

**Milestone Systems**

XProtect® Essential 2.1

## Administrator's Manual



The Open Platform Company



# Contents

---

<b>INTRODUCTION.....</b>	<b>9</b>
<b>XPROTECT ESSENTIAL OVERVIEW.....</b>	<b>9</b>
<b>CLIENTS.....</b>	<b>11</b>
XProtect Smart Client .....	11
XProtect Mobile client.....	14
XProtect Web Client .....	14
<b>RECORDING SERVER MANAGER .....</b>	<b>15</b>
<b>DOWNLOAD MANAGER.....</b>	<b>16</b>
<b>UPDATES .....</b>	<b>18</b>
<b>BEFORE YOU START .....</b>	<b>19</b>
<b>MINIMUM SYSTEM REQUIREMENTS.....</b>	<b>19</b>
<b>ADMINISTRATOR RIGHTS .....</b>	<b>20</b>
<b>IMPORTANT PORT NUMBERS .....</b>	<b>20</b>
<b>VIRUS SCANNING INFORMATION .....</b>	<b>21</b>
<b>TIME SERVER RECOMMENDED .....</b>	<b>21</b>
<b>INSTALL AND UPGRADE .....</b>	<b>22</b>
<b>ABOUT INSTALLING SURVEILLANCE SERVER SOFTWARE OR XPROTECT SMART CLIENT SILENTLY.....</b>	<b>22</b>
<b>INSTALL YOUR SURVEILLANCE SERVER SOFTWARE .....</b>	<b>22</b>
<b>INSTALL SILENTLY.....</b>	<b>22</b>
<b>UPGRADE.....</b>	<b>23</b>
About upgrading .....	23
Upgrade from a previous version.....	24



Remove the current version.....	25
VIDEO DEVICE DRIVERS .....	25
REMOVAL.....	25
<b>GETTING STARTED .....</b>	<b>26</b>
GET YOUR SYSTEM UP AND RUNNING.....	26
USE THE BUILT-IN HELP SYSTEM.....	27
<b>LICENSES.....</b>	<b>29</b>
ABOUT LICENSES.....	29
VIEWING YOUR LICENSE INFORMATION.....	30
ABOUT REPLACING CAMERAS .....	31
ABOUT ACTIVATING LICENSES.....	31
About activating licenses after grace period .....	32
Register SLC.....	32
Activate License - Online .....	32
Activate License - Offline .....	33
Change SLC .....	34
<b>APPLICATION SETTINGS .....</b>	<b>35</b>
ABOUT PRIVACY OPTIONS.....	35
DISABLE INFORMATION COLLECTION .....	36
CHANGE/RESTORE MANAGEMENT APPLICATION BEHAVIOR.....	36
CHANGE LANGUAGE .....	36
EVENT SERVER SETTINGS .....	36
<b>WIZARDS .....</b>	<b>38</b>
THE ADD HARDWARE DEVICES WIZARD.....	38
Express .....	38



Advanced .....	40
Manual .....	42
Import from CSV file.....	44
<b>THE CONFIGURE VIDEO AND RECORDING WIZARD .....</b>	<b>48</b>
Video settings and preview .....	48
Online schedule.....	49
Configure Video & Recording Wizard: Live & Recording Settings Motion-JPEG Cameras .....	49
Configure Video & Recording Wizard: Live & Recording Settings MPEG Cameras ...	51
Drive Selection .....	53
Recording and archiving settings .....	54
<b>ADJUST MOTION DETECTION WIZARD .....</b>	<b>56</b>
Exclude regions.....	56
Motion Detection .....	56
<b>CONFIGURE USER ACCESS WIZARD .....</b>	<b>58</b>
Server access settings .....	58
Basic & Windows Users .....	58
Configure User Access wizard: access summary .....	59
<b>ADVANCED CONFIGURATION.....</b>	<b>60</b>
<b>HARDWARE DEVICES.....</b>	<b>60</b>
About hardware devices.....	60
About recording audio.....	60
About the Replace Hardware Device wizard .....	60
About dedicated input/output devices.....	62
Configure hardware devices .....	63
Delete hardware devices .....	63
Replace hardware devices .....	63
Show or hide microphone .....	64
Hardware properties .....	64



<b>CAMERAS AND STORAGE INFORMATION .....</b>	<b>66</b>
About video and recording configuration .....	66
About database resizing.....	66
About motion detection settings .....	67
About motion detection and PTZ cameras .....	67
Configure camera-specific schedules .....	67
Configure when cameras should do what .....	69
Configure motion detection .....	69
Disable or delete cameras .....	70
Move PTZ type 1 and 3 to required positions .....	70
Recording and storage properties .....	71
Camera properties.....	83
<b>MICROPHONES .....</b>	<b>98</b>
About microphones .....	98
Configure microphones.....	99
Show or hide microphone .....	99
Microphone properties .....	99
<b>EVENTS AND OUTPUT .....</b>	<b>100</b>
About input and output.....	100
About events and output.....	100
Overview of events and output.....	100
Add a hardware input event .....	101
Add a hardware output .....	102
Add a manual event .....	102
Add a timer event .....	103
Configure hardware output on event .....	103
Configure general event handling .....	104
General event properties.....	104
Events and output properties .....	105
<b>SCHEDULING AND ARCHIVING .....</b>	<b>107</b>



About scheduling .....	107
About archiving .....	108
General scheduling properties .....	113
Camera-specific scheduling properties .....	116
<b>LOGS .....</b>	<b>117</b>
About logs .....	117
Configure system, event and audit logging .....	119
Log properties .....	120
<b>E-MAIL .....</b>	<b>121</b>
About e-mail .....	121
Configure e-mail notifications .....	121
E-mail properties .....	122
<b>SERVER ACCESS .....</b>	<b>123</b>
About server access .....	123
About registered services .....	124
Configure server access .....	124
Server access properties .....	124
<b>USERS .....</b>	<b>126</b>
Overview of users and groups .....	126
User properties .....	126
<b>SERVICES .....</b>	<b>128</b>
About services .....	128
<b>SERVERS .....</b>	<b>129</b>
Mobile Server .....	129
Mobile Server Manager .....	135
<b>ALARMS .....</b>	<b>137</b>
About alarms .....	137
Add a time profile (for Alarms) .....	138
Add an alarm .....	139



Configure analytics events in alarms.....	139
Alarms properties.....	139
<b>MIP PLUG-INS .....</b>	<b>143</b>
About MIP plug-ins.....	143
<b>BACKUP AND RESTORE CONFIGURATION .....</b>	<b>144</b>
ABOUT BACKUP AND RESTORE OF CONFIGURATIONS .....	144
BACK UP SYSTEM CONFIGURATION.....	144
RESTORE SYSTEM CONFIGURATION .....	145
EXPORT AND IMPORT MANAGEMENT APPLICATION CONFIGURATION .....	145
IMPORT CHANGES TO CONFIGURATION.....	146
RESTORE SYSTEM CONFIGURATION FROM A RESTORE POINT .....	147
<b>COMMON TASKS .....</b>	<b>148</b>
ABOUT HANDLING DAYLIGHT SAVING TIME .....	148
IMPROVE STABILITY WITH 3 GB VIRTUAL MEMORY .....	148
ABOUT PROTECTING RECORDING DATABASES FROM CORRUPTION .....	150
ABOUT VIEWING VERSION AND LICENSE INFORMATION .....	151
APPLY/SAVE CONFIGURATION CHANGES .....	151
CONFIGURE DEFAULT FILE PATHS .....	151
MONITOR STORAGE SPACE USAGE .....	152
VIEW VIDEO FROM CAMERAS IN MANAGEMENT APPLICATION.....	152
<b>GLOSSARY OF TERMS.....</b>	<b>154</b>
<b>INDEX.....</b>	<b>161</b>



# Copyright, trademarks and disclaimer

---

## Copyright

© 2012 Milestone Systems A/S.

## Trademarks

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

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

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

## Disclaimer

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

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

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

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

This product may make use of third party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file **3rd\_party\_software\_terms\_and\_conditions.txt** located in your Milestone surveillance system installation folder.





# Introduction

## ***XProtect Essential overview***

XProtect Essential is affordable video management software for small businesses, especially retail, that want to video enable their surveillance installation with support for up to 26 cameras. Due to the open platform environment, businesses can seamlessly integrate solutions, building management systems and third-party applications directly into XProtect Essential.

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

Name	Description
<b>Management Application</b>	The main application used by surveillance system administrators for configuring the XProtect Essential surveillance system server, upon installation or whenever configuration adjustments are required, for example when adding new cameras or users to the system.
<b>Recording Server service</b>	A vital part of the surveillance system. Video streams are only transferred to XProtect Essential while the Recording Server service is running. The Recording Server service is automatically installed and runs in the background on the XProtect Essential surveillance system server. You can manage the service through the Management Application.
<b>Event Server</b>	Will be used for handling Milestone plug-in related data. The event server is automatically installed on, and runs in the background of, your XProtect Essential surveillance system server.
<b>Microsoft® SQL Server Express Database</b>	Will in future be used for storing Milestone plug-in related data. The SQL Server Express database is a lightweight, yet powerful, version of a full SQL database which is automatically installed on, and runs in the background of, your XProtect Essential surveillance system server.
<b>Image Server service</b>	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 Essential surveillance system server. You can manage the service through the Management Application.
<b>Download Manager</b>	Manage which XProtect Essential-related features your organization's users will be able to access from a targeted welcome page on the surveillance system server.
<b>XProtect® Smart Client</b>	<p>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.</p> <p>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 Essential surveillance system.</p>
<b>XProtect® Mobile client</b>	A free application designed by Milestone that allows you to view video from your XProtect Essential 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.



Name	Description
<b>XProtect® Web Client</b>	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 11)
- **Install from a DVD** (on page 12)

#### Install from the surveillance server

1. Verify that your computer meets the XProtect Smart Client's minimum system requirements.
2. Open an Internet Explorer browser (version 6.0 or later) and connect to the surveillance system server using the URL or IP address specified by your system administrator.
3. On the Welcome page, click **Language** and select your required language.

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

4. If you receive a security warning (**Do you want to run or save this file?**, **Do you want to run this software?** or similar), accept this (by clicking **Run** or similar—the exact name depends on your browser version).
5. The XProtect Smart Client **setup** wizard starts. In the wizard, follow the installation instructions.



The wizard suggests an installation path. Normally, you can use the suggested installation path. However, if you have previously used add-on products, such as XProtect Analytics or XProtect Transact, this path might not be valid anymore (see "Install from a DVD" on page 12).

## Install from a DVD

1. Verify that your computer meets the XProtect Smart Client's minimum system requirements.
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 Essential plug-in for XProtect Analytics can only run on a 32-bit version of the XProtect Essential. The plug-in cannot run on a 64-bit installation. By default, in XProtect Essential versions **earlier than 4.0a**, the XProtect Essential is installed in:

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

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

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

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

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

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

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

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

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

## 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 Essential installation:

```
> MilestoneXProtectXProtect EssentialInstaller.exe --quiet
```

This will perform a quiet installation of the XProtect Smart Client/XProtect Essential 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 Essential:

```
> MilestoneXProtectXProtect EssentialInstaller.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 Essential:

```
> MilestoneXProtectXProtect EssentialInstaller.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 Essential, you must add a Mobile server (see "About Mobile server" on page 129) to establish the connection between the XProtect Mobile client and XProtect Essential.

### **Install XProtect Mobile client**

1. Access Google Play or App Store<sup>SM</sup> 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](http://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 Essential, you must add a Mobile server (see "About Mobile server" on page 129) to establish the connection between the XProtect Web Client and XProtect Essential.

### **Access XProtect Web Client**

If you have an XProtect Mobile server (see "About Mobile server" on page 129) 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 135).
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 Essential 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 116)).
  - The Recording Server service has been stopped.
- **Red** indicates that the server or camera is not running. This may be 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
<b>Resolution</b>	The resolution of the camera.
<b>FPS</b>	The number of frames per second (frame rate) currently used by the camera. The number updates each time the camera has received 50 frames.
<b>Resolution</b>	The resolution of the camera.
<b>Frame count</b>	The number of frames received from the camera since the Recording Server service was last started.
<b>Received KB</b>	The number of kilobytes sent the by camera since the Recording Server service was last started.
<b>Offline</b>	Indicates the number of times the camera has been offline due to an error.

## Download Manager

The Download Manager lets you manage which XProtect Essential-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 Essential 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://\[surveillance server IP address or hostname\]](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://\[surveillance server IP address or hostname\]:\[port number\]](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 Essential, 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 Essential 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 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](http://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	<ul style="list-style-type: none"><li>• Microsoft® Windows® XP Professional (32-bit or 64-bit*)</li><li>• Windows Server 2003 (32-bit or 64-bit*)</li><li>• Windows Server 2008 R1/R2 (32-bit or 64-bit*)</li><li>• Windows Vista™ Business (32-bit or 64-bit*)</li><li>• Windows Vista Enterprise (32-bit or 64-bit*)</li><li>• Windows Vista Ultimate (32-bit or 64-bit*)</li><li>• Windows 7 Professional (32-bit or 64-bit*)</li><li>• Windows 7 Enterprise (32-bit or 64-bit*)</li><li>• Windows 7 Ultimate (32-bit or 64-bit*).</li></ul>
CPU	Intel® Pentium® 4, 2.4 GHz or higher (Core™ 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	<ul style="list-style-type: none"><li>• Microsoft .NET 4.0 Framework.</li><li>• DirectX 9.0 or newer.</li><li>• Windows Help (WinHlp32.exe)</li></ul> <p>All can be downloaded from <a href="http://www.microsoft.com/downloads/">http://www.microsoft.com/downloads/</a>.</p>

#### XProtect Smart Client



Name	Description
<b>Operating system</b>	<ul style="list-style-type: none"> <li>• Microsoft® Windows® XP Professional (32-bit or 64-bit*)</li> <li>• Windows Server 2003 (32-bit or 64-bit*)</li> <li>• Windows Server 2008 R1/R2 (32-bit or 64-bit*)</li> <li>• Windows Vista™ Business (32-bit or 64-bit*)</li> <li>• Windows Vista Enterprise (32-bit or 64-bit*)</li> <li>• Windows Vista Ultimate (32-bit or 64-bit*)</li> <li>• Windows 7 Professional (32-bit or 64-bit*)</li> <li>• Windows 7 Enterprise (32-bit or 64-bit*)</li> <li>• Windows 7 Ultimate (32-bit or 64-bit*).</li> </ul>
<b>CPU</b>	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).
<b>RAM</b>	Minimum 1 GB (higher RAM recommended for Smart Clients running high number of cameras and multiple views and displays).
<b>Network</b>	Ethernet (100 Mbit or higher recommended).
<b>Graphics adapter</b>	AGP or PCI-Express, minimum 1024 x 768 (1280 x 1024 recommended), 16-bit colors.
<b>Hard disk space</b>	Minimum 1 GB free hard disk space available.
<b>Software</b>	<ul style="list-style-type: none"> <li>• Microsoft .NET 4.0 Framework.</li> <li>• DirectX 9.0 or newer.</li> </ul>

## Administrator rights

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

## Important port numbers

XProtect Essential 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 Essential:

Name	Description
<b>Port 20 and 21 (inbound and outbound)</b>	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.



