Target Audience for this Document

This document covers Milestone XProtect Essential from a surveillance system administrator’s perspective. It is solely aimed at XProtect Essential system administrators, and administrator rights are likely to be required in order to be able to access the majority of features described in this document.

This document provides detailed descriptions of XProtect Essential system administration features. It furthermore provides a large number of targeted "how-to" examples, guiding administrators through completing configuration and administration tasks in XProtect Essential.

This document contains very limited end-user related documentation. Administrators requiring information about end-user related client applications should refer to the targeted manuals available on the XProtect Essential software DVD as well as from www.milestonesys.com.

Users who do not have surveillance system administrator responsibilities—such as users of the Remote Client, Smart Client —will find that this manual is not of relevance to them. Such users will be able to find information targeted at their needs in the separate manuals available on the XProtect Essential software DVD as well as from www.milestonesys.com.
Copyright, Trademarks & Important Information

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.

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

Disclaimer
This document 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 this document’s examples are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.
Contents

INTRODUCTION................................................................. 11

SYSTEM AND REQUIREMENTS ............................................. 13
  Minimum System Requirements ........................................ 13
  Administrator Rights ................................................... 14
  Important Port Numbers ............................................... 14
  Virus Scanning ........................................................... 15
  Time Server ............................................................... 16
  MIP Plug-ins .............................................................. 16

INSTALLATION ................................................................. 17
  Upgrade from a Previous Version ................................. 18
  Be Sure to Get the Full Advantage of Upgrading .......... 19

GET YOUR SYSTEM UP AND RUNNING ............................. 21
  Access the Management Application ......................... 22
  Language Selection ..................................................... 22

MANAGEMENT APPLICATION .......................................... 23
  Apply/Save Configuration Changes .............................. 23
  Change/Reset Behavior ............................................... 23
  Privacy Option Settings .............................................. 24
    What Information Is Collected .................................. 24
    When Is Information Collected? ................................. 25
    How Is Information Collected? ................................. 25

WIZARDS ................................................................. 26
  Add Hardware Devices Wizard .................................... 26
Introduction

Express Method ................................................................. 27
Advanced Method ............................................................. 29
Manual Method ................................................................. 32
Import from CSV File Method ............................................. 34
CSV File Format and Requirements ..................................... 34

Configure Video and Recording Wizard .................................. 37
Video Settings and Preview .................................................. 37
Online Schedule .................................................................... 38
Live and Recording Settings (Motion-JPEG Cameras) ............... 39
Live and Recording Settings (MPEG Cameras) ....................... 40
Drive Selection ..................................................................... 42
Recording and Archiving Settings ......................................... 43

Adjust Motion Detection Wizard ........................................... 43
Exclude Regions .................................................................... 44
Motion Detection ................................................................... 44

Configure User Access Wizard .............................................. 45
Server Access Settings ........................................................... 46
Basic and Windows Users ....................................................... 46
Access Summary .................................................................... 47

Replace Hardware Device Wizard ......................................... 47
New Hardware Device Information ......................................... 48
Database Action .................................................................... 49

LICENSES ............................................................................. 51

Overview of Licenses ........................................................... 51
Which Devices Require a License? .......................................... 51
Replacing Cameras ................................................................. 51
Viewing License Information .................................................. 51
Getting Additional Licenses .................................................... 52

Manage Licenses .................................................................. 52
Register SLC .......................................................................... 53
Activate License - Online ....................................................... 53
Online Activation Error Messages .......................................... 54
Activate License - Offline ....................................................... 54
Activate License after Grace Period ....................................... 55
Change SLC ........................................................................... 55
HARDWARE DEVICES .......................................................... 56

Configuration ........................................................................ 56
Name and Video Channels ...................................................... 56
Network, Device Type and License ......................................... 56
PTZ Device ............................................................................. 57

Use Dedicated Input/Output Devices .................................... 58
Replace a Hardware Device .................................................... 58
Delete a Hardware Device ..................................................... 59

CAMERAS AND RECORDINGS .............................................. 60

General Recording and Storage Configuration ....................... 60
Recording and Archiving Paths .............................................. 61
Dynamic Path Selection ....................................................... 62
Video Recording .................................................................... 63
Manual Recording ................................................................ 65
Frame Rate – MJPEG ............................................................. 65
Frame Rate – MPEG ............................................................... 67
Audio Selection .................................................................... 68
Audio Recording .................................................................... 69
Storage Information .............................................................. 69

Camera-specific Configuration ............................................. 70
General ................................................................................. 70
Video (Frame Rate) ............................................................... 71
Audio .................................................................................... 72
Recording Settings ............................................................... 73
Recording and Archiving Paths ............................................. 74
Event Notification ............................................................... 75
Output .................................................................................. 76
Motion Detection and Exclude Regions ................................. 77
Fisheye .................................................................................. 79
Privacy Masking ................................................................. 80
360° Lens .............................................................................. 80
PTZ Preset Positions ........................................................... 81
PTZ on Event ....................................................................... 83
Configure When Cameras Should Do What ............................ 84
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Video in Management Application</td>
<td>84</td>
</tr>
<tr>
<td>Monitor Storage Space Usage</td>
<td>84</td>
</tr>
<tr>
<td>Database Resizing</td>
<td>85</td>
</tr>
<tr>
<td>Disable or Delete a Camera</td>
<td>85</td>
</tr>
<tr>
<td><strong>ARCHIVING</strong></td>
<td>86</td>
</tr>
<tr>
<td>Quick Explanation of the Archiving Feature</td>
<td>86</td>
</tr>
<tr>
<td>Benefits of Archiving</td>
<td>86</td>
</tr>
<tr>
<td>How Archiving Works</td>
<td>87</td>
</tr>
<tr>
<td>Dynamic Path Selection for Archives</td>
<td>88</td>
</tr>
<tr>
<td>Archiving Audio</td>
<td>88</td>
</tr>
<tr>
<td>Viewing Archived Recordings</td>
<td>88</td>
</tr>
<tr>
<td>Storage Capacity Required for Archiving</td>
<td>89</td>
</tr>
<tr>
<td>Backing up Archives</td>
<td>89</td>
</tr>
<tr>
<td>Automatic Response if Running Out of Disk Space</td>
<td>89</td>
</tr>
<tr>
<td>New Database if Archiving Fails</td>
<td>91</td>
</tr>
<tr>
<td>Virus Scanning and Archiving</td>
<td>91</td>
</tr>
<tr>
<td>Configure Archiving Locations</td>
<td>91</td>
</tr>
<tr>
<td>Configure Archiving Schedules</td>
<td>92</td>
</tr>
<tr>
<td><strong>AUDIO</strong></td>
<td>93</td>
</tr>
<tr>
<td>Configure Microphones</td>
<td>93</td>
</tr>
<tr>
<td><strong>SCHEDULING</strong></td>
<td>94</td>
</tr>
<tr>
<td>Configure General Scheduling and Archiving</td>
<td>94</td>
</tr>
<tr>
<td>Scheduling All Cameras</td>
<td>94</td>
</tr>
<tr>
<td>Scheduling Options</td>
<td>95</td>
</tr>
<tr>
<td>Archiving</td>
<td>96</td>
</tr>
<tr>
<td>Configure Camera-specific Scheduling</td>
<td>96</td>
</tr>
<tr>
<td>Online Period</td>
<td>97</td>
</tr>
<tr>
<td>Speedup</td>
<td>98</td>
</tr>
<tr>
<td>E-mail Notification</td>
<td>99</td>
</tr>
</tbody>
</table>
E-MAIL ................................................................. 100
  Configure E-mail Notifications ........................................ 100

EVENTS, INPUT AND OUTPUT .............................. 102
  Configure General Event Handling .................................... 103
  Add a Hardware Input Event ............................................. 104
  Add a Manual Event ..................................................... 105
  Add a Timer Event ...................................................... 106
  Add a Hardware Output .................................................. 107
  Configure Hardware Output on Event ................................ 108

SERVICES .............................................................. 109
  Start and Stop Services ................................................. 109

CLIENT ACCESS TO SURVEILLANCE SYSTEM ......... 110
  Wizard-driven Configuration ........................................... 110
  Advanced Configuration .................................................. 110
  Server Access ........................................................ 110
  Local IP Ranges ......................................................... 111
  Language Support and XML ........................................... 111

USERS ................................................................. 113
  Wizard-driven Configuration ........................................... 113
  Advanced Configuration .................................................. 113
  Add Basic Users .......................................................... 113
  Add Windows Users ....................................................... 114
  Add User Groups .......................................................... 115
  Configure User and Group Rights .................................... 115
  User and Group Properties ............................................. 116

LOGGING ............................................................. 119
  Configure System, Event, and Audit Logging .......................... 120
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Integrity Checks</td>
<td>121</td>
</tr>
<tr>
<td>CENTRAL</td>
<td>123</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>124</td>
</tr>
<tr>
<td>Find Version, License and Plug-in Information</td>
<td>124</td>
</tr>
<tr>
<td>Configure Default File Paths</td>
<td>124</td>
</tr>
<tr>
<td>Restore System Configuration from Restore Point</td>
<td>125</td>
</tr>
<tr>
<td>Export and Import Management Application Configuration</td>
<td>126</td>
</tr>
<tr>
<td>Export Management Application Configuration as Backup</td>
<td>126</td>
</tr>
<tr>
<td>Export Management Application Configuration as Clone</td>
<td>126</td>
</tr>
<tr>
<td>Import Previously Exported Management Application</td>
<td>127</td>
</tr>
<tr>
<td>Import Changes to Configuration</td>
<td>127</td>
</tr>
<tr>
<td>CSV File Format and Requirements</td>
<td>127</td>
</tr>
<tr>
<td>Back Up System Configuration</td>
<td>131</td>
</tr>
<tr>
<td>To Back Up</td>
<td>132</td>
</tr>
<tr>
<td>To Restore Your Backed-up Configuration</td>
<td>132</td>
</tr>
<tr>
<td>Handle Daylight Saving Time</td>
<td>132</td>
</tr>
<tr>
<td>Protect Recording Databases from Corruption</td>
<td>133</td>
</tr>
<tr>
<td>DRIVERS</td>
<td>135</td>
</tr>
<tr>
<td>Update Video Device Drivers</td>
<td>135</td>
</tr>
<tr>
<td>CLIENTS AND ANCILLARY APPLICATIONS</td>
<td>136</td>
</tr>
<tr>
<td>Smart Client</td>
<td>137</td>
</tr>
<tr>
<td>Install Smart Client from Server</td>
<td>137</td>
</tr>
<tr>
<td>Install Smart Client from DVD</td>
<td>138</td>
</tr>
<tr>
<td>Install Smart Client Silently</td>
<td>138</td>
</tr>
<tr>
<td>Remote Client</td>
<td>139</td>
</tr>
<tr>
<td>Download Manager</td>
<td>140</td>
</tr>
<tr>
<td>What Does It Look Like?</td>
<td>141</td>
</tr>
<tr>
<td>Default Configuration</td>
<td>142</td>
</tr>
<tr>
<td>Make New Features Available to Users</td>
<td>143</td>
</tr>
</tbody>
</table>
Introduction

XProtect Essential is an essential single-server video system managing up to 26 cameras per server, including flexible remote access tools. Designed with all the basic features required for small implementations, it is an inexpensive entry-level product.

Several Targeted Components in One

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

- **The Management Application:** 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. Read more about the Management Application on page 23.

- **The Recording Server service:** 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. Read more about the Recording Server service on page 109.

- **The Event Server:** 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.

- **The Microsoft® SQL Server Express Database:** 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.

- **The Image Server service:** Handles access to the surveillance system for users logging in with clients. The Image Server service is automatically installed and runs in the background on the XProtect Essential surveillance system server. You can manage the service through the Management Application. Read more about the Image Server service on page 109.

- **The Download Manager:** Lets you 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. Read more about the Download Manager on page 140.

- **The Remote Client and Smart Client:** Choice of two types of client, each providing users with intuitive access to the surveillance system. The Remote Client and Smart Client let users view live video, play back recorded video, activate output, print and export evidence, etc. The Remote Client is accessed straight from the surveillance system server through a browser. The extra feature-rich Smart Client should always be downloaded and installed on remote users' computers. In general, it is recommended to always use the latest version of the Smart Client to best utilize any possible new features and functions included in your XProtect Essential surveillance system. Read more about the Remote Client and Smart Client on page 136.
Updates

Milestone Systems regularly release service updates for our products, offering improved functionality and support for new devices. If you are a surveillance system administrator, it is recommended that you check www.milestonesys.com for updates at regular intervals in order to make sure you are using the most recent version of your surveillance software.
System and Requirements

Minimum System Requirements

The following are *minimum* system requirements for running XProtect Essential and associated applications. Visit the Milestone website, www.milestonesys.com, for the most recent system performance parameters.

**Tip:** DirectX is a software requirement for several of the components listed in the following. To check which DirectX version is installed on a computer, click *Start*, select *Run...*, and type `dxdiag`. When you click *OK*, the *DirectX Diagnostic Tool* window will open; version information is displayed near the bottom of its *System* tab. Should the server require a DirectX update, the latest versions of DirectX are available from http://www.microsoft.com/downloads/.

Surveillance System Server

- **Operating System**
  - Microsoft® Windows® XP Professional (32-bit or 64-bit*), Windows Server 2003 (32-bit or 64-bit*), Windows Server 2008 R1/R2 (32-bit or 64-bit*), Windows Vista™ Business (32-bit or 64-bit*), Windows Vista Enterprise (32-bit or 64-bit*), Windows Vista Ultimate (32-bit or 64-bit*), Windows 7 Professional (32-bit or 64-bit*), Windows 7 Enterprise (32-bit or 64-bit*) and Windows 7 Ultimate (32-bit or 64-bit*).

- **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**
  - Microsoft .NET 4.0.
  - DirectX 9.0 or newer.
  - Windows Help (WinHlp32.exe).
  - All are downloadable from http://www.microsoft.com/downloads/.

* Running as a 32-bit service/application.

Smart Client (unlicensed and free)

- **Operating System**
  - Microsoft Windows XP Professional (32-bit or 64-bit), Windows Server 2003 (32-bit or 64-bit), Windows Server 2008 R1/R2 (32-bit or 64-bit), Windows Vista Business (32-bit or 64-bit), Windows Vista Enterprise (32-bit or 64-bit), Windows Vista Ultimate (32-bit or 64-bit), Windows 7 Professional (32-bit or 64-bit), Windows 7 Enterprise (32-bit or 64-bit) and Windows 7 Ultimate (32-bit or 64-bit).

- **CPU**
  - Intel Core2™ Duo, minimum 2.4 GHz or higher (more powerful CPU recommended for Smart Clients running high number of cameras and multiple views and displays).

- **RAM**
  - Minimum 1 GB (higher RAM recommended for Smart Clients running high number of cameras and multiple views and displays).
number of cameras and multiple views and displays).

**Network**
- Ethernet (100 Mbit or higher recommended).

**Graphics Adapter**
- AGP or PCI-Express, minimum 1024 x 768 (1280 x 1024 recommended), 16-bit colors.

**Hard Disk Space**
- Minimum 1 GB free.

**Software**
- Microsoft .NET 4.0 Framework.
- DirectX 9.0 or newer.
* Running as a 32-bit service/application.

---

### Remote Client (unlicensed and free)

**Operating System**
- Microsoft Windows XP Professional (32-bit or 64-bit*), Windows Server 2003 (32-bit or 64-bit*), Windows Server 2008 R1/R2 (32-bit or 64-bit*), Windows Vista Business (32-bit or 64-bit*), Windows Vista Enterprise (32-bit or 64-bit*) and Windows Vista Ultimate (32-bit or 64-bit*), Windows 7 Professional (32-bit or 64-bit*), Windows 7 Enterprise (32-bit or 64-bit*) and Windows 7 Ultimate (32-bit or 64-bit*).

**CPU**
- Intel Pentium 4, 2.4 GHz or higher.

**RAM**
- Minimum 1 GB (2 GB or higher recommended on Microsoft Windows Vista).

**Network**
- Ethernet (100 Mbit or higher recommended).

**Graphics Adapter**
- AGP or PCI-Express, minimum 1024 x 768 (1280 x 1024 recommended), 16-bit colors.

**Hard Disk Space**
- Minimum 10 MB free.

**Software**
- DirectX 9.0 or newer.
* Running as a 32-bit service/application.

---

### 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 will not be able to configure the surveillance system. Consult your IT system administrator if in doubt about your rights.

---

### Important Port Numbers

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

**What is a port?** A port is a logical endpoint for data traffic. Networks use different ports for different types of data traffic. Therefore it is sometimes, but not always, necessary to specify which port to use for particular data communication. Most ports are used automatically based on the types of data included in the communication. On TCP/IP networks, port numbers range from 0 to 65536, but only ports 0 to 1024 are reserved for particular purposes. For example, port 80 is used for HTTP traffic when viewing web pages.

When using XProtect Essential, make sure that the following ports are open for data traffic on your network:
**Port 20 and 21 (inbound and outbound):** Used for FTP traffic. FTP (File Transfer Protocol) is a standard for exchanging files across networks. FTP uses the TCP/IP standards for data transfer, and is often used for uploading or downloading files to and from servers.

**Port 25 (inbound and outbound):** Used for SMTP traffic. SMTP (Simple Mail Transfer Protocol) is a standard for sending e-mail messages between servers. This port should be open since, depending on configuration, some cameras may send images to the surveillance system server via e-mail.

**Port 80 (inbound and outbound):** Used for HTTP traffic between the surveillance server and cameras, Remote Client and/or Smart Client, and the default communication port for the surveillance system’s Image Server service. HTTP (HyperText Transfer Protocol) is a standard for exchanging files across networks; widely used for formatting and transmission of data on the world wide web.

**Port 554 (inbound and outbound):** Used for RSTP traffic in connection with H.264 video streaming.

**Port 1024 and above (outbound only):** Used for HTTP traffic between cameras and the surveillance server.

**Port 1234 (inbound and outbound):** Used for event handling.

- Any other port numbers you may have selected to use, for example if you have changed the server access port (see page 110) from its default port number (80) to another port number.

Consult the administrator of your organization’s firewall if in doubt about how to open ports for traffic.

**Virus Scanning**

Virus scanning on the XProtect Essential server, and computers to which data is archived, should if possible be avoided:

- If you are using virus scanning software on the XProtect Essential server, or on a computer to which data is archived (see page 86), it is likely that the virus scanning will use a considerable amount of system resources on scanning all the data which is being archived. This may affect system performance negatively. Also, virus scanning software may temporarily lock each file it scans, which may further impact system performance negatively.

- Likewise, virus scanning software on the XProtect Essential server is likely to use a considerable amount of system resources on scanning data used by the Download Manager (see page 140).

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

All video is 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 supported by your cameras, we thus recommend you auto-synchronize camera and system time through a time server for consistent synchronization.

For information about configuring a time server searching www.microsoft.com for time server, time service, or similar.

MIP Plug-ins

Through the Milestone Integration Software Development Kit (MIP SDK), Milestone Systems A/S or third party vendors can develop custom plug-ins (for example, integration to external access control systems or similar) for XProtect Essential.

These plug-ins—if any—can be found in the Management Application's navigation pane, expand Advanced Configuration, under MIP Plug-ins.

It is possible to assign MIP-related user rights to users and user groups. If this is the case, 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.

Furthermore, if relevant, you can use online activation (see page 52) in connection with licensing schemes of MIP-related plug-ins.
Installation

This chapter covers installation/upgrade of the XProtect Essential server. For information about installing clients, etc., see the separate manuals for each application.

Do not install XProtect Essential on a mounted drive (that is a drive attached to an empty folder on an NTFS (NT File System) volume, with a label or name instead of a drive letter). If using 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 upgrading, read Upgrade from a Previous Version on page 18 first.

1. Insert the XProtect Essential software DVD, wait for a short while, and click the XProtect Essential installation link.

   Alternatively, if you are installing a version downloaded from the internet, run the downloaded installation file from the location you have saved it to.

   Depending on your security settings, you may receive one or more security warnings (such as *Do you want to run or save this file?*, *Do you want to run this software?* or similar). When this is the case, click the **Run** button.

2. When the installation wizard starts, select language for the installer and click **Continue**.

3. When asked, it is important that you:
   - Select installation language.
   - Specify the location of your license file.
   - Read and accept the license agreement.
   - Indicate if you wish to participate in the Milestone data collection program.
   - Select **Typical** installation (advanced users may select **Custom** installation, and choose application language, which features to install and where to install them).

4. 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.


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

If the problem continues, please contact Milestone Support (support@milestonesys.com) for help.

You can now begin configuring your XProtect Essential through its Management Application: Double-click the Management Application desktop shortcut or select **Start > All Programs > Milestone XProtect Essential > Management Application.** See more in Get Your System Up & Running on page 19.

To do a silent install of XProtect Essential, see instructions on page 138.
Upgrade from a Previous Version

Upgrading your entire XProtect Essential system configuration is a fairly easy task.

Back Up Your Current Configuration

When you install the new version of XProtect Essential, it will inherit the configuration from your old version.

However, we recommend that you make regular backups of your server configuration as a disaster recovery measure. Upgrading your server is no exception. While it is rare to lose your configuration (cameras, schedules, views, etc), it can happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration:

The following describes backup of a different XProtect product, such as XProtect Basis+, which is the most likely need when upgrading to XProtect Essential 2.0. If you need information about how to back up your XProtect Essential 2.0 configuration, see Back up System Configuration on page 131.

IMPORTANT:
If upgrading from XProtect Basis+ to XProtect Essential 2.0, do the following before upgrading:
If you installed XProtect Basis+ 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 running the XProtect Essential 2.0 installer, select Custom installation and when prompted for an installation folder, select the [relevant folder] created for restoring.

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)
   - The folder SmartClientViewGroups and all of its content
   - The folder RemoteClientViewGroup and all of its content

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

Remove the Current Version

In most cases, 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. Note, however, that XProtect Basis+ versions earlier than 6.0 must be removed manually before installing the new version.
Install the New Version

Run the installation file for the new software version. Select the installation options that best fit your needs.

Restore a Configuration Backup (if Required)

If for some reason, after installing the new software version, you have lost your configuration, you can restore your configuration, provided you have followed the previous instructions.

Since configuration is stored in a new format in XProtect Essential 1.0 and onwards, any XProtect Basis+ backed-up configuration must be converted to this new format before you can use it. Contact your Milestone vendor for information about how to convert and restore your configuration backup.

For restoring backups made in XProtect Essential 1.0 and onwards, see Back Up System Configuration on page 131 for information on how to back up your system configuration.

Upgrade Video Device Drivers

Video device drivers are small programs used for controlling/communicating with the hardware devices connected to an XProtect Essential system.

Video device drivers are installed automatically during the installation of your XProtect Essential system. However, new versions of the video device drivers—so-called Device Packs—are released and made available for free on the Milestone website (www.milestone.com) from time to time.

We therefore recommend that you regularly visit the Milestone website (look under Support > Downloads) and download the latest Device Pack.

When updating video device drivers, there is no need to remove the old video device drivers first; simply install the latest version on top of any old version you may have. For detailed information, see Update Video Device Drivers on page 135.

Be Sure to Get the Full Advantage of Upgrading

When you upgrade from one product to a more advanced product, you get access to new functionality, but you are also able to 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.

Example: If you upgrade from XProtect Go to XProtect Essential, there are several things you should 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 Enterprise 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.

For further information about the various differences between XProtect products, check the Milestone website at www.milestonesys.com.
Get Your System Up and Running

The following outlines the tasks typically involved in setting 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 will match 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 very 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.) once the system is running. The setup of events (see page 102) and associated actions typically also depends entirely on your organization’s needs.

You may print this topic, and check the boxes in 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.) you are going 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 on page 52.

- **Install XProtect Essential**
  See Install Surveillance Server Software on page 17. If upgrading an existing version of XProtect Essential, see Upgrade from a Previous Version on page 18.

- **Open the Management Application**
  See Access the Management Application on page 22.

- **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 on page 26.

- **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 recordings, any PTZ (Pan/Tilt/Zoom) preset positions, association with microphones etc. See Configure Video & Recording Settings on page 37.

  **What does “... archive recordings” mean?** Archiving—an integrated and automated feature—helps you store recordings beyond the capabilities of XProtect Essential’s standard database. Archiving thus maximizes storage capacity and minimizes risk. See Archiving Extends Recording Storage on page 86.

- **Configure Events, Input & Output**
  If required, system events, for example based on input from sensors, etc., 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, making PTZ cameras move to specific preset positions. Events can also be used for activating hardware output, such as lights or sirens. See Overview of Events, Input & Output on page 102.

- **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 as well as when you want to receive notifications from the system. See Configure General Scheduling & Archiving on page 94 and Configure Camera-specific Schedules on page 96.

- **Configure Clients’ Access to XProtect Essential**
  A number of different client applications (see Overview of Clients on page 136) 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 110.

- **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 Quickly Add Users with Access to All Cameras on page 45, Add Individual Users on page 113, Add User Groups on page 115 and Configure User & Group Rights on page 115.

### Access the Management Application

You access the Management Application by double-clicking the Management Application desktop shortcut.

Alternatively, use Windows’ Start menu: Start > All Programs > Milestone XProtect Essential > Management Application.

Read more about the Management Application in the following.

### Language Selection

To change the language of the Management Application, 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 containing the available languages for the Management Application. Choose the relevant language you want to switch to and click OK. The Management Application must be restarted for the change of language to take effect.
Management Application

The Management Application is XProtect Essential’s server-side user interface; all management of your surveillance system is handled here. You access the Management application by double-clicking the Management Application desktop shortcut. Alternatively, use Windows’ Start menu: Start > All Programs > Milestone XProtect Essential > Management Application.

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’s dialogs, you simply apply them by clicking OK.
- If you made the changes in one of the Management Application’s summary tables, click the Apply button below the summary table.

Applying a configuration change means that the change is stored by XProtect Essential in a restore point (so that you can return to a working configuration if something goes wrong; read more on page 125), but applying a configuration change does not mean that the changes will take immediate effect on the surveillance system.

- To actually store your configuration change in XProtect Essential’s configuration file, click the Save Configuration button in the Management Application’s toolbar (or select File > Save from the menu). Your configuration changes will then take effect the next time XProtect Essential’s services (see page 109) are restarted.
- If you want your configuration changes to have immediate effect, XProtect Essential’s services must be restarted: Click the Save Changes and Restart Surveillance Services button in the Management Application’s toolbar (or select File > Save Changes and Restart Services from the menu).

IMPORTANT: While services are restarted, it will not be possible to view or record video. Restarting the services typically only takes some 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.

Change/Reset Behavior

You can change the way the Management Application behaves. For example, the Management Application will by default ask you to confirm many of your actions. If you find this annoying, you can change the Management Application’s behavior, 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 cameras, 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 in the Management Application’s toolbar.

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

Privacy Option Settings

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 being collected.

Furthermore, if you accepted, a setting makes it possible to turn the collection of information off or on as needed (see the following for details).

How Do I Disable Information Collection?
1. In the Management Application's toolbar, click Help, Privacy Options.
2. On the Privacy options tab, clear the Yes, I would like to improve Milestone Essential check box.
3. Click OK.

What Information Is Collected

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

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

The automatic collection of information can be disabled by either removing XProtect Essential or by disabling it using the Management Application (see earlier for details on how).

**How Is Information Collected?**

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.
Wizards

This chapter describes the wizards that guide you through common tasks in XProtect Essential. Wizards are a great advantage, but they typically only cover the most important of XProtect Essential’s many configuration options. For detailed descriptions of all of XProtect Essential’s configuration options, see the subsequent chapters in this manual.

