Milestone Systems

Milestone Husky M30/M50

Administrator's Manual

The Open Platform Company

Contents

Introduction

Milestone Husky overview

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

Milestone Husky consists of a number of components, each targeted at specific tasks and user types:

Name	Description
Management Application	The main application used by surveillance system administrators for configuring the Milestone Husky surveillance system server, upon installation or whenever configuration adjustments are required, for example when you add new cameras or users to the system.
Recording Server service	A vital part of the surveillance system. The Recording Server service runs to ensure that devices transfer video streams to your system. The Recording Server service installs automatically and runs in the background on the surveillance system server. You manage the service through the Management Application.
Event Server service	Handles configuration of alarms and maps from all servers within Milestone Husky installations, including Master/slave setups (see "Configure master and slave servers" on page 168), throughout your organization. This enables monitoring and instant overview of alarms and possible technical problems within your systems. The event server is automatically installed on, and runs in the background of, the Milestone Husky surveillance system server.
Microsoft® SQL Server Express Database	The surveillance system's alarm data is stored in a SQL Server Express database. The SQL database is a lightweight, yet powerful, version of a full SQL server which is automatically installed on, and runs in the background of, your Milestone Husky surveillance system server.
Image Server service	Handles access to the surveillance system for users logging in with clients. The Image Server service is automatically installed and runs in the background on the surveillance system server. You can manage the service through the Management Application.
XProtect® Download Manager	Manage which Milestone Husky-related features your organization's users can access from a targeted welcome page on the surveillance system server.

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

Clients

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

Milestone Husky supports three different clients:

- XProtect Smart Client
- XProtect Web Client
- Milestone Mobile client

XProtect Smart Client

About XProtect Smart Client

Designed for Milestone XProtect® IP video management software, the XProtect Smart Client is an easy-to-use client application that provides intuitive control over security installations. Manage security installations with XProtect Smart Client which gives users access to live and recorded video, instant control of cameras and connected security devices, and an overview of recordings. Available in 26 languages, XProtect Smart Client has an adaptable user interface that can be optimized for individual operators' tasks and adjusted according to specific skills and authority levels.

The interface allows you to tailor your viewing experience to specific working environments by selecting a light or dark theme, depending on room lighting or brightness of the video. It also features work-optimized tabs and an integrated video timeline for easy surveillance operation. Using the Milestone Integration Platform, users can integrate various types of security and business systems and video analytics applications, which you manage through XProtect Smart Client.

XProtect Smart Client must be installed on users' computers. Surveillance system administrators manage clients' access to the surveillance system through the Management Application. Recordings viewed by clients are provided by your XProtect system's Image Server service. The service runs in the background on the surveillance system server. Separate hardware is not required.

To download XProtect Smart Client, you must connect to the surveillance system server which presents you with a welcome page that lists available clients and language versions. System

administrators can use the XProtect Download Manager to control what clients and language versions should be available to users on the welcome page of the XProtect Download Manager.

Install the XProtect Smart Client

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

Install from the surveillance server

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

   Tip: You can change the language in the **Options** menu of the XProtect Smart Client. Under XProtect Smart Client **Installers**, click the relevant XProtect Smart Client link to start the installer.
4. If you receive a security warning (**Do you want to run or save this file?**, **Do you want to run this software?** or similar), accept this (by clicking **Run** or similar—the exact name depends on your browser version).
5. The XProtect Smart Client **setup** wizard starts. In the wizard, follow the installation instructions.

The wizard suggests an installation path. Normally, you can use the suggested installation path. However, if you have previously used add-on products, such as XProtect <LPR>, this path might not be valid anymore.

Install from a DVD

1. Verify that your computer meets the XProtect Smart Client's minimum system requirements.
2. Insert the surveillance system software DVD, select the required language, and then click **Install** XProtect Smart Client.
3. If you receive a security warning (**Do you want to run or save this file?**, **Do you want to run this software?** or similar), accept this (by clicking **Run** or similar—the exact name depends on your browser version).
4. The XProtect Smart Client **installation** wizard starts. In the wizard, follow the installation instructions.

Install silently

Surveillance system administrators can deploy XProtect Smart Client or Milestone Husky 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 XProtect 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 is typically:
   C:¥Program Files (x86)¥Milestone¥Milestone Surveillance¥httpdocs¥Smart Client Installer¥[version number] [bit-version]¥All Languages¥en-US

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

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

a Run with default parameter settings:

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

- For XProtect Smart Client installation:

  >MilestoneXProtectSmart Client.exe -–quiet

- For Milestone Husky installation:

  > MilestoneXProtectXProtect ProfessionalInstaller.exe --quiet

This performs a quiet installation of the XProtect Smart Client/Milestone Husky using default values for parameters such as target directory and so on. To change the default settings, see below.

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

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

- For XProtect Smart Client:

  > MilestoneXProtectSmart Client.exe --generateargsfile=args.xml

- For Milestone Husky:

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

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

- For XProtect Smart Client:

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

- For Milestone Husky:

> MilestoneXProtectXProtect ProfessionalInstaller.exe --arguments=
C:¥MyFolder¥arguments.xml --quiet

Milestone Mobile client

About Milestone Mobile client

Milestone® Mobile client is a mobile surveillance solution closely integrated with the rest of your XProtect system. It runs on your Android tablet or smartphone or your Apple® device (tablet, smartphone or portable music player) and gives you access to cameras, views and other functionality set up in the Management Application. Use the Milestone Mobile client to view and play back live and recorded video from one or multiple cameras, control pan-tilt-zoom (PTZ) cameras, trigger output and events and use the Video push functionality to send video from your device to your XProtect system.

