list. Clicking the **Delete** button will remove the selected Matrix recipient. You will be prompted to confirm the removal.
Name	Name for the Matrix recipient. Used when adding a new Matrix recipient or editing the properties of an existing one. The name will appear in various day-to-day usage situations; it is therefore a good idea to use a descriptive and unambiguous name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
Address	IP address of the Matrix recipient, used when adding a new Matrix recipient or editing the properties of an existing one.
Port	Specify the port number to be used when sending commands to the Matrix recipient. Used when adding a new Matrix recipient or editing the properties of an existing one. The Matrix recipient will listen for commands on this port. By default, port 12345 is used; you can of course specify another port number.
Password	Specify the password to be used when communicating with the Matrix recipient. Used when adding a new Matrix recipient or editing the properties of an existing one
Matrix recipient is a Smart Client	Select if the Matrix recipient in question is a Smart Client. Matrix-triggered live video may also be displayed in usersSmart Clients. If a Smart Client is used, distribution of the Matrix -triggered live video takes place slightly differently.
Clear	Removes any content in the **Name**, **Address,** and **Password** fields.
Update	Updates the properties of the selected Matrix recipient with the changes made during editing. Available only if you have edited the properties of an existing Matrix recipient.
Add	Adds the new Matrix recipient to the list. Available only if you have added properties of a new Matrix recipient in the **Name**, **Address**, **Port**, **Password**, and possibly Smart Client fields.

Matrix event control

The **Matrix Event Control** tab is used for configuring the automatic sending of live video based on predefined events. You can define exactly which events and cameras to use on a per- Matrix recipient basis.

The **Matrix Event Control** tab displays the list of Matrix recipients defined on the **Matrix Recipients** tab.

Right-clicking a Matrix recipient brings up a list of devices with belonging events. When you select an event, it will initially be highlighted by a red exclamation mark, indicating that there is additional configuration to be done. Right-clicking an event brings up a list of options for the selected event:

Name	Description
Delete [selected event]	Deletes selected event on selected device.
Connect	Connects to the camera (actual camera is specified after selecting action to be taken).
Disconnect, then connect	Disconnect any existing connections, then connect again. With this option the live video will appear in the Matrix recipient on a first-in-first-out basis. Each time a new event occurs, video from the latest event is displayed prominently in a specific position on the Matrix recipient, while at the same time video from the older events is shifted to less prominent positions and eventually ”pushed out” of the Matrix recipient in order to make space for the latest event's video. With the **Connect** option, you may experience that if video triggered by one event on a camera is already shown on the Matrix recipient, videos triggered by another event on the same camera will not be displayed prominently as coming from the latest event – simply because the Matrix recipient is already showing video from the camera in a less prominent position. By selecting **Disconnect, then connect** you can avoid this issue, and ensure that video from the latest event is always displayed prominently.
Disconnect	Disconnects any existing connection. Use if a particular event should cause video to stop being displayed in the Matrix recipient, even if they are not yet old enough to be “pushed out” of the Matrix recipient.

If you selected Connect, another red exclamation mark will indicate that there is still some configuration to be done. Right-clicking an action to select which camera to apply the action on.

In this example, we have specified that when motion is detected on Camera b, the selected Matrix recipient should connect to Camera b:

Logs

About logs

XProtect Professional can generate various logs.

Log types

Name	Description
Management Application log files	These files log activity in the Management Application. A new log file is created for each day the Management Application is used. You cannot disable this type of logging. Management Application log files are named according to the structure AdminYYYYMMDD.log, for example Admin20091231.log.
Recording Server service log files	These files log Recording Server service (see "About services" on page 183) activity. A new log file is created for each day the service is used. You cannot disable this type of logging. Recording Server service log files are named according to the structure RecordingServerYYYYMMDD.log, for example RecordingServer20091231.log.
Image Server service log files	These files log activity on the Image Server service (see "About services" on page 183). A new log file is created for each day the service is used. You cannot disable this type of logging. Image Server service log files are named according to the structure ISLog_YYYYMMDD.log, for example ISLog_20091231.log.
Image Import service log files	These files log activity regarding the Image Import service, when this service is used for fetching pre-alarm images, and storing the fetched images in camera databases. Pre-alarm images is a feature available for selected cameras only. It enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. A new log file is created for each day the service is used. You cannot disable this type of logging. Image Import service log files are named according to the structure ImageImportLog_YYYMMDD.log, for example ImageImportLog20091231.log.

Name	Description
Event log files	These files log information about registered events. A new log file is created for each day on which events occur. You cannot disable this type of logging. Event log files should be viewed using the Smart Client (use the **Playback** tab's **Alerts** section).
Audit log files	These files log Smart Client user activity provided audit logging is enabled. A new log file is created for each day with audit logging enabled and client user activity. Audit log files are named according to the structure is_auditYYYMMDD.log, for example is_audit20091231.log. The _is prefix is due to the fact that the audit log files are generated by the Image Server service.

Log locations

All log files are by default placed in the appropriate **All Users** folder for the operating system you are using. By default, they are stored there for seven days. Note, however, that log file locations as well as the number of days to store the logs can be changed as part of the logging configuration.

Log structures

Most log files generated by XProtect Professional use a shared structure complying with the W3C Extended Log File Format. Each log file consists of a header and a number of log lines:

- The header outlines the information contained in the log lines.
- The log lines consist of two main parts: the log information itself as well as an encrypted part. The encrypted part makes it possible, through decryption and comparison, to assert that a log file has not been tampered with.

Log integrity checks

All log files, except Management Application log files, are subjected to an integrity check once every 24 hours. The integrity check is performed by the XProtect Professional Log Check service.

The result of the integrity check is automatically written to a file named according to the structure LogCheck_YYYYMMDD.log, for example LogCheck_20091231.log. Like the log files themselves, the log check files are by default placed in the appropriate **All Users** folder for the operating system you are using.

Any inconsistencies will be reported in the form of error messages written in the log check file. Possible error messages (other, non-error, messages may also appear in the log check file):

Name	Description
Log integrity information was not found. Log integrity can't be guaranteed.	The log file could not be checked for integrity.

Name	Description
Log information does not match integrity information. Log integrity can't be guaranteed.	The log file exists, but does not contain the expected information. Thus, log integrity cannot be guaranteed.
[Log file name] not found	The log file was not present.
[Log file name] is empty	The log file was present, but empty.
Last line changed/removed in [log file name]	The last line of the log file did not match validation criteria.
Encrypted data missing in [log file name] near line [#]	The encrypted part of the log line in question was not present.
Inconsistency found in [log file name] near line [#]	The log line does not match the encrypted part.
Inconsistency found in [log file name] at beginning of log file	The log file header is not correct. This situation is most likely to occur if a user has attempted to delete the beginning of a log file.

Configure system, event and audit logging

XProtect Professional can to generate various logs. To configure logging, do the following:

1. In the Management Application's Navigation pane, expand **Advanced Configuration**, right-click **Logs** and select **Properties**.
2. Specify required properties (see "Log properties" on page 163) for:
   - General system logs (Management Application log, Recording Server service log, Image Server service log, Image Import service log)
   - The event log
   - The audit log

   Note that only audit logging can be disabled/enabled by administrators; all other logs are compulsory. XProtect Professional comes with two simple schedule profiles, **Always on** and **Always off,** which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required.
3. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Log properties

XProtect Professional can generate various types of logs. When you configure logs, you can define the following:

Logs (Management Application log, Recording Server service log, Image Server service log, and Image Import service log)

Name	Description
Path	These log files are by default placed in the appropriate **All Users** folder for the operating system you are using. To specify another location for your log files, type the path to the required folder in the **Path** field, or click the browse button next to the field to browse to the required folder.
Days to log	A new log file is created each day the Management Application and/or the services are used. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day's activity is always logged, even with a value of 0 in the field. Therefore, if you specify 0, you will log current day's activity; if you specify 1, you will keep one day plus the current day's activity, and so on.

Event Log

Name	Description
Path	These log files are by default placed in the appropriate **All Users** folder for the operating system you are using. To specify another location for your log files, type the path to the required folder in the **Path** field, or click the browse button next to the field to browse to the required folder.
Days to log	A new log file is created for each day on which events occur. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day's activity is always logged, even with a value of 0 in the field. Therefore, if you specify 0, you will log current day's activity; if you specify 1, you will keep one day plus the current day's activity, and so on.

Audit Log

Name	Description
Enable audit logging	Audit logging is the only type of XProtect Professional logging which is not compulsory. Select/clear the check box to enable/disable audit logging.
Path	These log files are by default placed in the appropriate **All Users** folder for the operating system you are using. To specify another location for your log files, type the path to the required folder in the **Path** field, or click the browse button next to the field to browse to the required folder.

Name	Description
Days to log	A new log file is created for each day with audit logging enabled and client user activity. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day's activity is always logged (provided audit logging is enabled and there is user activity). Therefore, if you specify 1, you will keep one day plus the current day's activity. Note that if you specify 0 (zero), audit log files will be kept indefinitely (disk space permitting).
Minimum logging interval	Minimum number of seconds between logged events. Specifying a high number of seconds between logged events may help reduce the size of the audit log. Default is 60 seconds.
In sequence timespan	Number of seconds to pass for viewed images to be considered to be within the same sequence. Specifying a high number of seconds may help limit the number of viewed sequences logged, and thus reduce the size of the audit log. Default is ten seconds.

E-mail

About e-mail

With e-mail notifications, you can instantly get notified when your surveillance system requires attention. XProtect Professional can automatically send e-mail notifications to one or more recipients when:

- Motion (see "Motion detection & exclude regions" on page 110) is detected
- Events occur. You can select individually for each event whether you want to receive an e-mail notification or not.
- Archiving (see "About archiving" on page 143) fails (if e-mail notification has been selected as part of the archiving properties)

Configure e-mail notifications

Do the following:

1. In the Management Application's Navigation pane, expand **Advanced Configuration**, right-click **E-mail** and select **Properties**.
2. Specify required properties (see "E-mail properties" on page 166), including the important information about which SMTP mail server to use. XProtect Professional comes with two simple schedule profiles, **Always on** and **Always off,** which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for

each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required.

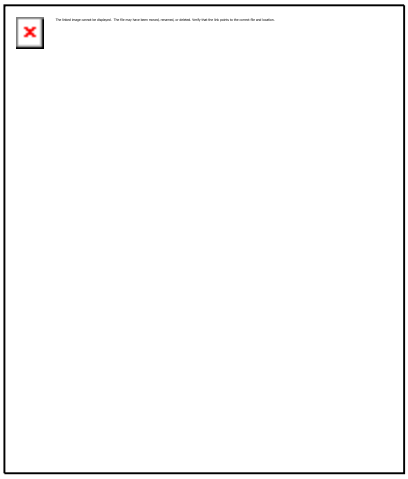
Tip: You can test your e-mail notification configuration by clicking the **Test** button. This will send a test e-mail to the specified recipients.

3. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

When you configure e-mail alerts, also consider the e-mail notification schedules (see "E-mail notification" on page 156) configured for each camera.

E-mail properties

With e-mail notifications (see "Configure e-mail notifications" on page 165), you and your colleagues can instantly get notified when your surveillance system requires attention.

Name	Description
Recipient(s)	Specify the e-mail addresses to which e-mail notifications should be sent. If specifying more than one e-mail address, separate the e-mail addresses with semicolons (example: aa@aa.aa; bb@bb.bb; cc@cc.cc).
Test	Sends a test e-mail to the specified recipients. If **Include Image** is selected, the test e-mail will have a still test JPEG image attached.
Subject text	Enter required subject text for e-mail notifications.
Message text	Enter required message text for e-mail notifications. Note that camera information as well as date and time information is automatically included in e-mail notifications.
Include Image	Select check box to include still images in e-mail notifications. When selected, a still JPEG image from the time the triggering event occurred will be attached to each e-mail notification.  Example of e-mail including a still image

Name	Description
Do not send e-mail on camera failures	If selected, e-mail notifications will not be sent if XProtect Professional loses contact with a camera. Otherwise, automatic e-mail notifications will be sent in such cases, regardless of any scheduled e-mail notification periods **(see "**E-mail notification**" on page 156).**
Time between motion- and database-related e-mails per camera	Minimum time (in minutes) to pass between the sending of each e-mail notification per camera. This interval only applies for e-mail notification generated by detected motion or database-related events; e-mail notification generated by other types of events will still be sent out whenever the events occur. Examples: If specifying **5**, a minimum of five minutes will pass between the sending of each motion- or database-related e-mail notification per camera, even if motion or database events are detected in between. If specifying **0**, e-mail notifications will be sent each time motion or database events are detected, potentially resulting in a very large number of e-mail notifications being sent. If using the value **0,** you should therefore consider cameras' motion detection (see "Motion detection & exclude regions" on page 110) sensitivity settings.
Sender e-mail address	Enter the e-mail address you wish to appear as the sender of the e-mail notification.
Outgoing mail (SMTP) server name	Type the name of the SMTP (Simple Mail Transfer Protocol) server which will be used for sending the e-mail notifications. Compared with other mail transfer methods, SMTP has the advantage that you will avoid automatically triggered warnings from your e-mail client. Such warnings may otherwise inform you that your e-mail client is trying to automatically send e-mail messages on your behalf. TLS (Transport Layer Security) and it s predecessor SSL (Secure Socket Layer) is not supported; if the sender belongs on a server that requires TLS or SSL, e-mail notifications will not work properly. Also, you may be required to disable any e-mail scanners that could prevent the application sending the e-mail notifications.
Server requires login	Select check box if a user name and password is required to use the SMTP server.
User name	Only required when **Server requires login** is selected. Specify the user name required for using the SMTP server.
Password	Only required when **Server requires login** is selected. Specify the password required for using the SMTP server.