Name	Description
<b>Port 25 (inbound and outbound)</b>	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.
<b>Port 80 (inbound and outbound)</b>	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.
<b>Port 554 (inbound and outbound)</b>	Used for RSTP traffic in connection with H.264 video streaming.
<b>Port 1024 (outbound only)</b>	Used for HTTP traffic between cameras and the surveillance server.
<b>Port 1234 (inbound and outbound)</b>	Used for event handling.
<b>Port 1237 (inbound and outbound))</b>	Used for communication with the XProtect Central add-on product (if used by your organization).
<b>Port 8081 and 8082</b>	Used for communication with the Mobile service.

Your organization may also have selected to use any other port numbers, for example if you have changed the server access (on page 124) 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 Essential server as well as on any archiving destinations.

## ***Time server recommended***

All images are time-stamped by XProtect Essential upon reception, but since cameras are separate units which may have separate timing devices, power supplies, etc., camera time and XProtect Essential 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](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 Essential 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 Essential 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 24) 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 Essential 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 Essential installation. The Microsoft hotfix can be downloaded here:

<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 Essential installation.

You can now begin to configure your XProtect Essential through its Management Application. See more under Get your system up and running (on page 26).

### *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 Essential installation:

```
> MilestoneXProtectXProtect EssentialInstaller.exe --quiet
```

This will perform a quiet installation of the XProtect Smart Client/XProtect Essential 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 Essential:

```
> MilestoneXProtectXProtect EssentialInstaller.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 Essential:

```
> MilestoneXProtectXProtect EssentialInstaller.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](http://www.milestonesys.com).

Example: If you upgrade from XProtect Go to XProtect Essential, 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 Essential 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 Essential system configuration from one XProtect Essential version to another. The following information applies if you upgrade from one XProtect Essential version to another and if you upgrade to XProtect Essential from a streamlined product in the XProtect product range.

### *Back up your current configuration*

When you install the new version of XProtect Essential, 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 Basis + or earlier, you must back up your configuration before you upgrade.

The following describes backing up XProtect Basis + or earlier. If you need information about how to back up configuration for XProtect Essential2.0 or newer, see Back up system configuration (on page 144).

1. Create a folder called **Backup** on a network drive, or on removable media.
2. On the XProtect Essential server, open **My Computer**, and navigate to the XProtect Essential 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 Essential 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 Essential before you install the new version. The old version is removed when you install the new version.

## **Remove the current version**

You do not need to manually remove the old version of XProtect Essential before you install the new version. The old version is removed when you install the new version.

## ***Video device drivers***

Video device drivers are installed automatically during the initial installation of your XProtect Essential 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 Essential 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 44) 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 Essential 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 Essential 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 Essential configuration files will remain on the server. This allows you to reuse your configuration if you install XProtect Essential 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 Essential 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 (see "Overview of events and output" on page 100) 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 Essential, 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 Essential.

### **Register your XProtect Essential software**



This step may not be required; your XProtect Essential 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 31**).

### **Install XProtect Essential**



See Install surveillance server software (**see "Install your surveillance server software" on page 22**). If you are upgrading an existing version of XProtect Essential, see Upgrade from a previous version (**on page 24**).

### **Open the Management Application**



See Access the Management Application.

### **Add hardware devices in XProtect Essential**



XProtect Essential 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 38).



- ☐ **Configure cameras in XProtect Essential**

You can specify a wide variety of settings for each camera connected to your XProtect Essential system. Settings include video format, resolution, motion detection sensitivity, where to store and archive (see "About archiving" on page 108) recordings, any PTZ (Pan/Tilt/Zoom) preset positions, association with microphones etc. See About video and recording configuration (on page 66).
- ☐ **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 Essential. 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 (see "Overview of events and output" on page 100).
- ☐ **Configure scheduling**

When do you want to archive? Do you want some cameras to transfer video to XProtect Essential 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 and Configure camera-specific schedules.
- ☐ **Configure clients' access to XProtect Essential**

A number of different client applications (see About clients) is included with XProtect Essential. You can specify whether you want clients to access the XProtect Essential server from the internet, how many clients you want to be able to connect simultaneously, etc. (see Configure server access (on page 124)).
- ☐ **Configure users**

Now specify who should be able to access your XProtect Essential 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 58), Add basic users, Add user groups and Configure user and group rights.

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 video sharing feature or similar.

Note that the behavior of the Management Application can be customized (see "Change/restore Management Application behavior" on page 36). Descriptions here are, however, always based on the Management Application's default behavior.

## ***Use the built-in help system***

To use the XProtect Essential 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 Essential itself. The help system is context-sensitive. This means that when you press F1 for help while you work in a particular XProtect Essential 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 Essential, 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, inputs, and outputs.

When you have installed the various XProtect Essential 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 31) 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 Essential system.

To get additional licenses for XProtect Essential, contact your vendor, or visit [www.milestonesys.com](http://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 required 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 Essential 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 60) to map all relevant databases of cameras, microphones, inputs, outputs, etc. Remember to activate the license once you are finished.

### Overview of license information

You get an excellent overview of your XProtect Essential 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
<b>Hardware Device Name</b>	Hardware devices (typically cameras but could also be dedicated input/output boxes).
<b>License</b>	Licensing status of your hardware devices. Can be either <b>Licensed</b> , <b>[number of] day(s) grace</b> , <b>Trial</b> , or <b>Expired</b> .
<b>Video Channels</b>	Number of available video channels on your hardware devices.
<b>Licensed Channels</b>	Number of video channels on each of your hardware devices for which you have a license.
<b>Microphone Channels</b>	Number of available microphone channels on your hardware devices.
<b>Address</b>	http addresses of your hardware devices.
<b>WWW</b>	Links to http addresses of your hardware devices.
<b>Port</b>	Port used by your hardware devices.
<b>Device Driver</b>	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 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 Essential system.

To get additional licenses for XProtect Essential, contact your vendor, or visit [www.milestonesys.com](http://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.

## Viewing your license information

You get an excellent overview of your XProtect Essential 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
<b>Hardware Device Name</b>	Hardware devices (typically cameras but could also be dedicated input/output boxes).



Name	Description
<b>License</b>	Licensing status of your hardware devices. Can be either <b>Licensed</b> , <b>[number of] day(s) grace</b> , <b>Trial</b> , or <b>Expired</b> .
<b>Video Channels</b>	Number of available video channels on your hardware devices.
<b>Licensed Channels</b>	Number of video channels on each of your hardware devices for which you have a license.
<b>Microphone Channels</b>	Number of available microphone channels on your hardware devices.
<b>Address</b>	http addresses of your hardware devices.
<b>WWW</b>	Links to http addresses of your hardware devices.
<b>Port</b>	Port used by your hardware devices.
<b>Device Driver</b>	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 replacing cameras

You can replace a camera that is licensed in XProtect Essential 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 60) to map all relevant databases of cameras, microphones, inputs, outputs, etc. Remember to activate the license once you are finished.

## About activating licenses

When you purchase XProtect Essential, 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 Essential 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](http://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 38) to your XProtect Essential 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](mailto: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](mailto: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 38) to your XProtect Essential 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 Essential). 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](http://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**.



# Application settings

---

## About privacy options

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

- If you **declined**, **no software** contributing statistical information is included in your XProtect Essential installation.
- If you **accepted**, a cookie issuing a Global Unique Identifier (GUID) is included as part of your XProtect Essential installation. As a result, XProtect Essential anonymously collects relevant information about your installation and operation of XProtect Essential 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 Essential?

No personal information about the equipment (PC) XProtect Essential 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 Essential version information
- Information about the number, and type of hardware devices (cameras) used with XProtect Essential
- Information on which XProtect Essential features are used, and how often they are used
- Information about which XProtect Essential menus and buttons are activated, and how often they are used
- Execution time for specific operations in your XProtect Essential installation
- Error reports and exceptions generated by your XProtect Essential installation.

### When is information collected from XProtect Essential?

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 Essential 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 Essential 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 Essential 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 26 cameras at a time on a single XProtect Essential server. If you add more than 26, 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.

## ***Event Server settings***

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



Name	Description
<b>Keep closed alarms for</b>	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.
<b>Keep all other alarms for</b>	<p>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.</p> <p><b>IMPORTANT:</b> 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.</p>
<b>Keep logs for</b>	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).
<b>Log server communication</b>	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 Essential system through the **Add Hardware Devices...** wizard. If microphones are attached to a hardware device, they are automatically added as well.

You can use up to 26 cameras per XProtect Essential 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
<b>Express (recommended)</b>	Scans your network for relevant hardware devices, and helps you quickly add them to your system.  To use the Express method, your XProtect Essential 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 38).
<b>Advanced</b>	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 40).
<b>Manual</b>	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 42).
<b>Import from CSV file</b>	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 44).

### 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 Essential server itself is located.

To use the Express method, **your XProtect Essential 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 Essential server and the cameras. If you know that routers are used on your network, use the advanced (on page 40) or manual (on page 42) method instead.



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

- Hardware detection and verification (on page 39)
- Overview and names (on page 40)

**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 Essential 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 Essential 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 Essential 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 Essential 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 Essential 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 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 Essential. If required, you can disable individual cameras or microphones, to prevent them from communicating with XProtect Essential.
- 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
<b>Device type + number</b>	The default name format. Example: Camera 1.
<b>Custom text - Device type + number</b>	Names will consist of a text of your choice (specified in the <b>Custom text</b> field) followed by a dash, type information and a number. Example: Airport Security - Camera 1
<b>Address - Device type + number</b>	Names will consist of the hardware device address followed by a dash, type information and a number. Example: 10.10.123.73 - Camera 1
<b>Custom text - Address - Device type + number</b>	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
<b>Hardware model - Device type + number</b>	Names will consist of hardware device model information followed by a dash, type information and a number. Example: Axis P1311 - Camera 1
<b>Hardware model - Custom text - Device type + number</b>	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
<b>Hardware model - Address - Device type + number</b>	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 41)
- Detected and verified hardware devices (on page 42)
- Overview and names (on page 40)

## ***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 Essential server is located. To add additional ranges, or edit existing ones, click the **Add** or **Edit** button as required, then specify:

Name	Description
<b>Start address</b>	Specify the first IP address in the required range.
<b>End address</b>	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.
<b>Use TCP port scanning</b>	If scanning for hardware devices which support TCP/HTTP—most devices do—keep the check box selected.
<b>Perform scanning on port number(s)</b>	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 Essential 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 Essential will need that for each hardware device.



<b>User name</b>	<p>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 &lt;default&gt; (do not type a manufacturer's default user name as this can be a source of error; trust that XProtect Essential 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.</p> <p><b>Tip:</b> User names you enter will subsequently be added to the list, so you can easily select them later.</p>
<b>Password</b>	<p>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.</p> <p><b>Tip:</b> 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.</p>

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 Essential 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 43)
- Overview and names (on page 40)

## 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
<b>Use</b>	Indicates that you want to include the hardware device in the scan. To begin with, leave the box cleared. Provided XProtect Essential can find a suitable driver for the hardware device, the <b>Use</b> box will automatically be selected later.
<b>Address</b>	IP address or host name of the hardware device.
<b>Port</b>	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.
<b>User name</b>	<p>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 &lt;default&gt; (do not type a manufacturer's default user name as this can be a source of error; trust that XProtect Essential 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.</p> <p><b>Tip:</b> User names you enter will subsequently be added to the list, so you can easily select them later.</p>
<b>Password</b>	<p>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.</p> <p><b>Tip:</b> 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.</p>
<b>Hardware Driver</b>	Driver to use with the hardware device. If the Auto-detect option is selected, the hardware the XProtect Essential can find the relevant driver automatically.
<b>Verified</b>	<p>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.</p> <p><b>Tip:</b> To save time, when using the <b>Auto-detect</b> feature, you can enter information about other devices while the auto-detection is in progress.</p>



## 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 45) from a file; a highly effective method if setting up several similar systems.