In order to use Milestone Mobile client with Milestone Husky, you must add a Mobile server (see "About Mobile server" on page 179) to establish the connection between the Milestone Mobile client and Milestone Husky. Once the Mobile server is set up, download the Milestone Mobile client for free from Google Play or App Store to start using Milestone Mobile.

Install Milestone Mobile client

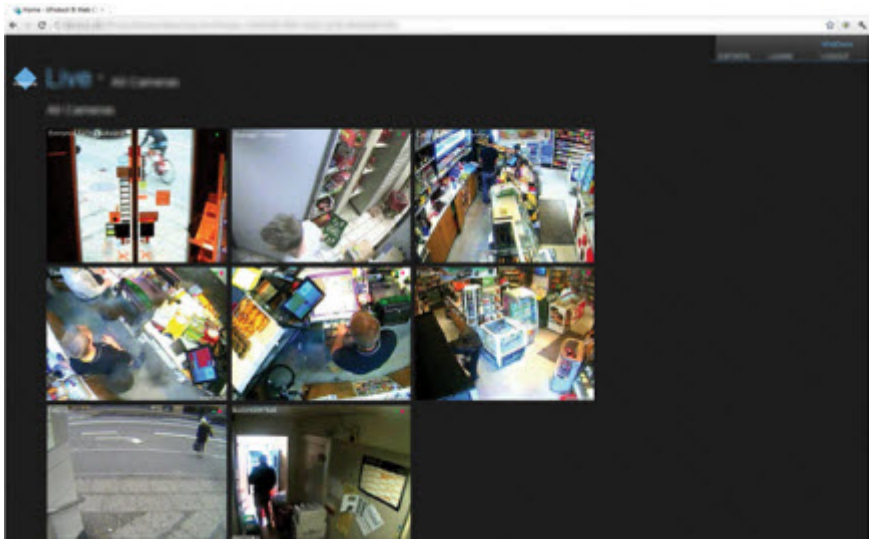
1. Access Google Play or App Store℠ on your device.
2. Search for and download the application Milestone Mobile.
3. Once the download of the application is completed, the Milestone Mobile client is ready for use on your mobile device.

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

XProtect Web Client

About XProtect Web Client

XProtect Web Client is a web-based client application for viewing, playing back and sharing video. It provides instant access to the most commonly used surveillance functions, such as viewing live video, play back recorded video, print and export evidence. Access to features depends on individual user rights which are set up in the Management Application.



To enable access to the XProtect Web Client, you must install a Mobile server (see "About Mobile server" on page 179) to establish the connection between the XProtect Web Client and Milestone Husky. The XProtect Web Client itself does not require any installation itself and works with most Internet browsers (see "Minimum system requirements" on page 21). Once the Mobile server is set up, you can monitor your XProtect system anywhere from any computer or tablet with Internet access (provided you know the right external/Internet address, user name and password).

Access XProtect Web Client

If you have a Milestone Mobile server (see "About Mobile server" on page 179) installed on your computer, you can use the XProtect® Web Client to access your cameras and views. Since you do not need to install XProtect Web Client, you can access it from the local computer on which you installed the Milestone Mobile server or any other computer you want to use for this purpose.

To access the XProtect Web Client:

1. Set up the Milestone Mobile server in the Management Application.
2. Open an Internet browser (Internet Explorer, Mozilla Firefox, Google Chrome or Safari) or click **Open XProtect Web Client** in the Mobile Server Manager (see "About Mobile Server Manager" on page 184).

3. Type in the IP address (that is, the external address and port of the server on which the Milestone Mobile server is running.

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

   In the address bar of your browser, type: http://127.2.3.4:8081/XProtectMobile/Web/ or https://127.2.3.4:8082/XProtectMobile/Web/, depending on whether you want to use a standard HTTP connection or a secure HTTPS connection. You can now begin using XProtect Web Client.

4. Add the address as a bookmark in your browser for easy future access to XProtect Web Client. If you use XProtect Web Client on the local computer on which you installed the Milestone Mobile server, you can also use the desktop shortcut created by the installer. Click the shortcut to launch your default browser and open XProtect Web Client.

Note that Internet browsers running the XProtect Web Client must have their cache cleared before you can use a new version of the XProtect Web Client.

System administrators must ask their XProtect Web Client users to clear out their browser's cache upon upgrade or force this action remotely (you can do this action only in Internet Explorer in a domain).

Recording Server Manager

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

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

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

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

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

Monitor System Status

Right-click the notification area's Recording Server icon and select **Show System Status** to get access to 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 is indicated in gray in the following situations:
  - The camera is not online (as defined in the camera's online period schedule (see "Online period" on page 142)).

  - 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 relevant camera. The information appears as a pop-up and updates approximately every 10 seconds.

Name	Description
Resolution	The resolution of the camera.
FPS	The number of frames per second (frame rate) currently used by the camera. The number updates each time the camera has received 50 frames.
Frame count	The number of frames received from the camera since the Recording Server service was last started.
Received KB	The number of kilobytes sent the by camera since the Recording Server service was last started.
Offline	Indicates the number of times the camera has been offline due to an error.

XProtect Download Manager

Manage which Milestone Husky-related features your organization's users can access from a targeted welcome page on the surveillance system server through the use of XProtect Download Manager.

Access XProtect Download Manager from Windows' **Start** menu: Select **All Programs** > **Milestone XProtect Download Manager** > **Download Manager**.

Examples of user-accessible features

- **XProtect Smart Client**. Users connect to the surveillance server through an Internet browser where they are presented with a welcome page. From the welcome page, users can download the XProtect Smart Client software and install it on their computers.

- **Language packs**, which let users add additional language versions to their existing XProtect Smart Client installations. Users download such language packs from the welcome page.

- **Various plug-ins**. Downloading such plug-ins can be relevant for users if your organization uses add-on products with the Milestone Husky system.