SMS

About SMS

With SMS notifications, you can instantly get notified on your mobile device when your surveillance system requires attention. XProtect Professional can automatically send SMS notifications when:

- Motion (see "Motion detection & exclude regions" on page 110) is detected
- Events occur. You can select individually for each event whether you want to receive an SMS notification or not.
- Archiving (see "About archiving" on page 143) fails (if an SMS notification has been selected as part of the archiving properties)

Use of the SMS notification feature requires that an external Siemens TC-35 GSM modem has been attached to a serial port (a.k.a. COM port) on the XProtect Professional server. Siemens TC-35 is a dual-band EGSM900/GSM1800 modem. Verify that the modem is compatible with mobile phone networks where you are going to use it with XProtect Professional.

Configure SMS notifications

To configure SMS notifications, do the following:

1. In the Management Application's Navigation pane, expand **Advanced Configuration**, right-click **SMS** and select **Properties**.
2. Enable the use of SMS by selecting the **Enable SMS** check box.
3. Specify required properties (see "SMS properties" on page 168).

   Tip: You can test your SMS notification configuration by clicking the **Test** button; this will send a test SMS to the specified recipient. Note that you must stop the Recording Server service (see "Start and stop services" on page 184) while you perform the test (remember to start the service again afterwards).
4. XProtect Professional comes with two simple schedule profiles, **Always on** and **Always off,** which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required.
5. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

When you configure SMS alerts, also consider the SMS notification schedules (see "SMS notification" on page 156) configured for each camera.

SMS properties

With SMS notifications (see "Configure SMS notifications" on page 168), you can instantly get notified when your surveillance system requires attention.

Name	Description
Enable SMS	Enables the use of SMS notifications, allowing you to specify further properties.
GSM modem connected to	Select port connecting the XProtect Professional server to the GSM modem.
SIM card PIN code	Specify PIN code for the SIM card inserted in the GSM modem.
SIM card PUK code	Specify PUK code (that is unlocking code) for the SIM card inserted in the GSM modem.
SMS central phone number	Specify the number of the SMS central to which the GSM modem should connect in order to send SMS notifications.
Recipient phone number	Specify the number of the mobile telephone to which SMS alerts should be sent. It is only possible to send SMS notifications to a single telephone number.
Message	Specify required message text for the SMS notification. Message text must be no longer that 160 characters, and must only contain the following characters: a-z, A-Z, 0-9 as well as commas (,) and full stops (.). Note that camera information as well as date and time information is automatically included in SMS notifications. **Tip:** While you write, the counter below the **Message** field indicates how many characters you have left to use.
Time between motion- and database-related SMSs per camera	Minimum time (in minutes) to pass between the sending of each SMS notification per camera. This interval only applies for SMS notification generated by detected motion or database-related events; SMS notification generated by other types of events will still be sent out whenever the events occur. Examples: If specifying 5, a minimum of five minutes will pass between the sending of each motion- or database-related SMS notification per camera, even if motion or database events are detected in between. If specifying 0, SMS notifications will be sent each time motion or database events are detected, potentially resulting in a very large number of SMS notifications being sent. If using the value 0, you should therefore consider cameras' motion detection (see "Motion detection & exclude regions" on page 110) sensitivity settings.
Test	Lets you test your SMS notification configuration by sending a test SMS to the specified recipient. Note that you must stop the Recording Server service (see "Start and stop services" on page 184) while you perform the test (remember to start the service again afterwards).
Do not send SMS on camera failures	If selected, SMS notifications will not be sent if XProtect Professional loses contact with a camera. Otherwise, automatic SMS notifications will be sent in such cases, regardless of any scheduled SMS notification periods (see "SMS notification" on page 156).

Central

About XProtect Central

The **XProtect Central Settings** lets you specify the login settings required for an XProtect Central server to access the surveillance system in order to retrieve status information and alarms. If you are a user of the Milestone Integration Platform, this is also the dialog that lets you specify the login settings for the Milestone Integration Platform to access the surveillance system.

Enable XProtect Central

1. In the Management Application's Navigation pane, expand **Advanced Configuration**, right-click Central and then select **Properties**.
2. Enable the use of Central connections by selecting the **Enable MilestoneXProtect Central** check box.
3. Specify required properties (see "Central properties" on page 170).
4. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Central properties

Name	Description
Enable Milestone XProtect Central connections	Enables the use of Central connections, allowing you to specify further properties.
Login Name	Type the name used for the connection between the XProtect Professional and XProtect Central servers or the Milestone Integration Platform. The name must match the name specified on the XProtect Central server or in the Milestone Integration Platform.
Password	Type the password used for the connection between XProtect Professional and XProtect Central servers or the Milestone Integration Platform. The password must match the password specified on the XProtect Central server or in the Milestone Integration Platform.
Port	Type the port number to which the XProtect Central server or the Milestone Integration Platform should connect when accessing the XProtect Professional server. The port number must match the port number specified on the XProtect Central server or in the Milestone Integration Platform. Default port is 1237.

Server access

About server access

You can configure clients' access to the XProtect Professional server in two ways:

- **Wizard-driven:** Guided configuration which lets you specify how clients access the server and which users can use clients. See Configure User Access wizard (on page 68).

  When you use the wizard, all users that you add have access to all cameras, including new cameras added at a later stage. If this is not acceptable, specify access settings, users and user rights separately; see the following.

- **Through advanced configuration:** In previous versions of XProtect Professional, this was known as Image Server administration, since technically it is the Image Server service (see "About services" on page 183) which handles clients' access to the surveillance system.

About registered services

Registered services displays the services installed to and running on your XProtect Professional system. It displays the following information about the individual services:

Name	Description
Enabled	Indicates if the relevant service is enabled
Name	The name of the service
Description	A description of the service
Addresses	The inside and outside addresses used by the service

You can change the inside and outside addresses for a service. To do this, you click the **Edit** button and then enter the relevant inside and/or outside addresses. Note that not all services can be edited. You can delete a service registration from the system by clicking the **Delete** button. You are prompted for confirmation before the service is deleted.

Configure server access

1. In the Management Application's navigation pane, expand **Advanced Configuration,** right-click **Server Access** and select **Properties**.

2. Specify required properties for Server Access (on page 172), Local IP Ranges (on page 173), and Language Support & XML Encoding (see "Language support and XML encoding" on page 173). XProtect Professional comes with two simple schedule profiles, **Always on** and **Always off,** which cannot be edited or deleted. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. When you create a customized schedule profile for one camera, you can reuse it with other cameras if required.

3. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

When you use this option, you configure client users separately from clients' access. See Add individual users (see "Add basic users" on page 177), Add user groups (on page 178), and Configure user and group rights (on page 179).

Server access properties

Properties in this window:

Server access

When you configure server access (on page 171) (that is clients' access to the XProtect Professional server), specify the following:

Name	Description
Server name	Name of the XProtect Professional server as it will appear in clients. Client users with rights to configure their clients will see the name of the server when they create views in their clients.
Local port	Port number to use for communication between clients and the surveillance server. The default port number is 80; you can change the port number if port 80 is used for other purposes in your organization.
Enable internet access	Select the check box if the server should be accessible from the internet through a router or firewall. If you select this option, also specify the public (“outside”) IP address and port number in the following fields. When using public access, the router or firewall used must be configured so requests sent to the public IP address and port are forwarded to the local (“inside”) IP address and port of the XProtect Professional server.
Internet address	Lets you specify a public IP address or hostname for use when the XProtect Professional server should be available from the internet.
Internet port	Specify a port number for use when the XProtect Professional should be available from the Internet. The default port number is 80. You can change the port number if needed.

Name	Description
Max. number of clients	You can limit the number of clients allowed to connect at the same time. Depending on your XProtect Professional configuration and the performance of the hardware and network used, limiting the number of simultaneously connected clients may help reduce server load. If more than the allowed number of simultaneously connected clients attempt to log in, only the allowed number of clients will be allowed access. Any clients in excess of the allowed number will receive an error message when attempting to log in. By default, a maximum of ten simultaneously connected clients are allowed. To specify a different maximum number, simply overwrite the value. **Tip:** To allow an unlimited number of simultaneously connected access clients, type **0** (zero) in the **Max. number of clients** field. A four-minute session timeout period applies for client sessions on XProtect Professional. In many cases, client users may not notice this at all. However, the session timeout period will be very evident if you set the **Max. number of clients** value to **1**. When that is the case, and the single allowed client user logs out, four minutes must pass before it will be possible to log in again.

Local IP ranges

You can specify IP address ranges which XProtect Professional should recognize as coming from a local network. This can be relevant if different subnets are used across you local network.

1. Click the **Add** button.
2. In the **Start Address** column, specify the first IP address in the required range.
3. In the **End Address** column, specify the last IP address in the required range.

   Tip: If required, an IP address range may include only one IP address (example: 192.168.10.1-192.168.10.1).
4. Repeat if other local IP address ranges are required.

Language support and XML encoding

You can select the language/character set that should be used by the XProtect Professional server and clients.

Name	Description
Character encoding/Language	Select required language/character set. Example: If the surveillance server runs a Japanese version of Windows, select Japanese. Provided access clients also use a Japanese version of Windows, this will ensure that the correct language and character encoding is used in clients' communication with the server.

Master/Slave

About master and slave

You can create a master/slave setup of XProtect Professional servers. A master/slave setup will allow remote users to transparently connect to more than one server at the same time. When remote users connect to the master server, they will instantly get access to the slave servers as well.

Configure master and slave servers

Configuring a master/slave setup

In the Management Application 's Navigation pane, expand **Advanced Configuration**, right-click **Master/Slave** and select **Properties**.

1. Select the **Enable as master server** check box.
2. Click **Add** to add a slave server.
3. Specify slave server properties. When ready, click **OK.**
4. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Adding a slave server

To add a slave server, expand **Advanced Configuration** in the Management Application , right-click **Master/Slave** and select **Add New Slave Server**, then specify slave server properties. Slave servers can also be added from the **Master/Slave Properties** window by clicking **Add.**

Tip: Instead of specifying a host name when adding a slave server, you may specify the IP address of the slave server. Simply type the IP address in the **Address** field when adding the slave server. Remember that if on a local network, the **local** IP address of the slave server must be used.

Before you start using your master/slave setup, remember to verify that:

- Required users have be defined on the master server as well as on each of the slave servers.

- Public Access (see "Configure server access" on page 171) has been enabled on all involved servers, and ports mapped accordingly in the routers or firewalls used, if the slave servers are to be accessed from the internet.

When using a master/slave setup, remote users and their rights **must be defined in the Management Application** 's **Users** section on the master server as well as on each of the slave servers. Only cameras to which a remote user has been given access will be visible to the user, regardless of whether the cameras are connected to the master server or to one of the slave servers. If they are to be accessed from the internet, **Public Access** must be enabled on all involved servers, and ports must be mapped accordingly in the routers and/or firewalls used.

Frequently asked questions about using master/slave

How many master servers can I use in a master/slave setup? An unlimited number of servers per SLC (Software License Code, specified during installation (see "Install your surveillance server software" on page 26)) can be designated as master servers. If required—for example if your organization is very large and spread over many geographical locations, or in case your organization wants to create a redundancy solution—this allows you to use several master servers in a master/slave setup.

How many slave servers can I use in a master/slave setup? Up to four servers can be defined as slave servers under a designated master server using the same Software License Code.

How do I switch around which server is master and which server is slave? If you want a slave server to become a master server, simply clear **Enable as master server** on the original master server and click **OK**. In the Management Application's navigation pane right-click the slave server which you want to become master server, and select **Properties**. Then select **Enable as master server.** Next click **Add** to add slave servers to the new master server.

How do I ensure that I am actually connected to my slaves? You can verify the connection to your slaves by clicking Update Status and let the system report the number of connected slaves back to you.

Event Server installation in a master/slave setup

If you are planning to run a master/slave setup, it is important that you run **Typical** installation on the master server and **Custom** installation, where you deselect installing the Event Server service, on the slave server(s). This is because there can only be one event server service in a master/slave setup. If more than one Event Server service is installed, the master server will have problems accessing cameras on slave servers.

However, if you have an Event Server installed on the master server and no Event Server installed on slave servers, you can create alarms that are triggered when events occur on the slave.

If you cannot see an event from the slave server when you are creating an alarm and entering the source in the Management Application, this could be because you need to be a user on the slave server with administrator access before you can see the events on the slave server.

A locally defined Windows user created on the Windows server will not be recognized on the slave server, and an event from the slave server will not be available for creating alarms. If you are a domain user, you be added to both the master server and the slave server with administrator access. This will allow you to see the events on the slave server and create alarms.

If you are set up as a basic user on both the master server and slave server, with administrator rights on both, you will be able to see events on the slave server and create alarms when you log in to the master server with this user ID.

By default, the Management Application will not prompt you for a login, but will log you in with the Windows user ID with which you have logged in to Windows. If you want to log in to the Management Application as a basic user, you must therefore do the following: Start the Management Application and go to **File** > **Logout**. This will open a login dialog where you can use your basic user ID to log in.

Master/slave properties

If you have several XProtect Professional servers, you can create a master/slave setup. A master/slave setup will allow users to connect—in a transparent way—to more than one server simultaneously. When users connect to the master server, they will instantly get access to the slave servers as well.

Master server properties

Name	Description
Enable as master server	Select to enable as master server.
Timeout	Set timeout of slave update. See Update Status on Slaves in the following.
Add	Lets you add slave servers. Select **Master Server** in the list and click the **Add** button.