First select whether cameras and the XProtect Essential 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 44) for detailed descriptions of all mandatory and optional parameters.

```
HardwareAddress;HardwarePort;HardwarePassword;CameraName1;CameraName2;Camera
Name3;CameraName4
192.168.200.220;80;TOP53cr3T;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;ttooppsscret;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
<b>HardwareOldMacAddress</b>	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 (:).
<b>HardwareNewMacAddress</b>	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 (:).
<b>HardwareAddress</b>	IP address of the hardware device.
<b>HardwareUsername</b>	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 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.
<b>HardwarePassword</b>	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 "leave 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.
<b>HardwareDeviceName</b>	Name of the hardware device. Name must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ?   [ ]
<b>HardwareDriverID</b>	If cameras and server are offline—specify a <b>HardwareDriverID</b> for each hardware device you want to add. Example: <b>ACTi ACD-2100 105</b> indicates that you should use <b>105</b> as the ID if adding an ACTi ACD-2100 hardware device.
<b>CameraName[number]</b>	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: < > & ' " \ / : * ?   [ ]
<b>CameraShortcut[number]</b>	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.



Name	Description
<b>GenerateNewCameraGuid</b> [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 145) as your template, since all GUIDs are removed from cloned configurations. If specified as, for example, <b>GenerateNewCameraGuid1</b> , information relates to a specific camera, otherwise to all cameras attached to the hardware device. Any character means "yes, generate a new GUID."•
<b>PreBufferLength</b> [optional number]	Required length (in seconds) of pre-recording. If specified as, for example, <b>PreBufferLength1</b> , information relates to a specific camera, otherwise to all cameras attached to the hardware device.
<b>PostBufferLength</b> [optional number]	Required length (in seconds) of post-recording. If specified as, for example, <b>PostBufferLength1</b> , information relates to a specific camera, otherwise to all cameras attached to the hardware device.
<b>RecordingPath</b> [optional number]	Path to the folder in which a camera's database should be stored. If specified as, for example, <b>RecordingPath1</b> , information relates to a specific camera, otherwise to all cameras attached to the hardware device.
<b>ArchivePath</b> [optional number]	Path to the folder in which the camera's archived (see "About archiving" on page 108) 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 73). If specified as, for example, <b>ArchivePath1</b> , information relates to a specific camera, otherwise to all cameras attached to the hardware device.
<b>OldRecordingsNewPath</b> [optional number]	Lets you specify what to do with old recordings in case <b>RecordingPath</b> or <b>ArchivePath</b> have been changed. If this parameter is not specified, default behavior is <b>Leave</b> (see the following). If specified as, for example, <b>OldRecordingsNewPath1</b> , information relates to a specific camera, otherwise to all cameras attached to the hardware device. Valid options are: <b>Delete</b> (deletes old recordings), <b>Leave</b> (leaves old recordings for offline investigation but unavailable for online system), or <b>Move</b> (moves old recordings to archive).
<b>OldRecordingsNewMac</b> [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 <b>Leave</b> (see the following). If specified as, for example, <b>OldRecordingsNewMac1</b> , information relates to a specific camera, otherwise to all cameras attached to the hardware device. Valid options are: <b>Delete</b> (deletes old recordings), <b>Leave</b> (leaves old recordings for offline investigation but unavailable for online system), or <b>Inherit</b> (renames all old recording folders according to the new MAC address, thus making them available for the online system).
<b>RetentionTime</b> [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, <b>RetentionTime1</b> , information relates to a specific camera, otherwise to all cameras attached to the hardware device.
<b>MjpegLiveFrameRate</b> [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, <b>MjpegLiveFrameRate1</b> , information relates to a specific camera, otherwise to all cameras attached to the hardware device.
<b>MotionSensitivity</b> [optional number]	A value between 0-256; corresponds to using the <b>Sensitivity</b> slider when configuring motion detection settings in the Management Application. If specified as, for example, <b>MotionSensitivity1</b> , information relates to a specific camera, otherwise to all cameras attached to the hardware device.





Name	Description
<b>MjpegRecordingFrameRate</b> [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, <b>MjpegRecordingFrameRate1</b> , information relates to a specific camera, otherwise to all cameras attached to the hardware device.
<b>MotionDetectionThreshold</b> [optional number]	A value between 0-10000; corresponds to using the <b>Motion</b> slider when configuring motion detection settings in the Management Application. If specified as, for example, <b>MotionDetectionThreshold1</b> , information relates to a specific camera, otherwise to all cameras attached to the hardware device.
<b>MotionDetectionInterval</b> [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, <b>MotionDetectionInterval1</b> , information relates to a specific camera, otherwise to all cameras attached to the hardware device.
<b>ServerName</b>	Name with which the XProtect Essential will appear when listed in clients. Name must be unique, and must not contain any of the following special characters: < > & ' " \ / : * ?   [ ]
<b>ServerPort</b>	Port number to use for communication between the XProtect Essential server and clients.
<b>OnlineVerification</b>	If this parameter is used, all online hardware devices found using <b>HardwareOldMacAddress</b> 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 .....	48
Online schedule .....	49
Configure Video & Recording Wizard: Live & Recording Settings Motion-JPEG Cameras .....	49
Configure Video & Recording Wizard: Live & Recording Settings MPEG Cameras .....	51
Drive Selection .....	53
Recording and archiving settings .....	54

## **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 Essential system time may therefore not correspond fully, and this may occasionally lead to confusion. As all frames are time-stamped by XProtect Essential 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 Essential 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 Essential 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 114).

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

## Configure Video & Recording Wizard: Live & 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
<b>Record on</b>	<p>Lets you select under which conditions video from the camera should be recorded:</p> <ul style="list-style-type: none"> <li>• <b>Always:</b> Record whenever the camera is enabled (see "General" on page 83) and scheduled to be online (see "Online period" on page 116) (the latter allows for time-based recording).</li> <li>• <b>Never:</b> 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.</li> <li>• <b>Motion Detection:</b> Select this to record video in which motion (see "Motion detection &amp; exclude regions" on page 92) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.</li> <li>• <b>Event:</b> Select this to record video when an event occurs and until another event occurs. Use of recording on event requires that events (see "Overview of events and output" on page 100) have been defined, and that you select start and stop events.</li> </ul> <p><b>Tip:</b> If you have not yet defined any suitable events, you can quickly do it: Use the <b>Configure events</b> list, located below the other fields.</p> <ul style="list-style-type: none"> <li>• <b>Motion Detection &amp; Event:</b> 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.</li> </ul>
<b>Pre-recording</b>	<p>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.</p> <p><b>How does pre- and post-recording work?</b> XProtect Essential 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 Essential 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.</p>
<b>Seconds [of pre-recording]</b>	<p>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 108) times. That can be problematic since pre-recording does not work well during archiving.</p>
<b>Post-recording</b>	<p>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.</p>



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

## Configure Video & Recording Wizard: Live & 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. 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
<b>Live Frame Rate</b>	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 <b>Live Frame Rate</b> column will be read-only with the value <b>Dual streaming—</b> which cannot be altered.



Name	Description
<b>Record on</b>	<p>Lets you select under which conditions video from the camera should be recorded:</p> <ul style="list-style-type: none"> <li>• <b>Always:</b> Record whenever the camera is enabled (see "General" on page 83) and scheduled to be online (see "Online period" on page 116) (the latter allows for time-based recording).</li> <li>• <b>Never:</b> 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.</li> <li>• <b>Motion Detection:</b> Select this to record video in which motion (see "Motion detection &amp; exclude regions" on page 92) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.</li> <li>• <b>Event:</b> Select this to record video when an event occurs and until another event occurs. Use of recording on event requires that events (see "Overview of events and output" on page 100) have been defined, and that you select start and stop events.</li> </ul> <p><b>Tip:</b> If you have not yet defined any suitable events, you can quickly do it: Use the <b>Configure events</b> list, located below the other fields.</p> <ul style="list-style-type: none"> <li>• <b>Motion Detection &amp; Event:</b> 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.</li> </ul>
<b>Pre-recording</b>	<p>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.</p> <p><b>How does pre- and post-recording work?</b> XProtect Essential 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 Essential 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.</p>
<b>Seconds [of pre-recording]</b>	<p>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 108) times. That can be problematic since pre-recording does not work well during archiving.</p>
<b>Post-recording</b>	<p>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.</p>



Name	Description
<b>Seconds [of post-recording]</b>	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
<b>Apply Template</b>	Select which cameras you want to apply the template for. You then use one of the two <b>Set</b> buttons to actually apply the template. <b>Tip:</b> To select all cameras in the list, click the <b>Select All</b> button.
<b>Select All</b>	Click button to select all cameras in the <b>Apply Template</b> column.
<b>Clear All</b>	Click button to clear all selections in the <b>Apply Template</b> column.
<b>Apply template on selected cameras</b>	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 108).

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

Name	Description
<b>Drive</b>	Letter representing the drive in question, for example C:.
<b>Purpose</b>	<p>Select what you want to use the drive for:</p> <p><b>Not in use:</b> Do not use the drive.</p> <p><b>Recording:</b> Only available if the drive is a local drive on the XProtect Essential server. Network drives cannot be used for recording. Use the drive for storing recordings in the regular database for XProtect Essential.</p> <p><b>Archiving:</b> 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.</p> <p><b>Rec. &amp; Archiving:</b> Only available if the drive is a local drive on the XProtect Essential server. Network drives cannot be used for recording. Use the drive for storing recordings in the regular database for XProtect Essential as well as for archiving.</p>



Name	Description
<b>Recording Path</b>	<p>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 <b>local</b> 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.</p> <p>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.</p> <p><b>Tip:</b> If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.</p>
<b>Archiving Path</b>	<p>Only editable if not using dynamic paths for archiving (see "About archiving" on page 108). Path to the folder in which the camera's archived recordings should be stored. Default is C:\MediaDatabase.</p> <p>To browse for another folder, click the browse icon next to the required cell. You can specify a path to a local 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 Essential 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.</p>
<b>Total Size</b>	Total size of the drive.
<b>Free Space</b>	Amount of unused space left on the drive.
<b>Dynamic path selection for archives</b>	<p>If using this option (highly recommended), you should select a number of different local drives for archiving. If the path containing the XProtect Essential database is on one of the drives you have selected for archiving, XProtect Essential will always try to archive to that drive first. If not, XProtect Essential 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.</p>
<b>Archiving Times</b>	<p>Specify when you want XProtect Essential 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 <b>up</b> and <b>down</b> buttons to increase or decrease values, or simply overwrite the selected value, and then click <b>Add</b>.</p> <p>The more you expect to record, the more often you should archive.</p>

## Recording and archiving settings

Select recording and archiving (see "About archiving" on page 108) paths for each individual camera.

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



Name	Description
<b>Recording Path</b>	<p>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 <b>local</b> drive. You cannot specify a path to a network drive. If you use a network drive, it is not possible to save recordings if the network drive becomes unavailable.</p> <p>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.</p> <p><b>Tip:</b> If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.</p>
<b>Archiving Path</b>	<p>Only editable if not using dynamic paths for archiving (see "About archiving" on page 108). Path to the folder in which the camera's archived recordings should be stored. Default is C:\MediaDatabase.</p> <p>To browse for another folder, click the browse icon next to the required cell. You can specify a path to a local 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 Essential 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.</p>
<b>Retention Time</b>	<p>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.</p> <p>Note that the retention time covers the <b>total</b> amount of time you want to keep recordings for. In earlier XProtect Essential versions, time limits were specified separately for the database and archives.</p>

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
<b>Apply Template</b>	<p>Select which cameras you want to apply the template for. You then use one of the two <b>Set</b> buttons to actually apply the template.</p> <p><b>Tip:</b> To select all cameras in the list, click the <b>Select All</b> button.</p>
<b>Select All</b>	Click button to select all cameras in the <b>Apply Template</b> column.
<b>Clear All</b>	Click button to clear all selections in the <b>Apply Template</b> column.
<b>Apply template on selected cameras</b>	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 the Recording Server service when configuring such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 152).

### Pages in this wizard:

Exclude regions .....	56
Motion Detection.....	56

## 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 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 152).

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 the Recording Server service when configuring such devices for motion detection and PTZ. See also View Video from Cameras in Management Application (on page 152).





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
<b>Sensitivity</b>	<p>Adjust the <b>Sensitivity</b> 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.</p> <p>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.</p>
<b>Motion</b>	<p>Adjust the <b>Motion</b> 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 <b>Level</b> 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.</p> <p>Alternatively, specify a value between 0 and 10000 in the field on the left to control the motion setting.</p> <p>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.</p>
<b>Detection interval</b>	<p>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.</p> <p>Adjusting this setting can help lower the amount of system resources used on motion detection.</p>
<b>Detection resolution</b>	<p>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.</p>



## Configure User Access wizard

The Configure User Access wizard helps you quickly configure clients' access to the XProtect Essential 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 separately. see Configure server access (on page 124). You cannot add users to groups through the wizard.

### Pages in this wizard:

Server access settings .....	58
Basic & Windows Users .....	58
Configure User Access wizard: access summary .....	59

### Server access settings

Name	Description
<b>Server name</b>	Name of the XProtect Essential 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.
<b>Local port</b>	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.
<b>Character encoding/Language</b>	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.
<b>Internet access</b>	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 Essential server.
<b>Internet address</b>	Lets you specify a public IP address or hostname for use when the XProtect Essential server should be available from the internet.
<b>Internet port</b>	Specify a port number for use when the XProtect Essential 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:** Lets you 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:** Lets you 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 **Select 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.



# Advanced configuration

---

## Hardware devices

### About hardware devices

You add cameras and other hardware devices, such as video encoders, to your XProtect Essential system through the **Add Hardware Devices...** wizard (see "The Add Hardware Devices wizard" on page 38). If microphones are attached to a hardware device, they are automatically added as well.

### 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.
- 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 Essential automatically archives (see "About archiving" on page 108) 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.

### 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 61)
- Database action (see "Camera and database action" on page 61)



## New hardware device information

Specify details about the new hardware device:

Name	Description
<b>Address</b>	IP address or host name of the hardware device.
<b>Port</b>	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.
<b>User name</b>	<p>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 &lt;default&gt; (do not type a manufacturer's default user name as this can be a source of error; trust that XProtect Essential 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.</p> <p><b>Tip:</b> User names you enter will subsequently be added to the list, so you can easily select them later.</p>
<b>Password</b>	<p>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.</p> <p><b>Tip:</b> 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.</p>

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 108) will be renamed to reflect the new hardware device's MAC address and video channels. The rights 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 Essential 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 Essential 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 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 Essential (see Add hardware devices (see "The Add Hardware Devices wizard" on page 38)). 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 Essential, and events in XProtect Essential 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 104). 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 38), 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 64), PTZ device (on page 65), and 360° Lens (see "Fisheye" on page 95) 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 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 the Recording Server service.

If deleting a hardware device is not the right thing to do, consider disabling the individual cameras 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 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 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 60), 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





## Show or hide microphone

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

## Hardware properties

### Properties in this window:

Hardware name and video channels .....	64
Network, device type, and license .....	64
PTZ device .....	65

### Hardware name and video channels

When you configure hardware devices (on page 63), specify the following properties:

Name	Description
<b>Hardware name</b>	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: < > & ' " \ / : * ?   [ ]
<b>Video channel # enabled</b>	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 63), specify the following properties:

Name	Description
<b>Address</b>	IP address or host name of the hardware device.
<b>HTTP Port</b>	Port to use for HTTP communication with the hardware device. Default is port 80. To use the default port, select Use default HTTP port.
<b>FTP port</b>	<ul style="list-style-type: none"> <li>Port to use for FTP communication with the hardware device. Default port is port 21. To use the default port, select <b>Use default FTP port</b>.</li> </ul>
<b>User name</b>	Only required when <b>Server requires login</b> is selected. Specify the user name required for using the SMTP server.





Name	Description
<b>User name</b>	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 Essential 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.  <b>Tip:</b> User names you enter will subsequently be added to the list, so you can easily select them later.
<b>Password</b>	Password for the hardware device's administrator account, a.k.a. the root password.
<b>Hardware type</b>	Read-only field displaying the type of video device driver used for communication with the hardware device.
<b>Serial number (MAC address)</b>	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).
<b>License information</b>	The current license status for the hardware.