The welcome page

The welcome page links to downloads of various features. It is available in a number of languages and users select the language they require from a menu in the top right corner of the welcome page.

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

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

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

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

The content of the welcome page is managed through the XProtect Download Manager and can look different in different organizations.

Initial look

Immediately after you install Milestone Husky, the welcome page provides access to the XProtect Smart Client in all languages. You can also download XProtectSmart Client 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.

Default configuration of XProtect Download Manager

XProtect 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 XProtect Download Manager configuration is represented in a tree structure.

Download Manager's tree structure explained:

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

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

You can make more features and/or languages available if you need to. See **Making new features available** in the following for more information.

Making new features available

When you install new features, these are by default selected in the XProtect Download Manager and are immediately available to users through the welcome page. You can always show or hide features on the welcome page by selecting or clearing check boxes in the tree structure.

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

Hiding and removing features

You can remove features in several ways:

- You can **hide features** from the welcome page by clearing check boxes in XProtect Download Manager's tree structure. In that case, the features are still installed on the surveillance system server, and by selecting check boxes in the tree structure, you can quickly make the features available again.
- You can **remove features** which have previously been made available through XProtect Download Manager. This removes the installation of the features on the surveillance system server. The features disappear from XProtect Download Manager, but installation files for the features are kept in the surveillance system server's **Installers** or relevant language folder, so you can re-install them later if required.

  1. In XProtect Download Manager, click **Remove features...**
  2. In the **Remove Features** window, select the features you want to remove.
  3. Click **OK** and then click **Yes**.

Updates

Milestone regularly releases service updates for its products, offering improved functionality and support for new devices. Milestone recommends that you check www.milestonesys.com for updates at regular intervals in order to make sure you are using the most recent version of your surveillance software.

Before you start

Minimum system requirements

Surveillance system server:

Component	Requirement
Operating system	• Microsoft® Windows® 8 Enterprise (64-bit) • Microsoft Windows 8 Pro (64-bit) • Microsoft Windows 7 Ultimate (64-bit) • Microsoft Windows 7 Enterprise (64-bit) • Microsoft Windows 7 Professional (64-bit) • Microsoft Windows Server 2012 (64-bit): Standard and Datacenter. • Microsoft Windows 2008 R2 (64-bit): Standard, Web, High Performance Computing (HPC), Enterprise and Datacenter • Microsoft Windows Server 2008 (64-bit) • Microsoft Windows Vista Business (64-bit) • Microsoft Windows Vista Enterprise (64-bit) • Microsoft Windows Vista Ultimate (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 10 GB free hard disk space available, excluding space needed for recordings.
Software	• Microsoft .NET 4.5 Framework. • Microsoft .NET 4.0 Framework. • DirectX 9.0 or newer. • Windows Installer 4.5. You can download all from the Microsoft website.

XProtect Smart Client:

Component	Requirement
Operating System	• Microsoft® Windows® 8 Enterprise (32-bit or 64-bit) • Microsoft Windows 8 Pro (32-bit or 64-bit) • Microsoft Windows 7 Ultimate (32-bit or 64-bit) • Microsoft Windows 7 Enterprise (32-bit or 64-bit) • Microsoft Windows 7 Professional (32-bit or 64-bit) • Microsoft Windows Server 2012 (64-bit): Standard and Datacenter. • Microsoft Windows Server 2008 R2 (64-bit): Standard, Web, High Performance Computing (HPC), Enterprise, and Datacenter. • Microsoft Windows Server 2008 (32-bit or 64-bit) • Microsoft Windows Server 2003 (32-bit or 64-bit) • Microsoft Windows Vista Ultimate (32-bit or 64-bit) • Microsoft Windows Vista Enterprise (32-bit or 64-bit) • Microsoft Windows Vista Business (32-bit or 64-bit) • Microsoft Windows XP® Professional (32-bit or 64-bit)
CPU	Intel® Core2™ Duo, minimum 2.4 GHz or higher (more powerful CPU recommended for XProtect Smart Clients running high number of cameras and multiple views and displays)
RAM	Minimum 1 GB (higher RAM recommended for systems running a high number of cameras and multiple views and displays)
Network	Ethernet (100 Mbit or higher recommended)
Graphics adapter	AGP or PCI-Express, minimum 1280 x 1024, 16 bit colors
Hard disk space	1 GB free
Software	• Microsoft .Net 4.0 Framework or newer • DirectX 9.0 or newer • Windows Help (WinHlp32.exe).

Milestone Mobile client:

Component	Requirement
Operating system	• iOS 6.0 or newer for Apple devices. • Android 2.2 or newer for Android devices.

XProtect Web Client:

Component	Requirement
Supported browsers	Internet browsers that support HTML 5 and JavaScript. XProtect Web Client runs on: • Microsoft Internet Explorer 9 or newer. • Mozilla Firefox 11 or newer. • Google Chrome 16 or newer. • Safari 5 or newer.

Administrator rights

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

Important port numbers

Available functionality depends on your product version.

Milestone Husky uses particular ports when communicating with other computers, cameras, and so on. Make sure that the following ports are open for data traffic on your network when you use Milestone Husky:

Name	Description
Port 20 and 21 (inbound and outbound)	Used for FTP traffic. FTP (File Transfer Protocol) is a standard for exchanging files across networks. FTP uses the TCP/IP standards for data transfer, and is often used for uploading or downloading files to and from servers.
Port 25 (inbound and outbound)	Used for SMTP traffic. SMTP (Simple Mail Transfer Protocol) is a standard for sending e-mail messages between servers. This port should be open since, depending on configuration, some cameras may send images to the surveillance system server via e-mail.
Port 80 (inbound and outbound)	Used for HTTP traffic between the surveillance server, cameras, and the XProtect Smart Client, and the default communication port for the surveillance system's Image Server service.