Slave server properties

Name	Description
Address	IP address of the slave server.
Port	Port number of the slave server.
Delete	Remove a slave server from the list of slave servers. Select the slave server in the list and click the **Delete** button.

When selecting **Master Server**, the **Delete** button is disabled and the **Add** button is enabled—provided that **Enable as master server** is selected—allowing you to add slave servers to the master server but preventing you from deleting the master server.

Update status on slaves

In the **Master Settings Summary** and **Slave Settings Summary** table area, it is possible to verify/update added slaves by clicking **Update Status**. A status dialog will run and subsequently inform you of the status of your slave server(s).

Users

About users

The term **users** primarily refers to users who connect to the surveillance system through their clients. You can configure such users in two ways:

- As **basic users**, authenticated by a user name/password combination.
- As **Windows users**, authenticated based on their Windows login

You can add both types of users through the Configure User Access wizard (on page 68) or individually (see Add basic users (on page 177) and Add Windows users (on page 177)).

By grouping users, you can specify rights (see "Configure user and group rights" on page 179) for all users within a group in one go. If you have many users performing similar tasks, this can save you significant amounts of work. User groups are logical groups created and used for practical purposes in the Management Application only. They are not in any way connected with user groups from central directory services. If you want to use groups, make sure you add groups (see "Add user groups" on page 178) before you add users: You cannot add existing users to groups.

Finally, the Administrators group is also listed under Users. This is a default Windows user group for administration purpose which automatically has access to the Management Application.

Add basic users

When you add a basic user, you create a dedicated surveillance system user account with basic user name and password authentication for the individual user. Note that if you add a user as a Windows user, this will provide better security.

If you want to include users in groups, make sure you add required groups (see "Add user groups" on page 178) before you add users: You cannot add existing users to groups.

You can add basic users in two ways: One is through the Configure User Access wizard (on page 68), the other is described here:

1. In the Management Application's navigation pane, expand **Advanced Configuration**, right-click **Users**, and select **Add New Basic User**.
2. Specify a user name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

   Then specify a password, and repeat it to be sure you have specified it correctly.
3. Click **OK**.
4. Specify General Access (on page 180) and Camera Access (on page 181) properties. These properties will determine the rights of the user.
5. Click **OK**.
6. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Add Windows users

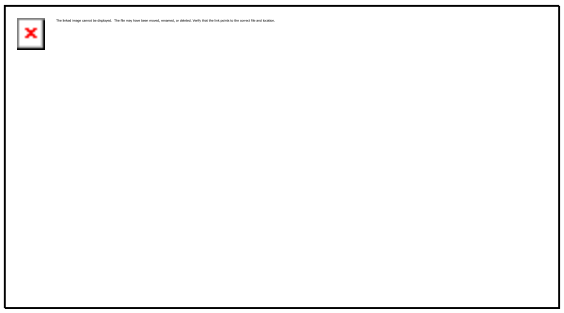
When you add Windows users, you import users defined locally on the server and authenticate them based on their Windows login. This generally provides better security than the basic user concept, and is the recommended method.

If you want to include users in groups, make sure you add required groups (see "Add user groups" on page 178) before you add users: You cannot add existing users to groups.

You can add Windows users in two ways: One is through the Configure User Access wizard (on page 68), the other is described here:

The users you want to add must have been defined as local PC users on the server. Simple file sharing must be disabled on the server. To disable simple file sharing, right-click Windows' **Start** button and select **Explore**. In the window that opens, select the **Tools** menu, then select **Folder Options...**, then the **View** tab. Scroll to the bottom of the tab's **Advanced Settings** list, and make sure that the **Use simple files sharing** check box is cleared. When ready, click **OK** and close the window.

1. In the Management Application's navigation pane, expand **Advanced Configuration**, right-click **Users**, and select **Add New Windows User**. This will open the S**elect Users or Groups** dialog.

   Note that you can only make selections from the local computer, even if you click the Locations... button.

2. In the **Enter the object names to select** box, type the required user name(s), then use the **Check Names** feature to verify it. If you type several user names, separate each name with a semicolon. Example: **Brian; Hannah; Karen; Wayne.**

3. When done, click **OK:**

4. Specify General Access (on page 180) and Camera Access (on page 181) properties. These properties will determine the rights of the user.

5. Click **OK**.

6. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Users who have been added from a **local database** logging in with a client should not specify any server name, PC name, or IP address as part of the user name. Example of a correctly specified user name: USER001. Example of an incorrectly specified user name: PC001/USER001. The user should of course still specify a password and any required server information.

Add user groups

User groups are logical groups created and used for practical purposes in the Management Application only. They are not in any way connected with user groups from central directory services such as, for example, Active Directory®.

By grouping users, you can specify rights (see "Configure user and group rights" on page 179) for all users within a group in one go. If you have many users performing similar tasks, this can save you significant amounts of work.

Make sure you add groups before you add users: You cannot add existing users to groups.

1. In the Management Application's navigation pane, expand **Advanced Configuration**, **right-click Users**, and select **Add New User Group**.
2. Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
3. Click **OK**.
4. Specify General access (on page 180) and Camera access (on page 181) properties. These properties will determine the rights of the group's future members.
5. Click **OK**.
6. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.
7. Now you can add users to the group: In the navigation pane, right-click the group you just created, and Add basic users **(on page 177) or** Add Windows users (on page 177) as required.

Configure user and group rights

User/group rights are configured during the process of adding users/groups, see Add basic Users (on page 177), Add Windows users (on page 177) and Add user groups (on page 178). Note that you can also add basic and Windows users through the Configure User Access wizard (on page 68). However, when using the wizard all users you add will have access all to cameras, including any new cameras added at a later stage.

If you at a later stage want to edit the rights of a user or group:

1. In the Management Application's navigation pane, expand **Advanced Configuration**, expand **Users**, right-click the required user or group, and select **Properties**.
2. Edit General Access (on page 180) and Camera Access (on page 181) properties. These properties will determine the rights of the user/group.
3. Click **OK**.
4. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

User properties

Properties in this window:

User information

Name	Description
User name	Only editable if the selected user is of the type basic user. Edit the user name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**
Password	Only editable if the selected user is of the type basic user. Edit the password. Remember to repeat the password to be sure you have specified it correctly.
User type	Non-editable field, displaying whether the selected user is of the type basic user or Windows user group.

Group information

Name	Description
Group name	Edit the group name. Names must be unique, and must not contain any of these special characters: **< > & ' " \ / : * ? | [ ]**

General access

When you add or edit basic users (see "Add basic users" on page 177), Windows users (see "Add Windows users" on page 177) or groups (see "Add user groups" on page 178), specify general access settings:

Name	Description
Live	Ability to access the **Live** tab in the Smart Client.
Playback	Ability to access the **Playback** tab in the Smart Client.
Setup	Ability to access setup mode in the Smart Client. **Tip:** By clearing the **Live**, **Playback** and **Setup** check boxes you can effectively disable the user's/group's ability to use the Smart Client. You can use this as a temporary alternative to deleting the user/group, for example while a user is on vacation.
Edit shared views	Ability to create and edit views in shared groups in the Smart Client. Views placed in shared groups can be accessed by every user. If a user/group does not have this right, shared groups will be protected, indicated by a padlock icon in the Smart Client.

Name	Description
Edit private views	Ability to create and edit views in private groups in the Smart Client. Views placed in private groups can only be accessed by the user who created them. If a user/group does not have this right, private groups will be protected, indicated by a padlock icon in the Smart Client. Denying users the right to create their own views may make sense in some cases; for example in order to limit bandwidth use. For more information about shared and private views, see the separate Smart Client documentation.
Administrator Access	Ability to access and work with the Management Application. Selected and non-editable for Administrators. Cleared and selectable for all other users.

Camera access

When you add or edit basic users (see "Add basic users" on page 177), Windows users (see "Add Windows users" on page 177) or groups (see "Add user groups" on page 178), you can specify camera access settings.

In the list of cameras, select the camera(s) you want to work with. Note the last item in the list, **Rights for new cameras when added to the system**, with which you can allow the user/group access to any future cameras.

Tip: If the same features should be accessible for several cameras, you can select multiple cameras by pressing SHIFT or CTRL on your keyboard while selecting.

For the selected camera(s), in the **Access** check box, specify if the user/group should have access to live viewing and playback at all. If so, specify if they should have access to **both** live viewing and playback and—if this is the case—which sub-features should be available when working with the selected camera(s).

The sub-features are listed in two columns in the lower part of the window: the left column lists features related to live viewing, the right column lists features related to playback.

The **Camera access settings** check boxes work like a hierarchy of rights. If the **Access** check box is cleared, everything else is cleared and disabled. If the **Access** check box is selected, but, for example, the **Live** check box is cleared, everything under the **Live** check box is cleared and disabled.

Depending on the selected column, the following default features for live or playback from the selected camera(s) will give you the ability to:

Live	Features
PTZ	Use navigation features for PTZ (Pan/Tilt/Zoom) cameras. A user/group will only be able to use this right if the user has access to one or more PTZ cameras.
PTZ preset positions	Use navigation features for moving a PTZ camera to particular preset positions. A user/group will only be able to use this right if having access to one or more PTZ cameras with defined preset positions.

Live	Features
Output	Activate output (lights, sirens, door openers, etc.) related to the selected camera(s).
Events	Use manually triggered events related to the selected camera(s). This feature is available in the XProtect Smart Client only.
Incoming audio	Listen to incoming audio from microphones related to the selected camera(s). This feature is available in the Smart Client only.
Outgoing audio	Talk to audiences through speakers related to the selected camera(s). This feature is available in the XProtect Smart Client only.
Manual recording	Manually start recording for a fixed time (defined (see "Manual recording" on page 92) by the surveillance system administrator).
Playback	**Features**
AVI/JPEG export	Export evidence as movie clips in AVI format and as still images in JPEG format.
Database export	Export evidence in database format. This feature is available in the Smart Client only.
Sequences	Use the **Sequences** feature when playing back video from the selected camera.
Smart search	Use the smart search feature, with which users can search for motion in one or more selected areas of images from the selected camera. This feature is available in XProtect Smart Client only.
Recorded audio	Listen to recorded audio from microphones related to the selected camera(s).

You cannot select a feature, if the selected camera does not support the relevant feature. For example, PTZ-related rights are only available if the relevant camera is a PTZ camera. Some features depend on the user's/group's General Access (on page 180) properties.

Square-filled check boxes can appear in the lower part of the window if you have selected several cameras and a feature applies for some but not all of the cameras. Example: For camera A, you have selected that use of the Events is allowed, for camera B, you have not allowed this. If you select both camera A and camera B in the list, the Events check box in the lower part of the window will be square-filled. Another example: Camera C is a PTZ camera for which you have allowed the PTZ preset positions feature whereas camera D is not a PTZ camera. If you select both camera C and camera D in the list, the PTZ preset positions check box will be square-filled.

Alarm Access (Properties)

When you add or edit basic users (see "Add basic users" on page 177), Windows users (see "Add Windows users" on page 177) or groups (see "Add user groups" on page 178), specify their Smart Client alarm access rights:

Name	Description
View	Allows users of the Smart Client to: • View alarms • Print alarms reports.

•

Services

About services

The following services are all automatically installed on the XProtect Professional server if you run a **Typical** installation. By default, services run transparently in the background on the XProtect Professional server. If you need to, you can start and stop services separately from the Management Application, see Start and stop services (on page 184).

Service	Description
Milestone Recording Server service	A vital part of the surveillance system. Video streams are only transferred to XProtect Professional while the Recording Server service is running.
Milestone Image Server service	Provides access to the surveillance system for users logging in with a Smart Client. Note: If the Image Server service is configured in Windows Services to log in with another account than the Local System account, for example as a domain user, Smart Clients on other computers than the surveillance server itself will not be able to log in to the server using the server's host name. Instead, those users must enter the server's IP address.
Milestone Image Import service	Used for fetching pre- and post-alarm images, and storing the fetched images in camera databases. Pre- and post-alarm images is a feature available for selected cameras only; it enables sending of images from immediately before and after an event took place from the camera to the surveillance system via e-mail. Pre- and post-alarm images should not be confused with the XProtect Professional pre- and post-recording feature (see "Recording" on page 105).
Milestone Log Check service	Performs integrity checks on XProtect Professional log files. For more information, see Overview of Logs.
Milestone Event Server service	Manages all alarms and map-related communication. It stores events, image files and map configurations, and makes status information about the surveillance system available.

Service	Description
Milestone Mobile service	Manages the communication between the Recording Server and mobile devices (such as smartphones and tablets) and between the Recording Server and web browsers.

If you run a Custom installation, you can choose not to install the Mobile server and/or the Event Server. If you do so, the Mobile service and/or the Event Server service will not be seen in your Services overview.

Start and stop services

On an XProtect Professional server, several services (see "About services" on page 183) by default run in the background. If you need to, you can start and stop each service separately:

1. In the Management Application's Navigation pane, expand **Advanced Configuration** and select **Services**. This will display the status of each service.
2. You can now stop each service by clicking the **Stop** button. When a service is stopped, the button changes to **Start**, allowing you to start the service again when required.

   Tip: Occasionally, you may want to stop a service and start it again immediately after. The **Restart** button allows you to do just that with a single click.

Servers

Mobile Server

About Mobile server

A Mobile server handles log-ins when a user wants to log into his/her XProtect video management setup via the XProtect Mobile client (see "About XProtect Mobile client" on page 16) from a mobile device or from XProtect Web Client (see "About XProtect Web Client" on page 17).