<b>Replace Hardware Device</b>	Opens a wizard (see "About the Replace Hardware Device wizard" on page 60), 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 63) video encoder hardware devices on which the use of PTZ (Pan/Tilt/Zoom) cameras is possible:

Name	Description
<b>Connected cameras have Pan/tilt/Zoom capabilities</b>	Select check box if any of the cameras attached to the video encoder device is a PTZ camera.
<b>PTZ type on COM#</b>	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
<b>Name</b>	Name of the camera attached to the video channel in question.



Name	Description
<b>Type</b>	Select whether the camera on the selected camera channel is fixed or moveable: <ul style="list-style-type: none"> <li>• <b>Fixed:</b> Camera is a regular camera mounted in a fixed position</li> <li>• <b>Moveable:</b> Camera is a PTZ camera</li> </ul>
<b>Port</b>	Available only if <b>Moveable</b> is selected in the <b>Type</b> column. Select which COM port on the video encoder to use for controlling the PTZ camera.
<b>Port Address</b>	Available only if <b>Moveable</b> is selected in the <b>Type</b> 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 108) 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 73), 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 128) 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 notification.

## About motion detection settings

Motion detection settings are linked to the Recording properties (see "Recording" on page 87) settings for the camera. Motion detection is enabled as default. Disabling it will improve CPU and RAM performance of your XProtect Essential 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
<b>Always</b>	Yes	Yes	Yes	Yes
<b>Never</b>	No	Yes	Yes	No
<b>Built-in Motion Detection</b>	Yes	Yes	Yes	Yes
<b>Built-in Motion Detection &amp; Event or Event only</b>	Yes	Yes	Yes	Yes

### Disabled motion detection

Camera's recording settings	Recordings	Motion-based events	Non-motion based events	Sequences
<b>Always</b>	Yes	No	Yes	No
<b>Never</b>	No	No	Yes	No
<b>Built-in Motion Detection</b>	No	No	Yes	No
<b>Built-in Motion Detection &amp; Event or Event only</b>	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.

## 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 Essential 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 66).

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:

XProtect Essential 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 Essential 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 Essential)
- Cameras should use speedup (that is use a higher than normal frame rate)
- You want to receive any e-mail notifications regarding cameras
- Archiving should take place

See Configure general scheduling and archiving and Configure camera-specific schedules.

## 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 67).
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 56) by selecting it with your mouse.

4. Fill in the relevant properties (see "Motion detection & exclude regions" on page 92).

There are some differences in motion-detection behavior for PTZ cameras (see "About motion detection and PTZ cameras" on page 67).

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 Essential provided that the cameras are scheduled to be online (see "Online period" on page 116).

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 63). If you delete the hardware device, you also delete any attached microphones. 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 .....	71
Dynamic path selection .....	73
Video recording .....	74
Manual recording .....	77
Frame rate - MJPEG .....	78
Frame Rate - MPEG .....	80
Audio selection .....	81
Audio recording .....	82
Storage information .....	82

### Recording and archiving paths

When you configure video and recording (see "About video and recording configuration" on page 66), 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
<b>Template</b>	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.
<b>Apply Template</b>	Select which cameras you want to apply the template for. You then use one of the two <b>Set</b> buttons to actually apply the template. <b>Tip:</b> To select all cameras in the list, click the <b>Select All</b> button.
<b>Camera Name</b>	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
<b>Shortcut</b>	<p>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.</p> <p>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.</p> <p>Examples of correct camera shortcut numbers: 3, 12345678. Examples of incorrect camera shortcut numbers: Cam#3, 123456789.</p> <p>More information about using the keyboard shortcuts is available in the separate documentation for the Smart Client.</p>
<b>Recording Path</b>	<p>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 <b>local</b> drive. You cannot specify a path to a network drive. If you use a network drive, it is not possible to save recordings if the network drive becomes unavailable.</p> <p>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.</p> <p><b>Tip:</b> If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.</p>
<b>Archiving Path</b>	<p>Only editable if not using dynamic paths for archiving (see "About archiving" on page 108). Path to the folder in which the camera's archived recordings should be stored. Default is C:\MediaDatabase.</p> <p>To browse for another folder, click the browse icon next to the required cell. You can specify a path to a local 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 Essential 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.</p>
<b>Retention Time</b>	<p>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.</p> <p>Note that the retention time covers the <b>total</b> amount of time you want to keep recordings for. In earlier XProtect Essential versions, time limits were specified separately for the database and archives.</p>
<b>Camera</b>	Click the <b>Open</b> button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
<b>Select All</b>	Click button to select all cameras in the <b>Apply Template</b> column.
<b>Clear All</b>	Click button to clear all selections in the <b>Apply Template</b> column.
<b>Set selected template value on selected cameras</b>	<p>Apply only a selected value from the template to selected cameras.</p> <p><b>Tip:</b> To select more than one value press CTRL while selecting.</p>





Name	Description
<b>Set all template values on selected cameras</b>	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 66), 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 108) paths, you specify a number of different archiving paths, usually across several drives. If the path containing the XProtect Essential database is on one of the drives you have selected for archiving, XProtect Essential will always try to archive to that drive first. If not, XProtect Essential 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
<b>Enable dynamic path selection archives</b>	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 <b>New path</b> feature below the list.
<b>Use</b>	Select particular paths for use as dynamic archiving paths. You can also select a previously manually added path for removal (see description of <b>Remove</b> button in the following).
<b>Drive</b>	Letter representing the drive in question, for example C:.
<b>Path</b>	Path to where you save the files, for example C:\ or <a href="#">\\OurServer\OurFolder\OurSubfolder\</a> .
<b>Drive Size</b>	Total size of the drive.
<b>Free Space</b>	Amount of unused space left on the drive.
<b>New path</b>	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: <a href="#">\\server\volume\directory\</a> . When the new path is added, you can select it for use as a dynamic archiving path.
<b>Add</b>	Add the path specified in the <b>New path</b> field to the list.
<b>Remove</b>	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 66), 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 Essential, 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 87).

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 <b>Set</b> buttons to actually apply the template. <b>Tip:</b> To select all cameras in the list, click the <b>Select All</b> 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: < > & ' " \ / : * ?   [ ]
Record on	Lets you select under which conditions video from the camera should be recorded: <ul style="list-style-type: none"> <li>• <b>Always:</b> Record whenever the camera is enabled (see "General" on page 83) and scheduled to be online (see "Online period" on page 116) (the latter allows for time-based recording).</li> <li>• <b>Never:</b> 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.</li> <li>• <b>Motion Detection:</b> Select this to record video in which motion (see "Motion detection &amp; exclude regions" on page 92) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.</li> <li>• <b>Event:</b> Select this to record video when an event occurs and until another event occurs. Use of recording on event requires that events (see "Overview of events and output" on page 100) have been defined, and that you select start and stop events. <b>Tip:</b> If you have not yet defined any suitable events, you can quickly do it: Use the <b>Configure events</b> list, located below the other fields.</li> <li>• <b>Motion Detection &amp; Event:</b> 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.</li> </ul>



Name	Description
<b>Start Event</b>	Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).
<b>Stop Event</b>	Select required stop event. Recording will end when the stop event occurs (or later if using post-recording; see the following).
<b>Pre-recording</b>	<p>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.</p> <p><b>How does pre- and post-recording work?</b> XProtect Essential 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 Essential 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.</p>
<b>Seconds [of pre-recording]</b>	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 108) times. That can be problematic since pre-recording does not work well during archiving.
<b>Post-recording</b>	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.
<b>Seconds [of post-recording]</b>	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.
<b>Camera</b>	Click the <b>Open</b> button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
<b>Select All</b>	Click button to select all cameras in the <b>Apply Template</b> column.
<b>Clear All</b>	Click button to clear all selections in the <b>Apply Template</b> column.
<b>Set selected template value on selected cameras</b>	<p>Apply only a selected value from the template to selected cameras.</p> <p><b>Tip:</b> To select more than one value press CTRL while selecting.</p>
<b>Set all template values on selected cameras</b>	Apply all values from the template to selected cameras.

## Properties in this window:

If the camera uses the MJPEG video format ..... 76  
 If the camera uses the MPEG video format..... 77



## If the camera uses the MJPEG video format

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

### Regular Frame Rate Mode:

Name	Description
<b>Frame Rate</b>	Required average frame rate for video from the camera. Select number of frames, then select the time unit interval (second, minute or hour).

### Speedup Frame Rate Mode:

Name	Description
<b>Enable speedup frame rate</b>	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.
<b>Frame Rate</b>	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.
<b>On motion</b>	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.
<b>On event</b>	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 (see "Overview of events and output" on page 100) have been defined, and that you select start and stop events in the neighboring lists.  <b>Tip:</b> If you have not yet defined any suitable events, you can quickly do it: Use the <b>Configure events</b> list, located below the other fields.
<b>Start Event</b>	Select required start event. The camera will begin using the speedup frame rates when the start event occurs.
<b>Stop Event</b>	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 116) 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
<b>Enable dedicated live stream</b>	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.



Name	Description
<b>Stream</b>	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.
<b>Resolution</b>	Select the resolution of the camera.
<b>FPS</b>	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:

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

## Dual Stream:

This feature is only available on cameras supporting dual stream.

Name	Description
<b>Enable dedicated live stream</b>	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.
<b>Stream</b>	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.
<b>Resolution</b>	Select the resolution of the camera.
<b>FPS</b>	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 66), 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 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 87) 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
<b>Enable manual recording</b>	Select check box to enable manual recording and specify further details.
<b>Default duration of manual recording</b>	Period of time (in seconds) during which user-driven recording will take place. Default duration is 300 seconds, corresponding to five minutes.
<b>Maximum duration of manual recording</b>	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 Essential 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 66), 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 87) using MJPEG.

### Properties in this window:

Template and common properties.....	78
Regular frame rate properties.....	79
Speedup frame rate properties.....	79

### Template and common properties

Name	Description
<b>Template</b>	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.
<b>Apply Template</b>	Select which cameras you want to apply the template for. You then use one of the two <b>Set</b> buttons to actually apply the template. <b>Tip:</b> To select all cameras in the list, click the <b>Select All</b> button.
<b>Select All</b>	Click button to select all cameras in the <b>Apply Template</b> column.
<b>Clear All</b>	Click button to clear all selections in the <b>Apply Template</b> column.
<b>Set selected template value on selected cameras</b>	Apply only a selected value from the template to selected cameras. <b>Tip:</b> To select more than one value press <b>CTRL</b> while selecting.
<b>Set all template values on selected cameras</b>	Apply all values from the template to selected cameras.



Name	Description
<b>Camera Name</b>	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
<b>Frame Rate</b>	Required average frame rate for video from the camera. Select number of frames, then select the time unit interval (second, minute or hour).
<b>Time Unit</b>	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 <b>second</b> in normal mode, you cannot specify 16 frames per <b>minute</b> or <b>hour</b> in speedup mode.
<b>Camera</b>	Click the <b>Open</b> 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
<b>Enable Speedup</b>	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.
<b>Frame Rate</b>	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.
<b>Time Unit</b>	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 <b>second</b> in normal mode, you cannot specify 16 frames per <b>minute</b> or <b>hour</b> in speedup mode.





Name	Description
<b>Speedup On</b>	<ul style="list-style-type: none"> <li>• <b>Motion Detection:</b> Select this to speed up when motion (see "Motion detection &amp; exclude regions" on page 92) is detected. Normal frame rates will be resumed immediately after the last motion <b>is detected</b>.</li> <li>• <b>Event:</b> Select this to speed up when an event occurs and until another event occurs. Use of speedup on event requires that events (see "Overview of events and output" on page 100) have been defined, and that you select start and stop events in the neighboring columns.   <b>Tip:</b> If you have not yet defined any suitable events, you can quickly do it: Use the <b>Configure events</b> list, located below the other fields.</li> <li>• <b>Motion Detection &amp; Event:</b> 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.</li> </ul>
<b>Schedule Only</b>	Select this to speed up according to the camera's speedup schedule (see "Speedup" on page 116) only.
<b>Start Event</b>	Select required start event. The camera will begin using the speedup frame rates when the start event occurs.
<b>Stop Event</b>	Select required stop event. The camera will return to the normal frame rates when the stop event occurs.
<b>Camera</b>	Click the <b>Open</b> 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 66), 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 87) using MPEG.

Name	Description
<b>Template</b>	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.
<b>Apply Template</b>	Select which cameras you want to apply the template for. You then use one of the two <b>Set</b> buttons to actually apply the template.  <b>Tip:</b> To select all cameras in the list, click the <b>Select All</b> button.





Name	Description
<b>Camera Name</b>	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: < > & ' " \ / : * ?   [ ]
<b>Dual Stream</b>	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 84) properties.
<b>Live FPS</b>	Select the camera's live frame rate per second (FPS).
<b>Camera</b>	Click the <b>Open</b> button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
<b>Select All</b>	Click button to select all cameras in the <b>Apply Template</b> column.
<b>Clear All</b>	Click button to clear all selections in the <b>Apply Template</b> column.
<b>Set selected template value on selected cameras</b>	Apply only a selected value from the template to selected cameras. <b>Tip:</b> To select more than one value press CTRL while selecting.
<b>Set all template values on selected cameras</b>	Apply all values from the template to selected cameras.

## Audio selection

When you configure video and recording (see "About video and recording configuration" on page 66), 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 selected for a camera, audio from the microphone 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
<b>Template</b>	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.
<b>Apply Template</b>	Select which cameras you want to apply the template for. You then use one of the two <b>Set</b> buttons to actually apply the template. <b>Tip:</b> To select all cameras in the list, click the <b>Select All</b> button.
<b>Camera Name</b>	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: < > & ' " \ / : * ?   [ ]
<b>Default Microphone</b>	Select required default microphone. <b>Tip:</b> Note that you can select microphones attached to another hardware device than the selected camera.



Name	Description
<b>Camera</b>	Click the <b>Open</b> button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
<b>Select All</b>	Click button to select all cameras in the <b>Apply Template</b> column.
<b>Clear All</b>	Click button to clear all selections in the <b>Apply Template</b> column.
<b>Set selected template value on selected cameras</b>	Apply only a selected value from the template to selected cameras. <b>Tip:</b> To select more than one value press CTRL while selecting.
<b>Set all template values on selected cameras</b>	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 66) for specific cameras, you can determine whether audio should be recorded or not. Your choice applies for all cameras on your XProtect Essential system.

Name	Description
<b>Always</b>	Always record audio on all applicable cameras.
<b>Never</b>	Never record audio on any cameras. Note that even though audio is never recorded, it is still 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 Essential automatically archives (see "About archiving" on page 108) 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.

## Storage information

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



Name	Description
<b>Drive</b>	Letter representing the drive in question, for example C:.
<b>Path</b>	Path to where you save the files, for example C:\ or \\OurServer\OurFolder\OurSubfolder\.
<b>Usage</b>	What the storage area is used for, for example recording or archiving.
<b>Drive Size</b>	Total size of the drive.
<b>Video Data</b>	Amount of video data on the drive.
<b>Other Data</b>	Amount of other data on the drive.
<b>Free Space</b>	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.....	83
Video .....	84
Audio .....	87
Recording .....	87
Recording and archiving paths .....	88
Event notification .....	90
Output.....	91
Motion detection & exclude regions.....	92
Privacy masking .....	93
360° lens .....	94
Fisheye .....	95
PTZ preset positions.....	96
PTZ on event.....	98

### General

When you configure video and recording (see "About video and recording configuration" on page 66) for specific cameras, properties include:

Name	Description
<b>Enabled</b>	Cameras are by default enabled, meaning that provided they are scheduled to be online (see "Online period" on page 116), they are able to transfer video to XProtect Essential. If required, you can disable an individual camera, in which case no video/audio will be transferred from the camera source to XProtect Essential.
<b>Camera Name</b>	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
<b>Camera shortcut number</b>	<p>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.</p> <p>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.</p> <p>More information about using the keyboard shortcuts is available in the separate documentation for the Smart Client.</p>

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 Essential system time may therefore not correspond fully, and this may occasionally lead to confusion. As all frames are time-stamped by XProtect Essential 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 66) 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
<b>Frame Rate</b>	Required average frame rate for video from the camera. Select number of frames, then select the time unit interval (second, minute or hour).
<b>Live Frame Rate</b>	<p>Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour).</p> <p>If the camera supports dual stream and dual stream is enabled, the <b>Live Frame Rate</b> column will be read-only with the value <b>Dual streaming—</b> which cannot be altered.</p>
<b>Recording Frame Rate</b>	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
<b>Enable speedup frame rate</b>	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.
<b>Frame Rate</b>	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.
<b>Live Frame Rate</b>	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 <b>Live Frame Rate</b> column will be read-only with the value <b>Dual streaming—</b> which cannot be altered.
<b>Recording Frame Rate</b>	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.
<b>On motion</b>	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.
<b>On event</b>	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 (see "Overview of events and output" on page 100) have been defined, and that you select start and stop events in the neighboring lists.  <b>Tip:</b> If you have not yet defined any suitable events, you can quickly do it: Use the <b>Configure events</b> list, located below the other fields.