- The Add Hardware Devices wizard (see the following) helps you add cameras and other hardware devices, such as video encoders, etc., to your XProtect Essential system. If microphones are attached to a hardware device, they are automatically added as well.
- The Configure Video and Recording wizard (see page 37) helps you quickly configure your cameras’ video and recording properties.
- The Adjust Motion Detection wizard (see page 43) helps you quickly configure your cameras’ motion detection properties.
- The Configure User Access wizard (see page 45) helps you quickly configure clients’ access to the XProtect Essential server as well as which users should be able to use clients.
- Finally, the Replace Hardware wizard (see page 47) helps you replace a hardware device—which you have previously added to and configured on your surveillance system—with a new one. This is relevant if you want to replace a physical camera on your network.

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 are allowed to use up to 26 cameras. Note that, if required, it is possible to add more cameras than you are allowed to use. If using 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:

- Express (recommended): Quickly scans your network for devices, and helps you quickly add them to your system. This method is quick and easy since it only scans for devices supporting device discovery, and only on the part of your network (subnet) where the XProtect Essential server itself is located. Device discovery is a method with which hardware devices make information about themselves available on the network. Based on such information, XProtect Essential can recognize relevant hardware devices on your network, and thus include, for example, cameras, but not printers, in the scan. 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 page 27.
- **Advanced**: Scans your network for hardware devices based on your specifications regarding required IP ranges, discovery methods, drivers, and device user names and passwords. See page 29.

- **Manual**: 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. See page 32.

- **Import from CSV file**: Lets you import data about cameras as comma-separated values from a file; an effective method if setting up several similar systems. See page 34.

### Express Method

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.

**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.

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 method** (see page 29) or **Manual method** (see page 32) instead.

When using the Express option, the wizard is divided into a number of pages:

### 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:

- 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.

- 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.

- 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.

- 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 in doubt about which password to use, ask yourself: Have you previously used a
web page to connect to the hardware device and view video? While you did this, were you
also able to configure camera settings, such as resolution, etc.? If you can answer yes to
both questions, you were in all likelihood using the hardware device’s administrator
account, in which case you will also know the password.

**Tip:** If you are still in doubt, look in the Device Pack Release Notes, available from the
Downloads section of www.milestonesys.com. This will show you the administrator account
user name for each supported hardware device. For obvious reasons it will not show you
the password.

- 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, then click **Next** again.

- The next wizard page will provide you with an overview, and ask you to select names for
cameras, etc.

**Overview and Names**

On the last page, the wizard provides you with a detailed overview, listing each camera and/or
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 are able to communicate with XProtect Essential. If required, you can disable
individual cameras or, microphones, and thus 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:

  - **Device type + number:** The default name format.
    Example: Camera 1

  - **Custom text - Device type + number:** Names will consist of a text of your choice (specified in the **Custom text** field) followed by a dash, type information and a number.
    Example: Airport Security - Camera 1

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

Hardware model - Device type + number: Names will consist of hardware device model information followed by a dash, type information and a number. Example: Axis P1311 - Camera 1

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

Hardware model - Address - Device type + number: Names will consist of hardware device model information followed by a dash, then the hardware device address, a dash, type information and a number. Example: Axis P1311 - 10.10.123.73 - Camera 1

Tip: Need other name formats? Remember you can change names manually by overwriting all or parts of them in the Name column. If you change camera names manually, remember that camera names must be unique, and must not contain any of the following special characters: < > & ” \ : * ? | [ ]

When ready, click Finish.

Advanced Method

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 a number of pages. All properties on a white background are editable; properties on a light blue background cannot be edited.

Device Discovery, IP Ranges, Drivers and Authentication

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:

- Start address: First IP address in required range.
- End address: Last IP address in required range. The start and end IP address may be identical, allowing you to only scan for a single hardware device.
- Use TCP port scanning: If scanning for hardware devices which support TCP/HTTP—most devices do—keep the check box selected.
- Perform scanning on port number(s): Port number(s) on which to scan. If you want to scan on more than one port number, separate them by commas (example: 80,88,90). If you want to scan on a range of port numbers, separate the first and last port number in the range by a colon (example: 80:90 will scan on all ports from 80 up to and including 90). You can also combine individual port numbers and ranges (example: 77,80:90,97,99).

Default is port 80. If your hardware devices are located behind a NAT-enabled router or a firewall, you may need to specify a different port number. When this is the case, also remember to configure the router/firewall so it maps the port and IP addresses used by the...
Now 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 the Select... button, then specify:

- **Detect**: Select drives 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.

Now you 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 is going to need that for each hardware device.

- **User name**: Select or type the user name required to access the administrator account on 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.

- **Password**: Specify the password required to access the administrator account.

  If different user name/password combinations are used across your hardware devices, make sure you add all required combinations.

  **Tip**: If in doubt about which user name/password to use, ask yourself: Have you previously used a web page to connect to the hardware device and view video? While you did this, were you also able to configure camera settings, such as resolution, etc.? If you can answer yes to both questions, you were in all likelihood using the hardware device’s administrator account, in which case you will also know the user name/password.

  **Tip**: If you are still in doubt, look in the Device Pack Release Notes, available from the Downloads section of www.milestonesys.com. This will show you the administrator account user name for each supported hardware device. For obvious reasons it will not show you the password.

- **Add**: Click to add user a name/password combination.

When ready, click Next.

**Detected and Verified Hardware Devices**

The wizard automatically scans required IP address ranges for hardware devices, and lists detected devices real-time as they are detected.

The scanning takes place in three tempi: first the express method (where the wizard quickly scans for devices supporting device discovery), then two more thorough methods. During the two thorough methods, the wizard continuously shows you which IP address it is scanning (Example: Now scanning 10.10.75.110).

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:

- 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.

- 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.

- 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.

- Click Next. The next wizard page will provide you with an overview, and ask you to select names for cameras, etc.

**Overview and Names**

On the last page, the wizard provides you with a detailed overview, listing each camera, microphone attached to the hardware devices.

- All cameras, etc. are by default enabled (selected in the Enable column). This means that they are able to communicate with XProtect Essential. If required, you can disable individual cameras or microphones, and thus 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:
  - **Device type + number**: The default name format.
    Example: Camera 1
  - **Custom text - Device type + number**: Names will consist of a text of your choice (specified in the Custom text field) followed by a dash, type information and a number.
    Example: Airport Security - Camera 1
  - **Address - Device type + number**: Names will consist of the hardware device address followed by a dash, type information and a number.
    Example: 10.10.123.73 - Camera 1
  - **Custom text - Address - Device type + number**: Names will consist of a text of your choice (specified in the Custom text field) followed by a dash, then the hardware device address followed by a dash, type information and a number.
    Example: Airport Security - 10.10.123.73 - Camera 1
  - **Hardware model - Device type + number**: Names will consist of hardware device model information followed by a dash, type information and a number.
    Example: Axis P1311 - Camera 1
  - **Hardware model - Custom text - Device type + number**: Names will consist of hardware device model information followed by a dash, then a text of your choice (specified in the Custom text field), a dash, type information and a number.
    Example: Axis P1311 - Airport Security - Camera 1
o **Hardware model - Address - Device type + number:** Names will consist of hardware device model information followed by a dash, then the hardware device address, a dash, type information and a number.
   Example: Axis P1311 - 10.10.123.73 - Camera 1

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

When ready, click Finish.

**Manual Method**

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 a number of pages:

**Hardware Device 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.

- **Use:** 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 Use box will automatically be selected later.

- **Address:** IP address or DNS host name of the hardware device.

- **Port:** Port number on which to scan. Default is port 80. If a hardware device is located behind a NAT-enabled router or a firewall, you may need to specify a different port number. When this is the case, also remember to configure the router/firewall so it maps the port and IP address used by the hardware device.

- **User name:** Select or type the user name required to access the administrator account on 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.

- **Password:** Password required for accessing the administrator account. A few hardware devices do not require user name/password for access; if such hardware devices are used in your organization, you can leave the field blank.
   **Tip:** If in doubt about which user name/password to use, ask yourself: Have you previously used a web page to connect to the hardware device and view video? While you did this, were you also able to configure camera settings, such as resolution, etc.? If you can answer yes to both questions, you were in all likelihood using the hardware device’s administrator account, in which case you will also know the user name/password.
   **Tip:** If you are still in doubt, look in the Device Pack Release Notes, available from the Downloads section of www.milestonesys.com. This will show you the administrator account
user name for each supported hardware device. For obvious reasons it will not show you the password.

- **Hardware Driver**: Ability to select which driver to use with the hardware device. Note that the default option is *Auto-detect hardware type*: XProtect Essential can itself find the right driver if you click the **Auto-detect** button.

- **Verified**: Read-only field indicating whether access to the hardware device has been verified. Hardware devices for which you have specified correct address, port, user name and password will be verified immediately if you use the auto-detect method. If you select drivers manually, access will be verified once you click **Next**.

**Tip**: If using the *Auto-detect* feature, you can enter information about other devices while the auto-detection goes on. Example: You enter information about one device, and use auto-detection to find the right driver for that device. While auto-detection for the first device takes place, you begin entering information about a second device. This can speed up things.

**Overview and Names**

On the last page, the wizard provides you with a detailed overview, listing each camera, microphone attached to the hardware devices.

- All cameras, etc. are by default enabled (selected in the *Enable* column). This means that they are able to communicate with XProtect Essential. If required, you can disable individual cameras or microphones, and thus 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:
  - **Device type + number**: The default name format.
    Example: Camera 1
  - **Custom text - Device type + number**: Names will consist of a text of your choice (specified in the *Custom text* field) followed by a dash, type information and a number.
    Example: Airport Security - Camera 1
  - **Address - Device type + number**: Names will consist of the hardware device address followed by a dash, type information and a number.
    Example: 10.10.123.73 - Camera 1
  - **Custom text - Address - Device type + number**: Names will consist of a text of your choice (specified in the *Custom text* field) followed by a dash, then the hardware device address followed by a dash, type information and a number.
    Example: Airport Security - 10.10.123.73 - Camera 1
  - **Hardware model - Device type + number**: Names will consist of hardware device model information followed by a dash, type information and a number.
    Example: Axis P1311 - Camera 1
  - **Hardware model - Custom text - Device type + number**: Names will consist of hardware device model information followed by a dash, then a text of your choice (specified in the *Custom text* field), a dash, type information and a number.
    Example: Axis P1311 - Airport Security - Camera 1
  - **Hardware model - Address - Device type + number**: Names will consist of hardware device model information followed by a dash, then the hardware device
address, a dash, type information and a number. Example: Axis P1311 - 10.10.123.73 - Camera 1.

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

When ready, click **Finish**.

**Import from CSV File Method**

This option lets you import data about hardware devices and cameras as comma-separated values (CSV) 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**.

**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, but note that the minimum required information is different depending on whether your server and cameras are online or offline.

**Cameras and Server Are Online**

If cameras and server are **online**, required information is:

- **HardwareAddress**
  IP address of the hardware device.

- **HardwarePort**
  Port to use for HTTP communication with the hardware device. Default is port 80.

- **HardwarePassword**
  Password for the hardware device’s administrator account. Most organizations use their own passwords rather than device manufacturers’ passwords.

**Camera and Server Are Offline**

If cameras and server are **offline**, required information is:

- **HardwareAddress**
  IP address of the hardware device.

- **HardwareMacAddress**
  MAC address of the hardware device. Examples of valid MAC address formats: 0011D81187A9, 0011d81187a9, 00:11:D8:11:87:A9, 00-11-D8-11-87-A9

- **HardwareDriverID**
  A numerical ID used for identifying which video device driver to use for the hardware device in question. For information about how to find the right ID for your devices, see the Hardware Driver IDs appendix on page 155.
• **HardwarePort**
  Port to use for HTTP communication with the hardware device. Default is port 80.

• **HardwarePassword**
  Password for the hardware device’s administrator account. For security reasons most organizations use their own passwords rather than device manufacturers' passwords.

**Optional Parameters**
You can furthermore include these optional parameters, regardless whether cameras and server are online or offline:

• **HardwareUserName** and **HardwarePassword**
  User name for the hardware device’s administrator account. If you do not specify a user name, XProtect Essential will use the device manufacturer's default user name for each hardware device. Many organizations use the hardware device manufacturers' default usernames for their hardware devices. If that is the case in your organization, there is no need to painstakingly type hardware device manufacturers' default user names as this can be a source of error; trust that XProtect Essential will know the manufacturers' default user names. Note that you must always specify a password (the HardwarePassword parameter) even when it is not necessary to specify user name.

If the extremely rare cases where the user name for a hardware device is [blank], you cannot use the CSV method, since the method interprets no password as "use the hardware device manufacturer’s default password." If the user name for a hardware device is [blank], use the wizard's Manual method instead; with the Manual method you can use a [blank] user name.

• **HardwareDeviceName**
  Name of the hardware device. Name must unique, and must not contain any of the following special characters: `< > & ' " \ / : * ? | [ ]`

• **CameraName[number]**
  Name of the camera. Must appear as CameraName1, CameraName2, etc. in the header line since a hardware device can potentially have more than one camera attached. Names must unique, and must not contain any of the following special characters: `< > & ' " \ / : * ? | [ ]`

• **CameraShortcut[number]**
  Number for keyboard shortcut access to the camera in the Smart Client. Must appear as CameraShortcut1, CameraShortcut2, etc. in the header line since a hardware device can potentially have more than one camera attached. A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits.

• **PreBufferLength[optional number]**
  Required length (in seconds) of pre-recording. If specified as, for example, PreBufferLength1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

• **PostBufferLength[optional number]**
  Required length (in seconds) of post-recording. If specified as, for example, PostBufferLength1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

• **RecordingPath[optional number]**
  Path to the folder in which a camera’s database should be stored. If specified as, for example, RecordingPath1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

• **ArchivePath[optional number]**
  Path to the folder in which the camera's archived recordings (see page 86) should be
stored. Remember that an archiving path is only relevant if not using dynamic paths for archiving (see page 62). If specified as, for example, ArchivePath1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **RetentionTime[optional number]**
  Required retention time (in minutes). Remember that retention time is the total of recording time plus archiving time. If specified as, for example, RetentionTime1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **MjpegLiveFrameRate[optional number]**
  Required MJPEG live frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If specified as, for example, MjpegLiveFrameRate1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **MjpegRecordingFrameRate[optional number]**
  Required MJPEG recording frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If you need to specify a value which includes a decimal separator, use the full stop character (example: 7.62). If specified as, for example, MjpegRecordingFrameRate1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **MotionSensitivity[optional number]**
  A value between 0-256; corresponds to using the Sensitivity slider when configuring motion detection settings in the Management Application. If specified as, for example, MotionSensitivity1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **MotionDetectionThreshold[optional number]**
  A value between 0-10000; corresponds to using the Motion slider when configuring motion detection settings in the Management Application. If specified as, for example, MotionDetectionThreshold1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **MotionDetectionInterval[optional number]**
  Lets you specify how often motion detection analysis should be carried out on video from the camera. Specified in milliseconds. The interval is applied regardless of the camera’s frame rate settings. If specified as, for example, MotionDetectionInterval1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

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:

---

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HardwareAddress</td>
<td>HardwareUsername</td>
</tr>
<tr>
<td>2</td>
<td>192.168.200.220</td>
<td>AdminAccountUserName:0p6eCR3tpa5SwOrd</td>
</tr>
<tr>
<td>3</td>
<td>192.168.200.221</td>
<td>AdminAccountUserName:TOPsecretPASSWord</td>
</tr>
<tr>
<td>4</td>
<td>192.168.200.222</td>
<td>RootAccountUserName:TOPsEcReTpAsSwOrd</td>
</tr>
<tr>
<td>5</td>
<td>192.168.200.223</td>
<td>AdminAccountUserName:TOPsScR3tP5sSwOrd</td>
</tr>
</tbody>
</table>

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;charset"; is interpreted as cam;charset
- ""camera""; is interpreted as "camera"
- ";"; is interpreted as an empty string
- ...; " cam" era " ... is interpreted as | cam| era | (where | 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|era"; is not valid as you cannot nest quotes
- cam"era"; is not valid as there are characters outside the quotes

Configure Video and Recording Wizard

The Configure Video and Recording wizard helps you quickly configure your cameras’ video and recording properties. The wizard is divided into a number of pages. All properties on a white background are editable; properties on a light blue background cannot be edited.

Video Settings and Preview

Video settings typically let you control bandwidth, brightness, compression, contrast, resolution, rotation, etc.
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 the **Open Settings Dialog** button 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 thus 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).

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 (see page 95).

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. Say you have 50 cameras and you want a particular online schedule on all of them. Instead of having to enter the same piece of information 50 times, you can simply enter it once in the template, and then apply the template to the 50 cameras with only two clicks.

- **Apply template**: Lets you select which cameras you want to apply the template for. You then use **Apply template on selected cameras** (see description in the following) to actually apply the template.

  **Tip:** To select all cameras in the list, click the **Select All** button.
- **Select All**: Click button to select all cameras in the Apply Template column.

- **Clear All**: Click button to clear all selections in the Apply Template column.

- **Apply template on selected cameras**: Lets you apply the value from the template to selected cameras.

## Live and Recording Settings (Motion-JPEG Cameras)

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

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

**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.

- **Frame Rate**: Frame rate for video from the camera. Select required number of frames per second.

- **Record on**: Lets you select under which conditions video from the camera should be recorded:
  - **Always**: Record whenever the camera is enabled and scheduled to be online (see page 97). The latter allows for time-based recording.
  - **Never**: Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera.
  - **Motion Detection**: Select this to record video in which motion (see page 77) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.
  - **Event**: Only available for individual cameras which have already been configured to be able to record on events; this option is never available in the template. Select this to use the camera’s existing events-based recording configuration. Read more about events on page 102.

- **Motion Detection & Event**: Only available for individual cameras which have already been configured to be able to record on events; this option is never available in the template. Select this to use the camera’s existing motion- and events-based recording configuration.

- **Pre-recording**: You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Remember to specify required number of seconds in the neighboring column.

- **Seconds [of pre-recording]**: Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving times.
Post-recording: You can store recordings from periods following detected motion and/or stop events. Select check box to enable this feature. Remember to specify required number of seconds in the neighboring column.

Seconds [of post-recording]: Specify the number of seconds for which you want to record video from after recording stop conditions (that is motion or stop event) are met. Usually, only some seconds of post-recording is required, but you can specify up to 65535 seconds of post-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long post-recording time, you can potentially run into a scenario where your post-recording time spans scheduled or unscheduled archiving times (you define these on one of the wizard’s next pages). That can be problematic since post-recording does not work well during archiving.

The template can help you configure similar properties quickly. Say you have 50 cameras and you want a particular frame rate on all of them. Instead of having to enter the same piece of information 50 times, you can simply enter it once in the template, and then apply the template to the 50 cameras with only two clicks.

Apply template: Lets you select which cameras you want to apply the template for. You then use Apply template on selected cameras (see description in the following) to actually apply the template.

Tip: To select all cameras in the list, click the Select All button.

Select All: Click button to select all cameras in the Apply Template column.

Clear All: Click button to clear all selections in the Apply Template column.

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

Live and Recording Settings (MPEG Cameras)

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

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

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.

Live Frame Rate: Frame rate for live video from the camera. Select required number of frames per second.

Record on: Lets you select under which conditions video from the camera should be recorded:

- Always: Record whenever the camera is enabled and scheduled to be online (see page 97). The latter allows for time-based recording.
Never: Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera.

Motion Detection: Select this to record video in which motion (see page 77) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.

Event: Only available for individual cameras which have already been configured to be able to record on events; this option is never available in the template. Select this to use the camera's existing events-based recording configuration. Read more about events on page 102.

Motion Detection & Event: Only available for individual cameras which have already been configured to be able to record on events; this option is never available in the template. Select this to use the camera's existing motion- and events-based recording configuration.

- Pre-recording: You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Remember to specify required number of seconds in the neighboring column.

- Seconds [of pre-recording]: Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving times (you define these on one of the wizard’s next pages). That can be problematic since pre-recording does not work well during archiving.

- Post-recording: You can store recordings from periods following detected motion and/or stop events. Select check box to enable this feature. Remember to specify required number of seconds in the neighboring column.

- Seconds [of post-recording]: Specify the number of seconds for which you want to record video from after recording stop conditions (that is motion or stop event) are met. Usually, only some seconds of post-recording is required, but you can specify up to 65535 seconds of post-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long post-recording time, you can potentially run into a scenario where your post-recording time spans scheduled or unscheduled archiving times (you define these on one of the wizard’s next pages). That can be problematic since post-recording does not work well during archiving.

The template can help you configure similar properties quickly. Say you have 50 cameras and you want a particular frame rate on all of them. Instead of having to enter the same piece of information 50 times, you can simply enter it once in the template, and then apply the template to the 50 cameras with only two clicks.

- Apply template: Lets you select which cameras you want to apply the template for. You then use Apply template on selected cameras (see description in the following) to actually apply the template.

  Tip: To select all cameras in the list, click the Select All button.

- Select All: Click button to select all cameras in the Apply Template column.

- Clear All: Click button to clear all selections in the Apply Template column.

- Apply template on selected cameras: Lets you apply the value from the template to selected cameras.
Drive Selection

Specify which drives you want to store cameras' recordings on. You can specify separate drives/paths for recording and archiving.

**What is archiving?** Archiving—an integrated and automated feature—helps you store recordings beyond the capabilities of XProtect Essential’s standard database. Archiving thus maximizes storage capacity and minimizes risk. For more detailed information, see page 86.

- **Drive**: Letter representing the drive in question, for example C:.
- **Purpose**: Lets you select what you want to use the drive for:
  - **Not in use**: Do not use the drive.
  - **Recording**: Only available if the drive is a local drive on the XProtect Essential server; network drives cannot be used for recording. Use the drive for storing recordings in XProtect Essential’s regular database.
  - **Archiving**: Use the drive for archiving. For archiving, it is generally a good idea to use a drive which has plenty of space.
    - **Tip**: With dynamic path selection for archives (see description in the following), you do not have to worry about drive space.
  - **Rec. & Archiving**: Only available if the drive is a local drive on the XProtect Essential server; network drives cannot be used for recording. Use the drive for storing recordings in XProtect Essential’s regular database as well as for archiving.

- **Recording Path**: Path to the folder in which to store recordings in XProtect Essential’s regular database. Default is [drive letter]:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You are only able to specify a path to a folder on the selected drive (which must be a local drive). If you change the recording path, and there are existing recordings at the old location, you will be asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them.

- **Archiving Path**: Only editable if not using dynamic path selection for archives (see description in the following). Path to the folder in which archived recordings should be stored. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to 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.

- **Total Size**: Total size of the drive.

- **Free Space**: Amount of unused space left on the drive.

- **Dynamic path selection for archives**: If using this option (highly recommended), you should select a number of different local drives for archiving. If the path containing the XProtect 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.
**Archiving schedule**: Lets you 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. As a rule of thumb, the more you expect to record, the more often you should archive.

## Recording and Archiving Settings

Select recording and archiving paths for each individual camera.

**What is archiving?** Archiving—an integrated and automated feature—helps you store recordings beyond the capabilities of XProtect Essential's standard database. Archiving thus maximizes storage capacity and minimizes risk. For more detailed information, see page 86.

- **Recording Path**: Path to the folder in which to store the camera's recordings in XProtect Essential's regular database. Default is C:\MediaDatabase. If you specified several recording paths on the wizard’s previous page, you can select between those paths.

- **Archiving Path**: Path to the folder in which archived recordings should be stored. Only relevant if not using dynamic path selection for archives.

- **Retention Time**: Total amount of time for which you want to keep recordings from the camera (that is recordings in XProtect Essential’s database as well as any archived recordings).

  Note that the retention time covers the total amount of time you want to keep recordings for; in earlier XProtect Essential versions time limits were specified separately for the database and archives.

The **template** can help you configure similar properties quickly. Say you have 50 cameras and you want a particular recording path for all of them. Instead of having to enter the same piece of information 50 times, you can simply enter it once in the template, and then apply the template to the 50 cameras with only two clicks.

- **Apply template**: Lets you select which cameras you want to apply the template for. You then use **Apply template on selected cameras** (see description in the following) to actually apply the template.

  **Tip**: To select all cameras in the list, click the **Select All** button.

- **Select All**: Click button to select all cameras in the **Apply Template** column.

- **Clear All**: Click button to clear all selections in the **Apply Template** column.

- **Apply template on selected cameras**: Lets you apply the value from the template to selected cameras.

## Adjust Motion Detection Wizard

The Adjust Motion Detection wizard helps you quickly configure your cameras’ motion detection properties. The wizard is divided into two pages.
Exclude Regions

Exclude region 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 (see page 109) when configuring such devices for motion detection and PTZ. See also View Video from Cameras in Management Application on page 84.

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 exclude regions in the preview, which is divided into small sections by a grid.

Do the following to define its exclude regions:

1. To make the grid visible, select the **Show Grid** check box.

2. 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 may be advantageous if you want to disable motion detection in most areas of the preview, in which case you can simply 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.

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.

Motion Detection

Motion detection is a key element in most surveillance systems. Depending on your further configuration, motion detection settings may determine when video is recorded (that is saved on the surveillance system server), when notifications are sent, when output (such as lights or sirens) is triggered, etc. Time spent on finding the best possible motion detection settings for each camera may thus help you later avoid unnecessary recordings, notifications, etc. Depending on the physical location of your cameras, it is often a good idea to test motion detection settings under different physical conditions (day/night, windy/calm weather, etc.).

Depending on your needs, you can configure motion detection settings individually for each camera, or for several cameras in one go. Use the list in the left side of the wizard window to select cameras; to select several cameras at a time, press CTRL or SHIFT on your keyboard 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. When you have selected one or more cameras, do the following to configure their motion detection settings:

1. Note any green areas in the preview. Green areas are areas with motion.
2. Adjust the Sensitivity slider so that irrelevant background noise is filtered out, and only real motion is shown in green.

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.

**Tip:** Technically, 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. If you find the concept of sensitivity difficult to grasp, try dragging the slider to the left: The more you drag the slider to the left, the more of the preview becomes green. This is because with a high sensitivity even the slightest change in a pixel will be regarded as motion.

3. Adjust the Motion slider so that motion detection is only triggered by the required level of motion. The selected motion level is indicated by the black vertical line in the Motion level bar above the sliders. The black vertical line serves as a threshold: When motion is above (that is to the right of) the selected level, the bar changes color from green to red, indicating a positive motion detection.

As an alternative to using the slider, you may specify a value between 0 and 10000 in the field next to the slider to control the motion setting.

**Tip:** Technically, the slider determines how many pixels must change before it is regarded as motion. The more you drag the slider to the left, the fewer pixels must change before you have a positive motion detection. Thus, as a rule of thumb, the more you drag the slider to the left, the more positive motion detections you are likely to get since less change will be required to trigger a positive motion detection. The number of positive motion detections may subsequently affect the amount of video you record, the amount of notifications you receive, etc.

Motion detection is vital on most surveillance systems, but also consumes system resources on the surveillance server. The next two settings enable you to specify settings which can help lower the amount of system resources used on motion detection.

4. In the Detection interval field, you are able to specify how often motion detection analysis should be carried out on video from the camera. Default is every 240 milliseconds (that is close to once every quarter of a second). The interval is applied regardless of your cameras’ frame rate settings.

5. In the Detection resolution field, you are able to specify if the full image or only a selected percentage of the image should be analyzed. By analyzing, for example 25%, only every fourth pixel is analyzed instead of all pixels, reducing the needed resources but also offering less accurate motion detection.