Upon correct login, the Mobile server distributes video streams from relevant recording servers to XProtect Mobile client. This offers an extremely secure setup, where recording servers are never connected to the Internet. When a Mobile server receives video streams from recording servers, it also handles the complex conversion of codecs and formats allowing streaming of video on the mobile device.

Important: Before you begin the installation of the Mobile server, make sure you are logged in with an account that has administrator rights. Installation will not be successful if you use a standard user account.

About Video push

Video push is feature in your Mobile client that allows you to use your mobile device's camera, for example, to collect evidence when you investigate an alarm or event. You do this by sending a video stream from your mobile device to your XProtect video management system. In the Mobile server settings, you can set up how many users should be able to use the Video push feature in the video management system.

About saving configuration changes in XProtect Enterprise 8.0 and streamlined XProtect software versions

The following applies to XProtect Enterprise 8.0, XProtect Professional 8.0, XProtect Express 1.0, XProtect Essential 2.0 and XProtect Go 2.0 software versions only.

If you are logged into the XProtect Mobile client and are watching one or more cameras views while at the same time changing configuration in the Management Application, the live video from the camera may freeze in the XProtect Mobile client if you click **Save Configuration and Restart Surveillance Services** in the Management Application**.**

To avoid this scenario, you must restart the Milestone XProtect Mobile service manually. See the Windows Help for information about how to do this. If you are using newer versions of XProtect, the Milestone XProtect Mobile service is restarted with the other services and no user action is required.

Add/edit a Mobile server

1. Do one of the following:
   - To add a new server, right-click **Mobile Servers.** From the menu that appears, select **Create New**.
   - To edit a Mobile server, select the wanted server.
2. Fill in/edit the needed properties.
3. In the lower right corner, click **Apply**.
4. In the top toolbar, click **File** > **Save**.

IMPORTANT: If you edit settings for **Login method, All cameras view** and **Outputs and events**, while you are connected to the XProtect Mobile client, you must restart the XProtect Mobile client for the new settings to take effect.

Delete a Mobile server

1. From the navigation pane, expand **Servers** > **Mobile Servers** in order to see existing servers.
2. Right-click the unwanted server and select **Delete**.
3. Click **Yes**.

Rename a Mobile server

1. From the navigation pane, expand **Servers** > **Mobile Servers** in order to see existing servers.
2. Select the required Mobile server.
3. On the **Info** tab, which opens once the Mobile server is selected, change the name of the server by typing in the **Server name** and **Description** fields.
4. In the lower right corner, click **Apply**.
5. In the toolbar, click **File** > **Save**.

Add a Video push channel

To add a Video push channel (see "About Video push" on page 184), do the following:

1. On the **Video Push** tab, select the **Video push** checkbox.
2. Add a video push channel by changing the number of channels from 0 (default) to the number of video push channels needed. Once added, video push channels appear in the **Channels mapping**.
3. Click **File** > **Save**.
4. Add the Mobile server as a hardware device (see "Add a Video push channel as a hardware device" on page 186) to the video management system by specifying the IP address of the Mobile server (the Mobile server must be added manually and will not be detected in automatic hardware searches). Once finished, click **Apply**.
5. On the **Video Push** tab, click **Find Cameras**. If successful, the newly added Video push hardware device appears in this list and is ready to use.
6. Click **Apply**.
7. **Click File > Save.**

Add a Video push channel as a hardware device

If you add a Video push channel, you must add the Video push driver to your Management Application/Management Client. To do so:

1. Open the **Add New Hardware Wizard** in your Management Application/Management Client.
2. Choose the **Manual** option. The Video push driver will not be detected in automatic hardware searches.
3. Specify hardware information settings and select the hardware driver manually.
4. Once finished, your Video push driver is ready and can be used in your XProtect Mobile client.

Add hardware devices settings

Specify the following settings when you add a Video Push driver in the **Add Hardware Devices** wizard:

Name	Description
Use:	Select if the Video push driver should added to the XProtect video management system.
Address:	Type in the XProtect Mobile server network address.

Name	Description
Port:	Type in the port number for your Video push driver. The default port is 80. Important: You must set the same port number as you set when you specify your Video push settings (see "Video push" on page 189). If these values are not identical, your Video push driver will not be able to work.
User name:	Select any user name from the drop down list.
Password:	Type in the password for the Video push driver. The password for your Video push driver is **Milestone** (this cannot be changed).
Hardware Driver:	Select the **Video Push Driver**.
Verified:	Select if the Video push driver runs on a secured HTTPS connection.

Mobile server settings

Properties in this window:

Info

Fill in and specify general settings for the Mobile server:

Name	Description
Server name:	Name of the Mobile server.
Description:	Description of the Mobile server.
Mobile server:	Choose between all Mobile servers currently installed to the specific XProtect® video management system. Only XProtect Mobile servers that are up and running are shown in the list.
Connection type:	Possible methods are: **HTTP only**, **HTTP and HTTPS** or **HTTPS Only**.
Client timeout (HTTP)	Default time frame (30 sec.) for how often the Mobile server client must indicate to the Mobile server server that it is up and running. Milestone recommends that you do not increase the time frame.
Login method:	Select how you want to log in to the Mobile server server should take place. Possible methods are: **Automatic, Windows Only** or **Basic Only.**

Name	Description
All cameras view:	Enable/disable viewing of **All Cameras** view. This view contains all cameras on a recording server (user rights permitting).
Output and events:	Enable/disable output and events.
Keyframes only	Enable/disable video stream to stream key frames only. Enabling key frames only reduces bandwidth usage.
Enabled:	Enable/disable logging of XProtect Mobile client' actions in a separate log file.
Log file location:	Path to where log files are saved.
Keep logs for:	Number of days to keep logs for (default 3 days).
CPU usage:	Default level of CPU usage which will trigger a warning in the log.
Internal bandwidth:	Default internal bandwidth usage which will trigger a warning in the log.
External bandwidth:	Default external bandwidth usage which will trigger a warning in the log.
Check every:	Default time frame (30 sec.) for checking warning levels.

Note that every time you change a setting in the Mobile server settings, you must click the **Apply** button followed by the **Save** button.

Server status

See the status details for your Mobile server. The details are read-only:

Name	Description
Server active since:	Shows how long the Mobile server has been running since it was last stopped.
CPU usage:	Shows current CPU usage on the Mobile server.
Internal bandwidth:	Shows the current bandwidth in use between the Mobile server and the relevant recording server.
External bandwidth:	Shows the current bandwidth in use between the mobile device and Mobile server.
User Name column:	Shows user name(s) of the Mobile server user(s) connected to the Mobile server.
State column:	Shows the current relation between the Mobile server and the XProtect Mobile client user in question. Is the user connected (a state preliminary to servers exchanging keys and encrypting credentials) or is he/she actually logged in? Possible states are: Connected and Logged In XProtect.
Bandwidth Usage column:	Shows the level of bandwidth used by the Mobile server client user in question.

Name	Description
Live Streams column:	Shows the number of live video streams currently open for the XProtect Mobile client user in question.
Playback Streams column:	Shows the number of playback video streams currently open for the Mobile server client user in question.

Note that every time you change a setting in the Mobile server settings, you must click the **Apply** button followed by the **Save** button.

Video push

If you enable Video push, specify the following settings:

Name	Description
Video push	Enable Video push on the Mobile server.
Number of channels	Specify the number of enabled Video push channels in your XProtect Professional system.
Channel column	Shows the channel number for the relevant channel. Non-editable.
Port	Port number for the relevant Video push channel.
MAC	MAC address for the relevant Video push channel.
User Name	Enter the user name associated with the relevant channel.
Camera Name	Shows the name of the camera if the cameras has been identified.

Once you have completed all necessary steps (see "Add a Video push channel" on page 186), click **Find Cameras** to search for the relevant camera.

Note that every time you change a setting in the Mobile server settings, you must click the **Apply** button followed by the **Save** button.

Export

Specify the settings for exported recordings:

Name	Description
Export	Enable export in clients.
Export to:	Specify the location to which recordings should be exported.
Delete exported recordings older than:	Enter the number of days to pass before recordings are deleted.
Limit size of exports folder to:	Enter a number to set a maximum limit for the folder to which the recordings are exported.
Include timestamps:	Add timestamps to exported video.

In the columns, see the following details for every individual exported recording:

Name column	Name of the exported recording.

State column	State of the exported recording.
Camera column	The camera that provided the exported recording.
Timestamp column	The point of time when the exported recording took place.
Duration column	The length of the exported recording.
User column	The name of the user who provided the exported recording.
MB column	The size of the exported recording.

Note that every time you change a setting in the Mobile server settings, you must click the **Apply** button followed by the **Save** button.

Mobile Server Manager

About Mobile Server Manager

The Mobile Server Manager is a tray-controlled feature connected to Mobile server.

Right-clicking the Mobile Server Manager icon in the system tray opens a menu from which Mobile server functionality can be easily accessed. You can:

- Open XProtect Web Client (see "Access XProtect Web Client" on page 17)
- Start, stop and restart the Mobile service (see "Start, stop and restart Mobile service" on page 192)
- Fill in or change surveillance server credentials (see "Fill in/edit surveillance server credentials" on page 192)
- Show/edit port numbers (on page 192)
- Edit certificate (on page 191)
- Open today's log file (see "Access logs and exports" on page 191)
- Open log folder (see "Access logs and exports" on page 191)
- Open export folder (see "Access logs and exports" on page 191)
- Show Mobile server status (see "About show status" on page 190)
- Access the XProtect Mobile Help website where you find manuals, FAQS and product demonstration videos.

About show status

If you right-click the Mobile Server Manager and select **Show Status...** (or double-click the Mobile Server Manager icon), a window opens, showing the status of the Mobile server. You can see the following:

Name	Description
Server running since:	Time and date of the time when the Mobile server was last started.
Connected users:	Number of users currently connected to the Mobile server.
CPU usage:	How many % of the CPU is currently being used by the Mobile server.
CPU usage history:	A graph detailing the history of CPU usage by the Mobile server.

Access logs and exports

The Mobile Server Manager lets you quickly access the log file of the day, open the folder to which logs files are saved, and open the folder to which exports are saved. To open any one of these, right-click the Mobile Server Manager and select **Open Today's Log File**, **Open Log Folder** or **Open Export Folder** respectively**.**

Important: If you uninstall XProtect Mobile from your system, its log files are not deleted. Administrators with proper rights can access these log files at a later timer, or decide to delete them if they are not needed any longer. The default location of the log files is in the ProgramData folder. If you change the default location of log files, existing logs are not copied to the new location nor are they deleted.

Edit certificate

If you want to use a secure HTTPS protocol to establish connection between your mobile device or the XProtect Web Client and the Mobile server, you must have a valid certificate for the device or web browser to accept it without warning. The certificate confirms that the certificate holder is authorized to establish the connection.

When you install the Mobile server, you generate a self-signed certificate if you run a **Typical** installation. If you run a **Custom** installation, you get the choice between generating a self-signed certificate or loading a file containing a certificate issued by another trusted site. If you, at a later point, want change the certificate you use, you can do this from the Mobile Server Manager.

1. Right-click the Mobile Server Manager and select **Edit Certificate...**
2. Choose whether you want to either:

- Generate a self-signed certificate or
- Load a certificate file.

Generate a self-signed certificate

1. Choose the **Generate a self-signed certificate** option and click **OK**.
2. Wait for a few seconds while the system installs the certificate.
3. Once finished, a window opens and informs you that the certificate was installed successfully. The Mobile service is restarted for the changes to take effect.

Locate a certificate file

1. Choose the **Load a certificate file** option.
2. Fill in the path for the certificate file or click the ... box to open a window where you can browse for the file.
3. Fill in the password connected to the certificate file.
4. When finished, click **OK**.

Note that HTTPS is not supported on Windows XP and Windows 2003 operating systems and works on Windows Vista or newer Windows OS only.

Fill in/edit surveillance server credentials

1. Right-click the Mobile Server Manager and select **Surveillance Server Credentials...**
2. Fill in the **Server URL**
3. Select what user you want to log in as:

- Local system administrator (no credentials needed) or
- A specified user account (credentials needed)

1. If you have chosen a specified user account, fill in **User Name** and **Password**.
2. When finished, click **OK**.

Show/edit port numbers

1. Right-click the Mobile Server Manager and select **Show/Edit Port Numbers...**
2. To edit the port numbers, fill in the relevant port number. You can indicate a standard port number (for HTTP connections) and/or a secured port number (for HTTPS connections).
3. When finished, click **OK**.

Start, stop and restart Mobile service

If needed, you can start, stop and restart the Mobile service from the Mobile Server Manager. To perform any of these tasks, right-click the Mobile Server Manager and select **Start Mobile service**, **Stop Mobile service** or **Restart Mobile service** respectively**.**

Alarms

About alarms

The Alarms feature is a Milestone Integration Platform (MIP) (see "About MIP plug-ins" on page 199) based feature using functionality handled by the Event server. It provides central overview and control of alarms in any number of XProtect Professional installations throughout your organization.

You can configure alarms to be generated based on either:

- **Internal events (system-related):** for example, motion, server responding/not responding, archiving problems, lack of disk space, etc.
- **External events (integrated):** for example, MIP plug-in events.

In addition, the Alarms feature deals with general alarms settings and alarm logging.

Configuring alarms

Alarm configuration includes among other things:

- Dynamic setup of alarm handling (see "Add an alarm" on page 195) based on users access rights
- Central overview of all components: servers, cameras, and external units
- Setup of central logging of all incoming alarms and system information
- Handling of plug-ins, allowing customized integration of other systems, for example external access control or VCA-based systems.

Viewing alarms

The following can play a role with regards to alarms and who can view/control/manage them and to what degree**.** This is because alarms are controlled by the visibility of the object causing the alarm.