<b>Start Event</b>	Select required start event. The camera will begin using the speedup frame rates when the start event occurs.
<b>Stop Event</b>	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 116) 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
<b>Enable dedicated live stream</b>	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.
<b>Stream</b>	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.



Name	Description
<b>Resolution</b>	Select the resolution of the camera.
<b>FPS</b>	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
<b>Frame rate per second</b>	Frame rate for viewing live and recorded video from the camera. Select number of frames per second.
<b>Record keyframes only</b>	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).
<b>Record all frames on motion</b>	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 <b>is detected</b> , the camera will return to recording keyframes only.
<b>Record all frames on event</b>	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 (see "Overview of events and output" on page 100) have been defined, and that you select start and stop events in the neighboring lists.  <b>Tip:</b> If you have not yet defined any suitable events, you can quickly do it: Use the <b>Configure events</b> list, located below the other fields.
<b>Start Event</b>	<b>Use when recording on Event or Motion Detection &amp; Event.</b> Select required start event. The camera will begin recording all frames when the start event occurs.
<b>Stop Event</b>	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
<b>Enable dedicated live stream</b>	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.
<b>Stream</b>	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.



Name	Description
<b>Resolution</b>	Select the resolution of the camera.
<b>FPS</b>	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 66) for specific cameras, properties include the possibility of selecting a default microphone for the camera.

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

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

Name	Description
<b>Default Microphone</b>	Select required default microphone.  <b>Tip:</b> Note that you can select microphones attached to another hardware device than the selected camera.

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

## Recording

In XProtect Essential, 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 66) for specific cameras, recording properties include:

Name	Description
<b>Always</b>	Record whenever the camera is enabled (see "General" on page 83) and scheduled to be online (see "Online period" on page 116) (the latter allows for time-based recording).
<b>Never</b>	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.
<b>Conditionally</b>	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 <b>Door Opened</b> and a stop event called <b>Door Closed</b> . With three seconds of pre-recording, video will be recorded from three seconds before <b>Door Opened</b> occurs and until <b>Door Closed</b> occurs





Name	Description
<b>Built-in motion detection</b>	Select this check box to record video in which motion (see "Motion detection & exclude regions" on page 92) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.
<b>On event</b>	Select this check box to record video when an event occurs and until another event occurs. Use of recording on event requires that events (see "Overview of events and output" on page 100) have been defined, and that you select start and stop events in the neighboring lists.  <b>Tip:</b> If you have not yet defined any suitable events, you can quickly do it: Use the <b>Configure events</b> list, located below the other fields.
<b>Start Event</b>	Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).
<b>Stop Event</b>	Select required stop event. Recording will end when the stop event occurs (or later if using post-recording; see the following).
<b>Enable pre-recording</b>	Available only when the option <b>Conditional</b> 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.
<b>Enable post-recording</b>	Available only when the option <b>Conditional</b> 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 Essential 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 Essential 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 77) may be enabled. With manual recording, Smart Client users with the necessary rights 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 66) for specific cameras, properties include:

Name	Description
<b>Recording Path</b>	<p>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 <b>local</b> drive. You cannot specify a path to a network drive. If you use a network drive, it is not possible to save recordings if the network drive becomes unavailable.</p> <p>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.</p> <p><b>Tip:</b> If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.</p>





Name	Description
<b>Delete Database</b>	<p>Click button to delete all recordings in the database for the camera. Archived recordings will not be affected.</p> <p><b>IMPORTANT:</b> 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.</p>
<b>Archiving Path</b>	<p>Only editable if not using dynamic paths for archiving (see "About archiving" on page 108). Path to the folder in which the camera's archived recordings should be stored. Default is C:\MediaDatabase.</p> <p>To browse for another folder, click the browse icon next to the required cell. You can specify a path to a local 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 Essential 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.</p>
<b>Delete Archives</b>	<p>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.</p> <p><b>IMPORTANT:</b> 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.</p>
<b>Retention Time</b>	<p>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.</p> <p>Note that the retention time covers the <b>total</b> amount of time you want to keep recordings for. In earlier XProtect Essential versions, time limits were specified separately for the database and archives.</p>



Name	Description
Database Repair Action	<p>Select which action to take if the database becomes corrupted:</p> <ul style="list-style-type: none"> <li>• <b>Repair, scan, delete if fails:</b> 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.</li> <li>• <b>Repair, delete if fails:</b> If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be deleted.</li> <li>• <b>Repair, archive if fails:</b> If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be archived.</li> <li>• <b>Delete (no repair):</b> If the database becomes corrupted, the contents of the database will be deleted.</li> <li>• <b>Archive (no repair):</b> If the database becomes corrupted, the contents of the database will be archived.</li> </ul> <p>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.</p> <p><b>Why archive a corrupt database?</b> 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.</p> <p><b>Tip:</b> 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 150).</p>
Configure Dynamic Paths	<p>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 Essential will always try to archive to that path first. If not, XProtect Essential 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 73).</p>

## Event notification

When you configure video and recording (see "About video and recording configuration" on page 66) for specific cameras, properties include event notification:






## About event notifications

Event notification lets you inform Smart Client users that an event (see "Overview of events and output" on page 100) has occurred on the XProtect Essential 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 Essential system, regardless whether events are manual, 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 66) for specific cameras, you can also associate a camera with particular hardware output (see "Add a hardware output" on page 102), 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 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 Essential 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 66) 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 83), 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 the Recording Server service when configuring such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 152).

Name	Description
<b>Enable</b>	Lets you enable or disable (see "About motion detection settings" on page 67) the built-in motion detection.
<b>Show grid</b>	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.
<b>Include All</b>	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.
<b>Exclude All</b>	Lets you quickly clear all grid sections in the preview image.



Name	Description
<b>Sensitivity</b>	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.
<b>Motion</b>	<p>Adjust the <b>Motion</b> 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 <b>Level</b> 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.</p> <p>Alternatively, specify a value between 0 and 10000 in the field on the left to control the motion setting.</p> <p>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.</p>
<b>Keyframe Only</b>	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 <b>Keyframe only</b> .
<b>Detection interval</b>	<p>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.</p> <p>Adjusting this setting can help lower the amount of system resources used on motion detection.</p>
<b>Detection resolution</b>	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
<b>Enable</b>	Enable the <b>Privacy Masking</b> feature.



Name	Description
<b>Show grid</b>	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.
<b>Show privacy mask</b>	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.
<b>Clear</b>	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
<b>Enable 360° lens</b>	Select check box to enable use of the 360° lens technology and to be able to specify further properties.
<b>Enable panomorph support</b>	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.
<b>ImmerVision Enables® panomorph RPL number</b>	<p>When enabling the panomorph support functionality, you must also select a Registered Panomorph Lens (RPL) number from the <b>ImmerVision Enables® panomorph RPL number</b> 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.</p> <p>If you, at some point, want to add additional types of lenses, go to <b>File</b> and select <b>Import new lens types</b>. Locate the .xml file that contains information about the lens type and press <b>OK</b>.</p> <p>For details of ImmerVision, panomorph lenses, and RPLs, see <a href="http://www.immervision.com/en/home/index.php">http://www.immervision.com/en/home/index.php</a>.</p>
<b>Enable fisheye support</b>	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 95) for the camera in question.
<b>License key</b>	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 Essential vendor for further information.



## Fisheye

When you configure video and recording (see "About video and recording configuration" on page 66) 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 63) 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
<b>Ceiling mount</b>	If the camera is mounted on a ceiling, you can adjust properties to reflect this by selecting the check box.
<b>Resolution</b>	Resolution values are automatically displayed above the fisheye image. When using fisheye, resolution will automatically be set to the highest possible value.
<b>X radius</b>	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.
<b>Milestone Recording Server service</b>	A vital part of the surveillance system. Video streams are only transferred to XProtect Essential while the Recording Server service is running.
<b>X center</b>	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.
<b>Y center</b>	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.
<b>Enable preview</b>	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.
<b>Set as Home</b>	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' <b>Home</b> button, their view of the camera changes to that position.





Name	Description
Button	Description
	Moves the flattened view up
	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. Preset positions also become selectable in clients, allowing users with required rights 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 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 the Recording Server service when configuring such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 152).





Name	Description
<b>PTZ type</b>	<p>Your configuration options depend on the type of PTZ camera in question:</p> <ul style="list-style-type: none"> <li>• <b>Type 1 (stored on server):</b> You define preset positions by moving the camera using the controls (see "Move PTZ type 1 and 3 to required positions" on page 70) in the upper half of the window, then storing each required position on the XProtect Essential server. You can define up to 260 preset positions this way.</li> <li>• <b>Type 2 (imported from camera):</b> 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.</li> <li>• <b>Type 3 (stored on camera):</b> You define preset positions by moving the camera with the controls (see "Move PTZ type 1 and 3 to required positions" on page 70) 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 Essential.</li> </ul>
<b>Import / Refresh</b>	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 Essential. 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.
<b>Add New</b>	<p>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.</p> <p>Remember that names of preset positions must contain only the characters A-Z, a-z and the digits 0-9.</p>
<b>Set New Position</b>	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.
<b>Delete</b>	<p>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.</p> <p>Before you delete a preset position, make sure it is not used in PTZ on event. Since the preset positions are stored on the camera, you can bring a deleted preset position back into XProtect Essential by clicking the <b>Import / refresh</b> button. If you bring back a preset position this way, and the preset position is to be used in PTZ on event, you must manually configure PTZ on event to use the preset position again.</p>
<b>Test</b>	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.



Name	Description
<b>PTZ control wheel</b>	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 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 96), it is possible to make the PTZ camera automatically go to a particular preset position when a particular event occurs (see "Overview of events and output" on page 100).

When associating events with preset positions on a PTZ camera, you can select between **all** events defined on your XProtect Essential 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.

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 recommend stopping the Recording Server service when configuring such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 152).

## 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 Essential, you can always manage the microphones attached to cameras; **not** microphones attached to Smart Client operators' computers.



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

## Configure microphones

1. In the Management Application's navigation pane, expand **Advanced Configuration**, expand **Hardware Devices**, and expand the hardware device to which the relevant microphones is attached.
2. Right-click the required microphones, and select **Properties**.
3. Specify properties as required.

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

## Show or hide microphone

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

## Microphone properties

When you configure video and recording (see "About video and recording configuration" on page 66) for specific cameras, you can determine when audio should be recorded or not. Your choice applies for all cameras on your XProtect Essential system.

### Microphone properties

<b>Enabled</b>	Microphones are by default enabled, meaning that they are able to transfer audio to XProtect Essential. If required, you can disable an individual microphone, in which case no audio will be transferred from the microphone to XProtect Essential.
<b>Microphone name</b>	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
<b>Always</b>	Always record audio on all applicable cameras.
<b>Follow video</b>	Record audio only when video is recorded.
<b>Never</b>	Never record audio on any cameras. Note that even though audio is never recorded, it is still 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 Essential.

**Hardware output** units can be attached to output ports on many hardware devices, allowing you to activate lights, sirens, and more from XProtect Essential. 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 Essential 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 Essential. The same goes for hardware output, but hardware output does require some simple configuration in XProtect Essential.

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 102) and Configure hardware output on event (on page 103).

### About events and output

Events and output of various types can be used for automatically triggering actions in XProtect Essential. Examples of actions: starting or stopping recording on cameras, switching to a particular video frame rate, triggering e-mail 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 137).

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
<b>Hardware input events:</b>	<ul style="list-style-type: none"> <li>Events based on input from hardware input units attached to hardware devices are called hardware input events.</li> <li>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 Essential considers such detections as input from the hardware, and you can use such detections as input events as well.</li> <li>Lastly, hardware input events can be based on XProtect Essential detecting motion in video from a camera, based on motion detection settings in XProtect Essential.</li> </ul> <p>This type of hardware input events is also called system motion detection events or VMD (Video Motion Detection) events. In earlier XProtect Essential versions, VMD events were an event type of their own; now they are simply considered a type of hardware input event.</p>
<b>Manual events:</b>	<p>Events may be generated manually by the users selecting them in their clients. These events are called manual events.</p> <p>Manual events can be of the type <b>Global events</b> or <b>Timer events</b>:</p> <p>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.</p> <p><b>Example:</b></p> <p>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.</p>

Before you configure events of any type, **configure general event handling**, such as which ports XProtect Essential 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 104).

When you are ready to **configure events**, see [Add a hardware input event](#) (on page 101) , and [Add a manual event](#) (on page 102). If you want to use timer events with your other events, see [Add a timer event](#) (on page 103).

## Add a hardware input event

With hardware input events, you can turn input received from input units attached to hardware devices into events (see "Overview of events and output" on page 100) in XProtect Essential.

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 92) is enabled in XProtect Essential 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 Essential 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. When ready, click **OK**, or click the **Add button** to add a timer event (on page 103) 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 Essential system. Once added, output can be activated automatically by events (see "Overview of events and output" on page 100) 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.
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 103). 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 91).

## Add a manual event

With manual events, your users with required rights 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 116). 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 98).



- For triggering output. Particular output can be associated (see "Configure hardware output on event" on page 103) with manual events.
- For triggering event-based e-mail 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. When ready, click **OK**, or click the **Add** button again to add a timer event (on page 103) 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 timer event

Timer events are separate events (see "Overview of events and output" on page 100), 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 106). XProtect Essential 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 102), such as lights, sirens, door openers, etc., you can associate the hardware output with events (see "Overview of events and output" on page 100). 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 Essential 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 107).





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 Essential 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 104). XProtect Essential 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.

## 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
<b>Alert port</b>	Specify port number to use for handling events. Default port is port 1234.
<b>SMTP event port</b>	Specify port number to use for sending event information from hardware devices to XProtect Essential via SMTP. Default port is port 25.
<b>FTP event port</b>	Port to use for FTP communication with the hardware device. Default port is port 21.
<b>Polling interval [1/10] second</b>	For a small number of hardware devices, primarily dedicated input/output devices (see "About dedicated input/output devices" on page 62), it is necessary for XProtect Essential 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:

Hardware input event .....	105
Manual Event.....	106
Timer event.....	106
Hardware output .....	107
Output control on event (Events and Output-specific properties) .....	107

### Hardware input event

When you add hardware input events (see "Add a hardware input event" on page 101), some properties depend on the selected type of input:

Name	Description
<b>Enable</b>	Select check box to use selected type of input as an event in XProtect Essential, and specify further properties.
<b>Event name</b>	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.
<b>Images from camera</b>	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 87) particular to XProtect Essential. Lets you select which camera you want to receive pre- and/or post-alarm images from.
<b>Number of pre-alarm images</b>	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.
<b>Frames per second</b>	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.
<b>Send e-mail if this event occurs</b>	Only available if e-mail notification (see "Configure e-mail notifications" on page 121) is enabled. Select if XProtect Essential 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 117).
<b>Attach image from camera</b>	Only available if e-mail notification (see "Configure e-mail notifications" on page 121) 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.
<b>Delete</b>	Delete a selected event.