**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 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.
When using the wizard, all users you add will have access all to cameras, including any new cameras added at a later stage. If this is not acceptable, specify access settings (see page 110), users (see page 113) and user rights (see page 115) separately. Also note that you cannot add users to groups (see page 115) through the wizard.

The wizard is divided into a number of pages:

**Server Access Settings**

- **Server name**: 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.
- **Local port**: Port number to use for communication between clients and the surveillance server. The default port number is 80; you can change the port number if port 80 is used for other purposes in your organization.
- **Character encoding (language)**: Select required language/character set. Example: If the surveillance server runs a Japanese version of Windows, select Japanese. Provided access clients also use a Japanese version of Windows, this will ensure that the correct language and character encoding is used in clients’ communication with the server.
- **Internet access**: Select the check box if the server should be accessible from the internet through a router or firewall. If selecting 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.
- **Internet address**: Lets you specify a public IP address or hostname for use when the XProtect Essential server should be available from the internet.
- **Internet port**: Lets you 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 port 80 is used for other purposes in your organization.

**Basic and 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 you want to add 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, turning of simple file sharing is 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 to disable file sharing. Click OK.

Add Windows users the following way:

1. Click the Add Windows User... button 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 the Enter the object names to select box, type the required user name(s), then use the Check Names feature to verify that the user name(s) you have entered are correct. If typing several user names, separate each name with a semicolon. Example: Brian; Hannah; Karen; Wayne.

3. When ready, click OK.

   When a user who has been added this way 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. Example of an incorrectly specified user name: PC001/USER001. The user should of course still specify a password and any required server information.

**Access Summary**

The access summary simply lists which cameras your users will have access to. When using the wizard, all users you have added will have access all to cameras, including any new cameras added at a later stage. You can, however, limit individual users’ access to cameras by changing their individual rights (see page 115).

**Replace Hardware Device Wizard**

The Replace Hardware wizard helps you 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. The Replace Hardware Device wizard 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
You access the Replace Device Hardware wizard from the Management Application’s navigation pane: Expand Advanced Configuration, expand Hardware Devices, right-click the hardware device you want to replace, and select Replace Hardware Device. You can access also the wizard when dealing with a hardware device’s Network, Device Type & License properties (see page 56).

The wizard is divided into two pages:

**New Hardware Device Information**

First specify details about the new hardware device:

- **Hardware device address**: IP address or host name of the new hardware device.

- **Hardware device port**: Port number to use for communicating with the hardware device. Default is port 80. If the new 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 addresses used by the new hardware device.

- **User name**: User name for the hardware device’s administrator account. Many organizations use the hardware device manufacturer’s default user names for their hardware devices. If that is the case in your organization, select <default> (do not type a manufacturer’s default user name as this can be a source of error; trust that XProtect 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.

- **Password**: Password required for accessing the new hardware device’s administrator account.

  **Tip**: If in doubt about which user name/password to use, ask yourself: Have you previously used a web page to connect to the hardware device and view video? While you did this, were you also able to configure camera settings, such as resolution, etc.? If you can answer yes to both questions, you were in all likelihood using the hardware device’s administrator account, in which case you will also know the user name/password.

  **Tip**: If you are still in doubt, look in the Device Pack Release Notes, available from the Downloads section of www.milestonesys.com. This will show you the administrator account user name for each supported hardware device. For obvious reasons it will not show you the password.

Then specify which device driver to use for the new hardware device. You can do this in two ways:

- By selecting the required video device driver in the **Hardware device type** list, then clicking the Auto-detect/Verify Hardware Device Type button to verify that the driver matches the hardware device.

  - or -

- By just clicking the Auto-detect/Verify Hardware Device Type button 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 ready, click **Next**.
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 page 86) will be renamed to reflect the new hardware device’s MAC address and video channels. The rights (see page 115) 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.
5. When ready, restart the Recording Server service (see page 109). The hardware replacement will not be evident in clients until you restart the Recording Server service.
Licenses

Overview of 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.

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 will not send data to the surveillance system. We therefore recommend that you activate your licenses (see page 52) before you make final adjustments to your system and its devices.

Tip: When 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. Select the required hardware device, right-click the relevant camera, and then select Enable or Disable.

Which Devices Require a License?

You need licenses for the number of device channels—typically cameras or dedicated input/output boxes—you want to run on your XProtect Essential system. 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.

Depending on your current number of licenses you might be able to get more licenses as your surveillance system grows. See Getting Additional Licenses in the following.

Replacing Cameras

You can replace a camera licensed in the XProtect Essential system with a new camera and have the new camera activated and licensed instead.

The total number of purchased device channels corresponds to the total number of cameras able to run on the surveillance system simultaneously. If you remove a camera from a recording server, you also free a license.

When replacing a camera, you must use the Management Application’s Replace Hardware Device wizard (see page 48) to map all relevant databases of cameras, microphones, inputs, outputs, etc. When done, remember to activate the license.

Viewing 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:
- **Hardware Device Name:** Hardware devices (typically cameras but could also be dedicated input/output boxes).

- **License:** Licensing status of your hardware devices. Can be either Licensed, [number of] day(s) grace, Trial, or Expired.

- **Video Channels:** Number of available video channels on your hardware devices.

- **Licensed Channels:** Number of video channels—on each of your hardware devices—for which you have a license.

- **Microphone Channels:** Number of available microphone channels on your hardware devices.

- **Address:** http addresses of your hardware devices.

- **WWW:** Links to http addresses of your hardware devices.

- **Port:** Port used by your hardware devices.

- **Device Driver:** Names of device drivers associated with your hardware devices.

You can activate licenses (see page 52) 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.

### Getting Additional Licenses

**Want to add—or have already added—more device channels than you currently have licenses for?** In that case, you must buy additional licenses before the cameras will be able to send data to your XProtect Essential system.

To get additional licenses for your XProtect Essential system visit www.milestonesys.com to log into the software registration service center.

When your license file (.lic) is updated, you can activate your licenses. See **Activate Licenses** for more information on activating.

### Manage 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 installing your system. Furthermore, in order to get your permanent license, you should register your SLC before you activate licenses.

When SLC registration is done, you can activate your licenses in two ways: **online** or **offline**.

**Tip:** If the computer running the Management Application has internet access, use online activation for a quick and convenient activation procedure.

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.

Register SLC

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

SLC registration is brief and easy:

1. Go to the Milestone Systems website at www.milestonesys.com, and click the Software registration link in the menu.
2. Log in to the Software Registration Service Center with your user name (e-mail address) and password.
   
   Tip: If you have not used the Software Registration Service Center before, click the New to the system? link, and follow the instructions for registering yourself as a user, then log in to the Software Registration Service Center using your registered user name and password.

1. In the Software Registration Service Center, click the Add SLC link.
2. Type your SLC. Confirm that you want to add the SLC to your account, and click OK.
3. Once your SLC has been added, click the Main menu link.
4. Click the Logout link to log out of the Software Registration Service Center.

   Tip: If you plan to use online activation when activating your licenses, make sure you use the same user name (e-mail address) and password for the activation as you did you when registering the SLC.

Activate License - Online

Precondition
Add at least one device (see page 26) to your XProtect Essential system.

This will start 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 click OK.
2. Next:
   - If you are an existing user, enter your user name and password to log in to 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 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.

5. Your license file (.lic) is now updated and permanent (updates are visible in your Hardware Device Summary table, see page 51).

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

**Online Activation Error Messages**

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

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

**Activate License - Offline**

**Precondition**
Add at least one device (see page 26) to your XProtect Essential system.

This will start 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 location for the license request (.lrq) file (automatically generated by XProtect Essential). If the computer you are working from 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 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.
   - Under *Current SLCs*, select the SLC.
   - In the menu for SLC properties, use the *Upload LRQ* function to upload the generated .lrq file.
How long will this process take? After uploading the .lrq file, you will immediately receive an e-mail with the updated license file.

4. Next, you will 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 using both step 1 and 2 in this process each time you add a new device.

**Activate License after Grace Period**

If the grace period is exceeded before activation, all cameras that are not activated within the given period will become unavailable and will not be able to 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 will not be removed from the Management Application if a license is activated too late.

**Change SLC**

If you—for some reason—need to change your SLC and 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**.
Hardware Devices

You add cameras and other hardware devices, such as video encoders, Digital Video Recorders, etc., to your XProtect Essential system through the Add Hardware Devices wizard (see page 26). If microphones are attached to a hardware device, they are automatically added as well.

You are allowed to 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 using 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.

Configuration

Once you have added hardware devices, 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 fisheye 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 & License, PTZ Device, and Fisheye properties as required. All of the properties are described in the following.
3. Save your configuration changes by clicking the Save Configuration button in the Management Application’s toolbar.

Name and Video Channels

- **Hardware name**: Name of the hardware device as it will appear in the Management Application. If required, you can overwrite the existing hardware device name with a new one. Hardware device names must be unique, and must not contain any of the following special characters: < > & * " / : * ? | [ ]

- **Video channel # enabled**: Lets you 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.

**Why are some of the channels unavailable?** This will be the case if 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 will only be able to 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

- **Address**: IP address or host name of the hardware device.
- **HTTP port**: Port to use for HTTP communication with the hardware device. Default is port 80. To use the default port, select *Use default HTTP port*.

- **FTP port**: Port to use for FTP communication with the hardware device. Default is port 21. To use the default port, select *Use default FTP port*.

- **User name**: User name for the hardware device’s administrator account. Many organizations use the hardware device manufacturer’s default user names for their hardware devices. If that is the case in your organization, select `<default>` (do not type a manufacturer’s default user name as this can be a source of error; trust that XProtect 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.

- **Password**: Password for the hardware device’s administrator account, a.k.a. the root password.

- **Hardware type**: Read-only field displaying the type of video device driver used for communication with the hardware device.

- **Serial number (MAC address)**: Read-only field displaying the serial number of device. The serial number is usually identical to the 12-character hexadecimal MAC address of the hardware device (example: 0123456789AF).

- **License information**: The current license status for the hardware.

- **Replace Hardware Device**: Opens a wizard (see page 47), 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: finding the DLK for the new hardware device, deciding what to do with recordings from cameras attached to the old hardware device, etc.

### PTZ Device

The *PTZ Device* properties are only available if configuring video encoder hardware devices on which the use of PTZ (Pan/Tilt/Zoom) cameras is possible.

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

- **PTZ type on COM#**: If a PTZ camera is controlled through the COM port (a.k.a. serial port) in question, select the required option. Options are device-specific, depending on which PTZ protocols are used by the device in question. If no PTZ cameras are controlled through the COM port in question, select *None*.

  **Some of the options concern absolute and relative positioning. What is that?**

  Absolute positioning is when the PTZ camera is controlled based on a single fixed position, against which all other positions are measured. Relative positioning is when the PTZ camera is controlled relative to its current position.

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

- **Type**: Lets you select whether the camera on the selected camera channel is fixed or moveable:
  - **Fixed**: Camera is a regular camera mounted in a fixed position
  - **Moveable**: Camera is a PTZ camera

- **Port**: Available only if Moveable is selected in the Type column. Lets you select which COM port on the video encoder to use for controlling the PTZ camera.

- **Port Address**: Available only if Moveable is selected in the Type column. Lets you specify port address of the camera. The port address will normally be 1. If using daisy chained PTZ cameras, the port address will identify each of them, and you should verify your settings with those recommended in the documentation for the camera.

### Use Dedicated Input/Output Devices

It is possible to add a number of dedicated input/output (I/O) hardware devices to XProtect Essential. For information about which I/O hardware devices are supported, see the release notes.

When such I/O hardware devices are added, 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 I/O hardware devices can be used in your events-based system setup in the same way as a camera.

When using some I/O hardware devices it is necessary for the surveillance system to regularly check the state of the hardware devices' input ports in order 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 XProtect Essential's general ports & polling properties (see page 103). 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.

### Replace a Hardware Device

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.

The Replace Hardware Device wizard (see page 47) 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

You access the replace Hardware wizard from the Management Application’s navigation pane: Expand **Advanced Configuration**, expand **Hardware Devices**, right-click the hardware device you want to replace, and select **Replace Hardware Device**.
You can access also the wizard when dealing with a hardware device’s Network, Device Type & License properties (see page 56).

**Delete a Hardware Device**

**IMPORTANT:** Deleting a hardware device will not only delete all cameras and microphones attached to the hardware device. It 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 in the Management Application’s toolbar.

4. Restart the Recording Server service (see page 109).

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

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 you want to disable, and select *Disable*.

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

4. Restart the Recording Server service (see page 109).
Cameras and Recordings

You add cameras and other hardware devices, such as video encoders, etc., to your XProtect Essential system through the Add Hardware Devices... wizard (see page 26). If microphones are attached to a hardware device, they are automatically added as well.

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 & Recording Wizard or page 37 and Adjust Motion Detection Wizard on page 43.

- **General**: Lets you specify video, recording and shared settings (such as dynamic archiving paths and whether audio should be recorded or not) for all your cameras.
  
  1. In the Management Application's navigation pane, expand Advanced Configuration, right-click Cameras and Storage Information, and select Properties.
  
  2. Specify properties as required for Recording & Archiving Paths (see page 61), Dynamic Path Selection (see page 62), Video Recording (see page 63), Manual Recording (see page 65), Frame Rate – MJPEG (see page 65), Frame Rate – MPEG (see page 67), Audio Selection (see page 68), Audio Recording (see page 69) and Storage Information (see page 69). When ready, click OK.
  
  3. Save your configuration changes by clicking the Save Configuration button in the Management Application's toolbar.

- **Camera-specific**: Lets you specify video, recording and camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for each individual camera.
  
  6. In the Management Application's navigation pane, expand Advanced Configuration, and expand Cameras and Storage Information.
  
  7. Right-click the required camera, and select Properties.
  
  8. Specify properties as required for General (see page 70), Video (see page 71), Audio (see page 72), Recording (see page 73), Recording Properties & Archiving Paths (see page 74), Event Notification (see page 75), Output (see page 76), Motion Detection & Exclude Regions (see page 77), Privacy Masking (see page 80) and—if applicable—Fisheye (see page 79), PTZ Preset Positions (see page 81), and PTZ on Event (see page 83).
  
  9. Save your configuration changes by clicking the Save Configuration button in the Management Application's toolbar.

**General Recording and Storage Configuration**

When you configure video and recording, you are able to specify certain properties for many cameras in one go. Either simply in order to speed up things, or because the properties in question are shared by all cameras rather than specific to individual cameras. To specify video, recording and shared settings (such as dynamic archiving paths and whether audio should be recorded or not) for all your cameras:
1. In the Management Application’s navigation pane, expand Advanced Configuration, right-click Cameras and Storage Information, and select Properties.

2. Specify properties as required for Recording & Archiving Paths, Dynamic Path Selection, Video Recording, Frame Rate - MJPEG, Frame Rate - MPEG, Audio Selection, and Audio Recording. All of the properties are described on the following pages. When ready, click OK.

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

**Recording and Archiving Paths**

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

- **Template:** The template can help you configure similar properties quickly. Say you have 50 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 50 times, you can simply enter them once in the template, and then apply the template to the 50 cameras with only two clicks.

- **Apply Template:** Lets you select which cameras you want to apply the template for. You then use one of the two Set buttons (see descriptions in the following) to actually apply the template.

  **Tip:** To select all cameras in the list, click the Select All button.

- **Camera Name:** Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: < > & ‘ " \ / : * ? | [ ]

- **Shortcut:** Users of the Smart Client can take advantage of keyboard shortcuts, some of which let the users toggle between viewing different cameras. Such shortcuts include numbers which are used to identify each camera. Shortcut numbers must be unique for each camera. A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits. Examples of correct camera shortcut numbers: 3, 12345678. Examples of incorrect camera shortcut numbers: Cam#3, 123456789. More information about using the keyboard shortcuts is available in the separate documentation for the Smart Client. In other applications, such as the Remote Client, the camera shortcut numbers cannot be used.

- **Recording Path:** Path to the folder in which the camera’s database should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You are only able to specify a path to a folder on a local drive. You cannot specify a path to a network drive. The reason for this limitation is that if you were using a network drive, it would not be possible to save recordings if the network drive became unavailable. If you change the recording path, and there are existing recordings at the old location, you will be asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them.

  **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras’ databases across several drives.

- **Archiving Path:** Only editable if not using dynamic paths for archiving (see page 86). Path to the folder in which the camera’s archived recordings should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse icon next to the required drive.
You can only specify a path to 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 moving archived recordings, XProtect Essential will also archive what is currently in the camera’s database; in case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.

- **Retention Time**: Total amount of time for which you want to keep recordings from the camera (that is recordings in the camera’s database as well as any archived recordings). Default is 30 days.

Note that the retention time covers the total amount of time you want to keep recordings for; in earlier XProtect Essential versions time limits were specified separately for the database and archives.

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

- **Select All**: Click button to select all cameras in the Apply Template column.

- **Clear All**: Click button to clear all selections in the Apply Template column.

- **Set selected template value on selected cameras**: Lets you apply one or more selected values from the template (rather than all values) to selected cameras.

<table>
<thead>
<tr>
<th>Recording Path</th>
<th>Archiving Path</th>
<th>Retention Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\MedaBase</td>
<td>D:\uria\ideoarchive</td>
<td>1 Days</td>
</tr>
</tbody>
</table>

Example: Only the selected values are applied using this method. To select more than one value press CTRL while selecting.

- **Set all template values on selected cameras**: Lets you apply all values from the template to selected cameras.

**Dynamic Path Selection**

When you configure video and recording, you can specify certain properties for many cameras in one go. In the case of Dynamic Path Selection, it is simply because the properties are shared by all cameras.

With dynamic paths for archiving (see page 86), 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.

- **Enable dynamic path selection archives**: Enables the use of dynamic path selection, allowing you to select which paths you want to use. The list of selectable paths initially represents all drives on the server, both local and mapped drives. You can add further...
paths with the *New path* feature below the list.

- **Use:** Lets you select particular paths for use as dynamic archiving paths. Also lets you select a previously manually added path for removal (see description of *Remove* button in the following).

- **Drive:** Indicates which drive the path belongs on.

- **Path:** Path to use as dynamic archiving path.

- **Drive Size:** Total amount of space on the drive, that is free space as well as used space.

- **Free Space:** Amount of free space available on the drive in question.

- **New path:** Lets you specify a new path, and add it to the list using the *Add* button. Paths must be reachable by the surveillance system server, and you must specify the path using the UNC (Universal Naming Convention) format, example: `\server\volume\directory\`. When the new path is added, you can select it for use as a dynamic archiving path.

- **Add:** Lets you add the path specified in the *New path* field to the list.

- **Remove:** Lets you 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

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 page 73).

- **Template:** The template can help you configure similar properties quickly. Say you have 50 cameras and you want 10 seconds of pre-recording on all of them. Instead of having to enter the same piece of information 50 times, you can simply enter it once in the template, and then apply the template to the 50 cameras with only two clicks.

- **Apply Template:** Lets you select which cameras you want to apply the template for. You then use one of the two *Set* buttons (see descriptions in the following) to actually apply the template.

  **Tip:** To select all cameras in the list, click the *Select All* button.

- **Camera Name:** Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: `< > & * " \ / : * ? | [ ]`

- **Dual Stream:** Allows you to check if dual streaming is enabled on the camera(s). Note that the information is read-only. For cameras that support dual streaming, this can be enabled/disabled as part of individual cameras’ *Video* properties.

- **Record on:** Lets you select under which conditions video from the camera should be recorded:
- **Always:** Record whenever the camera is enabled and scheduled to be online (see page 97). The latter allows for time-based recording.

- **Never:** Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera.

- **Motion Detection:** Select this to record video in which motion (see page 77) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.

- **Event:** Select this to record video when an event occurs and until another event occurs. Use of recording on event requires that events (see page 102) have been defined, and that you select start and stop events in the neighboring columns.

  **Tip:** If you have not yet defined any suitable events, you can quickly do it: Use the Configure events list, located in the bottom left corner of the window.

- **Motion Detection & Event:** Select this to record video in which motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.

- **Start Event:** Use when recording on Event or Motion Detection & Event. Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).

- **Stop Event:** Select required stop event. Recording will end when the stop event occurs (or later if using post-recording; see the following).

- **Pre-recording:** You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Remember to specify required number of seconds in the neighboring column.

  **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.

  **Seconds [of pre-recording]:** Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving times (read more about archiving on page 86). That can be problematic since pre-recording does not work well during archiving.

- **Post-recording:** You can store recordings from periods following detected motion and/or stop events. Select check box to enable this feature. Remember to specify required number of seconds in the neighboring column.

  **Seconds [of post-recording]:** Specify the number of seconds for which you want to record video from after recording stop conditions (that is motion or stop event) are met. Usually, only some seconds of post-recording is required, but you can specify up to 65535 seconds of post-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long post-recording time, you can potentially run into a scenario where your post-recording time spans scheduled or unscheduled archiving times. That can be problematic since post-recording does not work well during archiving.
- **Camera**: Click the Open button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.

- **Select All**: Click button to select all cameras in the Apply Template column.

- **Clear All**: Click button to clear all selections in the Apply Template column.

- **Set selected template value on selected cameras**: Lets you apply only a selected value from the template to selected cameras.

  ![Example: Only the selected value is applied using this method](image)

  Example: Only the selected value is applied using this method

- **Set all template values on selected cameras**: Lets you apply all values from the template to selected cameras.

### Manual Recording

When you configure video and recording, you can specify certain properties for many cameras in one go. In the case of Manual recording, it is simply because the properties are shared by all cameras.

When manual recording is enabled, Smart Client users with the necessary rights (see page 115) 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 thus take place even if recording for individual cameras (see page 73) 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.

- **Enable manual recording**: Select check box to enable manual recording and specify further details.

- **Default duration of manual recording**: Period of time (in seconds) during which user-driven recording will take place. Default duration is 300 seconds, corresponding to five minutes.

- **Maximum duration of manual recording**: Maximum allowed period of time for user-driven recording. This maximum is not relevant in connection with manual recording started from the Smart Client, since such manual recording will always take place for a fixed time. In some installations it is, however, also possible to combine manual recording with third-party applications if integrating these with XProtect 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

With MJPEG, you can define frame rates for regular as well as speedup modes. 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 using MJPEG (see page 70).
**Template and Common Properties**

- **Template**: The template can help you configure similar properties quickly. Say you have 50 cameras and you want a particular frame rate on all of them. Instead of having to enter the same piece of information 50 times, you can simply enter it once in the template, and then apply the template to the 50 cameras with only two clicks.

- **Apply Template**: Lets you select which cameras you want to apply the template for. You then use one of the two Set buttons (see descriptions in the following) to actually apply the template.

  **Tip**: To select all cameras in the list, click the **Select All** button.

- **Select All**: Click button to select all cameras in the **Apply Template** column.

- **Clear All**: Click button to clear all selections in the **Apply Template** column.

- **Set selected template value on selected cameras**: Lets you apply only a selected value from the template to selected cameras.

  Example: Only the selected value is applied using this method

- **Set all template values on selected cameras**: Lets you apply all values from the template to selected cameras.

- **Camera Name**: Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: < > & " / : * ? | [ ]

**Regular Frame Rate Properties**

- **Frame Rate**: Required average frame rate for video from the camera. Select number of frames, then select required interval (per second, minute or hour) in the **Time Unit** column.

- **Time Unit**: Select required unit for live and recording frame rates (per second, minute, or hour).

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

**Speedup Frame Rate Properties**

- **Enable Speedup**: The speedup feature lets you use a higher than normal frame rate if motion is detected and/or an event occurs. When you enable speedup, further columns for specifying speedup details become available.

- **Frame Rate**: Required average speedup frame rate for viewing video from the camera. Select number of frames, then select required interval (per second, minute or hour) in the **Time Unit** column. The frame rate must be higher than the frame rate specified under normal mode.

- **Time Unit**: Select required unit for live and recording speedup frame rates (per second, minute, or hour). Note that you can only select time bases that let you speed up frame rates. Example: If you have specified 15 frames per second in normal mode, you cannot
specify 16 frames per *minute or hour* in speedup mode.

- **Speedup On**: Lets you select under which conditions to use speedup frame rates:
  - **Motion Detection**: Select this to speed up when motion (see page 77) is detected. Normal frame rates will be resumed immediately after the last motion is detected.
  - **Event**: Select this to speed up when an event occurs and until another event occurs. Use of speedup on event requires that events (see page 102) have been defined, and that you select start and stop events in the neighboring columns.
    - **Tip**: If you have not yet defined any suitable events, you can quickly do it: Use the Configure events list, located in the bottom left corner of the window.
  - **Motion Detection & Event**: Select this to speed up when motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.
  - **Schedule Only**: Select this to speed up according to the camera’s speedup schedule (see page 98) only.

- **Start Event**: Select required start event. The camera will begin using the speedup frame rates when the start event occurs.

- **Stop Event**: Select required stop event. The camera will return to the normal frame rates when the stop event occurs.

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

### Frame Rate – MPEG

All properties on a white background are editable; properties on a *light blue background* cannot be edited. Note that the Frame Rate - MPEG properties can also be specified individually for each camera using MPEG (see page 70).

- **Template**: The template can help you configure similar properties quickly. Say you have 50 cameras and you want a particular frame rate on all of them. Instead of having to enter the same piece of information 50 times, you can simply enter it once in the template, and then apply the template to the 50 cameras with only two clicks.

- **Apply Template**: Lets you select which cameras you want to apply the template for. You then use one of the two Set buttons (see descriptions in the following) to actually apply the template.

  **Tip**: To select all cameras in the list, click the Select All button.

- **Camera Name**: Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: < > & * " / : * ? | [ ]

- **Live FPS**: Lets you select the camera’s live frame rate per second (FPS).

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

- **Select All**: Click button to select all cameras in the `Apply Template` column.
- **Clear All**: Click button to clear all selections in the `Apply Template` column.
- **Set selected template value on selected cameras**: Lets you apply only a selected value from the template to selected cameras.

<table>
<thead>
<tr>
<th>Live FPS</th>
<th>Record Keystroke only</th>
<th>Record All Frames on</th>
<th>Start Event</th>
<th>Stop Event</th>
</tr>
</thead>
</table>

Example: Only the selected value is applied using this method.

- **Set all template values on selected cameras**: Lets you apply all values from the template to selected cameras.

**Audio Selection**

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 Audio Selection properties can also be specified individually for each camera (see page 70).

- **Template**: The template can help you configure similar properties quickly. Say you have 50 cameras and you want a particular default microphone for all of them. Instead of having to enter the same piece of information 50 times, you can simply enter it once in the template, and then apply the template to the 50 cameras with only two clicks.
- **Apply Template**: Lets you select which cameras you want to apply the template for. You then use one of the two `Set` buttons (see descriptions in the following) to actually apply the template.

  **Tip**: To select all cameras in the list, click the `Select All` button.

- **Camera Name**: Name of the camera as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: `< > & " / : * ? | [ ]`
- **Default Microphone**: Select required default microphone.

  **Tip**: Note that you can select a microphone attached to another hardware device than the selected camera itself.

- **Camera**: Click the `Open` button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
- **Select All**: Click button to select all cameras in the `Apply Template` column.
- **Clear All**: Click button to clear all selections in the `Apply Template` column.
- **Set selected template value on selected cameras**: Lets you apply only a selected value from the template to selected cameras.
- **Set all template values on selected cameras**: Lets you apply all values from the template to selected cameras.
Audio Recording

Lets you determine whether audio should be recorded or not. Your choice will apply for all cameras on your XProtect Essential system.