Source/device visibility: if the device causing the alarm is not set to be visible to the user, the user will not be able to see the alarm in the alarm list in the Smart Client. See Configure User Access wizard (on page 68).

Right to trigger manually defined events: if manually defined events (see "Add a manual event" on page 128) are available in your XProtect Professional system, these can determine if the user can trigger selected manually defined events in the Smart Client. See Configure User Access wizard (on page 68).

External plug-ins: if any external plug-ins are set up in your system, these might control user's rights to handle alarms.

General access rights: can determine whether the user is allowed to (only) view or also to manage alarms. See Configure User Access wizard (on page 68).

Time profiles for alarms

Alarms can also be based on time profiles (for alarms) (see "Add a time profile (for Alarms)" on page 194). Alarm's time profiles are periods of time used when creating alarm definitions. You can, for example, create a time profile for alarms covering the period from 2.30 PM till 3.30 PM on Mondays, and then use the time profile to make sure that certain alarm definitions are only enabled within this period.

Frequently asked questions: XProtect Central and alarms

Does Alarms cover the same functionality as XProtect Central? Yes, to a large extent, since configuration of former XProtect Central functionality is now included in the Alarms feature. XProtect Central was an independent product consisting of two parts: a dedicated server and a number of dedicated clients. Alarms, on the other hand, is an integrated part of XProtect Professional. This

means that much configuration needed in XProtect Central has become redundant with the introduction of alarms. Client-wise the Alarms feature uses the XProtect Smart Client.

However, the features Alarms, Time Profiles (for Alarms) and General Settings, must still be configured in the Management Application and are very similar to XProtect Central.

Can I reuse old alarm and map definitions from XProtect Central? No, you will have to redefine your alarms and maps definitions in the Alarms feature.

Does the Alarms feature cover the same functionality as XProtect Analytics Generic VA? Yes, to a large extent, since what was before a plug-in to XProtect Analytics is now an integrated part of the Alarms feature and covers the same functionality. See also **'Does Alarms cover the same functionality as XProtect Central?'** FAQ earlier.

Tip: You can even use manual events for triggering alarms and, if required, the same event can be used to trigger several different alarms.

About alarms in the Smart Client

To ease overview, delegation and handling of alarms, these will appear in the Smart Client alarm list where it is possible to view and manage these (reassign, change status, comment, and similar). They can, if relevant, be integrated with map functionality. The Alarms feature is a powerful monitoring tool, providing instant overview of alarms and possible technical problems.

IMPORTANT: It is only possible to view alarms based on the Alarms feature in Smart Client 6.0 if you run Smart Client 6.0 in a 32-bit version—not in a 64-bit version.

Add a time profile (for Alarms)

Time Profiles are periods of time used for the Alarms (see "About alarms" on page 192) feature only.

Tip: For all other time scheduling and profiling purposes, use the general scheduler of XProtect Professional.

You can, for example, create a time profile covering the period from 2.30 PM till 3.30 PM on Mondays, and then use the time profile to make sure that a certain alarm definition is only enabled within this period.

They can be based on one or more single periods of time, on one or more recurring periods of time, or a combination of single and recurring times. Many users will be familiar with the concepts of single and recurring time periods from calendar applications, such as the one in Microsoft Outlook.

Time profiles always apply in the **XProtect Professional server's** local time.

To add a time profile (for an alarm (see "Add an alarm" on page 195)), do the following:

1. In the Management Application's navigation pane, expand **Alarms**, right-click **Time Profiles**, and select **Create New**.

   Tip: The small month overview in the top right corner of the **Time Profile Properties** window can help you get a quick overview of the time periods covered by the time profile, as dates containing specified times are highlighted in bold.

2. In the calendar, select the **Day View, Week View, or Month View** tab, then right-click inside the calendar and select either **Add Single Time...** or **Add Recurring Time...**.

3. If you select **Add Single Time...**, specify **Start time** and **End time**. If the time is to cover whole days, select the **All-day event** box.

—or—
If you select **Add Recurring Time...**, specify time range, recurrence pattern, and range of recurrence.

Tip: If you select a time period by dragging in the calendar before right-clicking, the selected period will automatically be used in the dialog that appears when you select **Add Single Time...** or **Add Recurring Time...**.

4. Click **OK**.
5. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Tip: When you edit an existing time profile, remember that a time profile may contain more than one time period, and that time periods may be recurring. If you want your time profile to contain additional periods of time, add more single times or recurring times.

Add an alarm

For a detailed overview of Alarms and how the feature works, see About alarms (on page 192).

To add/configure an alarm, do the following:

1. In the Management Application's navigation pane, expand **Alarms**, right-click **Alarm Definition** and select **Create New**.
2. Specify required properties (see "Alarms definition" on page 195).
3. Click **OK**.
4. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

Configure analytics events in alarms

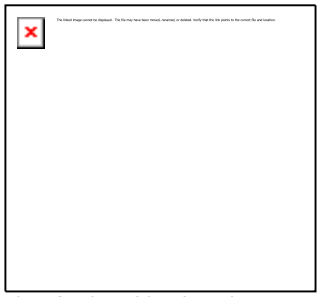
Analytics events (see "Overview of events and output" on page 125) are typically data received from external third-party video content analysis (VCA) (see "VCA" on page 222) providers. An example of a VCA-based system could be an access control system.

Alarms properties

Properties in this window:

Alarms definition

When you configure Alarm definitions (see "Add an alarm" on page 195), specify the following:

Name	Description
Enable	Enables the Alarms feature.
Name	Enter a name. The alarm's name will appear whenever the alarm is listed. **Tip:** Alarm names do not have to be unique, but using unique and descriptive alarm names are advantageous in many situations.
Description	Enter a description (optional).
Triggering event	This list offers both system-related events and plug-ins. You can select the event message which should be used when the alarm is triggered:  List of selectable triggering events; the highlighted one is created and customized using analytics events.
Sources	Select which cameras and/or other devices, including plug-in defined sources (VCA, MIP, etc) (see "About alarms" on page 192), the event should originate from in order to trigger the alarm. Your options depend upon which type of event you have selected.
Time profile	If you select **Time profile**, you must select when the alarm should be enabled for triggering. If you have not defined alarm time profiles (see "Add a time profile (for Alarms)" on page 194), you will only be able to select **Always**. If you have defined one or more time profiles, they will be selectable from this list.
Event based	If you select **Event based,** you must select which events should start and stop the alarm. Events available for selection are hardware events defined on cameras, video servers and input. Also global/manual event definitions (see "Add a manual event" on page 128) can be used. Note that when selecting **Event based** it is not possible to define alarms based on outputs—only on inputs.
Time Limit	Select the time-limit within which the operator must respond to the alarm.
Events triggered	Select the event to be triggered if the operator does not react withing the time limit specified in **Time limit**. This could be, for example, sending an email, SMS or similar.

Name	Description
Related cameras	Select (a maximum of 15) cameras for inclusion in the alarm definition even though they are not themselves triggering the alarm. This can be relevant, for example, if you have selected an external event message (such as a door being opened) as the source of your alarm. By defining one or more cameras near the door, you could attach the cameras' recordings of the incident to the alarm.
Related map	Select a map to tie to the alarm definition. The selected map will automatically be shown in the Smart Client whenever the alarm is listed. This might help you to quicker identify the physical location of the alarm.
Initial alarm owner	Select a default user responsible for the alarm. You can only select from users allowed to view **all** cameras and/or other devices selected as source(s) for the event causing the alarm.
Initial alarm priority	Select a priority (**High**, **Medium** or **Low)** for the alarm. Priorities can be used for sorting purposes and workflow control in the Smart Client.
Initial alarm category	Select a category to which the alarm should initially be assigned. This could be, for example, **Building01**, **Burglary**, **ElevatorEast** or similar, depending on which categories have been defined.
Event triggered by alarm	Define an event to be triggered by the alarm in the Smart Client (if needed).
Auto-close alarm	Select if the alarm should automatically be closed upon a particular event. This is possible for alarms triggered by some (but not all) events.

See also Alarm data settings (on page 197) and Alarm sound settings (see "Sound settings" on page 198) for further information on how to configure alarm settings.

Alarm data settings

When you configure alarm data settings, specify the following:

Alarm Data Levels **tab,** Priorities

Name	Description
Level	Add new priorities with level numbers of your choosing or use/edit the default priority levels (numbers **1**, **2** or **3)**. These priority levels are used to configure the **Initial alarm priority** setting (see "Alarms definition" on page 195).
Name	Type a name for the entity. You can create as many as you like.
Sound	Select the sound to be associated with the alarm. Use one if the default sounds or add more in Sound Settings (on page 198).

Alarm Data Levels tab, States

Level	In addition to the default state levels (numbers **1**, **4**, **9** and **11,** which can not be edited or reused), add new states with level numbers of your choosing. These state levels are only visible in the Smart Client's **Alarm List**.
Name	Type a name for the entity. You can create as many as you like.

Alarm Data Levels tab, Categories

Level	Add new categories with level numbers of your choosing. These category levels are used to configure the **Initial alarm category** setting (see "Alarms definition" on page 195).
Name	Type a name for the entity. You can create as many as you like.

Alarm List Configuration tab

In **Available columns,** use **>** to select which columns should be available in the Smart Client's **Alarm List**. Use **<** to clear selection. When done, **Selected columns** should contain the items to be included.

Reasons for Closing tab**Enable**	Select to enable that all alarms must be assigned a reason for closing before they can be closed.
Reason	Add reasons for closing that the user can choose between when closing alarms. Examples could be "**Solved-Trespasser**" or "**False Alarm**". You can create as many as you like.

Sound settings

When you configure Sound Settings, specify the following:

Name	Description
Sounds	Select the sound to be associated with the alarm. The list of sounds contain a number of default Windows sounds. These cannot be edited. However, you can add new sounds of the file type .wav, but only if these are encoded in Pulse Code Modulation (PCM). Although the default sounds are standard Windows sound-files, local Windows settings might cause these to sound different on different machines. Some users might also have deleted one or more of these sound-files and will therefore be unable to play them. To ensure an identical sound all over, you should import and use your own .wav files encoded in PCM.
Add	Lets you add sounds. Browse to the sound to upload one or several .wav files.
Remove	Remove a selected sound from the list of manually added sounds. Default sounds cannot be removed.

Name	Description
Test	Lets you test the sound. In the list, select the sound. The sound will be played once.

Time profile

When you configure Time profiles (see "Add a time profile (for Alarms)" on page 194), specify the following:

Name	Description
Name	Type a name for the time profile.
Description	Enter a description (optional).
Add Single Time	Right-click the calendar and select **Add Single Time**. Specify **Start time** and **End time**. If the time covers whole days, select **All-day event**.
Add Recurring Time	Right-click the calendar and select **Add Recurring Time**. Specify the time range, recurrence pattern, and range of recurrence.
Edit Time	Right-click the calendar and select **Edit Time**. Specify **Start time** and **End time**. If the time covers whole days, select **All-day event**. When you edit an existing time profile, remember that a time profile may contain more than one time period, and that time periods may be recurring. If you want your time profile to contain additional periods of time, add more single times or recurring times.

MIP plug-ins

About MIP plug-ins

If you install MIP (Milestone Integration Partner) plug-ins to your XProtect Professional, the plug-ins can be found in the Management Application's navigation pane, expand **Advanced Configuration**, under **MIP Plug-ins**.

You can assign MIP-related user rights to users and user groups. You do this from the Management Application's navigation pane, expand **Advanced Configuration**, expand **Users**, right-click the wanted user and select **Properties**. Under the **Alarm Management** tab, a tab allowing access to MIP settings for the selected user is located.

You can also use online activation (see "About activating licenses" on page 35) in connection with licensing schemes of MIP-related plug-ins.

Backup and restore configuration

About backup and restore of configurations

We recommend that you make regular backups of your XProtect Professional configuration (cameras, schedules, views, etc.) as a disaster recovery measure. While it is rare to lose your configuration, it can happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration.

Back up system configuration

The backup described here is a backup of your entire surveillance system setup (including, among other things, log files, event and Matrix configuration, restore points, view groups, and Management Application, and Smart Client configuration). Alternatively, you can export your configuration as a backup (see "Export and import management application configuration" on page 204), which is limited to the the Management Application configuration.

The following describes how to back up your configuration in XProtect Professional 7.0.

If you need information about how to back up a configuration from an earlier version of XProtect Professional—a typical need when upgrading—see Upgrade from a previous version (on page 28).

In the following, we assume that you have not changed the XProtect Professional default configuration path (see "Configure default file paths" on page 212), which is **C:\Documents and Settings\All Users\Application Data\Milestone\Milestone Surveillance** on servers running Windows® XP or Windows Server 2003, and **C:\Program Data\Milestone\Milestone Surveillance** on servers running all other supported operating systems. If you have changed the default configuration path, you must take your changes into consideration when using the method described in the following.

To back up:

1. If XProtect Professional is used on a server running Windows XP or Windows Server 2003, make a copy of the folder **C:\Documents and Settings\All Users\Application Data\Milestone\Milestone Surveillance** and all of its content.

   If XProtect Professional is used on a server running any other supported operating system, make a copy of the folder **C:\Program Data\Milestone\Milestone Surveillance** and all of its content.

2. Open the folder **C:\Program Files\Milestone\Milestone Surveillance\devices**, and verify if the file **devices.ini** exists. If the file exists, make a copy of it. The file will exist if you have configured video properties (see "General" on page 100) for certain types of cameras; for such cameras, changes to the properties are stored in the file rather than on the camera itself.