Name	Description
Port 554 (inbound and outbound)	Used for RSTP traffic in connection with H.264 video streaming.
Port 1024 (outbound only)	Used for HTTP traffic between cameras and the surveillance server.
Port 1234 (inbound and outbound)	Used for event handling.
Port 1237 (inbound and outbound)	Used for communication with the XProtect Central add-on product (if your organization uses this).
Port 8081 and 8082	Used for communication with the Mobile service.
Port 22331	Used for communication with the Event Server service.

Your organization may also have selected to use any other port numbers, for example if you have changed the server access (on page 166) port from its default port number (80) to another port number.

Virus scanning

Virus scanning uses a considerable amount of system resources on scanning all the data which XProtect Download Manager is archiving or using. The scanning process may temporarily lock each file it scans, which can further impact system performance negatively. Therefore, you should disable any virus scanning of affected areas (such as camera databases, and so on.) on the Milestone Husky server as well as on any archiving destinations if you are allowed to in your organization.

Time server use recommended

Once your system receives images, they are instantly time-stamped. However, since cameras are separate units which may have separate timing devices, power supplies and so on, camera time and your system time may not correspond fully. This may occasionally lead to confusion. If your cameras supports timestamps, Milestone recommends that you auto-synchronize camera and system time through a time server for consistent synchronization.

For information about how to configure a time server, try searching www.microsoft.com for **time server**, **time service**, or similar.

Installation

About installing surveillance server software or XProtect Smart Client silently

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

Install your surveillance server software

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

Before you start: Shut down any existing surveillance software.

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

You can now begin to configure your Milestone Husky through its Management Application. For more information, see Get your system up and running (on page 28).

Install silently

Surveillance system administrators can deploy XProtect Smart Client or Milestone Husky 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 XProtect 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 is typically:
C:¥Program Files (x86)¥Milestone¥Milestone Surveillance¥httpdocs¥Smart Client Installer¥[version number] [bit-version]¥All Languages¥en-US

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

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

a Run with default parameter settings:

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

- For XProtect Smart Client installation:

  >MilestoneXProtectSmart Client.exe -–quiet

- For Milestone Husky installation:

  > MilestoneXProtectXProtect ProfessionalInstaller.exe --quiet

This performs a quiet installation of the XProtect Smart Client/Milestone Husky using default values for parameters such as target directory and so on. To change the default settings, see below.

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

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

- For XProtect Smart Client:

  > MilestoneXProtectSmart Client.exe --generateargsfile=args.xml

- For Milestone Husky:

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

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

- For XProtect Smart Client:

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

- For Milestone Husky:

  > MilestoneXProtectXProtect ProfessionalInstaller.exe --arguments= C:¥MyFolder¥arguments.xml --quiet

Video device drivers

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

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

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

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

If you use the Add Hardware Devices Wizard's Import from CSV File (on page 50) option, you must—if cameras and server are offline—specify a **HardwareDriverID** for each hardware device you want to add. To view a current list of IDs, view the release notes for the XProtect Device Pack used in your organization. Alternatively, visit the Milestone website for the latest information.

Remove system components

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

You can also remove individual components, such as XProtect Smart Client and video drivers by using the standard Windows procedure for uninstalling programs.

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

First time use

Get your system up and running

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

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

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

Verify initial configuration of cameras and other hardware devices

☐ When your system opens for the first time, the Getting Started wizard opens to assist you with quickly adding hardware devices (cameras, video encoders and more) to your system and configuring them with proper user names and passwords. See Getting started wizard (see "Automatic configuration wizard" on page 46).

Register your software

☐ You may not need to go through this step as your vendor often takes care of the process for you. You must first register your software and next activate your licenses. See Manage licenses **(see "**About activating licenses**" on page 33).**

Install Milestone Husky

☐ See Install surveillance server software **(see "**Install your surveillance server software**" on page 25).**

Open the Management Application

☐ See Access the Management Application**.**

Add hardware devices

☐ Your system can quickly scan your network for relevant hardware devices (cameras, video encoders and more), and add them to your system. See Add hardware devices (see "Add hardware wizard" on page 47).

Configure cameras

☐ You can specify a wide variety of settings for each camera connected to your system. Settings include video format, resolution, motion detection sensitivity, where to store and archive (see "About archiving" on page 133) recordings, any PTZ (pan-tilt-zoom) preset positions, association with microphones, speakers and more. See About video and recording configuration (on page 71).

Configure events, input and output

☐ If required, use system events, for example based on input from sensors, to automatically trigger actions in your system.

Examples of actions: starting or stopping recording on cameras, switching to a particular video frame rate, making PTZ cameras move to specific preset positions. Also use events to activate hardware output, such as lights or sirens. See Overview of events.

Configure scheduling

☐ Set up when do you want to archive and if you want cameras to transfer video to your system at all times, and other cameras to transfer video only within specific periods of time as well as when specific events occur. Also specify when you want to receive notifications from the system. See Configure general scheduling and archiving (on page 138) and Configure camera-specific schedules (on page 73).

Configure clients' access to Milestone Husky

☐ A number of different client applications (see About clients) are included with your system. Specify whether you want clients to access the system server from the Internet, how many clients you want to be able to connect simultaneously and more. See Configure server access (on page 166).

Configure master/slave servers

This step is only required if you want to run several servers together.

☐ A master/slave setup allows you to combine several servers and, thereby, extend the number of cameras you can use beyond the maximum allowed number of cameras for a single server.

In such a setup, clients still have a single point of contact: they connect to the master server but also get access, transparently, to cameras and recordings on the slave servers. See Configure master and slave servers (on page 168).