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

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

- **Audio recording affects video storage capacity**: Audio is recorded to the associated camera’s database. It is thus important to bear in mind that the database is likely to become full earlier if recording audio and video than if only recording video. The fact that the database becomes full is not in itself a problem since XProtect Essential automatically archives data (see page 86) if the database becomes full. However, there is likely to be a greater need for archiving space if you record audio.
  
  - Example: If using 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. When this is the case, the database’s video storage capacity will be halved, because half of the database’s records will be used for storing audio. Consequently, the database will run full sooner, and automatic archiving will take place more often than if you were only recording video.
  
  - Example: If using 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. The database’s video storage capacity can thus in extreme cases be halved, because half of the database’s records will be used for storing audio. If using very high frame rates, where there is less time between each JPEG, a smaller portion of the database will be used for storing audio records, and consequently a larger portion will be available for storing video. Anyway, the database will run full sooner, and automatic archiving will take place more often than if you were only recording video.

Above examples are simplified, the exact available video storage capacity will also depend on GOP/JPEG and audio kilobyte size.

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:

- **Drive**: Letter representing the drive in question, for example C:.
- **Path**: Path to the storage area, for example C:\ or \OurServer\OurFolder\OurSubfolder\.
- **Usage**: What the storage area is used for, for example recording or archiving.
- **Drive Size**: Total size of the drive.
- **Video Data**: Amount of video data on the drive.
- **Other Data**: Amount of other data on the drive.
- **Free Space**: Amount of unused space left on the drive.
Tip: To quickly view disk space usage in a pie chart format, select the line representing the drive you are interested in.

Camera-specific Configuration

To specify video, recording and camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for each individual camera.

1. In the Management Application’s navigation pane, expand Advanced Configuration, and expand Cameras and Storage Information.

2. Right-click the required camera and select Properties.

3. Specify properties as required for Camera, Frame Rate, Video, Audio, Recording, Recording & Archiving Paths, Event Notification, Output, Motion Detection & Exclude Regions, and—if applicable—Fisheye, PTZ Preset Positions, and PTZ on Event. All of the properties are described on the following pages.

4. Save your configuration changes by clicking the Save Configuration button in the Management Application’s toolbar.

General

When you configure video and recording (see page 37) for specific cameras, properties include:

- **Enabled**: Cameras are by default enabled, meaning that provided they are scheduled to be online (see page 38), 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.

- **Camera name**: Name of the camera as it will appear in the Management Application as well as in clients, see page 136. If required, you can overwrite the existing camera name with a new one. Camera names must be unique, and must not contain any of the following special characters: < > & * " \ : * ? | [ ]

  Tip: Camera names can be very long if required: the upper limit is more than 2000 characters, although such long camera names are hardly ever needed.

- **Camera shortcut number**: Users of the Smart Client can take advantage of keyboard shortcuts, some of which let the users toggle between viewing different cameras. Such shortcuts include numbers which are used to identify each camera.

  Shortcut numbers must be unique for each camera. A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits. Examples of correct camera shortcut numbers: 3, 12345678. Examples of incorrect camera shortcut numbers: Cam#3, 123456789.

  More information about using the keyboard shortcuts is available in the separate documentation for the Smart Client. In other applications, such as the Remote Client, the camera shortcut numbers cannot be used.

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 adjusting video settings, you are—for most cameras—able to 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 thus 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 (Frame Rate)

#### 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:**

- **Frame rate:** Frame rate for viewing video from the camera. Select number of frames in the first field, and required interval (per second, minute or hour) in the second field.

**Speedup Frame Rate Mode:**

- **Enable speedup frame rate:** The speedup feature lets you use a higher than normal frame rate if motion is detected and/or an event occurs. When you enable speedup, further fields for specifying speedup details become available.

- **Live frame rate:** Speedup frame rate for viewing live video from the camera. Select number of frames in the first field, and required interval (per second, minute or hour) in the second field. The frame rate must be higher than the live frame rate specified under normal mode.

- **On motion:** Select this check box to use the speedup frame rates when motion is detected. The camera will return to the normal frame rates two seconds after the last motion is detected.

- **On event:** Select this check box to use the speedup frame rates when an event occurs and until another event occurs. Use of speedup on event requires that events (see page 102) have been defined, and that you select start and stop events in the neighboring lists.

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

- **Start event:** Select required start event. The camera will begin using the speedup frame rates when the start event occurs.

- **Stop event:** Select required stop event. The camera will return to the normal frame rates when the stop event occurs.
**Tip:** Speedup does not necessarily have to be based on motion- or events; you can also use scheduling to configure speedup based on particular periods of time (see page 98). 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.

- **Enable dedicated live stream:** This additional stream feature lets you use the alternative stream of the camera. It enables two independent streams to the recording server—a stream for live viewing and another stream for recording purposes, with different resolution, encoding, and frame rate. When using this, you can get a smoother video.

- **Stream:** Select the type of the live stream. Stream settings for viewing live video and for recording video may very well be different in order to get the best result.

- **Resolution:** Select the resolution of the camera.

- **FPS:** Select the camera's live frame rate per second (FPS).

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

**If the Camera Uses the MPEG Video Format**

With MPEG, you can define frame rate:

- **Frame rate per second:** 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.

- **Enable dedicated live stream:** This additional stream feature lets you use the alternative stream of the camera. It enables two independent streams to the recording server—a stream for live viewing and another stream for recording purposes, with different resolution, encoding, and frame rate. When using this, you can get a smoother video.

- **Stream:** Select the type of the live stream. Stream settings for viewing live video and for recording video may very well be different in order to get the best result.

- **Resolution:** Select the resolution of the camera.

- **FPS:** Select the camera's live frame rate per second (FPS).

**Audio**

When you configure video and recording 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.
Tip: Note that you can select a microphone attached to another hardware device than the selected camera itself.

- Default microphone: Select required microphone.

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 Settings

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 specific cameras, recording properties include:

- Always: Record whenever the camera is enabled and scheduled to be online. The latter allows for time-based recording; see also page 97.
- Never: Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera.
- Conditionally: Record when certain conditions are met. When you select this option, specify required conditions (see the following).
- On built-in motion detection: Select this check box to record video in which motion (see page 77) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected.
- On event: Select this check box to record video when an event occurs and until another event occurs. Use of recording on event requires that events (see page 102) have been defined, and that you select start and stop events in the neighboring lists.

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

- Start event: Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).
- Stop event: Select required stop event. Recording will end when the stop event occurs (or later if using post-recording; see the following).

When the option Conditionally is selected, you can store recordings from periods preceding and following detected motion and/or specified events. Example: If you have defined that video should be stored when a door is opened, being able to see what happened immediately prior to the door being opened may also be important. Say you have specified that video should be stored conditionally on event, with a start event called Door Opened and a stop event called Door Closed. With three seconds of pre-recording, video will be recorded from three seconds before Door Opened occurs and until Door Closed occurs.

- Enable pre-recording: Available only when the option Conditional is selected. Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met.
- Enable post-recording: Available only when the option Conditional is selected. Specify the number of seconds for which you want to record video after recording stop conditions (that is motion end or stop event) are met.
How does pre- and post-recording work? XProtect 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 (see page 65) may be enabled. With manual recording, Smart Client users with the necessary rights (see page 115) 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 thus take place even if recording for individual cameras is set to Never or Conditionally.

Recording and Archiving Paths

- **Recording path:** Path to the folder in which the camera’s database should be stored. Default is C:\MediaDatabase. To browse for another folder, click the browse button next to the Recording path field. You are only able to specify a path to a folder on a local drive. If using a network drive, it would not be possible to save recordings if the network drive became unavailable.

  If you change the recording path, and there are existing recordings at the old location, you will be asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them.

  **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.

- **Delete Database:** Click button to delete all recordings in the database for the camera. Archived recordings will not be affected.

  **IMPORTANT:** Use with caution; all recordings in the database for the camera will be permanently deleted. As a security measure, you will be asked to confirm the deletion.

- **Archiving path:** Only available if not using dynamic paths for archiving. Path to the folder in which the camera’s archived recordings should be stored. Default is C:\MediaDatabase\Archives. To browse for another folder, click the browse button next to the Archiving path field. You can only specify a path to 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 moving archived recordings, XProtect Essential will also archive what is currently in the camera’s database; in case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.

  **Delete Archives:** Click button to delete all archived recordings for the camera. Recordings in the camera’s regular database will not be affected. The ability to delete is available regardless of whether you use a single archiving path or dynamic archiving paths.

  **IMPORTANT:** 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.

  **Retention time:** Total amount of time for which you want to keep recordings from the camera (that is recordings in the camera's database as well as any archived recordings). Default is 30 days.
Note that the retention time covers the **total** amount of time you want to keep recordings for; in earlier XProtect Essential versions time limits were specified separately for the database and archives.

- **Database repair action:** Select which action to take if the database becomes corrupted:
  - *Repair, scan, delete if fails:* Default action. If the database becomes corrupted, two different repair methods will be attempted: a fast repair and a thorough repair. If both repair methods fail, the contents of the database will be deleted.
  - *Repair, delete if fails:* If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be deleted.
  - *Repair, archive if fails:* If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be archived.
  - *Delete (no repair):* If the database becomes corrupted, the contents of the database will be deleted.
  - *Archive (no repair):* If the database becomes corrupted, the contents of the database will be archived.

If you choose an action to repair a corrupt database, this corrupt database is closed while it is repaired. Instead, a new database is created to allow recordings to continue.

**Why archive a corrupt database?** Provided the corrupt database has been archived, it can often be repaired by the Smart Client. So when you open the corrupt database in the Smart Client, the Smart Client will repair it automatically if at all possible.

**Tip:** There are several things you can do to prevent that your databases become corrupt in the first place. See Protect Recording Databases from Corruption on page 133.

- **Configure Dynamic Paths:** With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. If the drive containing the camera’s database is among the path you have selected for dynamic archiving, XProtect 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 62.

### Event Notification

Event notification lets you inform Remote Client and Smart Client users that an event (see page 102) 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 Remote Client/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.

To select an event for use with event notification, do the following:

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**

Lets you associate a camera with particular hardware output (see page 107), 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 or Remote Client users with the necessary rights (see page 115) 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 outputs 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 Remote Client.
     - and/or -
   - the 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, simply select the output in question, and click the << button.
Motion Detection and Exclude Regions

When you configure specific cameras, adjusting motion detection is important since 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.).

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 (see page 109) when configuring such devices for motion detection and PTZ. See also page 84.

Before you configure motion detection for a camera, it is highly recommended that you have configured the camera’s video properties, such as compression, resolution, etc. (see page 63). When ready, do the following:

How to Configure Motion Detection Properties

1. Ask yourself whether there are any areas which should be excluded from motion detection (for example if the camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background). If so, you can avoid detection of irrelevant motion by following the points below. If not, continue to step 2.

   - Enable: Lets you enable or disable the built-in motion detection.

   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, the differences between enabling (table 1) and disabling (table 2) built-in motion detection for a camera are listed:

<table>
<thead>
<tr>
<th>Camera's recording settings:</th>
<th>Enabled motion detection: Will you get...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>...recordings?</td>
</tr>
<tr>
<td>Always</td>
<td>Yes</td>
</tr>
<tr>
<td>Never</td>
<td>No</td>
</tr>
<tr>
<td>Built-in Motion Detection</td>
<td>Yes</td>
</tr>
<tr>
<td>Built-in Motion Detection &amp; Event only</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Camera's recording settings:</th>
<th>Disabled motion detection: Will you get...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>...recordings?</td>
</tr>
<tr>
<td>Always</td>
<td>Yes</td>
</tr>
<tr>
<td>Never</td>
<td>No</td>
</tr>
<tr>
<td>Built-in Motion Detection</td>
<td>No</td>
</tr>
<tr>
<td>Built-in Motion Detection &amp; Event only</td>
<td>Yes</td>
</tr>
</tbody>
</table>

...depending on settings
• **Show grid:** Lets you toggle the grid on and off. Toggling the grid off may provide a less obscured view of the preview image; selection of areas which should be excluded from motion detection takes place the same way as when the grid is visible. When on, the preview image will be divided into small sections by a grid. To define areas which should be excluded from motion detection, drag the mouse pointer over the required areas in the preview image while pressing the mouse button down. Left mouse button selects a grid section; right mouse button clears a grid section. Selected areas are highlighted in blue.

• **Include All:** Lets you quickly select all grid sections in the preview image. This may be advantageous if you want to exclude motion detection in most areas of the image, in which case you can simply clear the few sections in which you do not want to exclude motion detection.

• **Exclude All:** Lets you quickly clear all grid sections in the preview image.

2. **Use the two sliders for configuring motion detection:**

• **Sensitivity:** Determines how much each pixel must change before it is regarded as motion. With a high sensitivity, very little change in a pixel is required before it is regarded as motion. Areas in which motion is detected are highlighted in green in the preview image. Select a slider position in which only detections you consider motion are highlighted. 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.

**Tip:** If you find the concept of sensitivity difficult to grasp, try dragging the slider to its leftmost position: 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.

• **Motion:** Determines how many pixels must change in the image before it is regarded as motion. The selected level is indicated by the black vertical line in the motion level indication bar below the preview image. The black vertical line serves as a threshold: When detected motion is above (that is to the right of) the selected sensitivity level, the bar changes color from green to red, indicating a positive detection. As an alternative to using the slider, you may specify a value between 0 and 10000 in the field next to the slider to control the motion setting.

3. **Specify your requirements for the following:**

• **Detection interval:** Determines how often motion detection analysis should be carried out on video from the camera. The interval is measured in milliseconds; default is 240 milliseconds (that is close to once every quarter of a second). The interval is applied regardless of the camera’s frame rate settings.

• **Detection resolution:** Determines settings for how much of the image should be analyzed. Should it be the full image or only a selected percentage of the image? By analyzing, for example 25%, only every fourth pixel in the image is analyzed instead of all pixels. Using optimized detection will reduce the amount of processing power used, but will also mean a less accurate motion detection.

**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.

**Fisheye**

When you configure 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 to which the fisheye camera is attached (see page 80).

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.

- **Ceiling mount:** If the camera is mounted on a ceiling, you can adjust properties to reflect this by selecting the check box.

- **Resolution:** Resolution values are automatically displayed above the fisheye image. When using fisheye, resolution will automatically be set to the highest possible value.

- **X radius:** Controls the horizontal (X) radius of the green circle. Move the slider to the left for a narrower circle, or to the right for a wider circle. Alternatively, specify a value between 0 and 800 in the field next to the slider. 0 corresponds to the slider’s leftmost position, 800 corresponds to the slider’s rightmost position.

- **Y radius:** Controls the vertical (Y) radius of the green circle. Move the slider to the left for a flat circle, or to the right for a taller circle. Alternatively, specify a value between 0 and 800 in the field next to the slider.

- **X center:** Controls the horizontal (X) position of the green circle. Move the slider to the left or right as required. Alternatively, specify a value between 0 and 800 in the field next to the slider.

- **Y center:** Controls the vertical (Y) position of the green circle. Move the slider to the left in order to move the circle up, or to the right in order to move the circle down. Alternatively, specify a value between 0 and 800 in the field next to the slider.

- **Enable preview:** Lets you toggle between viewing the circular fisheye view and the flattened rectangular view resulting from your settings. When previewing the flattened view, the following navigation buttons become available for moving around within the flattened view:
  - **Set as Home:** Use after navigating to a suitable viewpoint using the navigation buttons. Sets the current viewpoint as home position (that is default position), so that when client users viewing the camera click their clients’ Home button, their view of the camera changes to that position.
  - Moves the flattened view up and to the left
  - Moves the flattened view up
  - 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)

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.

- **Enable**: Lets you enable the Privacy Masking feature.
- **Show grid**: Lets you toggle the grid on and off. Toggling the grid off may provide a less obscured view of the preview image; selection of areas which should be excluded from 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 pointer over the required areas in the preview image while pressing the mouse button down. Left mouse button selects a grid section; right mouse button clears a grid section. Selected areas are highlighted in red.
- **Show privacy mask**: Lets you toggle the red area indicating privacy masking on and off. Toggling the red area off may provide a less obscured view of the preview image.
- **Clear**: Lets you clear the privacy masking.

360° Lens

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

- **Enable 360° lens**: Select check box to enable use of the 360° lens technology and to be able to specify further properties.
- **Enable panomorph support**: Select to enable panomorph support. Panomorph is an advanced technology can provide high resolution in zones of interest, while at the same time using fewer pixels than conventional fisheye solutions. In the list, also select whether the camera is located in the ceiling or on a wall.
- **Immervision Enables® panomorph RPL number**: In the drop down, select the type of 360° lens you require. If you, at some point, want to add additional types of lenses, go to
File and select Import new lens types. Locate the .xml file that contains information about the lens type and press OK.

- **Enable fisheye support:** Select to enable fisheye support. Fisheye technology uses a wide-angle lens to capture a hemispherical image, which can then be de-warped through configured fisheye settings (see page 79) for the camera in question.

- **License key:** If required, enter your special fisheye license key and click OK, after which it will be possible to configure fisheye settings for camera(s) attached to the hardware device.

**Where do I get the special fisheye license key?** Contact your XProtect Essential vendor for further information.

**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 (see page 115) 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 importing them.

**Restart services (see page 109) after having made changes to PTZ settings.**

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 (see page 109) when configuring such devices for motion detection and PTZ. See also page 84.

- **PTZ type:** Your configuration options depend on the type of PTZ camera in question:
  - Type 1 (stored on server): You define preset positions by moving the camera using the controls in the upper half of the window, then storing each required position on the XProtect Essential server. You can define up to 25 preset positions this way.
  - Type 2 (imported from camera): You import preset positions which have previously been defined and stored on the PTZ camera itself through the camera’s own configuration interface. The number of allowed preset positions depends on the PTZ camera and driver used.
  - Type 3 (stored on camera): You define preset positions by moving the camera with the controls in the upper half of the window, then storing each required position in the camera’s own memory. You are able to define up to 50 preset positions this way. If preset positions have already been defined for the camera, you can simply import them for use with XProtect Essential.

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

- By simply clicking the required position in the camera preview (if supported by the camera).
- By using 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).

- By using 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)

- **Import / Refresh**: Only available when you have selected PTZ type 2 or 3. Lets you import already defined preset positions from the camera’s memory for use with XProtect 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.

- **Add New**: Only available when you have selected PTZ type 1. When you have move the camera to a required position using the controls in the upper half of the window, type a name for the position in the blank field, then click the button to add the position to the list of defined preset positions. Remember that names of preset positions must contain only the characters A-Z, a-z and the digits 0-9.

- **Set New Position**: Only available when you have selected PTZ type 1 or 3. Lets you change an already defined preset position. In the list, select the preset position you want to change. Then move the camera to the new required position using the controls in the upper half of the window. Then click the button to overwrite the old position with the new one.

- **Delete**: Only available when you have selected PTZ type 1 or 3. Lets you delete an already defined preset. In the list, select the preset position you want to delete, then click the button.

Before you delete a preset position, make sure it is not used in PTZ on event (see page 83). Since the preset positions are stored on the camera, you can bring a deleted preset position back into XProtect Essential by clicking the Import / refresh button. If you bring back a preset position this way, and the preset position is to be used in PTZ on event, you must manually configure PTZ on event to use the preset position again.
- **Test**: Lets you try out a preset position. In the list, select the preset position you want to test, then click the button to view the camera move to the selected position.

- **and**: 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.

Example from client: Users select preset positions from a list. By moving preset positions up or down during configuration on the server, you can control the sequence in which the 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 page 80), it is possible to make the PTZ camera automatically go to a particular preset position when a particular event (see page 102) occurs.

Restart services (see page 109) after having made changes to PTZ settings.

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 (see page 109) when configuring such devices for motion detection and PTZ. See also page 84.

When associating events with preset positions on a PTZ camera, you are able to 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 you later want to end the association between a particular event and a particular preset position, simply clear the field containing the event.
Configure When Cameras Should Do What

Use XProtect Essential’s 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

Read more in the Configure General Scheduling & Archiving on page 94 and Configure Camera-specific Scheduling on page 96.

View Video 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 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 (see page 109) when configuring such devices for motion detection and PTZ.

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.

**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 page 86) 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 page 62), 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, thus temporarily limiting the size of all databases.

When the Recording Server service (see page 109) 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.

**Disable or Delete a Camera**

All cameras are by default enabled. This means video from the cameras can be transferred to XProtect Essential—provided that the cameras are scheduled to be online (see page 97).

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 in the Management Application’s toolbar.

To **delete** a camera, you technically have to delete the hardware device (see page 59). Deleting the hardware device will also delete any attached microphones. If you do not want this, consider disabling the camera instead.
Archiving

Archiving helps you store recordings, maximize storage capacity and minimize risk. You can keep recordings for as long as required, limited only by the available hardware storage capacity.

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 & Archiving Paths 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). Scheduled archiving is possible up to 24 times per day.

Quick Explanation of the Archiving Feature

Archiving is an integrated and automated feature in XProtect Enterprise with which recordings are moved after an amount of time in order to free up space for new recordings. The idea is that recordings are moved from one location to another in order to continuously have space for the most recent recordings on your default recording storage. This process is handled by the software.

You do not have to do anything yourself to enable Archiving; Archiving is a process that runs in the background, and it is enabled and carried out automatically from the moment XProtect Enterprise is installed. Recorded video can take up a lot of storage space, so only your hardware will place limits on the amount of recordings you can save. Archiving will ensure that recordings are moved in order to provide space for more recent recordings.

Client, such as the Smart Client, are used to archives and can locate the moved data without any problems.

The default settings for XProtect Enterprise is to perform archiving once a day, or if your database becomes full. It is possible to change the settings for when and how often archiving is to take place, under Advanced Configuration > Scheduling and Archiving in the Management Application. Scheduled archiving is possible up to 24 times per day. You can also change the retention time, which is the total amount of time you want to keep recordings from a camera (that is recordings in the camera's database as well as any archived recordings) under the properties of the individual camera.

The default archiving folder is located on the XProtect Enterprise server, by default in C:\MediaDatabase. 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. You can change the default archiving folder to any other location locally.

In the following, archiving is explained in detail. If you would rather begin configuring archiving straight away, see Configure Archiving Locations on page 91 and Configure Archiving Schedules on page 92.

Benefits of Archiving

With archiving, recordings are moved from their standard location to another location, the archiving location. With archiving, the amount of recordings you are able to store is thus limited only by the available hardware storage capacity:
By default, recordings are stored in XProtect Essential’s 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. Having sufficient archiving space is thus 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.

**How Archiving Works**

For each camera, the contents of the camera database will be moved to a default archiving folder, called *Archives*. This will happen automatically if a database becomes full, and one or more times every day, depending on your archiving settings.

The default archiving folder (see page 124) is located on the XProtect Essential server, by default in C:\MediaDatabase. 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. Since you can keep archives spanning many days of recordings, and since archiving may take place several times per day, further subfolders, named after the archiving date and time, are also automatically created.

The subfolders will be named according to the following structure:

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

Example: With the default archiving folder located under C:\MediaDatabase, video from an archiving taking place at 23.15 on 31st December 2009 for a camera attached to channel 2 on a video encoder hardware device with the MAC address 00408c51e181 would be stored at the following destination:

```
C:\MediaDatabase\Archives\00408c51e181_2\2009-12-31-23-15
```

If the hardware device to which the camera is attached is not a video encoder device with several channels, the video encoder channel indication in the sub-directory named after the hardware device’s MAC address will always be _1 (example: 00408c51e181_1).

You are of course also able to store archives at other locations than locally in the default archiving directory. You may, for example, specify that your archives should be stored on a network drive.

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

While this may at first glance seem unnecessary, it greatly speeds up the archiving procedure, and reduces delays in case of network problems. Archiving directly to a network drive would mean that archiving time would vary depending on the available bandwidth on the network. First storing the archive locally, then moving it, ensures that archiving is always performed as fast as possible.

If archiving to a network drive, note the regular camera database can only be stored on a local drive, that is a drive attached directly to the XProtect Essential server.
Dynamic Path Selection for Archives

With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. Using dynamic paths is highly recommended, and is the default setting when you configure cameras through the Configure Video & Recording Wizard (see page 37).

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 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.

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 page 124) 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 fairly quickly fill up the drive with data.

**Camera records to drive C: and archives to drive D:**
Obvious benefit is that 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. 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 of thumb is: “Do not cross recording and archiving drives.”

Archiving Audio

If an audio source (microphone) is enabled on a hardware device, audio recordings will be 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 will be 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.

Viewing Archived Recordings

You are able to view archived recordings via a client such as the Remote Client or the Smart Client. Use, for example, all of the Smart Client’s advanced features (video browsing, smart search, export, etc.) for archived recordings.
Exported Archives
For exported archives, for example archives stored on a CD, you also use the Remote Client or the Smart Client.

See the Remote Client and/or Smart Client documentation for more information.

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 (a.k.a. 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: As a rule of thumb, the capacity of the local drive should be at least twice the size required for storing the databases of all cameras.

When archiving, 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.

In short: When estimating storage capacity required for archiving, consider your organization’s needs, then plan for worst case rather than best case scenarios.

Tip: The Milestone Design Tool, found in the Support section of the Milestone website, www.milestonesys.com, can help you easily determine the storage capacity required for your surveillance system.

Backing up Archives
Many organizations want to back up recordings from cameras, using tape drives or similar. Creating such backups based on the content of camera databases is not recommended; it may cause sharing violations or other malfunctions.

Instead, create such backups based on the content of archives. If you have not specified separate archiving locations for separate cameras, you could simply back up the default local archiving directory, Archives.

When scheduling a backup, make sure the backup job does not overlap with any scheduled archiving times.

Automatic Response if Running Out of Disk Space
With archiving, XProtect Essential can automatically respond to the threat of running out of disk space. 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
  - 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.

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 Running Out of Disk Space

In case 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, XProtect Essential 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
- 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.

New Database 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 simply 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.

Virus Scanning and Archiving

If allowed in your organization, disable any virus scanning of camera databases and archiving locations. For more information see page 15.

Configure Archiving Locations

Before configuring archiving 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 & 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 page 74).

 General Recording & Archiving Paths: In the Management Application’s navigation pane, expand Advanced Configuration, double-click Cameras and Storage Information, and specify required properties (see page 61).

**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 thus 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 page 62).

If configuring your cameras through the Configure Video & Recording Wizard (see page 37), the wizard also lets you configure archiving paths.

---

**Configure Archiving Schedules**

XProtect Essential automatically archives recordings if a camera’s database becomes full (in earlier versions, this was an option configured individually for each camera).

You are furthermore able to schedule archiving at particular points in time up to 24 times per day, with minimum one hour between each one. This way, you can proactively archive recordings, so databases will never become full. As a rule of thumb, the more you expect to record, the more often you should archive.

There are two ways in which to configure archiving schedules:

- While configuring your cameras through the Configure Video & Recording Wizard (see page 37), in which case you configure your archiving schedule on the wizard’s Drive selection page.

- As part of the general Scheduling & Archiving properties: In the Management Application’s navigation pane, expand Advanced Configuration, right-click Scheduling and Archiving, select Properties, select Archiving in the dialog, and specify required properties (see page 96).
Audio

You add cameras and other hardware devices, such as video encoders, to your XProtect Essential system through the Add Hardware Devices... wizard (see page 26). If microphones are attached to a hardware device, they are automatically added as well.

When managing microphones in XProtect Essential, it is important to remember the basic concepts:

- **Microphones** are attached to hardware devices, and thus 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).

Configure Microphones

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

1. In the Management Application’s navigation pane, expand Advanced Configuration, expand Hardware Devices, and expand the hardware device to which the required microphone is attached.