<b>Add</b>	When a specific hardware input event is selected, clicking Add will add a timer event (on page 103) to the selected hardware input event.



## Manual Event

When you add manual events (see "Add a manual event" on page 102), specify the following properties:

Name	Description
<b>[List of defined global events and cameras]</b>	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.
<b>Event name</b>	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.
<b>Send e-mail if this event occurs</b>	Only available if e-mail notification (see "Configure e-mail notifications" on page 121) is enabled. Select if XProtect Essential 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 117).
<b>Attach image from camera</b>	Only available if e-mail notification (see "Configure e-mail notifications" on page 121) 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.
<b>Delete</b>	Delete a selected event.
<b>Add</b>	Add a new event. When <b>Global</b> or a specific camera is selected, clicking <b>Add</b> will add a new manual event. When a specific manual event is selected, clicking <b>Add</b> will add a timer event (on page 103) to the selected manual event.

## Timer event

When you add timer events (see "Add a timer event" on page 103), specify the following properties:

Name	Description
<b>Timer event name</b>	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.
<b>Timer event occurs after</b>	Specify the amount of time that should pass between the main event occurring and the timer event (in seconds or minutes).



## Hardware output

When you add hardware output (see "Add a hardware output" on page 102), specify the following properties:

Name	Description
<b>Output name</b>	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.
<b>Output connected to</b>	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 <b>Output 1</b> .
<b>Keep output for</b>	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.

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

When you add output controls on events (see "Configure hardware output on event" on page 103), specify the following properties:

Name	Description
<b>Event</b>	Select the required event.
<b>Output</b>	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 108)
- That some cameras transfer video to XProtect Essential 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 Essential)
- One of more cameras should use speedup (that is use a higher than normal frame rate)
- You want to receive any e-mail notifications regarding one or more cameras.
- Archiving takes place.

## About archiving

Archiving is an integrated and automated feature in XProtect Essential with which recordings are moved to free up space for new recordings. By default, recordings are stored in the XProtect Essential database for each camera. The database for each camera is capable of containing a maximum of 600,000 records or 40 GB. XProtect Essential automatically archives (see "About archiving" on page 108) 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 Essential 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 Essential is to perform archiving once a day, or if your database becomes full. You can change the settings for when and how often archiving takes place in the Management Application. You can also schedule archiving 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 Essential 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 71) 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 Essential this does not pose a threat. XProtect Essential 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.

## Benefits of archiving

By default, recordings are stored in the XProtect Essential database for each camera. The database for each camera is capable of containing a maximum of 600000 records or 40 GB.



However, the maximum size of a database is not in itself very important: If a database for a camera becomes full, XProtect Essential automatically begins archiving its content, freeing up space in the database. Consequently, having sufficient archiving space is more important (see *Storage Capacity Required for Archiving* in the following).

In addition to automatic archiving when a database becomes full, you can schedule archiving to take place at particular times up to 24 times per day. This way, you can proactively archive recordings, so databases will never become full.

By using archiving, you will also be able to back up archived records on backup media of your choice, using your preferred backup software.

## About archiving locations

The default archiving folder (see "Configure default file paths" on page 151) (C:\MediaDatabase) is located on the XProtect Essential 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 108) 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 88).
- **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 71).

**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 Essential will always try to archive to that drive first. If not, XProtect Essential 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 73).

If you configure your cameras through the Configure video and recording wizard (see "The Configure Video and Recording wizard" on page 48), the wizard also lets you configure archiving paths.

## 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 66).

If the path containing the camera's database is on one of the drives you have selected for dynamic archiving, XProtect Essential will always try to archive to that drive first. If not, XProtect Essential 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 151) 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 Essential 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 Essential 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."•

## 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 Essential 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 Essential 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 Essential runs out 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 Essential 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 Essential 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 Essential server is running out of disk space, and the archiving drive is identical to the camera database drive, XProtect Essential 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 Essential 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 Essential 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 notification.

1. First, XProtect Essential will attempt to delete 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

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 Essential 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.

## 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 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.

## General scheduling properties

### Properties in this window:





Scheduling All Cameras .....	113
Scheduling options .....	114
Archiving.....	115

## Scheduling All Cameras

When you configure general scheduling and archiving, 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** can also be specified individually for each camera.



Name	Description
<b>Template</b>	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.
<b>Apply Template</b>	Select which cameras you want to apply the template for. You then use one of the two <b>Set</b> buttons to actually apply the template. <b>Tip:</b> To select all cameras in the list, click the <b>Select All</b> button.
<b>Camera</b>	The name as it appears in the Management Application as well as in clients.
<b>Online</b>	<p>Select the required profile (for example <b>Always on</b>) for the online schedule for the camera(s) in question.</p> <p>You specify a camera's online periods by creating schedule profiles based on:</p> <ul style="list-style-type: none"> <li>Periods of time (example: Mondays from 08.30 until 17.45), shown in pink: </li> <li>Events within periods of time (example: from Event A occurs until Event B occurs Mondays from 08.30 until 17.45), shown in yellow: </li> </ul> <p>The two options can be combined , but they cannot overlap in time.</p>
<b>E-mail</b>	Select the required profile for the e-mail notification schedule (see "E-mail notification" on page 117) 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: 
<b>Select All</b>	Click button to select all cameras in the <b>Apply Template</b> column.
<b>Clear All</b>	Click button to clear all selections in the <b>Apply Template</b> column.
<b>Set selected template value on selected cameras</b>	Apply only a selected value from the template to selected cameras. <b>Tip:</b> To select more than one value press CTRL while selecting.
<b>New schedule profile</b>	Create a new schedule profile of any type by clicking the <b>Create...</b> button.

## Scheduling options

When you configure general scheduling and archiving, 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
<b>Start cameras on client requests</b>	<p>Cameras may be offline, for example because they have reached the end of an online recording schedule (see "Online period" on page 116), in which case client users will not be able to view live video from the cameras. However, if you select <b>Start cameras on client requests</b>, 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).</p> <p>You must select <b>Enable recording when started on client request</b> (see the following), if you want recording to take place.</p>
<b>Enable recording when started on client request</b>	<p>Enable recording on the camera when <b>Start cameras on client requests</b> (see the previous) is also selected.</p> <p>If a user does not have access to manual recording, selecting <b>Enable recording when started on client request</b>, will <b>not</b> enable the user to do manual recording.</p>
<b>Schedule profile for new cameras</b>	<p>Select which online schedule profile to use as default for cameras you subsequently add to your XProtect Essential system. Note that your selection only applies for the online schedule, not for any other schedules. Default selection is <b>Always on</b>, meaning that new cameras will always be online, that is transferring video to the XProtect Essential server for live viewing and further processing.</p>
<b>Maximum delay between reconnect attempts</b>	<p>Control the aggressiveness of reconnection attempts. If XProtect Essential 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.</p>

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 Essential automatically archives (see "About archiving" on page 108) recordings if a camera's database becomes full (in earlier versions, this was an option configured individually for each camera).

Name	Description
<b>Archiving Times</b>	<p>Specify when you want XProtect Essential 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 <b>up</b> and <b>down</b> buttons to increase or decrease values, or simply overwrite the selected value, and then click <b>Add</b>.</p> <p>The more you expect to record, the more often you should archive.</p>
<b>Send e-mail on archiving failure</b>	<p>If selected, XProtect Essential will automatically send an e-mail to selected recipients if archiving fails. This requires that the e-mail notification (on page 117) feature is enabled. Recipients are defined as part of the e-mail notification properties.</p>



## Camera-specific scheduling properties

### Properties in this window:




Online period .....	116
Speedup .....	116
E-mail notification .....	117

### Online period

When you configure scheduling for specific cameras, your **Online Period** settings are probably the most important, since they determine when each camera should transfer video to XProtect Essential.

By default, cameras added to XProtect Essential 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 114), in which case subsequently added cameras will not automatically be online.

The fact that a camera transfers video to XProtect Essential 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 66).

Name	Description
Online	<p>Select the required profile (for example <b>Always on</b>) for the online schedule for the camera(s) in question.</p> <p>You specify a camera's online periods by creating schedule profiles based on:</p> <ul style="list-style-type: none"> <li>Periods of time (example: Mondays from 08.30 until 17.45), shown in pink: </li> <li>Events within periods of time (example: from Event A occurs until Event B occurs Mondays from 08.30 until 17.45), shown in yellow: </li> </ul> <p>The two options can be combined , but they cannot overlap in time.</p>

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 114) and, if needed, the Enable recording when started on client request (see "Scheduling options" on page 114) 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 78) and Video (Camera-specific properties) (see "Video" on page 84).



Name	Description
<b>Speedup</b>	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 78). 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 for specific cameras, you can specify e-mail notification (see "Configure e-mail notifications" on page 121) periods. Before you can define this type of schedule, e-mail notification must be enabled (see "E-mail properties" on page 122).

Name	Description
<b>E-mail</b>	Select the required profile for the e-mail notification schedule (see "E-mail notification" on page 117) 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:

## Logs

### About logs

XProtect Essential can generate various logs.

#### Log types

Name	Description
<b>Management Application log files</b>	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.
<b>Recording Server service log files</b>	These files log Recording Server service (see "About services" on page 128) 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.



Name	Description
<b>Image Server service log files</b>	<p>These files log activity on the Image Server service (see "About services" on page 128). A new log file is created for each day the service is used.</p> <p>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.</p>
<b>Image Import service log files</b>	<p>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.</p> <p>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.</p> <p>You cannot disable this type of logging. Image Import service log files are named according to the structure ImageImportLog_YYYYMMDD.log, for example ImageImportLog20091231.log.</p>
<b>Event log files</b>	<p>These files log information about registered events (see "Overview of events and output" on page 100). A new log file is created for each day on which events occur.</p> <p>You cannot disable this type of logging. Event log files should be viewed using the Smart Client (use the <b>Playback</b> tab's <b>Alerts</b> section).</p>
<b>Audit log files</b>	<p>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_auditYYYYMMDD.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.</p>

## 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 Essential 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 Essential 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
<b>Log integrity information was not found. Log integrity can't be guaranteed.</b>	The log file could not be checked for integrity.
<b>Log information does not match integrity information. Log integrity can't be guaranteed.</b>	The log file exists, but does not contain the expected information. Thus, log integrity cannot be guaranteed.
<b>[Log file name] not found</b>	The log file was not present.
<b>[Log file name] is empty</b>	The log file was present, but empty.
<b>Last line changed/removed in [log file name]</b>	The last line of the log file did not match validation criteria.
<b>Encrypted data missing in [log file name] near line [#]</b>	The encrypted part of the log line in question was not present.
<b>Inconsistency found in [log file name] near line [#]</b>	The log line does not match the encrypted part.
<b>Inconsistency found in [log file name] at beginning of log file</b>	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 Essential can 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 120) 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 Essential 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 Essential 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
<b>Path</b>	<p>These log files are by default placed in the appropriate <b>All Users</b> folder for the operating system you are using.</p> <p>To specify another location for your log files, type the path to the required folder in the <b>Path</b> field, or click the browse button next to the field to browse to the required folder.</p>
<b>Days to log</b>	<p>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.</p>

## Event Log

Name	Description
<b>Path</b>	<p>These log files are by default placed in the appropriate <b>All Users</b> folder for the operating system you are using.</p> <p>To specify another location for your log files, type the path to the required folder in the <b>Path</b> field, or click the browse button next to the field to browse to the required folder.</p>
<b>Days to log</b>	<p>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.</p>

## Audit Log

Name	Description
<b>Enable audit logging</b>	<p>Audit logging is the only type of XProtect Essential logging which is not compulsory. Select/clear the check box to enable/disable audit logging.</p>
<b>Path</b>	<p>These log files are by default placed in the appropriate <b>All Users</b> folder for the operating system you are using.</p> <p>To specify another location for your log files, type the path to the required folder in the <b>Path</b> field, or click the browse button next to the field to browse to the required folder.</p>





Name	Description
<b>Days to log</b>	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).
<b>Minimum logging interval</b>	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.
<b>In sequence timespan</b>	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 Essential can automatically send e-mail notifications to one or more recipients when:

- Motion (see "Motion detection & exclude regions" on page 92) is detected
- Events (see "Overview of events and output" on page 100) 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 108) 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 122), including the important information about which SMTP mail server to use. XProtect Essential 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.

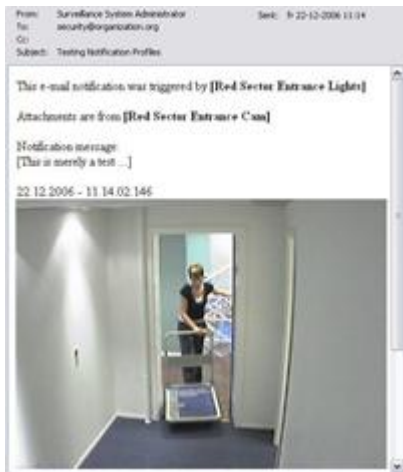


3. Save your configuration changes by clicking the **Save Configuration** button on the Management Application toolbar.

When you configure e-mail alerts, also consider the e-mail notification schedules (see "E-mail notification" on page 117) configured for each camera.

## E-mail properties

With e-mail notifications (see "Configure e-mail notifications" on page 121), you and your colleagues can instantly get notified when your surveillance system requires attention.

Name	Description
<b>Recipient(s)</b>	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: <a href="mailto:aa@aa.aa">aa@aa.aa</a> ; <a href="mailto:bb@bb.bb">bb@bb.bb</a> ; <a href="mailto:cc@cc.cc">cc@cc.cc</a> ).
<b>Test</b>	Sends a test e-mail to the specified recipients. If <b>Include Image</b> is selected, the test e-mail will have a still test JPEG image attached.
<b>Subject text</b>	Enter required subject text for e-mail notifications.
<b>Message text</b>	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.
<b>Include Image</b>	<p>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.</p>  <p>Example of e-mail including a still image</p>
<b>Do not send e-mail on camera failures</b>	If selected, e-mail notifications will not be sent if XProtect Essential 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 117).



Name	Description
<b>Time between motion- and database-related e-mails per camera</b>	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 <b>5</b> , 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 <b>0</b> , 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 <b>0</b> , you should therefore consider cameras' motion detection (see "Motion detection & exclude regions" on page 92) sensitivity settings.
<b>Sender e-mail address</b>	Enter the e-mail address you wish to appear as the sender of the e-mail notification.
<b>Outgoing mail (SMTP) server name</b>	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 its 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.
<b>Server requires login</b>	Select check box if a user name and password is required to use the SMTP server.
<b>User name</b>	Only required when <b>Server requires login</b> is selected. Specify the user name required for using the SMTP server.
<b>Password</b>	Only required when <b>Server requires login</b> is selected. Specify the password required for using the SMTP server.

## Server access

### About server access

You can configure clients' access to the XProtect Essential 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 58).

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 Essential, this was known as Image Server administration, since technically it is the Image Server service (see "About services" on page 128) which handles clients' access to the surveillance system.



## About registered services

Registered services displays the services installed to and running on your XProtect Essential system. It displays the following information about the individual services:

Name	Description
<b>Enabled</b>	Indicates if the relevant service is enabled
<b>Name</b>	The name of the service
<b>Description</b>	A description of the service
<b>Addresses</b>	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 124), Local IP Ranges (on page 125), and Language Support & XML Encoding (see "Language support and XML encoding" on page 126). XProtect Essential 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, Add user groups, and Configure user and group rights.

## Server access properties

### Properties in this window:

Server access.....	124
Local IP ranges.....	125
Language support and XML encoding.....	126

### Server access

When you configure server access (on page 124) (that is clients' access to the XProtect Essential server), specify the following:



Name	Description
<b>Server name</b>	Name of the XProtect Essential 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.
<b>Local port</b>	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.
<b>Enable internet access</b>	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 Essential server.
<b>Internet address</b>	Lets you specify a public IP address or hostname for use when the XProtect Essential server should be available from the internet.
<b>Internet port</b>	Specify a port number for use when the XProtect Essential should be available from the Internet. The default port number is 80. You can change the port number if needed.
<b>Max. number of clients</b>	<p>You can limit the number of clients allowed to connect at the same time. Depending on your XProtect Essential 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.</p> <p>By default, a maximum of ten simultaneously connected clients are allowed. To specify a different maximum number, simply overwrite the value.</p> <p><b>Tip:</b> To allow an unlimited number of simultaneously connected access clients, type <b>0</b> (zero) in the <b>Max. number of clients</b> field.</p> <p>A four-minute session timeout period applies for client sessions on XProtect Essential. In many cases, client users may not notice this at all. However, the session timeout period will be very evident if you set the <b>Max. number of clients</b> value to <b>1</b>. 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.</p>