Configure users

☐ Specify who should access your system and how. Set a password protection for the Management Application if needed. Decide who should have client access which rights they should have. See Configure User Access wizard (see "Manage user access wizard" on page 62), Add basic users (on page 171), Add user groups (on page 173) and Configure user and group rights (on page 173).

Configure XProtect Download Manager

☐ Manage which features users see on a targeted welcome page when they connect to the Milestone Husky server. The features can include access to client applications, additional client language versions, plug-ins and more. See Use XProtectDownload Manager.

XProtect Download Manager comes with a default configuration that ensures that users get access to XProtect Smart Client in the same language as your Milestone Husky server.

The above list represents the configuration steps that most administrators are likely to cover. You can, of course, do more configuration, for example if your organization wants to use the Matrix (see "About Matrix video sharing" on page 143) video-sharing feature or similar.

Note that you can customize (see "User Interface" on page 41) the behavior of the Management Application. Descriptions here are, however, always based on the Management Application's default behavior.

About saving changes to the configuration

As you set up your system, you must save any changes you make to the configuration in order for these to be applied to the system. When you change the configuration in the Management Application, for example in the Camera Summary or Users Properties, a yellow notification bar informs you that you have made changes to the configuration. The bar appears in order to make sure that your changes are applied to the system. If you want to apply the changes, click **Save**. If you do not want to save your changes, click **Discard**.

Once you have made changes to the configuration of your Management Application and saved these, your system contacts the system services (such as the Recording Server service and the Image Server service). If you make changes to your configuration, for example if you change the name of a camera or change motion detection settings, the relevant system services load the new configuration and the changes appear in your client immediately. In contrast, more resource-demanding configuration changes, for example if you add a new event, require that you restart the relevant services before they work properly. If a restart of services is necessary, your system carries out the restart automatically once you have saved the changes. If you make changes to settings in the Milestone Mobile server, your system applies all changes when you click **Save,** without restarting the Milestone Mobile server service.

IMPORTANT: While your system restarts services, you cannot view or record video. Restarting services typically only takes a few seconds, but in order to minimize disruption, you may want to restart services at a time when you do not expect that any important incidents take place. Users connected to your system through clients can remain logged in during the restart of services, but may experience a short video outage.

Note that the system stores changes in a restore point (see "Restore system configuration from a restore point" on page 201) (so that you can return to a working configuration if something goes wrong).

About the built-in help

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

The help system opens in your default Internet browser and allows you to switch between the help and your system itself. The help system is context-sensitive. This means that when you press F1 for help while you work in a particular dialog, the help system displays help that matches that dialog.

Navigate the built-in help system

To navigate between the contents of the help system, use the help tabs: **Contents**, **Index, Search,** or use the links inside the help topics.

- **Contents:** navigate the help system based on a tree structure.
- **Index:** contains an alphabetical indexation of help topics.

- **Search:** search for help topics that contain particular terms of interest. For example, you can search for the term **zoom** and every help topic that contains the term **zoom** is listed in the search results. When you double-click a help topic title in the search results list, the relevant topic opens.

Print help topics

If you need to print a topic, use your Internet browser's printing function. When you print a help topic, it is printed as you see it on your screen. This means that if a topic contains links that expand when you click on them (drop-down links) and you want the information in the drop-down links shown in your print output, you must click each relevant drop-down link to display the text to include it when you print. This allows you to create targeted printouts that contain exactly the amount of information you need.

About restarting services

Some changes in the Management Application require that your system restarts the Image Server service or Recording Server service. See a list of these below:

Image Server
Change of port number
Maximum number of clients
Enabling or disabling of master servers
Adding or removing slave servers
Change of log path
Change of license
Change of privacy mask
Removal of hardware devices
Turning evidence collection mode on or off. XProtect Enterprise only.

Recording Server
Change of license
Change of event database path
Turning on manual recording
Start on remote
Enabling and disabling of notifications
Change of events
Change of outputs
Adding or removing a dynamic archiving path
Adding or removing archive time
Change of scheduling
Setting up the Matrix functionality
Replacing hardware devices
Changing camera driver
Changing camera IP address
Deletion of all devices
Enabling or disabling of alarms on Customer Dashboard
Turning evidence collection mode on or off. XProtect Enterprise only.

Licenses

About licenses

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

When you have installed the various Milestone Husky components, configured the system, and added recording servers and cameras through the Management Application, the surveillance system initially runs on temporary licenses that you must activate before a certain period of time ends. This is called the grace period. If grace periods expires on one or more of your devices and you have not activated any licenses, recording servers and cameras do not send data to the surveillance system. Milestone recommends that you activate your licenses (see "About activating licenses" on page 33) before you make final adjustments to your system and its devices.

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

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

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

About devices and licenses

About replacing cameras

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

When you replace a camera, you must use the Management Application Replace Hardware Device wizard (on page 67) to map all relevant databases of cameras, microphones, inputs, outputs, etc. Remember to activate the license once you are finished.

About getting additional licenses

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

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

Overview of license information (on page 33)

Overview of license information

Available functionality depends on your product version.

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

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

You can activate licenses online or offline. On the Management Application's toolbar**,** click **File** and either **Activate License Online** or **Manage License Offline**. Cameras (or dedicated input/output boxes) for which you are missing a license do not send data to the surveillance system. Cameras added after all available licenses are used are unavailable.

About activating licenses

When you purchase Milestone Husky, you receive a temporary license file (.lic) including a Software License Code (SLC). You must use this temporary license file when you install your system. In order to get your permanent license, register your SLC before you activate licenses. When you have registered your SLC, you can activate your licenses in two ways: **online** or **offline**.

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. To get an overview

of your licenses, go to the Management Application's navigation pane > **Advanced Configuration** > **Hardware Devices** and view your **Hardware Device Summary** table.