3. Store the copies away from the XProtect Professional server, so that they will not be affected if the server is damaged, stolen or otherwise affected.

   Remember that a backup is a snapshot of your XProtect Professional system configuration at the time of backing up. If you later change your configuration, your backup will not reflect the most recent changes. Therefore, back up your system configuration regularly.

Tip: When you back up your configuration as described, the backup will include restore points (see "Restore system configuration from a restore point" on page 206). This allows you to not only restore the backed-up configuration, but also to revert to an earlier point in that configuration if required.

Restore system configuration

1. If XProtect Professional is used on a server running Windows XP or Windows Server 2003, copy the content of the backed-up **Milestone Surveillance** folder into **C:\Documents and Settings\All Users\Application Data\Milestone\Milestone Surveillance**.

   If XProtect Professional is used on a server running any other supported operating system, copy the content of the backed-up **Milestone Surveillance** folder into **C:\Program Data\Milestone\Milestone Surveillance.**

2. If you backed up the file **devices.ini**, copy the file into **C:\Program Files\Milestone\Milestone Surveillance\devices.**

Back up and restore Alarms configuration

It is important that you regularly back up your XProtect Professional Alarms configurations. You do this by backing up the event server, which handles your alarm and map configuration, and also the Microsoft® SQL Server Express database, which stores your alarm data. This enables you to restore your alarm and map configuration in a possible disaster recovery scenario.

Tip: Backing up also has the added benefit that it flushes the SQL Server Express database's transaction log.

When you back up and restore Alarms configuration, you must do it in the following order.

Prerequisites

- **You must have administrator rights on the SQL Server Express database** when you backup or restore your alarm configuration database on the SQL Server Express. Once you are done backing up or restoring, you only need to be a database owner of the SQL Server Express database.
- **Microsoft® SQL Server Management Studio Express**, a tool you can download for free from www.microsoft.com/downloads (see http://www.microsoft.com/downloads/ - http://www.microsoft.com/downloads/). Among its many features for managing SQL Server Express databases are some easy-to-use backup and restoration features. Download and install the tool on your existing surveillance system server and on a possible future surveillance system server (you will need it for backup as well as restoration).

Step 1: Stopping the Event Server service

Stop the event server service to prevent configuration changes from being made:

1. On your surveillance system server, click **Start** > **Control Panel** > **Administrative Tools** > **Services**.

2. Right-click the Event Server, click **Stop**.

This is important since any changes made to alarm configurations—between the time you create a backup and the time you restore it—will be lost. If changes are made after the backup, you will have to make a new backup.

Note that alarms will not be generated while the Event Server service is stopped; it is thus important to remember to start the service again once you have finished backing up the SQL database.

Step 2: Backing up alarms data in SQL Server Express database

1. Open Microsoft SQL Server Management Studio Express from Windows' **Start** menu by selecting **All Programs** > **Microsoft SQL Server 2008 > SQL Server Management Studio Express**.

   Tip: If you do not have **SQL Server Management Studio Express**, it can be downloaded for free from www.microsoft.com/downloads (see http://www.microsoft.com/downloads/ - http://www.microsoft.com/downloads/).

   When you open the tool, you are prompted to connect to a server. Specify the name of the required SQL Server and connect with admin user credentials.

   Tip: You do not have to type the name of the SQL server: If you click inside the **Server name** field and select **<Browse for more...>**, you can select the required SQL Server from a list instead.

2. Once connected, you will see a tree structure in the **Object Explorer** in the left part of the window. Expand the SQL Server item, then the **Databases** item, which contains your entire alarm configuration.

3. Right-click the **VIDEOOSDB** database, and select **Tasks** > **Back Up...**

4. On the **Back Up Database** dialog's **General** page, do the following:

   - Under **Source**: Verify that the selected database is **VIDEOOSDB** and that the backup type is **Full**.

   - Under **Destination**: A destination path for the backup is automatically suggested. Verify that the path is satisfactory. If not, remove the suggested path, and add another path of your choice.

5. On the **Back Up Database** dialog's **Options** page, under **Reliability**, select **Verify backup when finished** and **Perform checksum** before writing to media.

6. Click **OK** to begin the backup. When backup is finished, you will see a confirmation.

7. Exit Microsoft SQL Server Management Studio Express.

No VIDEOOSDB database? VIDEOOSDB is the default name of the database containing the system configuration. If you can find the database, but it is not called **VIDEOOSDB**, it could be because you gave the database another name during the installation. In the following, we will assume that the database uses the default name.

Step 3: Reinstalling XProtect Professional (if needed) (see "Install your surveillance server software" on page 26).

Step 4: Restoring alarms data in SQL Server Express database

Luckily, most users never need to restore their backed-up alarm data, but if you ever need to, do the following:

1. In the Windows Start menu, open Microsoft SQL Server Management Studio Express.

   Tip: If you do not have **SQL Server Management Studio Express**, it can be downloaded for free from www.microsoft.com/downloads (see http://www.microsoft.com/downloads/ - http://www.microsoft.com/downloads/).

2. Connect to a server. Specify the name of the required SQL Server, and connect using the user account the database was created with.

   Tip: You do not have to type the name of the SQL server: If you click inside the **Server name** field and select **<Browse for more...>**, you can select the required SQL Server from a list instead.

3. In the **Object Explorer** on the left, expand **SQL Server** < **Databases**, right-click the **VIDEOOSDB** database, and then select **Tasks** > **Restore** > Database...

   VIDEOOSDB is the default name of the database containing the system configuration. If you can find the database, but it is not called **VIDEOOSDB**, it could be because you gave the database another name during installation. In the following, we will assume that the database uses the default name.

4. In the **Restore Database** dialog, on the **General** page, under **Source for restore,** select **From device** and click <Browse for more...>, to the right of the field. In the Specify Backup dialog, make sure that **File** is selected in the **Backup media** list**.** Click **Add.**

5. In the **Locate Backup File** dialog, locate and select your backup file **VIDEOOSDB.bak**. Then click **OK.** The path to your backup file is now listed in the **Specify Backup** dialog.

6. Back on the **Restore Database** dialog's **General** page, your backup is now listed under **Select the backup sets to restore**. Make sure you select the backup by selecting the check box in the **Restore** column.

7. Now go to the **Restore Database** dialog's **Options** page, and select **Overwrite the existing database**. Leave the other options as they are, and then click **OK** to begin the restoration. When the restore is finished, you will see a confirmation.

   Tip: If you get an error message telling you that the database is in use, try exiting Microsoft SQL Server Management Studio Express completely, then repeat steps 1-9.

8. Exit Microsoft SQL Server Management Studio Express.

Step 5: Restarting the Event Server service

During the restore process, the Event Server service was stopped to prevent configuration changes being made until you were done. Remember to start the service again:

1. On your surveillance system server, click **Start** > **Control Panel** > **Administrative Tools** > **Services**.

2. Right-click the Event Server, click **Start**.

What is the SQL Server Express transaction log and why does it need to be flushed?

Each time a change in the XProtect Professional alarm data occurs, the SQL Server will log the change in its transaction log. The transaction log is essentially a security feature that makes it possible to roll back and undo changes to the SQL Server Express database. The SQL Server by default stores its transaction log indefinitely, and therefore the transaction log will over time build up more and more entries.

The SQL Server's transaction log is by default located on the system drive, and if the transaction log just grows and grows, it may in the end prevent Windows from running properly. Flushing the SQL Server's transaction log from time to time is therefore a good idea; flushing it does not in itself make the transaction log file smaller, but it prevents it from growing out of control. XProtect Professional does not, however, automatically flush the SQL Server's transaction log at specific intervals. This is because users have different needs. Some want to be able to undo changes for a very long time, others do not care; what would suit one organization's needs could be problematic for others.

You can do several things on the SQL Server itself to keep the size of the transaction log down, including truncating and/or shrinking the transaction log (for numerous articles on this topic, go to support.microsoft.com (see http://support.microsoft.com - http://support.microsoft.com) and search for SQL Server transaction log). However, backing up the XProtect Professional database is generally a better option since it flushes the SQL Server's transaction log and gives you the security of being able to restore your XProtect Professional alarm data in case something unexpected happens.

Export and import management application configuration

You can export the current configuration of your XProtect Professional Management Application, either as a safety measure in order to have a backup file of your configuration, or as a clone allowing you to use a similar Management Application configuration elsewhere. You can subsequently import previously exported Management Application configurations.

Export Management Application configuration as backup

With this option, all relevant XProtect Professional Management Application configuration files will be combined into one single .xml file, which can then be saved at a location specified by you. Note that if there are unsaved changes to your configuration, they will automatically be saved when you export the configuration.

1. In the Management Application's **File** menu, select **Export Configuration - Backup**.
2. Browse to the location at which you want to store the exported configuration, specify a suitable file name, and click **Save**.

If you intend to set up an identical version of your surveillance system elsewhere, **do not** export your configuration as **backup**, since this may lead to the same device information being used twice, in which case clients may get the following error message: **Application is not able to start because two (or more) cameras are using the same name or ID.** Instead, export your configuration as a **clone**. When you export as a clone, the export takes into account the fact that you will not use the

exact same physical cameras, etc. even though your new system may otherwise be identical to your existing one.

What is the difference between this Management Application configuration backup and the system configuration backup done from the Milestone Surveillance folder? Those are two different things. The backup described here is limited to a backup of the Management Application configuration. The type of system configuration backup done from the Milestone Surveillance folder is a backup of your entire surveillance system setup (including, among other things, log files, event configuration, restore points, view groups, and Management Application, and Smart Client configuration).

When you install the new version of XProtect Professional, it inherits the configuration from your previous version.

We recommend that you make regular backups of your server configuration as a disaster recovery measure. You should also do this when you upgrade your server. While it is rare that you lose your configuration (cameras, schedules, views, etc), it **can** happen under unfortunate circumstances. Fortunately, it takes only a minute to back up your existing configuration.

Export Management Application configuration as clone

With this option, all relevant XProtect Professional Management Application configuration files will be collected, and GUIDs (Globally Unique IDentifiers; unique 128-bit numbers used for identifying individual system components, such as cameras) will be marked for later replacement.

Why are GUIDs marked for replacement? GUIDs are marked for later replacement because they refer to specific components (cameras, etc.). Even though you wish to use the cloned configuration for setting up a new similar system using similar types of cameras, the new system will not use the exact same physical cameras as the cloned system. When the cloned configuration is later used in a new system, the GUIDs will therefore be replaced with GUIDs representing the specific components of the new system.

After GUIDs have been marked for replacement, the configuration files will be combined into one single .xml file, which can then be saved at a location specified by you. Note that if there are unsaved changes to your configuration, they will automatically be saved when you export the configuration.

1. In the Management Application's **File** menu, select **Export Configuration - Clone**.
2. Browse to the location at which you want to store the exported configuration, specify a suitable file name, and click **Save**.

Import previously exported Management Application configuration

The same import method is used regardless of whether the XProtect Professional Management Application configuration was exported as a backup or a clone.

1. In the Management Application's **File** menu, select **Import Configuration**.
2. Browse to the location from which you want to import the configuration, select the required configuration file, and click **Open**.
3. Only relevant if the system into which you import the configuration contains devices (cameras, etc.) which are not present in the imported configuration: You will be asked whether you want to delete or keep recordings from affected devices. If keeping the recordings, note that they will not be accessible until you add the affected devices to XProtect Professional again. Select the required option, and click **OK**.

4. In the Management Application's navigation pane, expand **Advanced Configuration,** and select **Services**.

5. For the Recording Server and Image Server services respectively, click the **Restart** button. When the two services are restarted, the imported Management Application configuration is applied.

Import changes to configuration

It is possible to imported changes to a configuration. This can be relevant if installing many similar XProtect Professional systems, for example in a chain of shops where the same types of server, hardware devices, and cameras are used in each shop. In such cases, you can use an existing configuration—typically a cloned configuration (see "Export and import management application configuration" on page 204)—as a template for the other installations. However, since the shops' installations are not exactly the same (the hardware devices and cameras are of the same type, but they are not physically the same, and therefore they have different MAC addresses), there needs to be an easy way of importing changes to the template configuration.

This is why XProtect Professional lets you import changes about hardware devices and cameras as comma-separated values (CSV) from a file (see "CSV file format and requirements" on page 52):

1. From the menu bar, select **File** > **Import Changes to Configuration...**

2. Select **Online verification** if the new hardware devices and cameras listed in your CSV file are connected to the server and you want to verify that they can be reached.

3. Then point to the CSV file, and click the **Import Configuration from File** button.

Restore system configuration from a restore point

Restore points allow you to return to a previous configuration state. Each time a configuration change is applied in the Management Application—either by clicking **OK** in a properties dialog or by clicking the **Apply** button in a summary pane—a new restore point is created.

All restore points in the current and previous five sessions are stored and can be selected again. A new session begins each time the Management Application is started as well as each time you save the whole configuration, for example by clicking the **Save Configuration** button in the Management Application's toolbar. For sessions older than the last five sessions, only the latest restore point of each session is stored. With the **Number of old sessions to keep** field you can control how many old sessions are kept.

When selecting to restore a configuration from a restore point, the configuration from the selected restore point will be applied and used once the services are restarted (see Start and stop services (on page 184)).

If you have added new cameras or other devices to XProtect Professional after the restore point was created, they will be missing if you load the restore point. This is due to the fact that they were not in the system when the restore point was created. In such cases, you will be notified and must decide what to do with recordings from the affected devices.

1. From the Management Application's **File** menu, select **Load Configuration from Restore Point...**

2. In the left part of the **Restore Points** dialog, select the required restore point.

Tip: When you select a restore point, you will in the right part of the dialog see information about the configuration state at the selected point in time. This can help you select the best possible restore point.