2. Right-click the required microphone, and select Properties.

3. Specify properties as required:
   - **Enabled**: 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.
   - **Microphone name**: Name of the microphone as it will appear in the Management Application as well as in clients. If required, you can overwrite the existing microphone name with a new one. Microphone names must be unique, and must not contain any of the following 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 thus verify whether the problem may be due to audio being disabled on the hardware device itself.

4. Save your configuration changes by clicking the Save Configuration button in the Management Application’s toolbar.
Scheduling

In XProtect Essential, you can configure scheduling on a general level, which also covers archiving (see page 86), as well as on a camera-specific level.

Configure General Scheduling and Archiving

XProtect Essential’s general Scheduling and Archiving feature lets you 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

Do the following:

1. In the Management Application’s navigation pane, expand Advanced Configuration, right-click Scheduling and Archiving, and select Properties.
2. Specify properties as required for Scheduling All Cameras, Scheduling Options, and Archiving. All of the properties are described on the following pages. When ready, click OK.
3. Save your configuration changes by clicking the Save Configuration button in the Management Application’s toolbar.

Scheduling All Cameras

When you configure general scheduling and archiving, you can specify certain properties for many cameras in one go. Either simply in order to speed up things, or because the properties in question are shared by all cameras rather than 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, and E-mail Notification can also be specified individually for each camera.

- **Template**: The template can help you configure similar properties quickly. Say you have 50 cameras and you want to change the online schedule profile for all of them. Instead of having to select the same 50 times, you can simply enter them once in the template, and then apply the template to the 50 cameras with only two clicks.

- **Apply Template**: Lets you select which cameras you want to apply the template for. You then use one of the two Set buttons (see descriptions in the following) to actually apply the template.

  **Tip**: To select all cameras in the list, click the Select All button.

- **Camera**: Name of each camera as it will appear in the Management Application as well as in clients.
- **Online**: Lets you select the required profile (for example Always on) for the online schedule (see page 97) for the camera(s) in question.

  **Tip**: If you lack a suitable profile, use the *New schedule profile* feature (described in the following) to configure one. This applies for the other schedule types as well.

- **Speedup**: Lets you select the required profile for the speedup schedule (see page 98) for the camera(s) in question.

- **E-mail**: Lets you select the required profile for the e-mail notification schedule (see page 99) for the camera(s) in question.

- **Select All**: Click button to select all cameras in the *Apply Template* column.

- **Clear All**: Click button to clear all selections in the *Apply Template* column.

- **Set selected template value on selected cameras**: Lets you apply only a selected value from the template to selected cameras.

- **New schedule profile**: Lets you create a new schedule profile of any type by clicking the *Create...* button.

### Scheduling Options

**Is it possible to view live and even record video from a camera outside its online recording schedule?** Yes, you simply 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.

- **Start cameras on client requests**: Cameras may be offline, for example because they have reached the end of an online recording schedule (see page 97), in which case client users will not be able to view live video from the cameras. However, if you select *Start cameras on client requests*, client users will be able to view live video from the camera outside online schedule—but without recording (technically: force the camera to be online outside its online schedule).

  You must select *Enable recording when started on client request* (see the following), if you want recording to take place.

- **Enable recording when started on client request**: Lets you enable recording on the camera when *Start cameras on client requests* (see the previous) is also selected.

  If a user does not have access to manual recording (see page 116), selecting *Enable recording when started on client request*, will not enable the user to do manual recording.

- **Schedule profile for new cameras**: Lets you 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 *Always on*, meaning that new cameras will always be online, that is transferring video to the XProtect Essential server for live viewing and further processing.

- **Maximum delay between reconnect attempts**: Lets you control the aggressiveness of reconnect 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 reconnect attempts.
Archiving

XProtect Essential automatically archives recordings if a camera’s database becomes full (in earlier versions, this was an option configured individually for each camera; read more about archiving on page 86).

You are furthermore able to schedule archiving at particular points in time every day. This way, you can proactively archive recordings, so databases will never become full. As a rule of thumb, the more you expect to record, the more often you should archive.

Archiving Time

The Archiving Times list shows the times at which you want to automatically archive the content of all camera databases on your XProtect Essential server. You can do this up to 24 times per day, with minimum one hour between each one.

To add archiving times to the list:

1. Specify required time in the time box to the right of the Archiving Times list. You specify the required time by selecting the hour, minute and second values respectively, then clicking the up and down buttons to increase or decrease values. Alternatively, you can simply overwrite selected hour, minute or second values.

2. Click the Add button.

Archive Failure Notification

You can automatically get notified if archiving fails:

- Send e-mail on archiving failure: If selected, XProtect Essential will automatically send an e-mail to selected recipients if archiving fails. This requires that the e-mail notification (see page 100) feature is enabled. Recipients are defined as part of the e-mail notification properties.

E-mail notifications are normally only sent during scheduled periods (see page 99). However, archiving failures are considered to be so serious that, if enabled, e-mail notifications regarding archiving failures are sent regardless of schedules.

Configure Camera-specific Scheduling

With camera-specific scheduling, you can configure when:

- A camera should be online (that is transfer video to XProtect Essential)

- A camera should use speedup (that is use a higher than normal frame rate)

- You want to receive any e-mail notifications regarding the camera

Do the following:

1. In the Management Application’s navigation pane, expand Advanced Configuration, expand Scheduling and Archiving, right-click the required camera, and select Properties.

2. Specify properties as required for Online Period, Speedup, E-mail Notification. When ready, click OK.

3. Save your configuration changes by clicking the Save Configuration button in the Management Application’s toolbar.
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 page 95), 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 page 60.

You specify a camera’s online periods by creating schedule profiles based on:

- Periods of time (example: Mondays from 08.30 until 17.45), shown in pink:
- Events (see page 102) 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.

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. To create a customized schedule profile:

1. In the field below the *Schedule profiles* list, specify a name for the new schedule profile. Schedule profile names must not contain any of the following special characters: `< > & ' " / : * ? | [ ]`
2. Click the *Add New* button (which becomes available when you specify a name).
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.

Is it possible to view live and even record video from a camera outside its online recording schedule? Yes, you simply select the *Start cameras on client requests* (see page 95) and, if needed, the *Enable recording when started on client request* (see page 95) options when setting up your scheduling properties for the camera in question.

**Speedup**

When you configure scheduling for specific MJPEG cameras, you can specify speedup periods. Before you can define this type of schedule, speedup must be enabled (see page 65). 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: ![Olive green](image)

Speedup may also take place based on events, but that is configured elsewhere: See Frame Rate - MJPEG on page 65 and Frame Rate - MPEG on page 6771.

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. To create a customized schedule profile:

1. In the field below the *Schedule profiles* list, specify a name for the new schedule profile. Schedule profile names not contain any of the following special characters: `< > & " \ : * ? | ]`
2. Click the *Add New* button (which becomes available when you specify a name).
3. 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.
   - 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.

**E-mail Notification**

When you configure scheduling for specific cameras, you can specify e-mail notification periods. Before you can define this type of schedule, e-mail notification must be enabled (see page 100). 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:

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. To create a customized schedule profile:

1. In the field below the *Schedule profiles* list, specify a name for the new schedule profile. Schedule profile names must not contain any of the following special characters: `< > & ’ " / : * ? | [ ]`

2. Click the *Add New* button (which becomes available when you specify a name).

3. 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.
   - 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.
E-mail

Configure E-mail Notifications

With e-mail notifications, you and your colleagues 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 page 77) is detected
- Events (see page 102) occur (you can select individually for each event whether you want to receive an e-mail notification or not, thus avoiding irrelevant e-mails)
- Archiving (see page 86) fails (if e-mail notification has been selected as part of the scheduling properties for archiving, see page 96)

Do the following:

1. In the Management Application’s Navigation pane, expand Advanced Configuration, right-click E-mail and select Properties.

2. You enable the use of e-mail alerts separately for the Recording Server service.
   - **Enable e-Mail (Recording Server):** Enables e-mail notifications whenever the Recording Server service (see page 113) is running. E-mail notifications will then be sent when the following conditions apply:
     - the Recording Server service is running
     - motion is detected or an event, for which the sending of an e-mail notification has been defined, occurs
     - motion is detected within a period of time for which an e-mail notification schedule has been defined.

3. Specify required properties, including the important information about which SMTP mail server to use. The properties are described on the following pages. When ready, click OK.

   **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.

4. Save your configuration changes by clicking the Save Configuration button in the Management Application’s toolbar.

When configuring e-mail alerts, also consider the e-mail notification schedules (see page 99) configured for each camera.

E-mail Properties

- **Recipient(s):** Lets you specify the e-mail addresses to which e-mail notifications should be sent. If specifying more than one e-mail address, separate the e-mail addresses with semicolons (example: aa@aa.a;bb@bb.bb;cc@cc.cc).

- **Test:** Sends a test e-mail to the specified recipients. If Include Image is selected, the test e-mail will have a still test JPEG image attached.
- **Subject text**: Specify required subject text for e-mail notifications.

- **Message text**: Specify required message text for e-mail notifications. Note that camera information as well as date and time information is automatically included in e-mail notifications.

- **Include Image**: Select check box to include still images in e-mail notifications. When selected, a still JPEG image from the time the triggering event occurred will be attached to each e-mail notification.

- **Do not send e-mail on camera failures**: 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 page 99).

- **Time between motion- and database-related e-mails per camera**: Minimum time (in minutes) to pass between the sending of each e-mail notification per camera. This interval only applies for e-mail notification generated by detected motion or database-related events; e-mail notification generated by other types of events will still be sent out whenever the events occur. Examples: If specifying 5, a minimum of five minutes will pass between the sending of each motion- or database-related e-mail notification per camera, even if motion or database events are detected in between. If specifying 0, e-mail notifications will be sent each time motion or database events are detected in between. If specifying 0, e-mail notifications will be sent out whenever events occur. You should therefore consider cameras' motion detection sensitivity settings (see page 77).

- **Sender e-mail address**: Type the e-mail address you wish to appear as the sender of the e-mail notification.

- **Outgoing mail (SMTP) server name**: Type the name of the SMTP (Simple Mail Transfer Protocol) server which will be used for sending the e-mail notifications. Compared with other mail transfer methods, SMTP has the advantage that you will avoid automatically triggered warnings from your e-mail client. Such warnings may otherwise inform you that your e-mail client is trying to automatically send e-mail messages on your behalf. TLS (Transport Layer Security) and 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.

- **Server requires login**: Select check box if a user name and password is required to use the SMTP server.

- **Username**: Only required when **Server requires login** is selected. Specify the user name required for using the SMTP server.

- **Password**: Only required when **Server requires login** is selected. Specify the password required for using the SMTP server.
Events, Input and Output

**Hardware input**, such as door sensors, etc. 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.

**Events** of various types (see the following for details) 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.

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

The following types of events exist:

- **Hardware input events**: Events based on input from hardware input units attached to hardware devices are called hardware input events.
  
  Some hardware devices have their own capabilities for detecting motion, for detecting moving and/or static objects, etc. (configured in the hardware devices’ own software; typically by accessing a browser-based configuration interface on the hardware device’s IP address). When this is the case, XProtect Essential considers such detections as input from the hardware, and you can use such detections as input events as well.

  Lastly, hardware input events can be based on XProtect Essential detecting motion in video from a camera, based on XProtect Essential’s motion detection (see page 77) settings. 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.

- **Manual events**: Events may be generated manually by users selecting them in their clients. These events are called manual events.

- **Timer events**: Timer events are separate events, triggered by the hardware input event or manual 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

**VMD events; where are they?** In previous versions of XProtect Essential, an event type called VMD events existed. VMD (Video Motion Detection) events were based on the XProtect Essential system detecting motion in the video stream from a camera. This is still possible, but now you configure such events as hardware input events.

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.

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. See Configure General Event Handling in the following.

When you are ready to configure events, see Add a Hardware Input Event on page 104 and Add a Manual Event on page 105. If you want to use timer events with your other events, see Add a Timer Event on page 106.

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 107 and Configure Hardware Output on Event on page 108.

**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:
   - **Alert port**: Lets you specify port number to use for handling events. Default port is port 1234.
   - **SMTP event port**: Lets you specify port number to use for sending event information from hardware devices to XProtect Essential via SMTP. Default port is port 25.
   - **FTP event port**: Lets you specify port number to use for sending event information from hardware devices to XProtect Essential via FTP. Default port is port 21.
   - **Polling interval [1/10] second**: For a small number of hardware devices, primarily dedicated input/output devices (see page 58), 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.

When ready, click OK.
3. Save your configuration changes by clicking the *Save Configuration* button in the Management Application’s toolbar.

### Add a Hardware Input Event

With hardware input events, you can turn input received from input units attached to hardware devices into events in XProtect 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’s 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 page 77) is enabled 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. All of the properties are described in the following.

5. When ready, click OK, or click the Add button to add a timer event (see page 106) to the event you have just created.

6. Save your configuration changes by clicking the *Save Configuration* button in the Management Application’s toolbar.

### Hardware Input Properties

Note that some properties depend on the selected type of input.

- **Enable**: Select check box to use selected type of input as an event in XProtect Essential, and specify further properties.

- **Event name**: Specify a name for the event. Hardware input event names must be unique, and must not contain the following characters: `< > & ' " \ / : * ? | [ ]`

  Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera’s documentation for exact details.

- **Images from camera**: Only relevant if using pre- and post-alarm images, a feature available for selected cameras only; it enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. Pre- and post-
alarm images should not be confused with XProtect Essential's own pre- and post-recording feature (see page 73). Lets you select which camera you want to receive pre- and/or post-alarm images from.

- **Number of pre-alarm images**: Only relevant if using pre-alarm images, a feature available for selected cameras only. Specify required number of pre-alarm images. Allowed number may differ from camera to camera; allowed range is displayed to the right of the field.

- **Frames per second**: Only relevant if using pre-alarm images, a feature available for selected cameras only. Specify required frame rate. Used in combination with the Number of pre-alarm images field, this field indirectly allows you to control how long before the event you want to receive pre-alarm images from.

- **Send e-mail if this event occurs**: Only available if e-mail notification (see page 100) 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 page 99).

- **Attach image from camera**: Only available if e-mail notification (see page 100) 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.

- **Delete**: Lets you delete a selected timer event.

- **Add**: When a specific hardware input event is selected, clicking Add will add a timer event (see page 106) to the selected hardware input event.

## Add a Manual Event

With manual events, your users with required rights (see page 115) can trigger events manually from their clients (see page 136). 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 page 97). 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 (see page 83).

- For triggering output. Particular output can be associated with manual events (see page 108).

- 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’s 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 (described in the following). When ready, click OK, or click the Add button again to add a timer event (see page 106) to the event you have just created.

4. Save your configuration changes by clicking the Save Configuration button in the Management Application’s toolbar.

**Manual Event Properties**

- **[List of defined global events and cameras]:** Contains a Global node and a list of all defined cameras. You can configure as many manual events as required, no matter whether they are global or camera-specific. A + sign next to the Global node indicates that one or more global manual events have already been configured. A + sign next to a camera indicates that one or more manual events have already been configured for that camera.

- **Event name:** Specify a name for the event; this is the name that client users will see. Manual event names must be unique, and must not contain the following 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.

- **Send e-mail if this event occurs:** Only available if e-mail notification (see page 100) 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 page 99).

- **Attach image from camera:** Only available if e-mail notification 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.

- **Delete:** Lets you delete a selected event.

- **Add:** Lets you add a new event. When Global or a specific camera is selected, clicking Add will add a new manual event. When a specific manual event is selected, clicking Add will add a timer event (see page 106) to the selected manual event.

**Add a Timer Event**

Timer events are separate events, triggered by the hardware input event (see page 104) or manual event (see page 105), 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 (described in the following). When ready, click OK, and save your configuration changes by clicking the Save Configuration button in the Management Application’s 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.

**Timer Event Properties**

- **Timer event name:** Specify a name for the event. Timer event names must be unique, and must not contain the following characters: `< > & ’ “ \ : * ? [ ]`

  Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera’s documentation for exact details.

- **Timer event occurs after:** Lets you specify the amount of time that should pass between the main event occurring and the timer event (in seconds or minutes).

**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 page 102) or detected motion, or manually by users of clients (see page 136).

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’s 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 (described in the following).

4. Click OK.

5. Save your configuration changes by clicking the Save Configuration button in the Management Application’s toolbar.

For information about how to configure automatic activation of hardware output when events occur, see Configure Hardware Output on Event (see page 108).

You configure output for manual activation in clients as well as for automatic activation on detected motion individually for each camera (see page 76).
Hardware Output Properties

- **Output name:** Specify a name for the event. If you are going to make the hardware output available for manual activation in clients, this is the name that client users will see. Hardware output names must be unique, and must not contain the following characters: < > & ' " \ / : * ? | [ ]

Some hardware devices only support hardware output names of a certain length and/or with a certain structure. Refer to the hardware device’s documentation for exact details.

- **Output connected to:** Lets you select which of the hardware device’s output ports the output is connected to. Many hardware devices only have a single output port; in that case simply select Output 1.

- **Keep output for:** Lets you specify the amount of time for which the output should be applied. Specify the required amount of time in either 1/10 seconds or seconds.

Some hardware devices are only able to apply output for a relatively short time, for example for up to five seconds. Refer to the documentation for the hardware device in question for exact information.

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

Configure Hardware Output on Event

Once you have added hardware output (see page 107), such as lights, sirens, door openers, etc., you can associate the hardware output with events (see page 102). 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. In the Event column, select the required event.

3. In the Output column, select the hardware output you want to be activated by the event.

4. Click OK.

5. Save your configuration changes by clicking the Save Configuration button in the Management Application’s 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.
Services

The following services are all automatically installed on the XProtect Essential server:

- **Milestone Recording Server service:** A vital part of the surveillance system; video streams are only transferred to XProtect Essential while the Recording Server service is running.

- **Milestone Image Server service:** Provides access to the surveillance system for users logging in with a Remote Client or a Smart Client. Read more about the clients on page 136.

  Note: If the Image Server service is configured in Windows Services to log in with another account than the Local System account, for example as a domain user, Smart Clients on other computers than the surveillance server itself will not be able to log in to the server using the server’s host name. Instead, those users must enter the server’s IP address.

- **Milestone Image Import service:** Used for fetching pre- and post-alarm images, and storing the fetched images in camera databases. Pre- and post-alarm images is a feature available for selected cameras only; it enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. Pre- and post-alarm images should not be confused with XProtect Essential’s own pre- and post-recording feature (see page 73).

- **Milestone Log Check service:** Performs integrity checks on XProtect Essential log files. For more information about logging, see page 119.

The services by default run transparently in the background on the XProtect Essential server.

**Start and Stop Services**

On an XProtect Essential server, four services by default run in the background. If required, you can start and stop each service separately:

1. In the Management Application’s Navigation pane, expand Advanced Configuration and select Services. This will display the status of each service.

2. You can now stop each service by clicking the Stop button. When a service is stopped, the button changes to Start, allowing you to start the service again when required.

  **Tip:** Occasionally, you may want to stop a service and start it again immediately after. The Restart button allows you to do just that with a single click.
Client Access to Surveillance System

You can configure clients' access to the XProtect Essential server in two ways: Through a wizard or through Advanced Configuration.

Wizard-driven Configuration

Guided configuration through a wizard lets you quickly specify how clients access the server as well as which users should be able to use clients. See Configure User Access Wizard on page 45.

When using the wizard, all users you add will have access to all cameras, including any new cameras added at a later stage. If this is not acceptable, specify access settings, users and user rights separately; see the following.

Advanced Configuration

In previous versions of XProtect Essential, this was known as Image Server administration, since technically it is the Image Server service (see page 109) which handles clients' access to the surveillance system.

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, Local IP Ranges, and Language Support & XML Encoding. The properties are described on the following pages. When ready, click OK.

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

When using this option, you configure client users separately from clients' access; see Add Basic Users on page 113, Add Windows Users on page 114, Add User Groups on page 115, and Configure User & Group Rights on page 115.

Server Access

- **Server name**: 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.

Example: In this case, the name Server was used
• **Local port**: Port number to use for communication between clients and the surveillance server. The default port number is 80; you can change the port number if port 80 is used for other purposes in your organization.

• **Enable internet access**: Select the check box if the server should be accessible from the internet through a router or firewall. If selecting 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.

• **Internet address**: Lets you specify a public IP address or hostname for use when the XProtect Essential server should be available from the internet.

• **Internet port**: Lets you 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 port 80 is used for other purposes in your organization.

• **Max. number of clients**: Up to five clients at a time are able to connect to the surveillance system from a remote location. 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.

   **Tip**: If required, you can run an unlimited number of Remote Clients or Smart Clients locally on the XProtect Essential server; they do not count among the maximum five allowed clients.

   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 in some cases, for example if you set the **Max. number of clients** value to 1: When this is the case, and the single allowed client user logs out, four minutes must pass before it will be possible to log in again.

### Local IP Ranges

You can specify IP address ranges which XProtect Essential should recognize as coming from a local network. This can be relevant if different subnets are used across your 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

You can select the language/character set used by the XProtect Essential server and clients.

• **Language**: Select required language/character set. Example: If the surveillance server runs a Japanese version of Windows, select **Japanese**. Provided access clients also use a
Japanese version of Windows, this will ensure that the correct language and character encoding is used in clients' communication with the server.
Users

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 are able to connect to the surveillance system through their clients (see page 136). 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 (see page 45) or individually (see Add Basic Users in the following and Add Windows Users on page 114).

By grouping users, you can specify rights (see page 115) 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 (see page 115) 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 (see page 13).

Wizard-driven Configuration

The Configure User Access Wizard (see page 45) helps you quickly configure clients' access to the XProtect Essential server as well as which users should be able to use clients.

When using the wizard, all users you add will have access all to cameras, including any new cameras added at a later stage. If this is not acceptable, specify access settings, users and user rights separately. Also note that you cannot add users to groups through the wizard.

Advanced Configuration

Add Basic Users

When adding a basic user, you create a dedicated surveillance system user account with basic user name and password authentication for the individual user. Note that adding the user as a Windows user (see page 114) will provide better security.

If you want to include users in groups, make sure you add required groups (see page 115) before you add users: You cannot add existing users to groups.

1. In the Management Application’s navigation pane, expand Advanced Configuration, right-click Users, and select Add New Basic User.

2. Specify a user name. User names must be unique, and must not contain the following characters: `< > & * ` / : * ? | [ ]`
Then specify a password, and repeat it to be sure you have specified it correctly.

3. Click OK.

4. Specify General Access and Camera Access properties (see page 116). These properties will determine the rights of the user.

5. Click OK

6. Save your configuration changes by clicking the **Save Configuration** button in the Management Application’s toolbar.

## Add Windows Users

When adding Windows users, you import users defined locally on the server and authenticate them based on their Windows login. This generally provides better security than the basic user concept (see 113), and is the recommended method.

*If you want to include users in groups, make sure you add required groups (see page 115) before you add users: You cannot add existing users to groups.*

You can add Windows users in two ways: One is through the Configure User Access Wizard (see page 113), the other is described here:

The users you want to add must have been defined as local PC users on the server. Simple file sharing must be disabled on the server. To disable simple file sharing, right-click Windows' **Start** button and select **Explore**. In the window that opens, select the **Tools** menu, then select **Folder Options...**, then the **View** tab. Scroll to the bottom of the tab’s **Advanced Settings** list, and make sure that the **Use simple files sharing** check box is cleared. When ready, click **OK** and close the window.

1. In the Management Application's navigation pane, expand **Advanced Configuration**, right-click **Users**, and select **Add New Windows User**. This will open the **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 the **Enter the object names to select** box, type the required user name(s), then use the **Check Names** feature to verify that the user name(s) you have entered are correct. If typing several user names, separate each name with a semicolon. Example:  *Brian; Hannah; Karen; Wayne*

3. When ready, click **OK**.

4. Specify General Access and Camera Access properties. These properties will determine the rights of the user.

5. Click **OK**

6. Save your configuration changes by clicking the **Save Configuration** button in the Management Application's toolbar.
Example of a correctly specified user name: USER001. Example of an incorrectly specified user name: PC001/USER001. The user should of course still specify a password and any required server information.

Add User Groups

User groups are logical groups created and used for practical purposes in the Management Application only. They are not in any way connected with user groups from central directory services such as, for example, Active Directory®.

By grouping users, you can specify rights for all users within a group in one go. If you have many users performing similar tasks, this can save you significant amounts of work.

Make sure you add groups before you add users: You cannot add existing users to groups.

1. In the Management Application’s navigation pane, expand Advanced Configuration, right-click Users, and select Add New User Group.
2. Specify a name for the group. Group names must be unique, and must not contain the following characters: < > & " / : * ? | [ ]
3. Click OK.
4. Specify General Access and Camera Access properties (see the following pages). These properties will determine the rights of the group’s future members.
5. Click OK
6. Save your configuration changes by clicking the Save Configuration button in the Management Application’s toolbar.
7. Now you can add users to the group: In the navigation pane, right-click the group you just created, and add Basic Users (see page 113) or Windows Users (see page 114) as required.

Configure User and Group Rights

User/group rights are configured during the process of adding users/groups, see Add Basic Users, Add Windows Users and Add User Groups in the previous.

Note that you can also add basic and Windows users through the Configure User Access wizard (see page 45). However, when using the wizard all users you add will have access all to cameras, including any new cameras added at a later stage.

If you at a later stage want to edit the rights of a user or group:

1. In the Management Application’s navigation pane, expand Advanced Configuration, expand Users, right-click the required user or group, and select Properties.
2. Edit General Access and Camera Access properties (see the following). These properties will determine the rights of the user/group.
3. Click OK
4. Save your configuration changes by clicking the Save Configuration button in the Management Application’s toolbar.
User and Group Properties

User Information

- **User name**: Only editable if the selected user is of the type basic user. Lets you edit the user name. User names must be unique, and must not contain the following characters: `< > & ' " \ / : * ? | [ ]`

- **Password**: Only editable if the selected user is of the type basic user. Lets you edit the password. Remember to repeat the password to be sure you have specified it correctly.

- **User type**: Non-editable field, displaying whether the selected user is of the type basic user or Windows user group.

Group Properties

- **Group name**: Lets you edit the group name. Group names must be unique, and must not contain the following characters: `< > & ' " \ / : * ? | [ ]`

General Access

When adding or editing basic users, Windows users or groups, specify general access settings:

- **Live**: Ability to access the Live tab in the Smart Client and Remote Client.

- **Playback**: Ability to access the Playback tab in the Smart Client and Remote Client.

- **Setup**: Ability to access the Setup tab in the Smart Client and Remote Client.

  **Tip**: By clearing the Live, Playback and Setup check boxes you can effectively disable the user’s/group’s ability to use the Smart Client and Remote Client. You can use this as a temporary alternative to deleting the user/group, for example while the user is on vacation.

- **Edit shared views**: Ability to create and edit views in shared groups in the Smart Client and Remote Client. Views placed in shared groups can be accessed by every user. If a user/group does not have this right, shared groups will be protected, indicated by a padlock icon in the Smart Client and Remote Client.

  Views created in a Smart Client can only be shared with other Smart Client users. Views created in a Remote Client can only be shared with other Remote Client users. It is not possible to share views across the two types of client.

- **Edit private views**: Ability to create and edit views in private groups in the Smart Client and Remote Client. Views placed in private groups can only be accessed by the user who created them. If a user/group does not have this right, private groups will be protected, indicated by a padlock icon in the Smart Client and Remote Client. Denying users the right to create their own views may make sense in some cases; for example in order to limit bandwidth use.

- **Administrator Access**: Ability to access and work with the Management Application. Selected and non-editable for Administrators, see page 113. Cleared and selectable for all other users.