The following example assumes that you have installed Milestone Husky with a temporary license (.lic) file.

About activating licenses after grace period

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

If you exceed the grace period before you activate a license, the license is not lost. You can activate the license as usual. Configuration, added cameras, and other settings are not removed from the Management Application if a license is activated too late.

Register SLC

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

1. Go to the Milestone website at www.milestonesys.com, and click the Software registration link in the menu.
2. Log in to the **Software Registration Service Center** with your user name (e-mail address) and password.
3. In the Software Registration Service Center, click the **Add SLC** link.
4. Type your SLC. Confirm that you want to add the SLC to your account, and then click **OK**.
5. Once your SLC has been added, click the **Main menu** link.
6. Click the **Logout** link to log out of the Software Registration Service Center.

Tip: If you have not used the Software Registration Service Center before, click the **New to the system?** link, and follow the instructions for registering yourself as a user, then log into the Software Registration Service Center by using your registered user name and password.

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

Activate License - Online

If your system is connected to the Internet, your system automatically activates licenses whenever you add devices to your system. You do not need to specify any user name or password.

The system checks every fifteen minutes if the license file corresponds to the number of installed cameras. If you have added or removed cameras in that time frame, the system automatically adds the license for these cameras as well.

Activate License - Offline

Precondition

Add at least one device (see "Add hardware wizard" on page 47) to your Milestone Husky system.

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

Step 1: Export license for activation (offline)

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

1. On the Management Application's toolbar, click **File**, **Manage License Offline, Export License for Activation.**
2. Specify a file name and a location for the license request (.lrq) file (automatically generated by Milestone Husky). If your computer does not have Internet access, use external, removable data storage.
3. If needed, move the external data storage with the .lrq file to a computer with Internet access. Open an Internet browser and go to Milestone's website at www.milestonesys.com. Select **Software Registration** from the top menu. If you have used the Software Registration Service Center before, log in with your e-mail and password. Otherwise, click **New to the System?** to create a new user account and register your SLC.
1. Under **Current SLCs**, select the SLC**.**
    2. In the menu for SLC properties, use the **Upload LRQ** function to upload the generated .lrq file.
4. Next, you receive the updated permanent license file (.lic) from Milestone via e-mail. Save it to a location accessible from the Management Application.

Step 2: Import license (offline)

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

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

1. On the Management Application's toolbar, click **File > Manage License Offline > Import License**, and select your saved .lic file to import it**.**
2. When the permanent license file is successfully imported, click **OK.**

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

Change SLC

If you need to change your SLC and 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 system.

1. On the Management Application's toolbar, click **File > Manage License Offline > Import License**, and select your saved .lic file to import it**.**
2. When the new permanent license file is successfully imported, click **OK.**

About replacing cameras

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

When you replace a camera, you must use the Management Application Replace Hardware Device wizard (on page 67) to map all relevant databases of cameras, microphones, inputs, outputs, etc. Remember to activate the license once you are finished.

Settings

About automatic device discovery

Automatic device discovery allows you to automatically add hardware devices to your system as soon as you connect these to your network. When you enable automatic device discovery, your system configures and set ups cameras automatically without the need for any user interaction, making the camera instantly accessible in XProtect Smart Client's default view after the automatic installation has completed.

Note that:

- Not all cameras support automatic device discovery.
- Cameras respond differently to automatic device discovery. The systems adds some devices (such as Axis models P3301 and P3304) to the system automatically, while some devices from other vendors (such as Sony models SNC-EB520, EM520 and E521) you must turn off and back on again before they are automatically added to your system.
- You must still manually activate licenses (see "About activating licenses" on page 33) for your camera. This is to ensure that you only activate cameras set up in an environment with multiple servers on one of the servers.

About system mode

At some point in time when you save recordings on your system, the storage you save recordings on may become full. Your system offers you two system modes which handle this scenario differently, **Classic mode** and **Evidence mode**.

- **Classic mode** means that the system automatically deletes the oldest saved recordings in order to make room for new recordings.When you remove a hardware device in the Management Application, recordings from the relevant device are deleted from your storage. You can no longer play back recordings from the removed camera in XProtect Smart Client as these recordings will be deleted from your storage.
- **Evidence mode** means that the system stops recording when you reach full storage capacity. All your old recordings are kept in the storage and the system does not save any new recordings. This ensures that video recorded as evidence is never deleted automatically and remains on the hard disk drive until you change system settings in your system or you manually remove the recordings from your storage. Similarly, if you remove a hardware device from the Management Application, recordings from the device are still kept on your storage. You can playback recordings in XProtect Smart Client even if you have removed the device in the Management Application.

Summary:

	Classic mode	Evidence mode
When the storage on which you are recording becomes full	The system deletes oldest recordings to make room for new recordings.	The system stops saving new recordings and keeps the oldest recordings.
When you delete a device in the Management Application	The system deletes all recordings from the removed device.	The system keeps all recordings from the removed device.
Playback in XProtect Smart Client	If you have removed the device from the Management Application, playback is no longer possible in XProtect Smart Client because the system deletes recordings from the device when you remove it.	Even if you have removed the device from the Management Application, playback is still possible in XProtect Smart Client as the system keeps the recordings.
Retention time	You can set and customize retention time for your recordings.	You cannot set retention time for your recordings as your system never deletes recordings.

Choose a system mode that fits your system needs. Most users need the most recent video to be available in their storage and should select **Classic** mode. **Evidence** mode provides an alternative in cases where any recorded video is considered evidence and therefore must remain on your storage.

Disable information collection

1. In the Management Application toolbar, click **Options** > **Settings** > **Privacy Options**.
2. On the **Privacy Options** tab, clear the **Yes, I would like to improve Milestone Husky** check box.
3. Click **OK**.