3. Click the **Load Restore Point** button.
4. If you are sure that you want to overwrite the current configuration with the one from the selected restore point, click **OK**.
5. Only relevant if the current configuration contains cameras or other devices which were not present in the selected restore point: You will be asked whether you want to delete or keep recordings from affected devices. If keeping the recordings, note that they will not be accessible until you add the affected devices to XProtect Professional again. Select the required option, and click **OK**.
6. Click **OK** in the Restore Points dialog.
7. In the Management Application's navigation pane, expand **Advanced Configuration**, and select **Services**.
8. For the Recording Server and Image Server services respectively, click the **Restart** button. When the two services are restarted, the configuration from the selected restore point is applied.

Common tasks

About handling daylight saving time

Daylight saving time (DST, also known as summer time) is the practice of advancing clocks in order for evenings to have more daylight and mornings to have less. Typically, clocks are moved forward one hour during the spring season and adjusted backward during the fall season. Note that use of DST varies between countries/regions.

When working with a surveillance system, which is inherently time-sensitive, it is important to know how the system handles DST.

Spring: Switch from Standard Time to DST

The change from standard time to DST is not much of an issue since you jump one hour forward. Typically, the clock jumps forward from 02:00 standard time to 03:00 DST, and the day thereby has 23 hours. In that case, there is no data between 02:00 and 03:00 in the morning since that hour, for that day, did not exist.

Fall: Switch from DST to Standard Time

When you switch from DST to standard time in the fall, you jump one hour back. Typically, the clock jumps backward from 02:00 DST to 01:00 standard time, repeating that hour, and the day thereby has 25 hours. In that case, you will reach 01:59:59, then immediately revert back to 01:00:00. If the system did not react, it would essentially re-record that hour, so the first instance of, for example, 01:30 would be overwritten by the second instance of 01:30.

Because of this, XProtect Professional will forcefully archive the current video in the event that the system time changes by more than five minutes. The first instance of the 01:00 hour will not be viewable directly from clients. However, the data is recorded and safe, and it can be browsed using the Smart Client application by opening the archived database directly.

Improve stability with 3 GB virtual memory

Microsoft Windows 32-bit operating systems can address 4 GB of virtual memory. The operating system kernel reserves 2 GB for itself, and each individual running process is allowed to address another 2 GB. This is a default setting in Windows, and for the vast majority of XProtect Professional installations it works fine.

As from XProtect Professional 6.5, the main components of the server—the Recording Server service and the Image Server service—have been compiled with the LARGEADDRESSAWARE flag. This means you can optimize the memory usage of the XProtect Professional Recording Server and Image Server services by configuring your 32-bit Windows operating system so that it restricts the kernel to 1GB of memory, leaving 3GB of address space for processes compiled with the LARGEADDRESSAWARE flag.

This should improve the stability of especially the Recording Server service by allowing it to exceed the previous 2 GB virtual memory limit, making it possible for it to use up to 3 GB of memory. The change in Windows configuration is known as 3 GB switching.

When is 3 GB switching relevant?

For very large XProtect Professional installations and/or for installations with many megapixel cameras it can be relevant to change Windows settings so that only 1 GB of virtual memory is reserved for the operating system kernel, leaving 3 GB for running processes.

If you use the Windows default setting, with only 2 GB virtual memory reserved for running processes, the Recording Server service in very large installations of XProtect Professional may:

- Behave erratically when it gets close to the 2 GB virtual memory limit. Symptoms can include database corruption, and client-server or camera-server communication errors.
- Become unstable and crash if it exceeds the 2 GB virtual memory limit. During such crashes, the code managing the surveillance system databases is not closed properly, and databases will become corrupt. In case of a crash, Windows will normally restart the Recording Server service. However, when the Recording Server service is restarted, one of its first tasks will be to repair the databases. The database repair process can in some cases take several hours, depending on the amount of data in the corrupted databases.

If you experience problems, and you run XProtect Professional 6.5 or newer, making Windows use 3 GB for running processes is likely to solve the problems. If you have not experienced problems, but you run XProtect Professional 6.5 or newer and your XProtect Professional installation is very large and/or features many megapixel cameras, 3 GB switching can help prevent the problems from occurring.

The way to configure 32-bit Windows to be LARGEADDRESSAWARE depends on your type of Windows operating system. In the following, you will see two methods outlining Microsoft's recommended procedure for increasing the per-process memory limit to 3 GB. Use the first method if running Windows XP Professional or Windows Server 2003. Use the second method if running Windows 2008 Server, Windows Vista Business, Windows Vista Enterprise or Windows Vista Ultimate.

What to do: If running Windows XP Professional or Windows Server 2003

The following technique can be used to add the 3 GB switch to the boot.ini file.

1. From a command prompt, enter the following to add the 3 GB switch to the end of the first line of the operating system section in the boot.ini file (requires administrative privileges):

   ```
   BOOTCFG /RAW "/3GB" /A /ID 1
   ```

   Where:

   - **/RAW** specifies the operating system options for the boot entry. The previous operating system options will be modified.
   - **"/3GB"** specifies the 3 GB switch.
   - **/A** specifies that the operating system options entered with the /RAW switch will be appended to the existing operating system options.
   - **/ID** specifies the boot entry ID in the OS Load Options section of the boot.ini file to add the operating system options to. The boot entry ID number can be obtained by performing the command **BOOTCFG /QUERY** (this displays the contents of the boot.ini file) at the command prompt.

2. Reboot after editing the boot.ini file for the changes to take effect.

Remove the 3 GB Switch

Remove the 3 GB switch

If you want to undo the 3 GB switch, follow this procedure:

1. Select **Start** > **Control Panel**, and double-click the **System** icon.
2. Select the **Advanced** tab, and click the **Settings** button in the **Startup and Recovery** section.
3. Click the **Edit** button in the **System Startup** section. The boot.ini file will launch in an editor.
4. Remove the **"/3GB"** from the end of the appropriate boot entry line under the [operating systems] section. Save and close the file.
5. Click **OK** in the **Startup and Recovery** section.
6. Reboot after editing the boot.ini file for the changes to take effect.

What to do: If running Windows 2008 Server or Windows Vista

1. Select **Start** > **All Programs** > **Accessories**, right-click **Command Prompt**, and select **Run as administrator**, then click **Continue**.
2. Enter the following command to add the 3 GB switch to the current operating system boot entry:

   ```
   BCDEDIT /SET INCREASEUSERVA 3072
   ```

   Where:

   - **USERVA** specifies an alternate amount of user-mode virtual address space for operating systems.
   - **3072** Specifies 3 GB (3072 MB).
3. Reboot after editing for the changes to take effect.

Remove the /3GB switch

1. Select **Start** > **All Programs** > **Accessories**, right-click **Command Prompt**, and select **Run as administrator**, then click **Continue**.
2. Enter the following command to remove the 3 GB switch from the current operating system boot entry:

   ```
   BCDEDIT /DELETEVALUE INCREASEUSERVA
   ```
3. Reboot after editing for the changes to take effect.

About protecting recording databases from corruption

In the Management Application, you can select which action to take if a camera database becomes corrupted. The actions include several database repair options. While being able to select such actions is highly valuable, it is of course even better to take steps to ensure that your camera databases do not become corrupted.

Power outages: use a UPS

The single most common reason for corrupt databases is the recording server being shut down abruptly, without files being saved and without the operating system being closed down properly. This may happen due to power outages, due to somebody accidentally pulling out the server's power cable, or similar.

The best way of protecting your recording servers from being shut down abruptly is to equip each of your recording servers with a UPS (Uninterruptible Power Supply).

The UPS works as a battery-driven secondary power source, providing the necessary power for saving open files and safely powering down your system in the event of power irregularities. UPSs vary in sophistication, but many UPSs include software for automatically saving open files, for alerting system administrators, etc.

Selecting the right type of UPS for your organization's environment is an individual process. When assessing your needs, however, do bear in mind the amount of runtime you will require the UPS to be able to provide if the power fails; saving open files and shutting down an operating system properly may take several minutes.

Windows Task Manager: Be careful when ending processes

When working in Windows Task Manager, be careful not to end any processes which affect the surveillance system. If you end an application or system service by clicking **End Process** in the Windows Task Manager, the process will not be given the chance to save its state or data before it is terminated. This may lead to corrupt camera databases.

Windows Task Manager will typically display a warning if you attempt to end a process. Unless you are absolutely sure that ending the process will not affect the surveillance system, click **No** when the warning message asks you if you really want to terminate the process.

Hard disk failure: Protect your drives

About viewing version and license information

Knowing the exact version of your XProtect Professional system may be relevant if you require support, or want to upgrade your system. It may also be relevant for you to know your license information and what contact details Milestone has registered about your organization.

If you have purchased a Software Upgrade Plan (SUP), information about the expiration date of the SUP may also be important you to know.

To view such information, select **About...** in the Management Application **Help** menu.

If you need to update any of your information, click the link provided at the bottom to log on to the Milestone website from which you can update your information.

Apply/save configuration changes

Whenever you make changes in your XProtect Professional configuration, you will be asked to apply them.

- If you made the changes in one of the Management Application dialogs, you apply them by clicking **OK**.

- If you made the changes in one of the Management Application summary tables, click **Apply.**

Applying a configuration change means that the change is stored by XProtect Professional in a restore point (see "Restore system configuration from a restore point" on page 206) (so that you can return to a working configuration if something goes wrong), but applying a configuration change does not mean that the changes will take immediate effect on the surveillance system.

To store your configuration change in the configuration file:

1. In the Management Application toolbar click the **Save Configuration** button.
2. For your configuration changes to have immediate effect, on the Management Application toolbar, click **Save Changes and Restart Surveillance Services**.

   If you do not restart immediately, your configuration changes will take effect the next time you restart XProtect Professional services (see "About services" on page 183).

   IMPORTANT: While services are restarted, you cannot view or record video. Restarting services typically only takes a few seconds, but in order to minimize disruption you may want to restart services at a time when you do not expect important incidents. Users connected to XProtect Professional through clients will typically remain logged in during the services restart, but they will experience a short video outage.

Configure default file paths

XProtect Professional uses a number of default file paths:

File paths	Description
Default recording path for new cameras	All new cameras you add will by default use this path for storing recordings. If required, you can change individual cameras' recording paths as part of their individual configuration (see "Recording and archiving paths" on page 106), but you can also change the default recording path so all new cameras you add will use a path of your choice.
Default archiving path for new cameras	All new cameras you add will by default use this path for archiving (see "About archiving" on page 143). If required, you can change individual cameras' archiving paths as part of their individual configuration, but you can also change the default recording path so all new cameras you add will use a path of your choice. Note that camera-specific archiving paths are not relevant if using dynamic path selection (on page 86) for archiving.
Configuration path	The path by default used for storing your XProtect Professional system configuration.

To change any of the default file paths:

1. If you want to change the configuration path, stop (see "Start and stop services" on page 184) all services. This step is not necessary if you want to change the default recording or archiving path.
2. On the Management Application menu bar, select **Application Settings** > **Default File Paths...**

3. You can now overwrite the necessary paths. Alternatively, click the browse button next to the field and browse to the location.

   For the default recording path, you can only specify a path to a folder on a **local** drive. If you are using a network drive, you cannot save recordings if the network drive becomes unavailable.

   If you change the default recording or archiving paths and there are existing recordings at the old locations, you must select whether you want to move the recordings to the new locations (recommended), leave them at the old locations, or delete them.

4. Click **OK**.

5. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

6. Restart (see "Start and stop services" on page 184) all services.

Monitor storage space usage

To view how much storage space you have on your XProtect Professional system—and not least how much of it is free—do the following:

1. In the Management Application's navigation pane, expand **Advanced Configuration**, and select **Cameras and Storage Information**.

2. View the **Storage Usage Summary** for information about, which drives are available, what drives are used for, the size of each drive, as well as how much video data, other data, and free space there is in each drive.

View video from cameras in Management Application

You can view live video from single cameras directly in the Management Application:

1. In the Management Application's navigation pane, expand **Advanced Configuration**, and expand **Cameras and Storage Information**.

2. Select the required camera to view live video from that camera. Above the live video, you will find a summary of the most important properties for the selected camera. Below the live video, you will find information about the camera's resolution and average image file size. For cameras using MPEG or H.264, you will also see the bit rate in Mbit/second.

   IMPORTANT: Viewing of live video in the Management Application may under certain circumstances affect any simultaneous recording from the camera in question. Especially three scenarios are important to consider:

   1) Some cameras supporting multistreaming may halve their frame rate or respond with other negative effects when a second stream is opened.

   2) If a camera delivers live video in a very high quality, de-coding of images may increase the load on the Recording Server service, which may in turn affect ongoing recordings negatively.

   3) Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, we

recommended stopping (see "Start and stop services" on page 184) the Recording Server service when configuring such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 213).

Glossary of terms

Symbols & Numeric

360 degrees panomorph support

Cameras with 360 degrees panomorph support offer—as the name indicates—360 degree coverage and can survey an entire area without blind spots or distorted images.

A

Administrator

1) System administrator. 2) In previous versions of XProtect Professional: the main application used by XProtect Professional administrators for configuring the surveillance system server. Now called the Management Application.

Analytics Events

Analytics events are typically data received from an external third-party video content analysis (VCA) provider. An example of a VCA-based system is an access control system. Analytics events can be integrated seamlessly with the **Alarms** feature.

API

Application Program Interface—set of tools and building blocks for creating or customizing software applications.

Aspect ratio

The height/width relationship of an image.

ATM

Automatic teller machine—machine that dispenses money when a personal coded card is used.