For more information about shared and private views, see the separate Smart Client and Remote Client documentation.
Camera Access

When adding or editing basic users, Windows users or groups, 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.

In the **Live** column, the following features, all selected by default, are available:

- **Live:** Ability to view live video from the selected camera(s).
  - **PTZ:** Ability to use navigation features for PTZ (Pan/Tilt/Zoom) cameras. A user/group
    will only be able to use this right if having access to one or more PTZ cameras.
  - **PTZ preset positions:** Ability to 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.
  - **Output:** Ability to activate output (lights, sirens, door openers, etc.) related to the
    selected camera(s).
  - **Events:** Ability to use manually triggered events related to the selected camera(s).
    This feature is available in the Smart Client only.
  - **Incoming audio:** Ability to listen to incoming audio from microphones related to the
    selected camera(s). This feature is available in the Smart Client only.
  - **Manual recording:** Ability to manually start recording for a fixed time (defined by the
    surveillance system administrator, see page 65).

In the **Playback** column, the following features, all selected by default, are available:

- **Playback:** Ability to play back recorded video from the selected camera.
  - **AVI/JPEG Export:** Ability to export evidence as movie clips in the AVI format and as
    still images in the JPEG format.
  - **Database Export:** Ability to export evidence in database format. This feature is
    available in the Smart Client only.
  - **Sequences:** Ability to use the Sequences feature when playing back video from the
    selected camera.
- **Recorded audio**: Ability to listen to recorded audio from microphones related to the selected camera(s).

**Why can I not select certain features?** Typically, because the selected camera does not support the features. For example, you can only select PTZ-related features if the camera is a PTZ camera. Also, some of the features depend on the user’s/group’s General Access properties (see page 116): For example, in order have access to PTZ or output features, the user/group must have access to viewing live video; in order to use AVI/JPEG export, the user/group must have access to playing back recorded video.

**Why are some feature check boxes filled with squares?** 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 it is not allowed. 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; 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.
Logging

XProtect Essential is able to generate various logs:

- **Management Application log files.** These files log activity in the Management Application. A new log file is created for each day the Management Application is used. You cannot disable this type of logging. Management Application log files are named according to the structure AdminYYYYMMDD.log, for example Admin20091231.log.

- **Recording Server service log files.** These files log Recording Server service activity (see page 109). A new log file is created for each day the service is used. You cannot disable this type of logging. Recording Server service log files are named according to the structure RecordingServerYYYYMMDD.log, for example RecordingServer20091231.log.

- **Image Server service log files.** These files log activity on the Image Server service (see page 109). A new log file is created for each day the service is used. You cannot disable this type of logging. Image Server service log files are named according to the structure ISLog_YYYYMMDD.log, for example ISLog_20091231.log.

- **Image Import service log files.** These files log activity regarding the Image Import service, when this service is used for fetching pre-alarm images, and storing the fetched images in camera databases. Pre-alarm images is a feature available for selected cameras only; it enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. A new log file is created for each day the service is used. You cannot disable this type of logging. Image Import service log files are named according to the structure ImageImportLog_YYYYMMDD.log, for example ImageImportLog20091231.log.

- **Event log files.** These files log information about registered events (see page 102). A new log file is created for each day on which events occur. You cannot disable this type of logging. Event log files should be viewed using the Smart Client (use the Playback tab’s Alerts section).

- **Audit log files:** These files log Remote Client and 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.

All log files are by default placed in the appropriate All Users folder for the operating system used, for example C:\ProgramData\Milestone if running Windows Vista. 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.

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.
Configure System, Event, and Audit Logging

1. In the Management Application’s Navigation pane, expand Advanced Configuration, right-click Logs and select Properties.

2. Specify required properties (see the following) 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. When ready, click OK.

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

Log Properties

When you configure logging, you can define the following properties:

Logs (that is Management Application log, Recording Server service log, Image Server service log, Image Import service log)

- **Path**: These system log files are by default placed in the appropriate All Users folder for the operating system used, for example C:\ProgramData\Milestone if running Windows Vista. To specify another location for your log files, type the path to the required folder in the Path field, or click the browse button next to the field to browse to the required folder.

- **Days to log**: A new log file is created each day the Management Application and/or the services are used. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day’s activity is always logged, even with a value of 0 in the field. Therefore, if you specify 0, you will log current day’s activity; if you specify 1, you will keep one day plus the current day’s activity, and so on.

Event Log

- **Path**: Event log files are by default placed in the appropriate All Users folder for the operating system used, for example C:\ProgramData\Milestone if running Windows Vista. To specify another location for your event log files, type the path to the required folder in the Path field, or click the browse button next to the field to browse to the required folder.

- **Days to log**: A new log file is created for each day on which events occur. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day’s activity is always logged, even with a value of 0 in the field. Therefore, if you specify 0, you will log current day’s activity; if you specify 1, you will keep one day plus the current day’s activity, and so on.

Audit Log
Enable audit logging: Audit logging is the only type of XProtect Essential logging which is not compulsory. Select/clear the check box to enable/disable audit logging.

Path: Audit log files are by default placed in the appropriate All Users folder for the operating system used, for example C:\ProgramData\Milestone if running Windows Vista. To specify another location for your audit log files, type the path to the required folder in the Path field, or click the browse button next to the field to browse to the required folder.

Days to log: A new log file is created for each day with audit logging enabled and client user activity. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day’s activity is always logged (provided audit logging is enabled and there is user activity). Therefore, if you specify 1, you will keep one day plus the current day’s activity. Note that if you specify 0 (zero), audit log files will be kept indefinitely (disk space permitting).

Minimum logging interval: Minimum number of seconds between logged events. Specifying a high number of seconds between logged events may help reduce the size of the audit log. Default is 60 seconds.

In sequence timespan: Number of seconds to pass for viewed images to be considered to be within the same sequence. Specifying a high number of seconds may help limit the number of viewed sequences logged, and thus reduce the size of the audit log. Default is ten seconds.

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 XProtect Essential’s 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 used, for example C:\ProgramData\Milestone if running Windows Vista.

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):

Log integrity information was not found. Log integrity can’t be guaranteed.  
The log file could not be checked for integrity.

Log information does not match integrity information. Log integrity can’t be guaranteed.  
The log file exists, but does not contain the expected information. Thus, log integrity cannot be guaranteed.

[Log file name] not found  
The log file was not present.

[Log file name] is empty  
The log file was present, but empty.

Last line changed/removed in [log file name]  
The last line of the log file did not match validation criteria.

Encrypted data missing in [log file name] near line [#]  
The encrypted part of the log line in question was not present.
- **Inconsistency found in [log file name] near line [#]**
  The log line does not match the encrypted part.

- **Inconsistency found in [log file name] at beginning of log file**
  The log file header is not correct. This situation is most likely to occur if a user has attempted to delete the beginning of a log file.
Central

Certain variants of XProtect Essential do not support XProtect Central. This means that you might see this information even if XProtect Central is not present in your surveillance system setup.

In XProtect Essential, this XProtect Central dialog is used for specifying login settings for Milestone Integrate Platform (MIP).

The XProtect Central Settings lets you specify the login settings required for an XProtect Central server to access the surveillance system in order to retrieve status information and alarms.

1. In the Management Application’s Navigation pane, expand Advanced Configuration, right-click Central and select Properties.

2. Enable the use of Central connections by selecting the Enable Milestone XProtect Central check box.

3. Specify required properties:
   - **Enable Milestone XProtect Central connections:** Enables the use of XProtect Central connections, allowing you to specify further properties.
   - **Login Name:** Type the name used for the connection between the XProtect Essential and XProtect Central servers. The name must match the name specified on the XProtect Central server itself. Default name is Name.
   - **Password:** Type the password used for the connection between the XProtect Essential and XProtect Central servers. The password must match the password specified on the XProtect Central server itself. Default password is Pass.
   - **Port:** Type the port number to which the XProtect Central server should connect when accessing the XProtect Essential server. The port number must match the port number specified on the XProtect Central server itself. Default port is 1237.

   When ready, click OK.

4. Save your configuration changes by clicking the Save Configuration button in the Management Application’s toolbar.
System

Find Version, License and Plug-in Information

Knowing the exact version of your XProtect Essential system can be important if you require support, want to upgrade your system, etc. In such cases, you may also want to know which plug-ins your XProtect Essential system uses.

To view such information, select About... in the Management Application’s Help menu.

Configure Default File Paths

XProtect Essential uses a number of default file paths:

- **Default recording path for new cameras**: All new cameras you add will by default use this path for storing recordings. If required, you can change individual cameras’ recording paths as part of their individual configuration (see page 74), but you can also change the default recording path so all new cameras you add will use a path of your choice.

- **Default archiving path for new cameras**: All new cameras you add will by default use this path for archiving (see page 86). 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 for archiving (see page 62).

- **Configuration path**: The path by default used for storing your XProtect Essential system’s configuration.

To change any of the default file paths:

1. If changing the configuration path, stop all services (see page 109). This step is not necessary if changing the default recording or archiving path.

2. In the Management Application’s menu bar, select Application Settings > Default File Paths...

3. You can now overwrite required paths. Alternatively, click the browse button next to the required field and browse to the required location.

   For the default recording path, you are only able to specify a path to a folder on a local drive. If using a network drive, it would not be possible to save recordings if the network drive became unavailable.

   If you change the default recording or archiving paths, and there are existing recordings at the old locations, you will be asked 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 in the Management Application’s toolbar.

6. Restart all services (see page 109).

## Restore System Configuration from 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 & Stop Services on page 109).

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.
**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 are subsequently able to 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 (see page 131) is a backup of your entire surveillance system setup (including, among other things, log files, event configuration, restore points, view groups, and Management Application, Smart Client and Remote Client 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**

The same import method is used regardless of whether the 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 configuration is applied.

**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:
- **HardwareOldMacAddress**
  The MAC address of the hardware device used in the template configuration. Required format: 12 hex characters without spaces or six groups of two hex characters separated with dashes (-) or colons (:).

You can furthermore include these optional parameters:

- **HardwareNewMacAddress**
  The MAC address of the new hardware device to be used in the real configuration. Required format: 12 hex characters without spaces or six groups of two hex characters separated with dashes (-) or colons (:).

- **HardwareAddress**
  IP address of the hardware device.

- **HardwareUsername**
  User name for hardware device’s administrator account.

  In the extremely rare cases where a particular user name has previously been required for a device, but you now want the user name to be <blank>, you cannot use the CSV file to specify <blank>. The reason is that no information is interpreted as “leave the user name as it currently is.” If you need the new user name to be <blank>, you should not change it through the CSV file. Instead, change it as part of the hardware device’s Network, Device Type & License properties (see page 56) after you have imported the other changes through the CSV file.

- **HardwarePassword**
  Password for hardware device’s administrator account.

  In the extremely rare cases where a particular password has previously been required for a device, but you now want the password to be <blank>, you cannot use the CSV file to specify <blank>. The reason is that no information is interpreted as “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 & License properties (see page 56) after you have imported the other changes through the CSV file.

- **HardwareDeviceName**
  Name of the hardware device. Name must unique, and must not contain any of the following special characters: < > & ' \ : * ? | [ ]

- **CameraName[number]**
  Name of the camera. Must appear as CameraName1, CameraName2, etc. in the header line since a hardware device can potentially have more than one camera attached. Names must be unique, and must not contain any of the following special characters: < > & ' \ : * ? | [ ]

- **CameraShortcut[number]**
  Number for keyboard shortcut access to the camera in the Smart Client. Must appear as CameraShortcut1, CameraShortcut2, etc. in the header line since a hardware device can potentially have more than one camera attached. A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits.

- **GenerateNewCameraGuid[optional number]**
  Lets you specify whether to generate a new GUID for a camera; this is especially relevant if using a cloned configuration (see page 126) as your template, since all GUIDs are removed from cloned configurations. If specified as, for example, GenerateNewCameraGuid1, information relates to a specific camera, otherwise to all cameras attached to the hardware device. Any character means “yes, generate a new GUID.”
- **PreBufferLength [optional number]**
  Required length (in seconds) of pre-recording. If specified as, for example, `PreBufferLength1`, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **PostBufferLength [optional number]**
  Required length (in seconds) of post-recording. If specified as, for example, `PostBufferLength1`, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **RecordingPath [optional number]**
  Path to the folder in which a camera’s database should be stored. If specified as, for example, `RecordingPath1`, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **ArchivePath [optional number]**
  Path to the folder in which the camera’s archived recordings (see page 86) should be stored. Remember that an archiving path is only relevant if not using dynamic paths for archiving (see page 62). If specified as, for example, `ArchivePath1`, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **OldRecordingsNewPath [optional number]**
  Lets you specify what to do with old recordings in case `RecordingPath` or `ArchivePath` have been changed. If this parameter is not specified, default behavior is `Leave` (see the following). If specified as, for example, `OldRecordingsNewPath1`, information relates to a specific camera, otherwise to all cameras attached to the hardware device. Valid options are: `Delete` (deletes old recordings), `Leave` (leaves old recordings for offline investigation but unavailable for online system), or `Move` (moves old recordings to archive).

- **OldRecordingsNewMac [optional number]**
  Lets you specify what to do with old recordings in case a new MAC address has been specified for the hardware device. If this parameter is not specified, default behavior is `Leave` (see the following). If specified as, for example, `OldRecordingsNewMac1`, information relates to a specific camera, otherwise to all cameras attached to the hardware device. Valid options are: `Delete` (deletes old recordings), `Leave` (leaves old recordings for offline investigation but unavailable for online system), or `Inherit` (renames all old recording folders according to the new MAC address, thus making them available for the online system).

- **RetentionTime [optional number]**
  Required retention time (in minutes). Remember that retention time is the total of recording time plus archiving time. If specified as, for example, `RetentionTime1`, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **MjpegLiveFrameRate [optional number]**
  Required MJPEG live frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If specified as, for example, `MjpegLiveFrameRate1`, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **MjpegRecordingFrameRate [optional number]**
  Required MJPEG recording frame rate (in number of frames; depending on what has been configured on the camera, it will then know whether it is frames per second, minute, or hour). If you need to specify a value which includes a decimal separator, use the full stop character (example: 7.62). If specified as, for example, `MjpegRecordingFrameRate1`, information relates to a specific camera, otherwise to all cameras attached to the hardware device.
- **MotionSensitivity[optional number]**
  A value between 0-256; corresponds to using the Sensitivity slider when configuring motion detection settings in the Management Application. If specified as, for example, MotionSensitivity1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **MotionDetectionThreshold[optional number]**
  A value between 0-10000; corresponds to using the Motion slider when configuring motion detection settings in the Management Application. If specified as, for example, MotionDetectionThreshold1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **MotionDetectionInterval[optional number]**
  Lets you specify how often motion detection analysis should be carried out on video from the camera. Specified in milliseconds. The interval is applied regardless of the camera’s frame rate settings. If specified as, for example, MotionDetectionInterval1, information relates to a specific camera, otherwise to all cameras attached to the hardware device.

- **ServerName**
  Name with which the XProtect Essential will appear when listed in clients. Name must be unique, and must not contain any of the following special characters: < > & ` " \ / : * ? | [ ]

- **ServerPort**
  Port number to use for communication between the XProtect Essential server and clients.

- **OnlineVerification**
  If this parameter is used, all online hardware devices found using HardwareOldMacAddress are updated. All other hardware devices are not updated. Any character means “yes, use online verification.”

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

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

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HardwareAddress</td>
<td>HardwareUsername</td>
<td>HardwarePassword</td>
</tr>
<tr>
<td>2</td>
<td>192.168.200.220 AdminAccountUsername</td>
<td>005eCR3tqa56w0rd</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>192.168.200.221 AdminAccountUsername</td>
<td>T0PsecretPASSword</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>192.168.200.222 RootaccountUsername</td>
<td>T0PsEcReTpaSvOcd</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>192.168.200.223 AdminAccountUsername</td>
<td>T0P3CR3Tpa55w0rd</td>
<td></td>
</tr>
</tbody>
</table>

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

### Back Up System Configuration

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.

The following describes backup of the configuration in XProtect Essential version 1.0. If you need information about how to back up configuration from a different XProtect product, such as XProtect Basis+, see Upgrade from a Previous Version on page 18.

In the following, we assume that you have not changed XProtect Essential's default configuration path (see page 124), 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 page 63) 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 page 125). This allows you to not only restore the backed-up configuration, but also to revert to an earlier point in that configuration if required.

To Restore Your Backed-up 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.

Handle 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 adjusted forward one hour sometime during the spring season and adjusted backward sometime during the fall season, hence the saying spring forward, fall back. 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 thus has 23 hours. In that case, there is simply 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 thus 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 by opening the archived database directly.

**Protect 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 biggest reason for corrupt databases is the surveillance system 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 surveillance system server from being shut down abruptly is to equip your surveillance system server 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 in question will not be given the chance to save its state or data before it is terminated. This may in turn 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, make sure you click the *No* button when the warning message asks you if you really want to terminate the process.

**Hard Disk Failure: Protect Your Drives**

Hard disk drives are mechanical devices, and as such they are vulnerable to external factors. The following are examples of external factors which may damage hard disk drives and lead to corrupt camera databases:

- Vibration (make sure the surveillance system server and its surroundings are stable)
- Strong heat (make sure the server has adequate ventilation)
- Strong magnetic fields (avoid)
- Power outages (make sure you use a UPS; see more information in the previous)
- Static electricity (make sure you ground yourself if you are going to handle a hard disk drive).
- Fire, water, etc. (avoid)
Drivers

Update Video Device Drivers

Video device drivers are small programs used for controlling/communicating with the camera devices connected to the XProtect Essential system. Video device drivers are installed automatically during the initial installation of your XProtect Essential system. However, new versions of video device drivers—so-called Device Packs—are released and made available for free on www.milestonesys.com from time to time.

We recommend that you always use the latest version of video device drivers. When updating video device drivers, there is no need to remove the old video device drivers first; simply install the latest version on top of any old version you may have.

**IMPORTANT:** When you install new video device drivers, your system will not be able to 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. Double-click the downloaded video device driver file DeviceInstaller.exe to begin installation.

   Depending on your security settings, one or more Windows security warnings may appear after you click the link. If such security warnings appear, accept security warnings by clicking the Run button (button may have other name; exact button name depends on your operating system version).

3. Select required language, and click OK. This will open the Video Device Driver Setup Wizard, which will guide you through the installation. Click the Next button and follow the wizard.

4. When the wizard is complete, remember to start the Recording Server service again.

**Driver IDs**

You find the list of hardware driver IDs for use with the Replace Hardware Wizard as an appendix on page 155 of this manual.
Clients and Ancillary Applications

Users can get client access to the XProtect Essential surveillance system in different ways:

- **With a Smart Client.** Very feature-rich and highly flexible for future integration of plugins, etc. Installed locally on users' computers. In general, it is recommended to always use the latest version of the Smart Client to best utilize any possible new features and functions included in your XProtect Essential surveillance system. Once installed, the Smart Client has its own built-in help system.

  Alternatively, refer to the Smart Client User's Manual, available on the XProtect Essential software DVD as well as from www.milestonesys.com. Related topics in this manual: Install Smart Client from Server (page 137) • Install Smart Client from DVD (page 138) • Install Smart Client Silently (page 138).

- **With a Remote Client.** Does not offer nearly as many features as the Smart Client. The main benefit of the Remote Client is that it is accessed through a browser and run directly from the surveillance system server. This eliminates the need for installing any client software on the user's computer.


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.

In order to get hold of a Remote Client or 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 (see page 140) to control which clients and language versions should be available to users on the welcome page.

When deciding which access client solution is the best choice for your organization, you may find it helpful to review the following. Note that systems and requirements differ from organization to organization. The following questions and answers are thus for guidance only.

**Is it acceptable to install client software on remote users' computers?**
- **Yes:** Use the Smart Client.
- **No:** Use the Remote Client; remote users run the Remote Client straight from the XProtect Essential server.

**Will you require a large amount of future flexibility from your remote access solution?**
- **Yes:** Use the Smart Client. The Smart Client offers a high degree of flexibility for integration of new features, plugins, etc.
- **No:** Use the Remote Client.
Do you require a very feature-rich client application?

- **Yes:** Use the Smart Client. The Smart Client offers considerably more features than the other solutions.
- **No:** Use the Remote Client.

Do you require a large amount of flexibility re. remote users' ability to export data for use as evidence, etc.?

- **Yes:** Use the Smart Client. The Smart Client offers the ability to—individual user rights permitting—export data in the AVI (movie clip) and JPEG (still image) as well as XProtect Enterprise database formats.
- **No:** Use the Remote Client. The Remote Client offers the ability to—individual user rights permitting—export evidence in the AVI and JPEG formats.

Will you use a .NET-based client application?

The .NET software development platform allows the interconnection of computers and services for the exchange and combination of data and objects. The platform makes extensive use of so-called web services, which provide the ability to use the web rather than single applications for various services. This in turn provides the ability for centralized data storage as well as automated updating and synchronization of information. The .NET platform enhances software developers' ability to create re-usable and customizable modules, which makes it possible to develop highly flexible software solutions. You can therefore, as a rule of thumb, expect .NET-based software to be highly flexible, ready for integration of new features, plugins, etc. However, organizations and their requirements are different, and some organizations find that the high degree of interconnection of services and computers inherent in a .NET-based solution is not desirable. Instead, such organizations rely on more classic Windows solutions.

- **Yes:** Use the Smart Client. The .NET-based Smart Client offers more features for remote users than the other solutions. .NET Framework, downloadable from http://www.microsoft.com/downloads/, is required on computers running the Smart Client. See separate the Smart Client documentation for exact system requirements.
- **No:** Use the Remote Client. The Remote Client is not a .NET-based solution.

## Smart Client

### Install Smart Client from Server

Typically, you download the Smart Client from the surveillance system server, then install it on your computer. Alternatively, your surveillance system administrator may ask you to install the Smart Client from a DVD (see Install Smart Client from DVD on page 138).

Surveillance system administrators can automatically get a Smart Client installed on the surveillance system server; this happens as part of the surveillance system server installation. To download and install the Smart Client from the surveillance system server, do the following:

1. Verify that your computer meets the Smart Client’s minimum system requirements (see page 13).
2. Open an Internet Explorer browser (version 6.0 or later), and connect to the surveillance system server at the URL or IP address specified by your system administrator. When you are connected to the surveillance system server, you will see a welcome page.
3. On the welcome page, select your required language in the menu in the top right corner. Then go to the welcome page's Smart Client *Installers* section, and click *All Languages*.
under the required bit version.

4. Depending on your security settings, you may receive one or more security warnings (Do you want to run or save this file?, Do you want to run this software? or similar; exact wording depends on your browser version). When this is the case, accept the security warnings (by clicking Run or similar; exact button names depend on your browser version).

5. The Smart Client Setup Wizard begins. In the wizard, click Continue, and follow the installation instructions.

Install Smart Client form DVD

Typically, you download the Smart Client from the surveillance system server, then install it on your computer. Alternatively, your surveillance system administrator may ask you to install the Smart Client from a DVD:

1. Verify that your computer meets the Smart Client’s minimum system requirements (see page 13).

2. Insert the surveillance system software DVD, wait for a short while, select required language, then click the Install Milestone XProtect Smart Client link.

3. Depending on your security settings, you may receive one or more security warnings (Do you want to run or save this file?, Do you want to run this software? or similar; exact wording depends on your browser version). When this is the case, accept the security warnings (by clicking Run or similar; exact button names depend on your browser version).

4. When the installation wizard starts, click Continue to continue the installation and follow the steps in the installation wizard.

Install Smart Client Silently

For surveillance system administrators, it is possible to deploy the Smart Client or XProtect Essential to users’ computers using tools such as Microsoft Systems Management Server (SMS). Such tools let 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, such as the Smart Client, over local networks.

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 would thus typically be:
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. When performing silent installation of the software there are generally two cases:

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 Smart Client installation:
   >MilestoneXProtectSmartClient.exe -quiet

   For XProtect Essential installation:
   >MilestoneXProtectEssentialInstaller.exe -quiet

   This will perform a quiet installation of the 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 Smart Client:
   >MilestoneXProtectSmartClient.exe --generateargsfile=arg.xml

   For XProtect Essential:
   >MilestoneXProtectEssentialInstaller.exe --generateargsfile=arg.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 Smart Client:
   >MilestoneXProtectSmartClient.exe --arguments=arg.xml --quiet

   For XProtect Essential:
   >MilestoneXProtectEssentialInstaller.exe --arguments=arg.xml --quiet

Remote Client

The main benefit of the Remote Client is that it is accessed through a browser and run directly from the surveillance system server. This eliminates the need for installing any client software on the user’s computer. To access the Remote Client:
1. Open an Internet Explorer browser (version 6.0 or later), and connect to surveillance system server. The address format is typically:

   http://[surveillance_system_server_address]:[port_number]

   **Tip:** The port number is only required if using another port than the default port for XProtect Essential’s Image Server service, port 80.

   When you connect to the server, you will see a welcome page. On the welcome page, click the Remote Client link in order to view the Remote Client login dialog.

2. To log in, specify information in the following fields:

   - **Previous Logins:** Only available if you have logged in before. Lets you reuse previously specified login details (except any password, which you must always type yourself). This can greatly speed up the login process.

   - **Address:** Type the URL or IP address of the surveillance system server.

   - **Port:** Specify the port number to use when logging in to the Remote Client. In most circumstances, port 80 is used.

   - **Authentication:** Select required authentication method.

     - **Windows (current user),** with which you will be authenticated through your current Windows login, and do not have to specify any user name or password. This is the default authentication method, that is the method which is automatically used unless you select another method.

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

     - **Basic,** with which you will be authenticated through a user/password combination defined on the surveillance system server.

   - **Username:** Type your user name. The user name is case-sensitive, that is there is a difference between typing, for example, amanda and Amanda.

   - **Password:** Type your password. The password is case-sensitive.

3. Click the **Login** link. After a short wait, you get access to the Remote Client. Content in the Remote Client is grouped on three tabs: **Live, Playback** and **Setup**.

   The **Live** tab is used for viewing live video from cameras, the **Playback tab** is used for finding and playing back recorded video, and the **Setup tab** is used for configuring the Remote Client.


---

**Download Manager**

The Download Manager lets you 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.
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.

- **The Remote Client.** Users connect to welcome page and log in to the Remote Client, which runs in a browser without any need for software installation.

- **Various plugins.** Downloading such plugins can be relevant for users if your organization uses add-on products with the XProtect Essential solution.

**What Does It Look Like?**

The welcome page is a simple web page with links to downloading or running various features. It is available in a number of languages; users select their required language from a menu in the top right corner of the welcome page.

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

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

If the Image Server service has been configured with a port number other than the default port 80 (you configure this as part of the server access properties, see page 11046), users must specify the port number as well, separated from the IP address or hostname by a colon:

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

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

**Initial Look**

Immediately after you install XProtect Essential, the welcome page will provide access to two features: A Smart Client in all languages and a Remote Client in a language version matching the language version of your XProtect Essential system. Furthermore, 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 in the following.
This example shows the welcome page as it looks immediately after installation of an English-language version of XProtect Essential:

Welcome page from the English-language version of XProtect Essential Download Manager. By default, it provides access to an All language version of the Smart Client and to the Remote Client in a language version matching your XProtect Essential system.

Default Configuration

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 default configuration provides users with access to two features: A Smart Client with all languages and a Remote Client in a language version matching the language version of your XProtect Essential system.

The Download Manager’s configuration is represented in a tree structure.