Change default file paths

To change any of the default file paths:

1. If you want to change the configuration path, stop (see "Start and stop services" on page 178) all services. This step is not necessary if you want to change the default recording or archiving path.
2. On the Management Application menu bar, select **Options** > **Default File Paths...**
3. You can now overwrite the necessary paths. Alternatively, click the browse button next to the field and browse to the location. For the default recording path, you can only specify a path to a folder on a **local** drive. If you are using a network drive, you cannot save recordings if the network drive becomes unavailable.

If you change the default recording or archiving paths and there are existing recordings at the old locations, you must select whether you want to move the recordings to the new locations (recommended), leave them at the old locations, or delete them.

4. Once changes are confirmed, restart (see "Start and stop services" on page 178) all services.

Options

In this section

General

In the General settings, you can change a number of settings that affect the general behavior and look of the Management Application.

Automatic device discovery

Automatic device discovery (see "About automatic device discovery" on page 37) is turned off by default in your system. Select the check box to enable this functionality. If the camera should use an additional user name and password besides the camera's default user name and password, select the **Use the camera's default user name and password as well as the following credentials** check box and type the relevant credentials.

Note: Not all devices support automatic device discovery. If your system does not detect your camera and add it to your system, you must manually add the camera.

Customer Dashboard

Choose if your system should send system information to the Customer Dashboard.

System mode

Important: Do **not** change system mode unless you are absolutely sure that you want the new setting to be in effect immediately after saving.

At some point in time when you save recordings on your system, the storage you save recordings on may become full. Your system offers you two system modes which handle this scenario differently, **Classic mode** and **Evidence collection mode**.

- **Classic mode** means that the system automatically deletes the oldest saved recordings in order to make room for new recordings. When you remove a hardware device in the Management Application, recordings from the relevant device are deleted from your storage. You can no longer play back recordings from the removed camera in XProtect Smart Client as these recordings will be deleted from your storage.

- **Evidence collection mode** means that the system stops recording when you reach full storage capacity. All your old recordings are kept in the storage and the system does not save any new recordings. This ensures that video recorded as evidence is never deleted automatically and remains on the hard disk drive until you change system settings in your

system or you manually remove the recordings from your storage. Similarly, if you remove a hardware device from the Management Application, recordings from the device are still kept on your storage. You can playback recordings in XProtect Smart Client even if you have removed the device in the Management Application.

Summary:

	Classic mode	Evidence collection mode
When the storage on which you are recording becomes full	The system deletes oldest recordings to make room for new recordings.	The system stops saving new recordings and keeps the oldest recordings.
When you delete a device in the Management Application	The system deletes all recordings from the removed device.	The system keeps all recordings from the removed device.
Playback in XProtect Smart Client	If you have removed the device from the Management Application, playback is no longer possible in XProtect Smart Client because the system deletes recordings from the device when you remove it.	Even if you have removed the device from the Management Application, playback is still possible in XProtect Smart Client as the system keeps the recordings.
Retention time	You can set and customize retention time for your recordings.	You cannot set retention time for your recordings as your system never deletes recordings.

Choose a system mode that fits your system needs. Most users need the most recent recordings to be available in their storage and should select **Classic** mode. **Evidence** mode provides an alternative in cases where all recorded video is considered evidence and therefore must remain on your storage.

Important: Evidence Collection mode is only supported in XProtect Enterprise 2013. If you run your system in trial mode, only **Classic** mode is available.

Language

The Management Application is available in several languages. From the list of languages, select the language you want to use. Restart the Management Application to make the change of language take effect.

User Interface

You can change the way the Management Application behaves. For example, by default, the Management Application asks you to confirm many of your actions. If you feel this is not necessary, you can change the behavior of the Management Application to not ask you again. Go to **User Interface** to make changes for each action.

Examples of actions you can change:

- When you attempt to delete a hardware device, should the Management Application ask you to confirm that you want to delete the hardware device, or should it delete the hardware device straight away without asking?

- You can use a maximum of 64 cameras at a time on a single Milestone Husky server. If you add more than 64, should the Management Application warn you or not?
- Should your system show live video when you preview camera or would you rather see a snapshot or no preview of the camera?

Click **Restore Default Settings** below the behavior list to restore your system to its default behavior.

Default File Paths

Your system uses a number of default file paths:

File paths	Description
Default recording path for new cameras	All new cameras you add use this path by default for storing recordings. If required, you can change individual cameras' recording paths as part of their individual configuration (see "Recording and archiving paths" on page 98), but you can also change the default recording path so all new cameras you add use a path of your choice.
Default archiving path for new cameras	All new cameras you add use this path by default for archiving (see "About archiving" on page 133). 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 use a path of your choice. Note that camera-specific archiving paths are not relevant if you use dynamic path selection (on page 79) for archiving.
Configuration path	The path by default used for storing your system configuration.

Privacy Options

When you installed your system, you were presented with the option **Sign me up for the Customer Experience Improvement Program.** The Customer Experience Improvement Program has been set up to improve the usability and customer experience of Milestone Husky.

- If you **declined**, your system installation does not include **any software** that contributes statistical information.
- If you **accepted**, a cookie that issues a Global Unique IDentifier (GUID) is included as part of your system installation. As a result, your system anonymously collects relevant information about your installation and operation of your system at regular intervals. See the following for a detailed list of what is collected.

If you initially accept the collection of information during the installation, you can turn it off again whenever you want. This is done in the Management Application.

What information is collected from Milestone Husky?

No information is collected about the equipment (PC) Milestone Husky is installed on, nor about any of the recordings you make.

The following information is collected:

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

When is information collected from Milestone Husky?

Information is only collected when the Management Application or XProtect Smart Client is active. You can disable the automatic collection of information by either removing Milestone Husky or by disabling it in the Management Application.