## Local IP ranges

You can specify IP address ranges which XProtect Essential 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 Essential server and clients.



Name	Description
<b>Character encoding/Language</b>	<p>Select required language/character set.</p> <p>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.</p>

## Users


### Overview of users and groups

To get an overview of your XProtect Essential system's users, expand **Advanced Configuration** in the Management Application's navigation pane, then expand **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 58) or individually (see Add basic users and Add Windows users).

By grouping users, you can specify rights 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 such as, for example, Active Directory®. If you want to use groups, make sure you add groups 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.

## User properties

### Properties in this window:

User information .....	127
Group information .....	127
Camera access .....	127



## User information

Name	Description
<b>User name</b>	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: < > & ' " \ / : * ?   [ ]
<b>Password</b>	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.
<b>User type</b>	Non-editable field, displaying whether the selected user is of the type basic user or Windows user group.

## Group information

Name	Description
<b>Group name</b>	Edit the group name. Names must be unique, and must not contain any of these special characters: < > & ' " \ / : * ?   [ ]

## Camera access

When you add or edit basic users, Windows users or groups, 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
<b>PTZ</b>	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.
<b>PTZ preset positions</b>	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
<b>Output</b>	Activate output (lights, sirens, door openers, etc.) related to the selected camera(s).
<b>Events</b>	Use manually triggered events related to the selected camera(s). This feature is available in the XProtect Smart Client only.
<b>Incoming audio</b>	Listen to incoming audio from microphones related to the selected camera(s). This feature is available in the Smart Client only.
<b>Manual recording</b>	Manually start recording for a fixed time (defined (see "Manual recording" on page 77) by the surveillance system administrator).
Playback	Features
<b>AVI/JPEG export</b>	Export evidence as movie clips in AVI format and as still images in JPEG format.
<b>Database export</b>	Export evidence in database format. This feature is available in the Smart Client only.
<b>Sequences</b>	Use the <b>Sequences</b> feature when playing back video from the selected camera.
<b>Smart search</b>	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.
<b>Recorded audio</b>	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 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.

## Services

### About services

The following services are all automatically installed on the XProtect Essential server if you run a **Typical** installation. By default, services run transparently in the background on the XProtect Essential server. If you need to, you can start and stop services separately from the Management Application, see Start and stop services.

Service	Description
<b>Milestone Recording Server service</b>	A vital part of the surveillance system. Video streams are only transferred to XProtect Essential while the Recording Server service is running.





Service	Description
<b>Milestone Image Server service</b>	Provides access to the surveillance system for users logging in with a Smart Client.  <b>Note:</b> 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.
<b>Milestone Image Import service</b>	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 Essential pre- and post-recording feature (see "Recording" on page 87).
<b>Milestone Log Check service</b>	Performs integrity checks on XProtect Essential log files. For more information, see Overview of Logs.
<b>Milestone Event Server service</b>	Manages all alarms and map-related communication. It stores events, image files and map configurations, and makes status information about the surveillance system available.
<b>Milestone Mobile service</b>	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.

## 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 14) from a mobile device or from XProtect Web Client (see "About XProtect Web Client" on page 14).

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 129), 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 you need. Once added, video push channels appear in the **Channels mapping**.
3. Select a user name from a user account already set up in your XProtect system to associate with the relevant Video push channel. If you do not associate the Video push channel with an already created user, then you will not have a **Push** button (iOS)/**Record** button (Android) in the XProtect Mobile client when you log in.
4. Click **File > Save**.
5. Add the Video push driver as a hardware device (see "Add a Video push driver as a hardware device" on page 131) to the video management system. You must choose the **Manual** hardware device detection method as the Video push driver will not show up in automatic hardware searches. Once finished, click **Apply**.
6. On the **Video Push** tab, click **Find Cameras**. If successful, the newly added Video push driver appears in this list and is ready to use.
7. Click **Apply**.
8. Click **File > Save**.
9. Restart all Milestone services. Once completed, you can log in and use Video push in your XProtect Mobile client.

## Add a Video push driver 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 device settings (see "Add hardware devices settings" on page 131) and select the hardware driver manually.
4. Once finished, your Video push driver must be associated with your Video push channel. To do so, return to your Mobile server > **Video Push** tab and click **Find Cameras**.

## Add hardware devices settings

Specify the following settings when you add a Video Push driver in the **Add Hardware Devices** wizard:

Name	Description
<b>Use:</b>	Select if the Video push driver should added to the XProtect video management system.
<b>Address:</b>	Type in the XProtect Mobile server IP address.



Name	Description
<b>Port:</b>	Type in the port number for your Video push driver. The default port is 80. The port is for communication between the XProtect Mobile server and your XProtect server.  <b>Important:</b> The port number you set must be identical with the port number you set when you specify your Video push settings (see "Video push" on page 133). If the port numbers are not identical, your Video push channel will not work.
<b>User name:</b>	Select the same user name as associated with the Video push channel when you added (see "Add a Video push channel" on page 131) this.
<b>Password:</b>	Type in the password for the Video push driver. The password for your Video push driver is <b>Milestone</b> (this cannot be changed).
<b>Hardware Driver:</b>	Select the <b>Video Push Driver</b> .
<b>Verified:</b>	Select if the Video push driver runs on a secured HTTPS connection.

Once finished, go back to your XProtect Mobile server > **Video Push** tab and click **Find Cameras** to finish setting up the Video push channel.

## Mobile server settings

### Properties in this window:

Info .....	132
Server status .....	133
Video push.....	133
Export .....	134

### Info

Fill in and specify general settings for the Mobile server:

Name	Description
<b>Server name:</b>	Name of the Mobile server.
<b>Description:</b>	Description of the Mobile server.
<b>Mobile server:</b>	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.
<b>Connection type:</b>	Possible methods are: <b>HTTP only</b> , <b>HTTP and HTTPS</b> or <b>HTTPS Only</b> .
<b>Client timeout (HTTP)</b>	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.
<b>Login method:</b>	Select how you want to log in to the Mobile server server should take place. Possible methods are: <b>Automatic</b> , <b>Windows Only</b> or <b>Basic Only</b> .
<b>All cameras view:</b>	Enable/disable viewing of <b>All Cameras</b> view. This view contains all cameras on a recording server (user rights permitting).



Name	Description
<b>Output and events:</b>	Enable/disable output and events.
<b>Keyframes only</b>	Enable/disable video stream to stream key frames only. <i>Enabling key frames only reduces bandwidth usage.</i>
<b>Enabled:</b>	Enable/disable logging of XProtect Mobile client' actions in a separate log file.
<b>Log file location:</b>	Path to where log files are saved.
<b>Keep logs for:</b>	Number of days to keep logs for (default 3 days).
<b>CPU usage:</b>	Default level of CPU usage which will trigger a warning in the log.
<b>Internal bandwidth:</b>	Default internal bandwidth usage which will trigger a warning in the log.
<b>External bandwidth:</b>	Default external bandwidth usage which will trigger a warning in the log.
<b>Check every:</b>	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
<b>Server active since:</b>	Shows how long the Mobile server has been running since it was last stopped.
<b>CPU usage:</b>	Shows current CPU usage on the Mobile server.
<b>Internal bandwidth:</b>	Shows the current bandwidth in use between the Mobile server and the relevant recording server.
<b>External bandwidth:</b>	Shows the current bandwidth in use between the mobile device and Mobile server.
<b>User Name column:</b>	Shows user name(s) of the Mobile server user(s) connected to the Mobile server.
<b>State column:</b>	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.
<b>Bandwidth Usage column:</b>	Shows the level of bandwidth used by the Mobile server client user in question.
<b>Live Streams column:</b>	Shows the number of live video streams currently open for the XProtect Mobile client user in question.
<b>Playback Streams column:</b>	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
<b>Video push</b>	Enable Video push on the Mobile server.
<b>Number of channels</b>	Specify the number of enabled Video push channels in your XProtect system.
<b>Channel column</b>	Shows the channel number for the relevant channel. Non-editable.
<b>Port</b>	Port number for the relevant Video push channel.
<b>MAC</b>	MAC address for the relevant Video push channel.
<b>User Name</b>	Enter the user name associated with the relevant channel.
<b>Camera Name</b>	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 131), 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
<b>Export</b>	Enable export in clients.
<b>Export to:</b>	Specify the location to which recordings should be exported.
<b>Delete exported recordings older than:</b>	Enter the number of days to pass before recordings are deleted.
<b>Limit size of exports folder to:</b>	Enter a number to set a maximum limit for the folder to which the recordings are exported.
<b>Include timestamps:</b>	Add timestamps to exported video.

In the columns, see the following details for every individual exported recording:

<b>Name column</b>	Name of the exported recording.
<b>State column</b>	State of the exported recording.
<b>Camera column</b>	The camera that provided the exported recording.
<b>Timestamp column</b>	The point of time when the exported recording took place.
<b>Duration column</b>	The length of the exported recording.
<b>User column</b>	The name of the user who provided the exported recording.
<b>MB column</b>	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 14)
- Start, stop and restart the Mobile service (see "Start, stop and restart Mobile service" on page 137)
- Fill in or change surveillance server credentials (see "Fill in/edit surveillance server credentials" on page 136)
- Show/edit port numbers (on page 137)
- Edit certificate (on page 136)
- Open today's log file (see "Access logs and exports" on page 135)
- Open log folder (see "Access logs and exports" on page 135)
- Open export folder (see "Access logs and exports" on page 135)
- Show Mobile server status (see "About show status" on page 135)
- 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
<b>Server running since:</b>	Time and date of the time when the Mobile server was last started.
<b>Connected users:</b>	Number of users currently connected to the Mobile server.
<b>CPU usage:</b>	How many % of the CPU is currently being used by the Mobile server.
<b>CPU usage history:</b>	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 143) based feature using functionality handled by the Event server. It provides central overview and control of alarms in any number of XProtect Essential 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 139) 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 58).

Right to trigger manually defined events: if manually defined events (see "Add a manual event" on page 102) are available in your XProtect Essential system, these can determine if the user can trigger selected manually defined events in the Smart Client. See Configure User Access wizard (on page 58).



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 58).

## Time profiles for alarms

Alarms can also be based on time profiles (for alarms) (see "Add a time profile (for Alarms)" on page 138). 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 Essential. 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.

## Add a time profile (for Alarms)

Time Profiles are periods of time used for the Alarms (see "About alarms" on page 137) feature only.

**Tip:** For all other time scheduling and profiling purposes, use the general scheduler of XProtect Essential.

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 Essential server's** local time.

To add a time profile (for an alarm (see "Add an alarm" on page 139)), 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 137).

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 139).
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 are typically data received from external third-party video content analysis (VCA) providers. An example of a VCA-based system could be an access control system.

## Alarms properties

### Properties in this window:

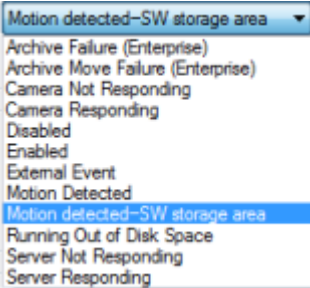
Alarms definition .....	139
Alarm data settings .....	141
Sound settings .....	142
Time profile .....	142

### Alarms definition

When you configure Alarm definitions (see "Add an alarm" on page 139), specify the following:

Name	Description
<b>Enable</b>	Enables the Alarms feature.



Name	Description
<b>Name</b>	Enter a name. The alarm's name will appear whenever the alarm is listed. <b>Tip:</b> Alarm names do not have to be unique, but using unique and descriptive alarm names are advantageous in many situations.
<b>Description</b>	Enter a description (optional).
<b>Triggering event</b>	<p>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:</p>  <p>List of selectable triggering events; the highlighted one is created and customized using analytics events.</p>
<b>Sources</b>	Select which cameras and/or other devices, including plug-in defined sources (VCA, MIP, etc) (see "About alarms" on page 137), the event should originate from in order to trigger the alarm. Your options depend upon which type of event you have selected.
<b>Time profile</b>	If you select <b>Time profile</b> , 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 138), you will only be able to select <b>Always</b> . If you have defined one or more time profiles, they will be selectable from this list.
<b>Event based</b>	<p>If you select <b>Event based</b>, 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 (see "Overview of events and output" on page 100). Also global/manual event definitions (see "Add a manual event" on page 102) can be used.</p> <p>Note that when selecting <b>Event based</b> it is not possible to define alarms based on outputs—only on inputs.</p>
<b>Time Limit</b>	Select the time-limit within which the operator must respond to the alarm.
<b>Events triggered</b>	Select the event to be triggered if the operator does not react withing the time limit specified in <b>Time limit</b> . This could be, for example, sending an email, SMS or similar.
<b>Related cameras</b>	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.
<b>Related map</b>	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.



Name	Description
<b>Initial alarm owner</b>	Select a default user responsible for the alarm. You can only select from users allowed to view <b>all</b> cameras and/or other devices selected as source(s) for the event causing the alarm.
<b>Initial alarm priority</b>	Select a priority ( <b>High</b> , <b>Medium</b> or <b>Low</b> ) for the alarm. Priorities can be used for sorting purposes and workflow control in the Smart Client.
<b>Initial alarm category</b>	Select a category to which the alarm should initially be assigned. This could be, for example, <b>Building01</b> , <b>Burglary</b> , <b>ElevatorEast</b> or similar, depending on which categories have been defined.
<b>Event triggered by alarm</b>	Define an event to be triggered by the alarm in the Smart Client (if needed).
<b>Auto-close alarm</b>	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 141) and Alarm sound settings (see "Sound settings" on page 142) 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
<b>Level</b>	Add new priorities with level numbers of your choosing or use/edit the default priority levels (numbers <b>1</b> , <b>2</b> or <b>3</b> ). These priority levels are used to configure the <b>Initial alarm priority</b> setting (see "Alarms definition" on page 139).
<b>Name</b>	Type a name for the entity. You can create as many as you like.
<b>Sound</b>	Select the sound to be associated with the alarm. Use one if the default sounds or add more in Sound Settings (on page 142).

### Alarm Data Levels **tab**, States

<b>Level</b>	In addition to the default state levels (numbers <b>1</b> , <b>4</b> , <b>9</b> and <b>11</b> , 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 <b>Alarm List</b> .
<b>Name</b>	Type a name for the entity. You can create as many as you like.

### Alarm Data Levels **tab**, Categories

<b>Level</b>	Add new categories with level numbers of your choosing. These category levels are used to configure the <b>Initial alarm category</b> setting (see "Alarms definition" on page 139).
<b>Name</b>	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.

<b>Reasons for Closing tab</b>	<b>Enable</b>	Select to enable that all alarms must be assigned a reason for closing before they can be closed.
<b>Reason</b>		Add reasons for closing that the user can choose between when closing alarms. Examples could be " <b>Solved-Trespasser</b> " or " <b>False Alarm</b> ". You can create as many as you like.

## Sound settings

When you configure Sound Settings, specify the following:

Name	Description
<b>Sounds</b>	<p>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).</p> <p>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.</p>
<b>Add</b>	Lets you add sounds. Browse to the sound to upload one or several .wav files.
<b>Remove</b>	Remove a selected sound from the list of manually added sounds. Default sounds cannot be removed.
<b>Test</b>	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 138), specify the following:

Name	Description
<b>Name</b>	Type a name for the time profile.
<b>Description</b>	Enter a description (optional).
<b>Add Single Time</b>	Right-click the calendar and select <b>Add Single Time</b> . Specify <b>Start time</b> and <b>End time</b> . If the time covers whole days, select <b>All-day event</b> .
<b>Add Recurring Time</b>	Right-click the calendar and select <b>Add Recurring Time</b> . Specify the time range, recurrence pattern, and range of recurrence.





Name	Description
<b>Edit Time</b>	<p>Right-click the calendar and select <b>Edit Time</b>. Specify <b>Start time</b> and <b>End time</b>. If the time covers whole days, select <b>All-day event</b>.</p> <p>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.</p>

## ***MIP plug-ins***

### **About MIP plug-ins**

If you install MIP (Milestone Integration Partner) plug-ins to your XProtect Essential, 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 31) 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 Essential 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 145), which is limited to the the Management Application configuration.

The following describes how to back up your configuration in XProtect Essential 2.0.

If you need information about how to back up a configuration from an earlier version of XProtect Essential—a typical need when upgrading—see Upgrade from a previous version (on page 24).

In the following, we assume that you have not changed the XProtect Essential default configuration path (see "Configure default file paths" on page 151), 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 Essential 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 Essential 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 83) 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 Essential 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 Essential 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 147). 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 Essential 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 Essential 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**.

## Export and import management application configuration

You can export the current configuration of your XProtect Essential 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 Essential 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 Essential, 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 Essential 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 Essential 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 Essential 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 import changes to a configuration. This can be relevant if installing many similar XProtect Essential 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 145)—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 Essential 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 45):

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).

If you have added new cameras or other devices to XProtect Essential 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 Essential 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 Essential 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 Essential installations it works fine.

As from XProtect Essential 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 Essential 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 Essential 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 Essential 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 Essential 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 Essential 6.5 or newer and your XProtect Essential 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 INCREASEUSERSVA 3072
```