Download Manager’s Tree Structure Explained:

- The first level of the tree structure (1 in the example illustration) simply indicates that you are working with a XProtect Essential system.
- The second level (2) indicates that this is the default setup.
- The third level (3) 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, etc.).
- The fourth level (4) refers to the features which are—or can be made—available to users. In the example, these features are limited to the Smart Client and the Remote Client.
- The fifth level (5) refers to particular versions of each feature, such as 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. And for the Remote Client, in this example, only English versions are initially listed.

In the example, XProtect Essential has been installed an English-language version. If we expand one of the other languages in the tree structure's second level, for example Arabic, we will see that users who select the Arabic version of the welcome page will have access to all language versions of the Smart Client, but also only access to the English version of the Remote Client.

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 until it is needed.
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.

**Make New Features Available to Users**

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

**Installing New Features on Server**

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

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.

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 they will by default be selected in the Download Manager, and thus 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 Download Manager's tree structure.

**Tip:** You can change the sequence in which features and languages are displayed on the welcome page: In the Download manager’s tree structure, simply drag items and drop them at the required position.

**Hide or Remove 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 Download Manager’s 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 folder or relevant language folder, so you can re-install them later if required.

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

  2. In the Remove Features window, select the features you want to remove. In the following example, we have selected to remove a Spanish Smart Client installer and a Spanish Remote Client.
3. Click OK. Confirm by clicking Yes.

Virus Scanning

If you are using virus scanning software on the XProtect Essential server, it is likely that the virus scanning will use a considerable amount of system resources on scanning data from the Download Manager. If allowed in your organization, disable virus scanning on all or parts of the XProtect Essential server. Read more about virus scanning on page 15.

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 (a.k.a. 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.

Right-click the icon to start and stop the Recording Server service, open the Management Application, monitor system status, view log files, and view version information. The Recording Server Manager’s features are very simple and self-explanatory. Only the ability to monitor system status deserves a special mention:

By right-clicking the notification area’s Recording Server icon and then selecting Show System Status, you get access to the Status window. 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 page 97).
  - the Recording Server service has been stopped.
- **Red** indicates that the server or camera is not running. This may because it has been unplugged or due to a network or hardware error. Errors are listed in the Recording Server log file.
Place your mouse pointer over a camera in the status window to view details about the camera in question. The information updates approximately every 10 seconds.

- **Resolution**: The resolution of the camera.
- **FPS**: The number of frames per second (a.k.a. frame rate) currently used by the camera. The number updates each time the camera has received 50 frames.
- **Frame count**: The number of frames received from the camera since the Recording Server service was last started.
- **Received KB**: The number of kilobytes sent by the camera since the Recording Server service was last started.
- **Offline**: Indicates the number of times the camera has been offline due to an error.
Removal

Remove the Entire Surveillance System

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, do the following:

1. Shut down all XProtect Essential components.

   The following procedure describes standard system component removal in recent Windows versions; the procedure may be slightly different in older Windows versions:

2. In Windows' Start menu, select Control Panel, and then...
   - If using Category view, find the Programs category, and click Uninstall a program.
   - If using Small icons or Large icons view, select Programs and Features.

3. In the list of currently installed programs, right-click the Milestone XProtect Essential entry.

4. Select Uninstall and follow the removal instructions.

What happens to my recordings and configuration files? 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 later install XProtect Essential again.

Remove Individual Components

Remove the Smart Client

To remove a Smart Client which was installed separately, do the following on the computer on which the Smart Client is installed:

1. In Windows' Start menu, select Control Panel, and then...
   - If using Category view, find the Programs category, and click Uninstall a program.
   - If using Small icons or Large icons view, select Programs and Features.

2. In the list of currently installed programs, right-click the Milestone XProtect Smart Client entry.

3. Select Uninstall and follow the removal instructions.

It is only possible to remove a Smart Client in this way if it was installed as a separate program, see page 137. This is due to the fact that if a Smart Client is installed as part of an entire XProtect Essential surveillance system installation, it does not have its own entry in the list of programs.
To remove a Smart **Client which was installed as part of an entire surveillance system installation**, you must remove your entire surveillance system, see page 146. Alternatively, you can replace your Smart Client by installing a new separate Smart Client (see page 137) on top of your surveillance system. Both tasks must take place on the computer on which the Smart Client is installed.

**Remove Video Device Drivers**

Video device drivers are small programs used for controlling/communicating with the camera devices connected to an XProtect Essential system. To remove the video device drivers, do the following:

1. In Windows' **Start** menu, select **Control Panel**, and then...
   - If using Category view, find the Programs category, and click **Uninstall a program**.
   - If using Small icons or Large icons view, select **Programs and Features**.

2. In the list of currently installed programs, right-click the **Video Device Pack V. [version number]** entry.

3. Select **Uninstall** and follow the removal instructions.
Built-in Help System

To use XProtect Essential’s built-in help system, simply click the Help button in the Management Application’s toolbar. Alternatively, press the F1 key on your keyboard while using XProtect Essential. The help system opens in a separate window, allowing 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 working in a particular XProtect Essential dialog, the help system automatically displays help matching that dialog.

Navigating the Built-in Help System

To navigate between the help system’s contents, simply 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 will be familiar with this type of navigation from, for example, Windows Explorer.

- **Search Tab:** Search for help topics containing particular terms of interest. For example, you can search for the term zoom and every help topic containing the term zoom will be listed in the search results. Double-clicking a help topic title in the search results list will open the required topic.

- **Favorites Tab:** Build a list of your favorite help topics. Whenever you find a help topic of particular interest to you, simply 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. Clicking such a link will display detailed information immediately below the link itself; the content on the topic simply expands. Expanding drop-down links thus help save space.

**Tip:** To quickly hide all texts from expanding drop-down links in a help topic, simply 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 click OK.

**Tip:** When printing a help topic, it will be printed as you see it on your screen. Therefore, if a topic contains expanding drop-down links, click each required drop-down link to display the text in order for it to be included when you print. This allows you to create targeted printouts, containing exactly the amount of information you require.
Hardware Input ........................................................................................................ 103

Hardware input events ................................................................. 103, 106

Hardware Input Events ........................................................................... 105

Hardware Output .............................................................................. 103, 108

Hardware Output on Event .............................................................. 109

Help System, Built-in ................................................................. 149

—I—

IIS ........................................................................................................ 13

Image Import Service ................................................................. 110

Image Import Service Log .................................................................. 120, 121

Image Server Service ........................................................................ 110

Image Server Service Log ................................................................. 120, 121

Import Changes to Surveillance System Configuration ....................... 128

Import from CSV File Method, Add Hardware Devices Wizard ............. 34

Inherit/Delete/Leave Existing Database ............................................... 49

Input ........................................................................................................ 103

Installation .......................................................................................... 17

Integrity Checks, Log ........................................................................... 122

Internet Information Services .............................................................. 13

IPIX ...................................................................................................... See Fisheye

—L—

Language Support & XML, Properties for Client Access to Surveillance System .................................................................................. 112

Licenses .................................................................................................. 51

Live Video, View in Management Application ..................................... 84

Local IP Ranges .................................................................................... 112

Log Check Service ................................................................................ 110

Logging .................................................................................................. 120

—M—

Management Application ................................................................. 23

Management Application Behavior, Change/Reset .............................. 23

Management Application Configuration ............................................. 127

Management Application Log ............................................................. 120, 121

Management Application, View Live Video in .................................... 84

Manual events ................................................................. 103, 106, 108, 110

Manual Events ................................................................................... 106

Manual Method, Add Hardware Devices Wizard .................................. 32

Manual Recording, Camera Properties ............................................ 65

Microphone, Default ........................................................................... 68

Microphones, Configuration .............................................................. 93

Milestone Integrate Platform ............................................................. 124

MIP ........................................................................................................ 124

MJPEG .............................................................................................. 65, 71, 98
Milestone XProtect Essential 2.0; Administrator’s Manual

Motion Detection..........................43, 77
Motion Detection & Exclude Regions, Camera Properties .................77
MPEG ...............................................67, 72
Name & Video Channels, Hardware Device Properties ..................56
Network, Device Type & License, Hardware Device Properties ..........56
Network, Minimum Requirements ...........................................13
Online Activation Error ..................................................54
Online Period, Scheduling Property for Cameras ......................97
Operating System, Minimum Requirements ..........................13
Output.............................................103, 108
Output Control on Event .............................................109
Output, Camera Properties .............................................76
Pan/Tilt/Zoom ........................................... See PTZ
Paths, Default............................................125
PDA Client.............................................137
Plug-in Information .............................................125
Polling Interval ..........................................104
Post-alarm Images ..........................................110
Post-recording ..........................................64, 73
Pre-alarm Images ..........................................110, 120
Pre-recording ..........................................64, 73
Preset Positions, PTZ .........................................81
Privacy Masking............................................80
Privacy Option ............................................24
PTZ ................................................57, 81
PTZ Device, Hardware Device Properties ................................57
PTZ on Event, Camera Properties ..................................83
PTZ Preset Positions, Camera Properties ................................81
PTZ Type ................................................81
RAM, Minimum Requirements ........................................13
Recording & Archiving Paths, Camera Properties ......................61, 74
Recording Path for New Cameras, Default ..........................125
Recording Server Manager .........................................145
Recording Server Service ..........................................110
Recording Server Service Log .........................................120, 121
Recording Settings, Camera Properties ................................73
Recordings ...............................................60
—V—
Version Information .................................................................................................................................. 125
Video Device Drivers .................................................................................................................................. 136
Video Encoder ................................................................................................................................................ 56, 57
Video Recording, Camera Properties ............................................................................................................. 63
Video Server .................................................................................................................................................. 52
See Video Encoder
Video, View Live in Management Application .............................................................................................. 84
Virus Scanning ................................................................................................................................................ 15
VMD ................................................................................................................................................................. 43, 77

—W—
Windows User................................................................................................................................................ 46
Wizards ........................................................................................................................................................... 26

—X—
XProtect Central ............................................................................................................................................. 124
Appendix: Hardware Driver IDs

If using the Add Hardware Devices Wizard’s Import from CSV File option (see page 34), you must—if cameras and server are offline—specify a HardwareDriverID for each hardware device you want to add. In the following, IDs for all hardware devices supported at the time of release of this version of XProtect Essential are listed.

The list is sorted alphabetically by device, with the corresponding ID at the end of each line. Example: ACTI ACD-2100 105 indicates that you should use 105 as the ID if adding an ACTi ACD-2100 hardware device.

This list is for guidance only; IDs are subject to change without notice. More devices may be supported by the time you read this, as new versions of video device drivers—so-called Device Packs—are released at regular intervals. To view a current list of IDs, view the release notes for the Device Pack used in your organization. Alternatively visit www.milestonesys.com for the latest information.