AVI

A popular file format for video. Files in this format carry the .avi file extension.

B

Browser

A software application for finding and displaying web pages.

C

Carousel

A feature for displaying video from several cameras, one after the other, in a single camera position. The required cameras and the intervals between changes are specified by the XProtect Professional administrator. The carousel feature is available, if configured, in the Smart Client.

Central

A product available as an add-on to XProtect Professional. XProtect Central provides a complete overview of status and alarms from any number of XProtect Professional servers, regardless of location.

Codec

A technology for compressing and decompressing audio and video data, for example, in an exported AVI file. MPEG and Indeo are examples of frequently used codecs.

CSV

Comma-separated values data format that stores tabular data, where the lines represent rows in a table and commas define the columns, in a simple file. For example, data about cameras may appear as comma-separated values in a .csv file, which can then be imported into XProtect Professional. A simple but effective method if setting up several similar systems.

D

Device

In XProtect Professional : a camera, video encoder, input device, or output device connected to a recording server.

DirectX

A Windows extension providing advanced multimedia capabilities.

DNS

Domain Name System—system allowing translation between alphabetic host names (for example, mycomputer) or domain names (for example, www.mydomain.com) and numeric IP addresses (for example, 192.168.212.2). Many people find alphabetic names easier to remember than numeric IP addresses.

Driver

A program used for controlling/communicating with a device.

DST

Daylight saving time; temporarily advancing of clocks during the summer so that afternoons have more daylight and mornings have less.

Dual stream

Some cameras support two independent streams (which can be sent to the recording server): one for live viewing and another for playback purposes. Each stream has its own resolution, encoding, and frame rate.

DVR

Digital video recorder—device that records video in a digital format to a hard disk drive embedded in the DVR itself.

E

Event Server

A server that stores and handles incoming alarm data and events from all XProtect Professional servers. The Event Server enables powerful monitoring and provides an instant overview of alarms and possible technical problems within your systems.

F

Fisheye

A type of lens that allows the creation and viewing of 360-degree images.

FPS

Frames per second—measurement indicating the amount of information contained in a motion 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 appears. Note, however, that a high FPS may also lead to a large file size when video is saved.

Frame rate

A measurement indicating the amount of information contained in motion video—typically measured in FPS.

FTP

File Transfer Protocol—standard for exchanging files across the internet. FTP uses the TCP/IP standards for data transfer and is often used for uploading or downloading files to and from servers.

G

Generic events

XProtect Professional can receive and analyze input in the form of TCP or UDP data packages which, if they match specified criteria, can be used to generate events. Such events are called generic events.

GOP

Group of pictures; individual frames grouped together, forming a video-motion sequence.

Grace period

When you install XProtect Professional, configure the system and add recording servers and cameras, XProtect Professional runs on temporary licenses. These need to be activated before a certain period ends. This is the grace period.

GSM

Global System for Mobile communications—a standard for mobile telephony.

GUID

Globally unique identifier—unique 128-bit number used to identify components on a Windows system.

H

H.264

A standard for compressing and decompressing video data (a codec). H.264 is a relatively recent codec; it compresses video more effectively than older codecs, and it provides more flexibility for use in a variety of network environments.

Hardware device

Technically speaking, cameras are not added to XProtect Professional, rather to hardware devices. This is because hardware devices have their own IP addresses or host names. Being IP-based, XProtect Professional primarily identifies units based on their IP addresses or host names. Even though each hardware device has its own IP address or host name, several cameras, microphones, and so on, can be attached to a single hardware device and share the same IP address or host name. This is typically the case with cameras attached to video encoder devices. Each camera, microphone, and so on, can be configured individually, even when several of them are attached to a single hardware device.

Host

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

Hotspot

Particular position for viewing enlarged and/or high quality video in the Smart Client.

HTTP

HyperText Transfer Protocol—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

Input/Output; refers to the communication between a computer and a person. Inputs are the signals or data received by the system and outputs are the signals or data sent from it.

I-frame

Short name for intra-frame; used in the MPEG standard for digital video compression. An I-frame is a single frame stored at specified intervals. The I-frame records the entire view of the camera, whereas the frames that follow (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.

Image Server

A service that handles access to XProtect Professional for remote users logging in with Smart Client The Image Server service does not require separate hardware; it runs in the background on the XProtect Professional server. The Image Server service is not

configured separately as it is configured through XProtect Professional 's Management Application.

IP

Internet Protocol—protocol (or standard) specifying the format and addressing scheme used for sending data packets across networks. IP is often combined with another protocol, TCP. 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. It is 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 periods (example: 192.168.212.2).

IPIX

A technology that allows the creation and viewing of 360-degree panomorph (fisheye) images.

J

JPEG

(Also JPG) Joint Photographic Experts Group—widely used lossy compression technique for images.

K

Keyframe

Used in the MPEG standard for digital video compression, a keyframe is a single frame stored at specified intervals. The keyframe records the entire view of the camera, whereas the frames between the keyframes record only the pixels that change. This helps greatly reduce the size of MPEG files.

M

MAC address

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

Manual events

You can generate an event manually from the client. These events are called manual events.

Master/Slave

A setup of servers where one server (the master server) is of higher importance than the remaining servers (the slave servers). With a master/slave setup in XProtect Professional, it is possible to combine several XProtect Professional servers and extend the number of cameras you can use beyond the maximum allowed number of cameras for a single server. In such a setup, clients will still have a single point of contact: they connect to the master server but also get access, transparently, to cameras and recordings on the slave servers.

Matrix

A feature enabling the control of live camera views on remote computers for distributed viewing. Once configured, Matrix-triggered live video can be viewed in the Smart Client.

Matrix recipient

A computer equipped with Smart Client software and therefore capable of displaying Matrix-triggered live video.

MJPEG

Motion JPEG—compressed video format where each frame is a separately compressed JPEG image. The method used is quite similar to the I-frame method used for MPEG, but no interframe prediction is used. This allows for somewhat easier editing, and makes

compression independent of the amount of motion.

Monitor

1) A computer screen. 2) An application used in previous versions of XProtect Professional for recording and displaying video. The Monitor application has been discontinued.

MPEG

Compression standards and file formats for digital video developed by the Moving Pictures Experts Group. MPEG standards use so-called lossy compression as they store only the changes between frames, removing often considerable amounts of redundant information. Keyframes stored at specified intervals record the entire view of the camera, whereas the frames that follow record only pixels that change. This helps greatly reduce the size of MPEG files.

N

NTLM

In a Windows network, NT LAN Manager is a network authentication protocol.

P

Panomorph

A type of lens that allows the creation and viewing of 360-degree images.

P-frame

Predictive frame—the MPEG standard for digital video compression uses P-frames together with I-frames. An I-frame, also known as a keyframe, is a single frame stored at specified intervals. The I-frame records the entire view of the camera, whereas the frames that follow (the P-frames) record only the pixels that change. This helps greatly reduce the size of MPEG files.

PIN

Personal identification number (or personal identity number)—number used to identify and authenticate users.

Ping

A computer network administration utility used to determine whether an IP address is available, by sending a small amount of data to see if it responds. The word ping was chosen because it mirrors the sound of a sonar. You send the ping command using a Windows command prompt.

Polling

Regularly checking the state of something, for example, whether input has been received on a particular input port of a device. The defined interval between such state checks is often called a polling frequency.

Port

Logical endpoint for data traffic. Networks use different ports for different types of data traffic. Therefore it is sometimes, but not always, necessary to specify which port to use for particular data communication. Most ports are used automatically based on the types of data included in the communication. On TCP/IP networks, port numbers range from 0 to 65536, but only ports 0 to 1024 are reserved for particular purposes. For example, port 80 is used for HTTP traffic, which is used when viewing web pages.

POS

(Also PoS) Point of sale; the physical place where a sale is made, for example, at the cash register.

Post-recording

The ability to store recordings from periods following motion and/or specified events. Based on incoming video being buffered on the XProtect Professional server in case it is going to be needed for a motion- or event-triggered recording. Using post-recording can

be highly advantageous: if, for example, you have defined that video should be recorded while a gate is open, being able to see what happens immediately after the gate is closed may also be important.

Pre-alarm

Pre-alarm images is a feature available for selected cameras only; it enables the sending of images from immediately before an event took place from the camera to XProtect Professional via e-mail.

Pre-buffer

See the description of Pre-recording.

Pre-recording

The ability to store recordings from periods preceding detected motion and/or specified events. Based on incoming video being buffered on the XProtect Professional server in case it is going to be needed for a motion- or event-triggered recording. Using pre-recording can be highly advantageous: if, for example, you have defined that video should be recorded when a door is opened, being able to see what happened immediately prior to the door being opened may also be important.

Privacy masking

The ability to define if and how selected areas of a camera's view should be masked before distribution. For example, if an XProtect Professional camera films a street, you can mask certain areas of a building (for example, windows and doors) with privacy masking in order to protect residents' privacy.

PTZ

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

PUK

Personal Unblocking Key or PIN Unlock Key—number used as an extra security measure for SIM cards.

R

Recording

On IP video surveillance systems, recording means **saving video and, if applicable, audio from a camera in the cameraâ€™s database on the surveillance system**. In many IP surveillance systems, all the video/audio received from cameras is not necessarily saved. Saving of video and audio in a cameraâ€™s database is in many cases started only when there is a reason to do so, for example, when motion is detected, when an event occurs, or when a specific period of time begins. Recording is then stopped after a specified amount of time, for example, when motion is no longer detected, when an event occurs, or when a time period ends. The term **recording** originates from the analog video era, when images were taped only when the record button was pressed.

Recording Server service

Windows service (without any user interface) used by XProtect Professional for recording and displaying video. Video is only transferred to the surveillance system while the Recording Server service is running.

Restore point

Restore points allow you to return to a previous configuration state. When a configuration change is applied in XProtect Professional, a restore point is created. If something goes wrong in your configuration, you can browse through restore points, and return to a suitable one.

S

SCS

A file extension (.scs) for a script type targeted at controlling clients.

SDK

Software Development Kit—programming package enabling software developers to

create applications for use with a specific platform.

SIM

Subscriber identity module—circuit stored on a small card inserted into a mobile phone or computer, or other mobile device. The SIM card is used to identify and authenticate the user.

SLC

Software license code—product registration code required for using the XProtect Professional software. If you do not have system administration responsibilities, you do not have to deal with SLCs. System administrators use SLCs when installing and registering the software.

SMS

Short Message Service or Systems Management Server; 1) Short Message Service, a system for sending text messages to mobile phones. 2) 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.

SMTP

Simple Mail Transfer Protocol—standard for sending e-mail messages between mail servers.

Subnet

A part of a network. Dividing a network into subnets can be advantageous for management and security reasons, and may in some cases also help improve performance. On TCP/IP-based networks, a subnet is basically a part of a network on which all devices share the same prefix in their IP addresses, for example 123.123.123.xxx, where the first three numbers (123.123.123) are the shared prefix. Network administrators use subnet masks to divide networks into subnets.

T

TCP

Transmission Control Protocol—protocol (or 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—combination of protocols (or standards) used when connecting computers and other devices on networks, including the internet.

Telnet

Terminal emulation program used on TCP/IP networks. With Telnet, you can connect to a server from a computer on the network and execute commands through Telnet as if you were entering them directly on the server. Windows includes a client for use with Telnet.

Transact

An add-on to XProtect Professional. XProtect Transact can help you prevent loss and shrinkage through video evidence combined with time-linked POS or ATM transaction data.

U

UDP

User Datagram Protocol—connectionless protocol for sending data packets across networks. Primarily used for broadcasting messages. UDP is a fairly simple protocol, with less error recovery features than, for example, the TCP protocol.

UPS

A UPS (Uninterruptible Power Supply) works as a battery-driven secondary power source, providing the necessary power for saving open files and safely powering down your system in the event of power irregularities. UPSs vary in sophistication, but many UPSs include software for automatically saving open files, for alerting system administrators, etc.

URL

Uniform Resource Locator; an address of a resource on the World Wide Web. The first part of a URL specifies which protocol (or 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. For example, www.milestonesys.com.

V

VCA

Video content analysis (VCA) is a system that detects various types of previously specified behavior, both of humans and vehicles. A VCA-based system provides third-party video content analysis, spanning from face recognition, over advanced motion detection, to complex behavioral analysis. VCA systems and their output can seamlessly be integrated with the **Alarms** feature and used for, for example, triggering alarms. Here, the events resulting from VCA systems are called analytics events.

Third-party VCA tools are developed by independent partners delivering solutions based on an a Milestone open platform. These solutions can impact performance on XProtect Professional.

Video encoder

A device, typically a standalone device, that can stream video from a number of connected client cameras. Video encoders contain image digitizers, making it possible to connect analog cameras to a network.

Video server

Another name for a video encoder.

View

In XProtect Professional, a collection of video from one or more cameras, presented together in the Smart Client. A view may include other content, such as HTML pages and static images, in addition to video from cameras.

VMD

Video motion detection; way of defining activity in a scene by analyzing image data and the differences in a series of images.

W

Wizard

A utility to help perform a particular task quickly, while also ensuring coverage of all relevant parameters. For example, the **Adjust Motion Detection** wizard quickly helps you configure motion detection on each of XProtect Professional 's cameras without the risk of forgetting to set any key parameters.

X

XProtect Smart Client

An advanced client application for letting remote users access XProtect Professional in order to view live images, play back recorded images, activate output, print and export evidence, and so on (access to features depend on individual user rights). Some of the features include live and playback video, digital zoom, and timeline browsing. The Smart Client should always be downloaded from XProtect Professional and installed locally on remote users' computers.

Index

W

X

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.