Where:

  - **USERSVA** 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 INCREASEUSERSVA
```
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 Essential 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 Essential 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 Essential in a restore point (see "Restore system configuration from a restore point" on page 147) (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 Essential services (see "About services" on page 128).

**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 Essential through clients will typically remain logged in during the services restart, but they will experience a short video outage.

## Configure default file paths

XProtect Essential uses a number of default file paths:



File paths	Description
<b>Default recording path for new cameras</b>	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 88), but you can also change the default recording path so all new cameras you add will use a path of your choice.
<b>Default archiving path for new cameras</b>	All new cameras you add will by default use this path for archiving (see "About archiving" on page 108). 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 73) for archiving.
<b>Configuration path</b>	The path by default used for storing your XProtect Essential system configuration.

To change any of the default file paths:

1. If you want to change the configuration path, stop 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 all services.

## Monitor storage space usage

To view how much storage space you have on your XProtect Essential 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 the Recording Server service when configuring such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 152).



# 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 Essential: the main application used by XProtect Essential administrators for configuring the surveillance system server. Now called the Management Application.

### 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

### 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 Essential. A simple but effective method if setting up several similar systems.

## D

### Device

In XProtect Essential : 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](http://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.

## E

### Event Server

A server that stores and handles incoming alarm data and events from all XProtect Essential 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

### GOP

Group of pictures; individual frames grouped together, forming a video-motion sequence.

### Grace period

When you install XProtect Essential, configure the system and add recording servers and cameras, XProtect Essential runs on temporary licenses. These need to be activated before a certain period ends. This is the grace period.

### 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 Essential, rather to hardware devices. This is because hardware devices have their own IP addresses or host names. Being IP-based, XProtect Essential 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 Essential 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 Essential server. The Image Server service is not configured separately as it is configured through XProtect Essential'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.

### 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 Essential 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 Essential 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 Essential 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 Essential 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 Essential 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 camera'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 camera'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 Essential 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 Essential, 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 Essential 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 Essential. XProtect Transact can help you prevent loss and shrinkage through video evidence combined with time-linked POS or ATM transaction data.

[www.milestonesys.com](http://www.milestonesys.com)

## 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](http://www.milestonesys.com).

## V

### 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 Essential, 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 Essential '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 Essential 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 Essential and installed locally on remote users' computers.



# Index

---

## 3

360 degrees panomorph support • 155

360° lens • 95

## A

About activating licenses • 27, 30, 32, 144

About activating licenses after grace period • 33

About alarms • 101, 138, 139, 140, 141

About archiving • 28, 47, 51, 53, 54, 55, 56, 61, 63, 67, 73, 74, 76, 83, 90, 108, 109, 110, 116, 122, 153

About archiving audio • 111

About archiving locations • 110

About backup and restore of configurations • 145

About database resizing • 67

About dedicated input/output devices • 63, 105

About dynamic archive paths • 111

About e-mail • 122

About events and output • 101

About handling daylight saving time • 149

About hardware devices • 61

About input and output • 101

About installing surveillance server software or XProtect Smart Client silently • 22

About licenses • 30

About logs • 118

About microphones • 99

About MIP plug-ins • 138, 144

About Mobile server • 14, 130

About Mobile Server Manager • 14, 136

www.milestonesys.com

About motion detection and PTZ cameras • 68, 70

About motion detection settings • 68, 70, 93

About privacy options • 36

About protecting recording databases from corruption • 91, 151

About recording audio • 61

About registered services • 125

About replacing cameras • 32

About saving configuration changes in XProtect Enterprise 8.0 and streamlined XProtect software versions • 131

About scheduling • 108

About server access • 124

About services • 68, 118, 119, 124, 129, 152

About show status • 136

About the Replace Hardware Device wizard • 30, 32, 61, 64, 66

About upgrading • 24

About video and recording configuration • 28, 67, 69, 72, 74, 75, 78, 79, 81, 82, 83, 84, 85, 88, 89, 91, 92, 93, 96, 100, 111, 117

About Video push • 130, 132

About viewing version and license information • 152

About XProtect Mobile client • 14, 130

About XProtect Smart Client • 11

About XProtect Web Client • 14, 130

Access logs and exports • 136

Access XProtect Web Client • 14, 136

Activate License - Offline • 34

Activate License - Online • 33

Add a hardware input event • 102, 106



Add a hardware output • 92, 101, 103, 104, 108

Add a manual event • 102, 103, 107, 139, 141

Add a time profile (for Alarms) • 139, 141, 143

Add a timer event • 102, 103, 104, 106, 107

Add a Video push channel • 132, 133, 135

Add a Video push driver as a hardware device • 132

Add an alarm • 138, 139, 140

Add hardware devices settings • 132

Add Hardware Devices wizard - Import from CSV  
File - example of CSV file • 45

Add/edit a Mobile server • 131

Adjust Motion Detection wizard • 57

Administrator • 155

Administrator rights • 20

Advanced • 39, 41

Advanced configuration • 61

Alarm data settings • 142

Alarms • 138

Alarms definition • 140, 142

Alarms properties • 140

API • 155

Application settings • 36

Apply/save configuration changes • 152

Archiving • 116

Aspect ratio • 155

ATM • 155

Audio • 88

Audio recording • 83

Audio selection • 82

Automatic response if running out of disk space • 112

AVI • 155

**B**

Back up system configuration • 24, 145

Back up your current configuration • 24

Backup and restore configuration • 145

Basic & Windows Users • 59

Before you start • 19

Benefits of archiving • 109

Browser • 155

**C**

Camera access • 128

Camera and database action • 61, 62

Camera properties • 84

Cameras and storage information • 67

Camera-specific scheduling properties • 117

Change language • 37

Change SLC • 35

Change/restore Management Application behavior • 28, 37

Clear your Internet browser's cache upon upgrade • 15

Clients • 11

Codec • 155

Common tasks • 149

Configure analytics events in alarms • 140

Configure camera-specific schedules • 68

Configure default file paths • 110, 111, 145, 152

Configure e-mail notifications • 106, 107, 118, 122, 123



Configure general event handling • 102, 105

Configure hardware devices • 64, 65, 66, 96

Configure hardware output on event • 101, 103, 104, 108

Configure microphones • 100

Configure motion detection • 70

Configure server access • 28, 59, 125

Configure system, event and audit logging • 120

Configure User Access wizard • 28, 59, 124, 127, 138, 139

access summary • 60

Configure Video & Recording Wizard

Live & Recording Settings Motion-JPEG Cameras • 50

Live & Recording Settings MPEG Cameras • 52

Configure when cameras should do what • 70

Copyright, trademarks and disclaimer • 8

CSV • 155

CSV file format and requirements • 45, 46, 147

## D

Delete a Mobile server • 131

Delete hardware devices • 64, 71

Detected and verified hardware devices • 42, 43

Device • 155

DirectX • 155

Disable information collection • 37

Disable or delete cameras • 71

DNS • 155

Download Manager • 16

Drive Selection • 54

Driver • 155

DST • 155

[www.milestonesys.com](http://www.milestonesys.com)

Dual stream • 156

Dynamic path selection • 47, 67, 74, 91, 111, 153

## E

Edit certificate • 136, 137

E-mail • 122

E-mail notification • 106, 107, 115, 116, 118, 123

E-mail properties • 118, 122, 123

Event notification • 91

Event Server • 156

Event Server settings • 37

Events and output • 101

Events and output properties • 106

Exclude regions • 57, 70

Export • 135

Export and import management application configuration • 47, 145, 146, 147

Express • 39

## F

Fill in/edit surveillance server credentials • 136, 137

Fisheye • 64, 95, 96, 156

FPS • 156

Frame rate • 156

Frame rate - MJPEG • 79, 117, 118

Frame Rate - MPEG • 81

FTP • 156

## G

General • 51, 53, 75, 84, 88, 93, 145

General event properties • 105

General scheduling properties • 114

Get your system up and running • 22, 27

Getting started • 27





GOP • 156

Grace period • 156

Group information • 128

GUID • 156

## H

H.264 • 156

Hardware detection and verification • 40

Hardware device • 156

Hardware devices • 61

Hardware input event • 106

Hardware name and video channels • 65

Hardware output • 108

Hardware properties • 65

Host • 156

Hotspot • 156

HTTP • 157

## I

I/O • 157

If the camera uses the MJPEG video format • 77

If the camera uses the MPEG video format • 78

I-frame • 157

Image Server • 157

Import changes to configuration • 147

Import from CSV file • 25, 39, 45

Important port numbers • 20

Improve stability with 3 GB virtual memory • 149

Info • 133

Information, driver selection and verification • 44

Install and upgrade • 22

Install from a DVD • 11, 12

Install from the surveillance server • 11

Install silently • 13, 23

Install the XProtect Smart Client • 11

Install XProtect Mobile client • 14

Install your surveillance server software • 22, 27

Introduction • 9

IP • 157

IP address • 157

IP ranges, drivers and authentication • 42

IPIX • 157

## J

JPEG • 157

## K

Keyframe • 157

## L

Language support and XML encoding • 125, 127

Licenses • 30

Local IP ranges • 125, 126

Log properties • 120, 121

Logs • 118

## M

MAC address • 157

Manual • 39, 43

Manual Event • 107

Manual recording • 78, 89, 129

Matrix • 157

Matrix recipient • 157

Microphone properties • 100

Microphones • 99

Minimum system requirements • 19



MIP plug-ins • 144

MJPEG • 157

Mobile Server • 130

Mobile Server Manager • 136

Mobile server settings • 133

Monitor • 158

Monitor storage space usage • 153

Motion Detection • 57

Motion detection & exclude regions • 51, 53, 70, 75,  
81, 89, 93, 103, 122, 124

Move PTZ type 1 and 3 to required positions • 71,  
98

MPEG • 158

## **N**

Network, device type, and license • 64, 65

New hardware device information • 61, 62

NTLM • 158

## **O**

Online period • 15, 51, 53, 71, 75, 84, 88, 103, 116,  
117

Online schedule • 50

Output • 92, 103

Output control on event (Events and Output-specific  
properties) • 104, 108

Overview and names • 40, 41, 42, 44

Overview of events and output • 27, 28, 51, 53, 75,  
77, 81, 86, 87, 89, 92, 99, 101, 102, 103, 104,  
119, 122, 141

Overview of users and groups • 127

## **P**

Panomorph • 158

P-frame • 158

PIN • 158

Ping • 158

Polling • 158

Port • 158

Ports and polling • 63, 105

POS • 158

Post-recording • 158

Pre-alarm • 158

Pre-buffer • 159

Pre-recording • 159

Privacy masking • 94, 159

PTZ • 159

PTZ device • 64, 66

PTZ on event • 99, 103

PTZ preset positions • 97, 99

PUK • 159

## **R**

Recording • 68, 75, 78, 79, 81, 88, 106, 130, 159

Recording and archiving paths • 72, 89, 109, 110,  
153

Recording and archiving settings • 55

Recording and storage properties • 72

Recording Server Manager • 15

Recording Server service • 159

Register SLC • 33

Regular frame rate properties • 80

Removal • 25

Remove the current version • 25

Rename a Mobile server • 131

Replace hardware devices • 64



Restore point • 159

Restore system configuration • 146

Restore system configuration from a restore point •  
145, 148, 152

## **S**

Scheduling All Cameras • 114

Scheduling and archiving • 108

Scheduling options • 50, 115, 117

SCS • 159

SDK • 159

Server access • 21, 124, 125

Server access properties • 125

Server access settings • 59

Server status • 134

Servers • 130

Services • 129

Show or hide microphone • 65, 100

Show/edit port numbers • 136, 138

SIM • 159

SLC • 159

SMS • 160

SMTP • 160

Sound settings • 142, 143

Speedup • 77, 81, 86, 117

Speedup frame rate properties • 80

Start, stop and restart Mobile service • 136, 138

Storage capacity required for archiving • 112

Storage information • 83

Subnet • 160

## **T**

TCP • 160

TCP/IP • 160

Telnet • 160

Template and common properties • 79

The Add Hardware Devices wizard • 27, 33, 34, 39,  
61, 63, 64

The Configure Video and Recording wizard • 49,  
111

Time profile • 143

Time server recommended • 21

Timer event • 104, 107

Transact • 160

## **U**

UDP • 160

Updates • 18

Upgrade • 24

Upgrade from a previous version • 22, 24, 27, 145

UPS • 160

URL • 160

Use the built-in help system • 28

User information • 128

User properties • 127

Users • 127

## **V**

Video • 82, 85, 117

Video device drivers • 25

Video encoder • 160

Video push • 133, 134

Video recording • 75

Video server • 160



Video settings and preview • 49

View • 161

View archived recordings • 114

View video from cameras in Management  
Application • 57, 93, 97, 99, 153, 154

Viewing your license information • 31

Virus scanning information • 21

VMD • 161

## **W**

Wizard • 161

Wizards • 39

## **X**

XProtect Essential overview • 9

XProtect Mobile client • 14

XProtect Smart Client • 11, 161

XProtect Web Client • 14



#### **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](http://www.milestonesys.com).