360 Vision IP Dome 320
ACTi ACD-2000Q 361
ACTi ACD-2100 105
ACTi ACD-2200 173
ACTi ACD-2300 152
ACTi ACD-2400 228
ACTi ACM-1011 105
ACTi ACM-1100 series 105
ACTi ACM-1230 series 105
ACTi ACM-1310 series 105
ACTi ACM-1430 series 105
ACTi ACM-1511 105
ACTi ACM-3001 105
ACTi ACM-3011 105
ACTi ACM-3100 series 105
ACTi ACM-3210 series 105
ACTi ACM-3300 series 105
ACTi ACM-3400 series 105
ACTi ACM-3511 105
ACTi ACM-3601 105
ACTi ACM-3701 105
ACTi ACM-4000 series 105
ACTi ACM-4100 series 105
ACTi ACM-4200 series 105
ACTi ACM-5001 105
ACTi ACM-5600 series 105
ACTi ACM-5711 105
ACTi ACM-5801 105
ACTi ACM-7400 series 105
ACTi ACM-7511 105
ACTi ACM-8100 series 105
ACTi ACM-8200 series 105
ACTi ACM-8201 105
ACTi ACM-8211 105
ACTi ACM-8511 105
ACTi CAM-5100H 105
ACTi CAM-5100M 105
ACTi CAM-5100S 105
ACTi CAM-5120 105
ACTi CAM-5130 105
ACTi CAM-5140 105
ACTi CAM-5150 105
ACTi CAM-5200 series 105
ACTi CAM-5220 series 105
ACTi CAM-5300 series 105
ACTi CAM-5320 series 105
ACTi CAM-5500 105
ACTi CAM-5520 105
ACTi CAM-6100 105
ACTi CAM-6110 105
ACTi CAM-6120 105
ACTi CAM-6200 105
ACTi CAM-6210 105
ACTi CAM-6220 105
ACTi CAM-6230 105
ACTi CAM-6500 105
ACTi CAM-6510 105
ACTi CAM-6520 105
ACTi CAM-6600 105
ACTi CAM-6610 105
ACTi CAM-6620 105
ACTi CAM-6630 105
ACTi CAM-7100-series 105
ACTi CAM-7200-series 105
ACTi CAM-7300-series 105
ACTi SED-2100R 105
ACTi SED-2100S 105
ACTi SED-2120/2120T 105
ACTi SED-2130 105
ACTi SED-2140 105
ACTi SED-2200 105
ACTi SED-2300Q 117
ACTi SED-2310Q 117
ACTi SED-2320Q 117
ACTi SED-2400 105
ACTi SED-2410 141
ACTi SED-2420 141
ACTi SED-2600 152
ACTi SED-2610 152
ACTi TCD-2100 385
ACTi TCD-2500 385
ACTi TCM-1231 334
ACTi TCM-1511 334
ACTi TCM-3011 334
ACTi TCM-3411 334
ACTi TCM-3511 334
ACTi TCM-4101 327
ACTi TCM-4201 334
ACTi TCM-4301 327
ACTi TCM-5001 334
ACTi TCM-5311 334
ACTi TCM-5601 334
ACTi TCM-7011 334
ACTi TCM-7411 334
ACTi TCM-7811 334
ACTi TMU-9501 385
ACTi TMU-9611 385
ACTi TMU-9811 385
ACTi TMU-9911 385
Adam 6050 129
Adam 6060 108
Adam 6066 108
AgileMesh 100 145
American Dynamics VideoEdge Dome 157
American Dynamics VideoEdge IP Box Camera 157
APPRO LC-7224 series 156
APPRO LC-7226 series 157
Apro Technology H1000 series 255
Arecont AV1300 140
Arecont AV1305 140
Arecont AV1310 140
Arecont AV1315 140
Arecont AV1325 140
Arecont AV1355 140
Arecont AV2100 140
Arecont AV2105 140
Arecont AV2110 140
Arecont AV2155 140
Arecont AV2805 140
Arecont AV2815 140
Arecont AV2825 140
Arecont AV3100 140
Arecont AV3105 140
Arecont AV3110 140
Arecont AV3130 140
Arecont AV3135 140
Arecont AV3155 140
Arecont AV5100 140
Arecont AV5105 140
Arecont AV5110 140
Arecont AV5155 140
Arecont AV8180 154
Arecont AV8185 154
Arecont AV8360 154
Arecont AV8365 154
Arecont AV10005 140
AVS Uriel Mpix 13 382
AXIS 200+ 1
AXIS 205 15
AXIS 206 19
AXIS 206M 19
AXIS 206W 19
AXIS 207 18
AXIS 207MW 18
AXIS 207W 18
Axis 209FD 168
Axis 209MFD 168
AXIS 210 18
AXIS 210A 18
AXIS 211 18
AXIS 211A 18
AXIS 211M 18
Axis 211W 18
AXIS 212 PTZ 138
AXIS 213 PTZ 22
AXIS 214 PTZ 123
Axis 215 PTZ 123
Axis 215 PTZ-E 123
AXIS 216FD 122
AXIS 216MFD 122
AXIS 221 25
AXIS 223M 153
AXIS 225FD 25
AXIS 231D 23
AXIS 231D+ 23
AXIS 232D 23
AXIS 232D+ 23
AXIS 233D 23
AXIS 240 2
AXIS 240Q 16
AXIS 241Q 16
AXIS 241QA 16
AXIS 241S 17
AXIS 241SA 17
Axis 242S IV 17
AXIS 243Q 160
AXIS 243SA 17
AXIS 247S 172
AXIS 282 130
AXIS 2100 5
AXIS 2110 5
AXIS 2120 6
AXIS 2130 12
AXIS 2400 OSYS 3
AXIS 2400 Linux 8
AXIS 2400+ 8
AXIS 2401 OSYS 4
AXIS 2401 Linux 11
AXIS 2401+ 11
AXIS 2411 14
AXIS 2420 10
AXIS 2420 10
Axis M1011 283
Axis M1031 284
Axis M1054 441
Axis M1103 283
Axis M1104 283
Axis M1113 283
Axis M1114 283
Axis M3011 285
Axis M3014 342
Axis M3113 342
Axis M3114 342
Axis M3203 342
Axis M3204 342
Axis M7001 286
Axis P1311 288
Axis P1343 288
Axis P1344 288
Axis P1346 288
Axis P1347 437
Axis P3301 246
Axis P3304 246
Axis P3343 339
Axis P3344 339
Axis P3346 437
Axis P3346-E 437
Axis P5532 373
Axis P5532-E 373
Axis P5534 373
Axis P5534-E 373
Axis P8221 389
Axis Q1755 278
Axis Q1910 380
Axis Q1921 380
Axis Q1921-E 380
Axis Q6032-E 335
Axis Q6034 440
Axis Q6034-E 335
Axis Q7401 256
Axis Q7404 337
Axis Q7406 268
Barix Barionet 272
Basler BIP-640c 242
Basler BIP-640c-dn 242
Basler BIP-1000c 242
Basler BIP-1000c-dn 242
Basler BIP-1300c 242
Basler BIP-1300c-dn 242
Basler BIP-1600c 242
Basler BIP-1600c-dn 242
Basler BIP-D1000c-dn 242
Basler BIP-D1300c-dn 242
Baxall X-Stream 91
Black BLK-IPD101 525
Black BLK-IPD102 525
Black BLK-IPE101 525
Black BLK-IPS101 525
Black BLK-IPS102M 525
Bosch Autodome Easy II IP 402
Bosch Dinion NWC-0455-10P 133
Bosch Dinion NWC-0495-10P 133
Bosch FlexiDome NWD-0455 133
Bosch FlexiDome NWD-0455 402
Bosch FlexiDome NWD-0495 133
Bosch Extreme NEI-828 190
Bosch NBC-200 series 402
Bosch NBN-498-11P 402
Bosch VideoJet X10 253
Bosch VideoJet X20 253
Bosch VideoJet X40 253
Bosch VIP X1 127
Bosch VIP X2 132
Bosch VIP X1600 M4SA 162
Bosch VIP X1600 XFM4 455
Bosch VG4 Series 190
Brickcom CB-100Ae 450
Brickcom CB-100Ap 450
Brickcom FB-100Ae 450
Brickcom FB-100Ap 450
Brickcom FD-100Ae 450
Brickcom FD-100Ap 450
Brickcom WCB-100Ae 450
Brickcom WCB-100Ap 450
Brickcom WFB-100Ae 450
Brickcom WFB-100Ap 450
Canon VB-C10 31
Canon VB-C50FSi 212
Canon VB-C50i 212
Canon VB-C50IR 212
Canon VB-C60 276
<table>
<thead>
<tr>
<th>Device</th>
<th>Hardware Driver ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canon VB-C300 174</td>
<td></td>
</tr>
<tr>
<td>Canon VB-C500D 330</td>
<td></td>
</tr>
<tr>
<td>Canon VB-C500VD 330</td>
<td></td>
</tr>
<tr>
<td>Canon VB-M40 477</td>
<td></td>
</tr>
<tr>
<td>CBC Ganz ZA-NVE12K 483</td>
<td></td>
</tr>
<tr>
<td>CBC Ganz ZN-D2024 207</td>
<td></td>
</tr>
<tr>
<td>CBC Ganz ZN-NH21VPE 481</td>
<td></td>
</tr>
<tr>
<td>CBC Ganz ZN-PT304L 179</td>
<td></td>
</tr>
<tr>
<td>CBC Ganz ZN-PT304WL 179</td>
<td></td>
</tr>
<tr>
<td>CBC Ganz ZN-PTZ500VPE 480</td>
<td></td>
</tr>
<tr>
<td>CBC Ganz ZN-RS4000 R12/R40 482</td>
<td></td>
</tr>
<tr>
<td>Checkview 9128702 275</td>
<td></td>
</tr>
<tr>
<td>Cisco IPC-2500 322</td>
<td></td>
</tr>
<tr>
<td>Cisco IPC-4300 322</td>
<td></td>
</tr>
<tr>
<td>Cisco IPC-4500 322</td>
<td></td>
</tr>
<tr>
<td>CNB IDC4000T 395</td>
<td></td>
</tr>
<tr>
<td>CNB IDP4000VD 391</td>
<td></td>
</tr>
<tr>
<td>CNB IDP4000VR 391</td>
<td></td>
</tr>
<tr>
<td>CNB IDP4030VR 391</td>
<td></td>
</tr>
<tr>
<td>CNB IGP1030 391</td>
<td></td>
</tr>
<tr>
<td>CNB INS2000 393</td>
<td></td>
</tr>
<tr>
<td>CNB IPM3063P 388</td>
<td></td>
</tr>
<tr>
<td>CNB ISM1063P 388</td>
<td></td>
</tr>
<tr>
<td>CNB ISS2766PW 388</td>
<td></td>
</tr>
<tr>
<td>CNB IVP4000VR 391</td>
<td></td>
</tr>
<tr>
<td>CNB IVP4030VR 391</td>
<td></td>
</tr>
<tr>
<td>Convision S1 21</td>
<td></td>
</tr>
<tr>
<td>Convision V100 21</td>
<td></td>
</tr>
<tr>
<td>Convision V200 20</td>
<td></td>
</tr>
<tr>
<td>Convision V6xx 7</td>
<td></td>
</tr>
<tr>
<td>Convision V7xx 7</td>
<td></td>
</tr>
<tr>
<td>D-Link DCS1000/1000W 55</td>
<td></td>
</tr>
<tr>
<td>D-Link DCS-2000 101</td>
<td></td>
</tr>
<tr>
<td>D-Link DCS-2100+/2100/2100G 101</td>
<td></td>
</tr>
<tr>
<td>D-Link DCS-3110 386</td>
<td></td>
</tr>
<tr>
<td>D-Link DCS-3220/3220G 118</td>
<td></td>
</tr>
<tr>
<td>D-Link DCS-3410 524</td>
<td></td>
</tr>
<tr>
<td>D-Link DCS-3415 387</td>
<td></td>
</tr>
<tr>
<td>D-Link DCS-5300 99</td>
<td></td>
</tr>
<tr>
<td>D-Link DCS-5300G 99</td>
<td></td>
</tr>
<tr>
<td>D-Link DCS-5610 387</td>
<td></td>
</tr>
<tr>
<td>D-Link DCS-6110 386</td>
<td></td>
</tr>
<tr>
<td>D-Link DCS-6511 402</td>
<td></td>
</tr>
<tr>
<td>D-Link DCS-6620/6620G 116</td>
<td></td>
</tr>
<tr>
<td>Darim Vision PVE400 298</td>
<td></td>
</tr>
<tr>
<td>Dedicated Micros Digital Sprite 2 247</td>
<td></td>
</tr>
<tr>
<td>Digimerge DNB6320 177</td>
<td></td>
</tr>
<tr>
<td>Digimerge DND7220 177</td>
<td></td>
</tr>
<tr>
<td>Digimerge DNP5220E 177</td>
<td></td>
</tr>
<tr>
<td>Digimerge DNP5320E 177</td>
<td></td>
</tr>
<tr>
<td>Digimerge DNS1010 177</td>
<td></td>
</tr>
<tr>
<td>Digimerge DNZ-9320W 244</td>
<td></td>
</tr>
<tr>
<td>DirectShow camera 214</td>
<td></td>
</tr>
<tr>
<td>Discrete DIV2300 188</td>
<td></td>
</tr>
<tr>
<td>DvTel DVT-7101 262</td>
<td></td>
</tr>
<tr>
<td>DvTel DVT-7601 464</td>
<td></td>
</tr>
<tr>
<td>DvTel DVT-7608 261</td>
<td></td>
</tr>
<tr>
<td>DvTel DVT-7612E 371</td>
<td></td>
</tr>
<tr>
<td>DvTel DVT-9460 514</td>
<td></td>
</tr>
<tr>
<td>DvTel DVT-9540DW 514</td>
<td></td>
</tr>
</tbody>
</table>
Dynacolor Diva Standard 296
Dynacolor Diva Zoom 282
Dynacolor Diva Mini 297
Etrovision EV3130A 236
Etrovision EV3131 237
Etrovision EV3131A 237
Etrovision EV3151A 443
Etrovision EV3830 238
Etrovision EV6130 239
Etrovision EV6150A 443
Etrovision EV6230 240
Etrovision EV6250A 443
Etrovision EV6530 240
Etrovision EV8150A 443
Everfocus EAN800 362
Everfocus EAN850 362
Everfocus EAN890 362
Everfocus EDN800 362
Everfocus EDN850 362
Everfocus EDN890 362
Everfocus EPN3100 363
Everfocus EPN3600 363
Everfocus EZN850 394
Extreme CCTV EX7 103
Extreme CCTV EX30 103
Extreme CCTV EX36 103
Extreme CCTV EX80 103
Extreme CCTV EX82 103
Extreme CCTV EX85 140
Extreme CCTV REG-L1-IP 103
Eyevi CMI-110 245
Eyevi CMI-H230 245
Eyevi CMI-H260 245
Eyevi EYENET-250A 245
Eyevi GPOWER IP Basement 245
Eyevi IPM-100 245
Eyevi IPM-150 245
Eyevi IPM-300 245
Eyevi IPM-500 245
Eyevi IPR-220 245
Eyevi IPR-330 245
Eyevi IPR-6000 245
Eyevi IPR-6600 245
Eyevi IPS-110 245
Eyevi IPS-220 245
Eyevi IPS-300 245
Eyevi IPS-330 245
Eyevi IPS-400 245
Eyevi IPS-500 245
Eyevi IPS-600 245
Eyevi IPS-800 245
Eyevi IPS-830 245
Eyevi IPS-900 245
FLIR 241S 95
GE Security GEC-IP2B 225
GE Security GEC-IP2B-C 225
GE Security GEC-IP2B-P 225
GE Security GEC-IP2D 225
GE Security GEC-IP2D-C 225
GE Security GEC-IP2D-P 225
<table>
<thead>
<tr>
<th>Brand</th>
<th>Model Number</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE Security</td>
<td>GEC-IP2VD</td>
<td>225</td>
</tr>
<tr>
<td></td>
<td>GEC-IP2VD-C</td>
<td>225</td>
</tr>
<tr>
<td></td>
<td>GEC-IP2VD-P</td>
<td>225</td>
</tr>
<tr>
<td></td>
<td>GEC-IP2VD-DN</td>
<td>225</td>
</tr>
<tr>
<td></td>
<td>GEC-IP2VD-DNC</td>
<td>225</td>
</tr>
<tr>
<td>Grandeye Halocam</td>
<td>IPC</td>
<td>249</td>
</tr>
<tr>
<td></td>
<td>IPW</td>
<td>249</td>
</tr>
<tr>
<td>HikVision DS</td>
<td>2CD702P(N)F</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD702P(N)-FB</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD712P(N)F</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD712P(N)-FB</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD732P(N)F</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD732P(N)-FB</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD752MF-E</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD752MF-FB</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD762MF</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD762MF-E</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD782P(N)F</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD782P(N)-FB</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD802P(N)F</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD802P(N)-FB</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD812P(N)F</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD812P(N)-E</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD832P(N)F</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD832P(N)-E</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD852MF-E</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD862MF-E</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD892P(N)F</td>
<td>519</td>
</tr>
<tr>
<td></td>
<td>2CD892P(N)-E</td>
<td>519</td>
</tr>
<tr>
<td>Hitron</td>
<td>HECMC4V4C4</td>
<td>217</td>
</tr>
<tr>
<td></td>
<td>HEV0104</td>
<td>223</td>
</tr>
<tr>
<td></td>
<td>HEV0407</td>
<td>224</td>
</tr>
<tr>
<td></td>
<td>HNCA-811-NZ1</td>
<td>222</td>
</tr>
<tr>
<td></td>
<td>HNCB-811NZ1</td>
<td>219</td>
</tr>
<tr>
<td></td>
<td>HNCB-F1SN</td>
<td>218</td>
</tr>
<tr>
<td></td>
<td>HNCG-F1SAW0S4</td>
<td>220</td>
</tr>
<tr>
<td></td>
<td>HNCV-811PZ0S4</td>
<td>221</td>
</tr>
<tr>
<td></td>
<td>HWD-12SMP</td>
<td>187</td>
</tr>
<tr>
<td>Honeywell</td>
<td>ACUIXIP</td>
<td>350</td>
</tr>
<tr>
<td></td>
<td>HCSS541P</td>
<td>336</td>
</tr>
<tr>
<td></td>
<td>HCD5541P</td>
<td>336</td>
</tr>
<tr>
<td></td>
<td>HCX13M</td>
<td>364</td>
</tr>
<tr>
<td></td>
<td>HCX3</td>
<td>364</td>
</tr>
<tr>
<td></td>
<td>HCX5D</td>
<td>364</td>
</tr>
</tbody>
</table>
Honeywell HD3MDIP 390
Honeywell HD3MDIPX 390
Honeywell HD4DIP 336
Honeywell HD4MDIP 390
Honeywell HD4MDIPX 390
Honeywell HNVE1 431
Hunt HLC-7RI 200
Hunt HLC-15M 202
Hunt HLC-15V 203
Hunt HLC-79G 203
Hunt HLC-79M 202
Hunt HLC-81AD 270
Hunt HLC-81AG 200
Hunt HLC-81I 201
Hunt HLC-81M 201
Hunt HLC-83M 202
Hunt HLC-83V 203
Hunt HLC-84AM 202
Hunt HLC-84AV 203
Hunt HLC-84M 202
Hunt HLC-84V 203
Hunt HLT-86F 198
Hunt HLT-87Z 209
Hunt HLT-87ZA 209
Hunt HLV-1CAD 270
Hunt HLV-1CI 200
Hunt HLV-1CM 270
Hunt HVT-01HT 199
Hunt HWS-01AD 204
Hunt HWS-01HD 204
Hunt HWS-04AD 205
Hunt HWS-04HD/W 205
i3 Annexxus 301 392
ICanServer 510 257
ICanServer 512 257
ICanServer 540 259
ICanView 220 258
ICanView 222 258
ICanView 230 258
ICanView 232 258
ICanView 240 257
ICanView 250 257
ICanView 260 258
ICanView 270 257
ICanView 280 258
ICanView 290 257
Infinova V1492N-M series 381
Infinova V2500-M series 435
Infinova V6100-M series 435
Infinova V6200-M series 434
Infinova V6600-M series 435
Infinova V6800-M series 435
Infinova V1700N-C series NetDome 119
Infinova V1700N-L series NetDome 137
Infinova V1700N-M series 381
Intellinet MNC-L10 / 550710 104
IPIX IS2000 CVD2000 CVN2000 57
IPIX CVD3000 57
Ipx DDK-1000 157
Ipx DDK-1500 157
Ipx DDK-1500D 157
Ipx VE-3500 157
IQEye 101 83
IQEye 300 series 83
IQEye 4 series 83
IQEye 501 83
IQEye 510 83
IQEye 511 83
IQEye 600 series 83
IQEye 700 series 83
IQEye 732 83
IQEye 800 Sentinel series 83
IQEye 832 83
IQEye Alliance series 83
IQEye Cameo 442
IQEye IQA25 83
IQEye IQD30S 83
IQEye IQD31S 83
IQEye IQM30NE 83
IQEye IQM31NE 83
IQEye IQM32NE 83
Johnson Controls DVN5008 293
Johnson Controls DVN5016 340
Johnson Controls DVN5032 341
JVC VN-A1U 43
JVC VN-C10U 44
JVC VN-C20U 126
JVC VN-C30U 42
JVC VN-C3WU 40
JVC VN-C205 169
JVC VN-C215 146
JVC VN-C625U 45
JVC VN-C655U 45
JVC VN-E4/-E4E/-E4U 121
JVC VN-V25U 185
JVC VN-V26U 185
JVC VN-V225U/VN-V225VPU 185
JVC VN-V685U 196
JVC VN-V686U/V686WPU 196
JVC VN-V686BU/V686WPBU 196
JVC VN-X35U 235
JVC VN-X235U (VN-X235VPU 235
Lenel ICT-220 345
Lenel ICT-230 345
Lenel ICT-250 346
Lenel ICT-510 345
Lenel LC-330FDX 345
Linudix LWS800 511
Linudix LWS820 512
Linudix LWS840 511
Lumenera LE165 84
Lumenera LE175 84
Lumenera LE256 84
Lumenera LE259 84
Lumenera LE275 84
Lumenera LE375 84
Lumenera LE575 84
Messoa NCB-855 344
Messoa NCR-875 344
Messoa NDR-895 344
Messoa NDZ-860 343  
Messoa NIC-830 354  
Messoa NIC-835 354  
Mobotix D10 86  
Mobotix D12 86  
Mobotix D22M 86  
Mobotix D24 86  
Mobotix M1 86  
Mobotix M10 86  
Mobotix M12 86  
Mobotix M22M 86  
Mobotix M24 86  
Mobotix Q22 260  
Mobotix Q24 328  
Mobotix T24 459  
ONVIF Conformant Device 402  
ONVIF Conformant Device 16 Chnl. 407  
Optelecom Siqura BC-2x series 281  
Optelecom Siqura C-50 269  
Optelecom Siqura C-54 289  
Optelecom Siqura C-60 321  
Optelecom Siqura FD-2x series 281  
Optelecom Siqura HD-20 353  
Optelecom Siqura HD-22 353  
Optelecom Siqura HD-26 353  
Optelecom Siqura HD-60 353  
Optelecom Siqura HD-62 353  
Optelecom Siqura HD-66WDR 353  
Optelecom Siqura MD-20 353  
Optelecom Siqura MD-22 353  
Optelecom Siqura MD-60 353  
Optelecom Siqura S-50 269  
Optelecom Siqura S-54 289  
Optelecom Siqura S-60 321  
Optelecom Siqura S-64 399  
Optelecom Siqura S-68 430  
Optelecom Siqura V-30 295  
Panasonic BB-HCE481 series 24  
Panasonic BB-HCM311 series 24  
Panasonic BB-HCM331 series 24  
Panasonic BB-HCM371A 24  
Panasonic BB-HCM381 series 24  
Panasonic BB-HCM403 24  
Panasonic BB-HCM511 180  
Panasonic BB-HCM515 180  
Panasonic BB-HCM527 180  
Panasonic BB-HCM531 180  
Panasonic BB-HCM547 180  
Panasonic BB-HCM580 180  
Panasonic BB-HCM581 180  
Panasonic BB-HCM700 series (Fixed) 383  
Panasonic BB-HCM700 series (PTZ) 375  
Panasonic BB-HCS301 24  
Panasonic BL-C1 series 24  
Panasonic BL-C10 series 24  
Panasonic BL-C20 series 24  
Panasonic BL-C30 series 24  
Panasonic BL-C111 182  
Panasonic BL-C131 182
<table>
<thead>
<tr>
<th>Panasonic BL-C160</th>
<th>356</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panasonic DG-SP304V</td>
<td>449</td>
</tr>
<tr>
<td>Panasonic KX-HCM8</td>
<td>63</td>
</tr>
<tr>
<td>Panasonic KX-HCM10 series</td>
<td>63</td>
</tr>
<tr>
<td>Panasonic KX-HCM110A series</td>
<td>24</td>
</tr>
<tr>
<td>Panasonic KX-HCM230 series</td>
<td>63</td>
</tr>
<tr>
<td>Panasonic KX-HCM250 series</td>
<td>63</td>
</tr>
<tr>
<td>Panasonic KX-HCM270 series</td>
<td>63</td>
</tr>
<tr>
<td>Panasonic KX-HCM280 series (except 280A)</td>
<td>63</td>
</tr>
<tr>
<td>Panasonic KX-HCM280A</td>
<td>24</td>
</tr>
<tr>
<td>Panasonic WJ-GXE500</td>
<td>377</td>
</tr>
<tr>
<td>Panasonic WJ-NT104</td>
<td>60</td>
</tr>
<tr>
<td>Panasonic WJ-NT304</td>
<td>183</td>
</tr>
<tr>
<td>Panasonic WV-NF284</td>
<td>120</td>
</tr>
<tr>
<td>Panasonic WV-NF302</td>
<td>211</td>
</tr>
<tr>
<td>Panasonic WV-NP240/WV-NP244</td>
<td>120</td>
</tr>
<tr>
<td>Panasonic WV-NP304</td>
<td>211</td>
</tr>
<tr>
<td>Panasonic WV-NP472</td>
<td>61</td>
</tr>
<tr>
<td>Panasonic WV-NP502</td>
<td>351</td>
</tr>
<tr>
<td>Panasonic WV-NP1000/WV-NP1004</td>
<td>120</td>
</tr>
<tr>
<td>Panasonic WV-NS202/NS202A</td>
<td>143</td>
</tr>
<tr>
<td>Panasonic WV-NS320 series</td>
<td>64</td>
</tr>
<tr>
<td>Panasonic WV-NS950</td>
<td>197</td>
</tr>
<tr>
<td>Panasonic WV-NS954</td>
<td>197</td>
</tr>
<tr>
<td>Panasonic WV-NW470</td>
<td>85</td>
</tr>
<tr>
<td>Panasonic WV-NW484</td>
<td>175</td>
</tr>
<tr>
<td>Panasonic WV-NW502</td>
<td>351</td>
</tr>
<tr>
<td>Panasonic WV-NW960</td>
<td>197</td>
</tr>
<tr>
<td>Panasonic WV-NW964</td>
<td>197</td>
</tr>
<tr>
<td>Panasonic WV-SC385</td>
<td>461</td>
</tr>
<tr>
<td>Panasonic WV-SF332</td>
<td>398</td>
</tr>
<tr>
<td>Panasonic WV-SF335</td>
<td>398</td>
</tr>
<tr>
<td>Panasonic WV-SF336</td>
<td>398</td>
</tr>
<tr>
<td>Panasonic WV-SF346</td>
<td>398</td>
</tr>
<tr>
<td>Panasonic WV-SP102</td>
<td>449</td>
</tr>
<tr>
<td>Panasonic WV-SP105</td>
<td>449</td>
</tr>
<tr>
<td>Panasonic WV-SP302</td>
<td>398</td>
</tr>
<tr>
<td>Panasonic WV-SP305</td>
<td>398</td>
</tr>
<tr>
<td>Panasonic WV-SP306</td>
<td>398</td>
</tr>
<tr>
<td>Panasonic WV-SW355</td>
<td>461</td>
</tr>
<tr>
<td>Panasonic WV-SW395</td>
<td>461</td>
</tr>
<tr>
<td>Pentax Versacam IC-4</td>
<td>50</td>
</tr>
<tr>
<td>Pelco Camclosure IP series</td>
<td>149</td>
</tr>
<tr>
<td>Pelco DX8000</td>
<td>446</td>
</tr>
<tr>
<td>Pelco DX8100</td>
<td>446</td>
</tr>
<tr>
<td>Pelco Endura NET5301T</td>
<td>144</td>
</tr>
<tr>
<td>Pelco Endura NET5308T</td>
<td>166</td>
</tr>
<tr>
<td>Pelco Endura NET5316T</td>
<td>167</td>
</tr>
<tr>
<td>Pelco Endura NET5401T</td>
<td>456</td>
</tr>
<tr>
<td>Pelco Endura NET5402T</td>
<td>456</td>
</tr>
<tr>
<td>Pelco Endura NET5404T</td>
<td>456</td>
</tr>
<tr>
<td>Pelco ID10</td>
<td>254</td>
</tr>
<tr>
<td>Pelco ID30</td>
<td>254</td>
</tr>
<tr>
<td>Pelco IDE20</td>
<td>254</td>
</tr>
<tr>
<td>Pelco IDS0</td>
<td>254</td>
</tr>
<tr>
<td>Pelco IE10</td>
<td>254</td>
</tr>
<tr>
<td>Pelco IE30</td>
<td>254</td>
</tr>
<tr>
<td>Pelco IEE10</td>
<td>254</td>
</tr>
<tr>
<td>Pelco IEE20</td>
<td>254</td>
</tr>
<tr>
<td>Pelco IES0</td>
<td>254</td>
</tr>
</tbody>
</table>
Pelco IM10 254
Pelco IMS0 254
Pelco IP3701 176
Pelco IX10 254
Pelco IX30 254
Pelco IXE20 254
Pelco IXS0 254
Pelco NET300 208
Pelco NET350 208
Pelco SPECTRA HD 436
Pelco Spectra IV-IP 213
Pelco Spectra IV-IP H.264 436
Pelco SpectraMini IV-IP 213
Philips NETSVR-1 93
Philips NETSVR-6 92
Pixord 120 72
Pixord 126 75
Pixord 200 73
Pixord 201 73
Pixord 205 77
Pixord 207 77
Pixord 24X 74
Pixord 261 78
Pixord 1000 75
Pixord 400/400W 151
Pixord 461 148
Pixord 463 148
Pixord 1401/1401W 136
Pixord 2000 76
Pixord 4000 151
Pixord P600 439
Pixord PD636/PD636E 485
Polar Industries zPan100 501
Provideo SD-606W 279
Provideo SD-705VPRO-1 280
PSIA Conformant Device 403
PSIA Conformant Device 16-Chnl. 404
Samsung SCC-C6475 131
Samsung SHR-2040 165
Samsung SNB-5000 402
Samsung SNB-7000 402
Samsung SNC-550 191
Samsung SNC-570 291
Samsung SNC-1300 432
Samsung SNC-B2315 227
Samsung SNC-B2331 374
Samsung SNC-B2335 372
Samsung SNC-B5368 374
Samsung SNC-B5395 248
Samsung SNC-B5399 372
Samsung SNC-C6225 325
Samsung SNC-C7225 325
Samsung SNC-C7478 299
Samsung SNC-M300 226
Samsung SND-460V 329
Samsung SND-560 292
Samsung SND-3080 374
Samsung SND-7080 402
Samsung SNP-1000/SNP-1000A 195
Samsung SNP-3301 396
<table>
<thead>
<tr>
<th>Hardware Driver IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung SNP-3301H 396</td>
</tr>
<tr>
<td>Samsung SNP-3300/SNP-3300A 194</td>
</tr>
<tr>
<td>Samsung SNP-3370 396</td>
</tr>
<tr>
<td>Samsung SNP-3370TH 396</td>
</tr>
<tr>
<td>Samsung SNS-100 192</td>
</tr>
<tr>
<td>Samsung SNS-400 193</td>
</tr>
<tr>
<td>Samsung SNT-1010 147</td>
</tr>
<tr>
<td>Samsung SNV-3080 372</td>
</tr>
<tr>
<td>Samsung SNV-7080 402</td>
</tr>
<tr>
<td>Sanyo VCC-400N 206</td>
</tr>
<tr>
<td>Sanyo VCC-9500 206</td>
</tr>
<tr>
<td>Sanyo VCC-9500P 206</td>
</tr>
<tr>
<td>Sanyo VCC-9600 206</td>
</tr>
<tr>
<td>Sanyo VCC-9600P 206</td>
</tr>
<tr>
<td>Sanyo VCC-9700 206</td>
</tr>
<tr>
<td>Sanyo VCC-9700P 206</td>
</tr>
<tr>
<td>Sanyo VCC-9800 206</td>
</tr>
<tr>
<td>Sanyo VCC-9800P 206</td>
</tr>
<tr>
<td>Sanyo VCC-HD2100 367</td>
</tr>
<tr>
<td>Sanyo VCC-HD2100P 367</td>
</tr>
<tr>
<td>Sanyo VCC-HD2300 367</td>
</tr>
<tr>
<td>Sanyo VCC-HD2300P 367</td>
</tr>
<tr>
<td>Sanyo VCC-HD2500 358</td>
</tr>
<tr>
<td>Sanyo VCC-HD2500P 358</td>
</tr>
<tr>
<td>Sanyo VCC-HD4000 206</td>
</tr>
<tr>
<td>Sanyo VCC-HD4000P 206</td>
</tr>
<tr>
<td>Sanyo VCC-HD4600 368</td>
</tr>
<tr>
<td>Sanyo VCC-HD5400 369</td>
</tr>
<tr>
<td>Sanyo VCC-HD5600 370</td>
</tr>
<tr>
<td>Sanyo VCC-HDN1(S) 206</td>
</tr>
<tr>
<td>Sanyo VCC-N6584 206</td>
</tr>
<tr>
<td>Sanyo VCC-N6695P 206</td>
</tr>
<tr>
<td>Sanyo VCC-WB2000/VCC-WB4000 56</td>
</tr>
<tr>
<td>Sanyo VCC-P450 206</td>
</tr>
<tr>
<td>Sanyo VCC-P450NA 206</td>
</tr>
<tr>
<td>Sanyo VCC-P470 206</td>
</tr>
<tr>
<td>Sanyo VCC-P470NA 206</td>
</tr>
<tr>
<td>Sanyo VCC-P7574 142</td>
</tr>
<tr>
<td>Sanyo VCC-P7575P 142</td>
</tr>
<tr>
<td>Sanyo VCC-P9574 142</td>
</tr>
<tr>
<td>Sanyo VCC-P9574N 142</td>
</tr>
<tr>
<td>Sanyo VCC-P9575P 142</td>
</tr>
<tr>
<td>Sanyo VCC-PN9575P 142</td>
</tr>
<tr>
<td>Sanyo VCC-PT490 206</td>
</tr>
<tr>
<td>Sanyo VCC-PT490NA 206</td>
</tr>
<tr>
<td>Sanyo VCC-PT500 206</td>
</tr>
<tr>
<td>Sanyo VCC-PT500NA 206</td>
</tr>
<tr>
<td>Sanyo VCC-XZ200 206</td>
</tr>
<tr>
<td>Sanyo VCC-XZ200P 206</td>
</tr>
<tr>
<td>Sanyo VCC-XZ600P 206</td>
</tr>
<tr>
<td>Sanyo VCC-XZN600P 206</td>
</tr>
<tr>
<td>Sanyo VCC-ZM600P 206</td>
</tr>
<tr>
<td>Sanyo VCC-ZMN600P 206</td>
</tr>
<tr>
<td>Sanyo VDC-DP7584 142</td>
</tr>
<tr>
<td>Sanyo VDC-DP7585P 142</td>
</tr>
<tr>
<td>Sanyo VDC-DP9584 142</td>
</tr>
<tr>
<td>Sanyo VDC-DP9584N 142</td>
</tr>
<tr>
<td>Sanyo VDC-DP9585 142</td>
</tr>
<tr>
<td>Sanyo VDC-DPN9585P 142</td>
</tr>
</tbody>
</table>
Sanyo VDC-HD3100 367
Sanyo VDC-HD3100P 367
Sanyo VDC-HD3300 367
Sanyo VDC-HD3300P 367
Sanyo VDC-HD3500 358
Sanyo VDC-HD3500P 358
Sanyo VSP-SV2000 56
Siemens CCIC1345 252
Siemens CCIS1345 252
Siemens CCIS1345-DN 252
Siemens CCIW1345 252
Sony SNC-CH110 453
Sony SNC-CH120 451
Sony SNC-CH140 378
Sony SNC-CH160 452
Sony SNC-CH180 378
Sony SNC-CH210 453
Sony SNC-CH220 452
Sony SNC-CH240 378
Sony SNC-CH260 452
Sony SNC-CH280 378
Sony SNC-CM120 215
Sony SNC-CS3 54
Sony SNC-CS10 88
Sony SNC-CS11 88
Sony SNC-CS20 216
Sony SNC-CS50 125
Sony SNC-DF40 88
Sony SNC-DF50 178
Sony SNC-DF70 88
Sony SNC-DF80 178
Sony SNC-DF85 178
Sony SNC-DH110 453
Sony SNC-DH110T 453
Sony SNC-DH120 451
Sony SNC-DH120T 452
Sony SNC-DH140 376
Sony SNC-DH160 452
Sony SNC-DH180 376
Sony SNC-DH210 453
Sony SNC-DH210T 453
Sony SNC-DH220 451
Sony SNC-DH240 378
Sony SNC-DH240T 378
Sony SNC-DH260 452
Sony SNC-DH280 378
Sony SNC-DM110 215
Sony SNC-DM160 215
Sony SNC-DS10 216
Sony SNC-DS60 216
Sony SNC-M1/Sony SNC-M1W 102
Sony SNC-M3/Sony SNC-M3W 102
Sony SNC-P1 88
Sony SNC-P5 98
Sony SNC-RH124 352
Sony SNC-RH164 352
Sony SNC-RS44N 352
Sony SNC-RS44P 352
Sony SNC-RS46N 352
Sony SNC-RS46P 352
Sony SNC-RS84N 352
Sony SNC-RS84P 352
Sony SNC-RS86N 352
Sony SNC-RS86P 352
Sony SNC-RX530 124
Sony SNC-RX550 124
Sony SNC-RX570 124
Sony SNC-RZ25 89
Sony SNC-RZ30 52
Sony SNC-RZ30/2 52
Sony SNC-RZ50 128
Sony SNC-Z20 53
Sony SNC-VL10 51
Sony SNT-EP104 360
Sony SNT-EP154 360
Sony SNT-EX101 359
Sony SNT-EX101E 359
Sony SNT-EX104 357
Sony SNT-EX154 357
Sony SNT-V304 9
Sony SNT-V501 82
Sony SNT-V704 113
Speco Technologies SIPB1/SIPB2 501
Speco Technologies SIPB3/SIPB4 501
Speco Technologies SIPMPTS 501
Speco Technologies SIPSD10X 501
Stardot Express 2 448
Stardot Express 4 448
StarDot NetCam XL 186
StarDot NetCam SC 5 MP 186
Stardot SDH5008N 447
Toshiba IK-WB01A 115
Toshiba IK-WB02A 114
Toshiba IK-WB11A 59
Toshiba IK-WB15A 115
Toshiba IK-WB16A 471
Toshiba IK-WB21A 115
Toshiba IK-WB30A 472
Toshiba IK-WD01A 473
Toshiba IK-WR01A 114
Toshiba IK-WR12A 473
Toshiba Teli CI7010 181
Toshiba Teli CI8010 263
Toshiba Teli CI8110D 263
Toshiba Teli CI8210D 250
Toshiba Teli EJ7000 170
Toshiba Teli GE2000 484
UDP IPC1100 231
UDP IPC3100 231
UDP IPC3500 231
UDP IPC4100 229
UDP IPC4500 229
UDP IPE100 525
UDP IPE1100 525
UDP IPE1100M 525
UDP IPE3500 525
UDP IPE3500L 525
UDP IPE3510 525
UDP IPE4100 524
UDP IPE4500 524
Milestone XProtect Essential 2.0; Administrator's Manual

Appendix: Hardware Driver IDs

- UDP IPE5500 524
- UDP NVC1000 525
- UDP NVC4000 R12/R40 526
- UDP NVE12K 230
- UDP NVE40K 230
- UDP NVE100 232
- UDP NVE1000 233
- UDP NVE2000 234
- UDP NVE4000 230
- Universal driver 400
- Universal driver 16 Chnl. 401
- USB Camera driver 445
- Vantage VIPC1100E 501
- Vantage VIPC1311EP 501
- Vantage VIPC1431EP 501
- Vantage VIPC3100E 501
- Vantage VIPC3211EP 501
- Vantage VIPC3311EP 501
- Vantage VIPC5300 501
- Vantage VIPC5320 501
- Vantage VIPC6510F 501
- Vantage VIPC6610F 501
- Vantage VIPC7100 series 501
- Vantage VIPC7200 series 501
- Vantage VIPC7300 series 501
- Vantage VIPS2120 501
- Vantage VIPS2310Q 501
- Vantage VIPS2410 506
- VCS VideoJet 10 96
- VCS VideoJet 400 94
- VCS VIP 10 96
- Veo Observer XT 32
- Verint Nextiva S1700e 103
- Verint Nextiva S1704e 135
- Verint Nextiva S1708e 111
- Verint Nextiva S1712e 163
- Verint Nextiva S1724e 164
- Verint S1801e 466
- Verint S1802e 468
- Verint S1808e 469
- Verint S1816e 470
- Verint Nextiva S1900e 103
- Verint Nextiva S1950e 103
- Verint Nextiva S1970e 103
- Verint Nextiva S2600e/S2610e 103
- Verint Nextiva S2600e-AS/2610e-AS 103
- Verint Nextiva S2700e 103
- VideoIQ VIQ-CRD series 326
- VideoIQ VIQ-CT2xx series 326
- VideoIQ VIQ-E series 355
- Videology 20N758 184
- Videology 21N758 184
- Videology Server Board 189
- VideoTec Albert VA01001 462
- VideoTec Albert VA01002 462
- VideoTec Albert VA02001 462
- VideoTec Albert VA02002 462
- VideoTec Albert VA03001 462
- VideoTec Albert VA03002 462
- VideoTec Ulisse 463
Vivotek FD6100 series 109
Vivotek FD7130 366
Vivotek FD7131 331
Vivotek FD7132 331
Vivotek FD7141 331
Vivotek FD7141V 331
Vivotek FD7160 366
Vivotek IP2121 58
Vivotek IP2122 58
Vivotek IP3121 97
Vivotek IP3122 97
Vivotek IP3135 97
Vivotek IP6124 109
Vivotek IP7130 333
Vivotek IP7131 155
Vivotek IP7133 348
Vivotek IP7134 348
Vivotek IP7135 155
Vivotek IP7137 155
Vivotek IP7138 331
Vivotek IP7139 331
Vivotek IP7142 251
Vivotek IP7151 251
Vivotek IP7152 251
Vivotek IP7153 251
Vivotek IP7154 251
Vivotek IP7160 251
Vivotek IP7161 251
Vivotek IP7251 347
Vivotek IP7330 333
Vivotek IP7361 251
Vivotek IP8161 402
Vivotek IZ7151 349
Vivotek MD7530 366
Vivotek MD7560 366
Vivotek PT3124 107
Vivotek PT7135 158
Vivotek PT7137 158
Vivotek PZ6122 110
Vivotek PZ7111 332
Vivotek PZ7112 332
Vivotek PZ7121 332
Vivotek PZ7122 332
Vivotek PZ7131 332
Vivotek PZ7132 332
Vivotek PZ7151 349
Vivotek PZ7152 349
Vivotek SD6122V 110
Vivotek SD7151 338
Vivotek SD7313 338
Vivotek SD7323 338
Vivotek VS2101 58
Vivotek VS2402 68
Vivotek VS2403 0
Vivotek VS3100 97/107
Vivotek VS3102 97/107
Vivotek VS7100 251
WebEye E10 50
Weldex WDNC-64072C 365
Xview AP-400/Linudix 81
Zylotech IPSmartCAM2 523
Milestone Systems offices are located across the world. For details about office addresses, phone and fax numbers, visit www.milestonesys.com.