How does Milestone protect collected information?

Milestone is committed to protecting the security of the information collected from Milestone Husky 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.

Analytics Event Settings

Analytics Event Settings let you specify the following:

Name	Description
Enabled	Lets you enable the analytics event feature
Port	Specify the port used by this service. Default port is 9090. Make sure that relevant VCA tool providers also use this port number. If you change the port number, make sure that VCA tool providers change their port number accordingly.

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

Event Server Settings

Specify the following Event Server settings:

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

Name	Description
Log server communication	Specify if you want to save a separate log of server communication in addition to the regular log for the number of days specified.

Getting started

About the Getting started page

The Getting started window is always shown when you open the Management Application. The Getting started page provides you with an easy way to go through wizards and serves as a place of reference for users.

To know how many of your system's camera licenses you are using, or to know the expiration date of your Software Upgrade Plan (SUP), you can find this information in the bottom-left and bottom-center columns on the Getting started page. To access information about your SUP, you must be connected to the Internet.

You can also access and view video tutorials that show and explain how to go through each step of your system's wizards. To access these, click the **View tutorials** link to this in the bottom-right column. The link takes you to an external web page with video tutorials for your system.

Automatic configuration wizard

The **Automatic configuration** wizard is for easy configuration for first time use of the system. Use the wizard to automatically add cameras to your system using this step-by-step procedure.

Steps in this wizard:

Automatic configuration wizard: First page

When you open the Management Application for the first time, the Automatic configuration wizard opens to guide you through the process of adding hardware devices to your system. If you are new to the system, click **Yes, configure** to scan your network for available cameras and configure your system. To exit and use a more advanced way of adding devices to your system, click **Skip** to leave the wizard and go to the Management Application to get more options for setting up your system's device configuration.

Automatic configuration wizard: Scanning options

Choose where you want your system to scan for cameras and devices.

By default, the **Scan local network** checkbox is selected, which means that you only scan your local network for devices. However, if you know the IP address or a range of IP addresses to which cameras and devices are attached, specify these by clicking the Plus icon next to **Add the IP**

addresses or IP ranges to be scanned. You can add more than one range of IP addresses if you need to.

Automatic configuration wizard: Select hardware manufacturers to scan for

If you know the specific manufacturer of your hardware device(s), select these in the dropdown on this page. You can select as many manufacturers as you want to.

Note: By default, all manufacturers are selected. If you want to reduce the scanning time or know the specific manufacturers of your cameras, only select the checkboxes that represents these manufacturers.

Automatic configuration wizard: Scanning for hardware devices

Scanning for hardware devices that match your selected manufacturers begins. A status bar indicates how far in the scan process you are. Once scanning for cameras and devices is complete, you may need to provide user name and password for your selected devices or cameras. When you have typed in the relevant credentials, click the **Verify** button to add the device to your system.

Note: Not all devices and cameras need a user name and password. You can add such devices to your system without any need to type in credentials.

Automatic configuration wizard: Continue after scan

Once you have added the number of devices and cameras you want to add, your system sets up storage for you. Storage is the location to which your system saves recordings. By default, your system chooses the location with most available disk space.

When the system has finished configuring storage, you are given the option to automatically add new cameras to your system as they are detected on the network. Enabling this allows you to set up your system so that any devices or cameras are automatically set up for you in the future as soon as they are connected to your network. Note that not all devices and cameras support automatic discovery. If your device/camera does not show up automatically after you have connected it to your network, you must add it manually.

To go directly to XProtect Smart Client once you have completed the wizard, select the check box in the bottom-left corner of the wizard page.

Add hardware wizard

You add cameras and other hardware devices, such as video encoders, to your system through the **Add Hardware wizards**. If the hardware device has microphones or speakers attached, the tool automatically adds these as well.

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

The wizard offers you four different ways of adding cameras:

Name	Description
Advanced	Scans your network for relevant hardware devices based on your specifications regarding required IP ranges, discovery methods, drivers, and device user names and passwords. See Add Hardware Devices wizard - Advanced.
Manual	Specify details about each hardware device separately. A good choice if you only want to add a few hardware devices, and you know their IP addresses, required user names and passwords, etc. See Add Hardware Devices wizard - Manual (see "Manual" on page 49).
Import from CSV file	Import data about cameras as comma-separated values from a file. An effective method if you are setting up several systems. See Add Hardware Devices Wizard - Import from CSV File (see "Import from CSV file" on page 50).

Steps in this wizard:

Express

Note: Device discovery is a method with which hardware devices make information about themselves available on the network. Based on such information, your system can quickly recognize relevant hardware devices, such as cameras and video encoders, and include them in a scan.

The **Scan for hardware** method gives you the option to scan your network for relevant hardware devices and quickly add them to your system in just a few steps.

Choose between these two options for adding hardware:

- **Scan local network**: Let the wizard perform an automated scan for available hardware on your local network that support device discovery, on the part of your network (subnet) where the system server itself is located.
- **Add IP address or IP range to be scanned:** Let the wizard add hardware to your system by indicating IP ranges and ports from which the system begin scanning for hardware.

To use the **Scan local network** method, **your system server and your cameras must be on the same layer 2 network**, that is a network where all servers, cameras, and so on can communicate without the need for a router. The reason for this is that device discovery relies on direct communication between the system server and the cameras. If you use routers on your network, specify the IP range where you hardware is located using the **Add IP address or IP range to be scanned**-option or choose one of the Manually specify the hardware to add (see "Manual" on page 49)-methods.

Add hardware: Scanning options

Choose where you want your system to scan for cameras and devices.

By default, the **Scan local network** checkbox is selected, which means that you only scan your local network for devices. However, if you know the IP address or a range of IP addresses to which cameras and devices are attached, specify these by clicking the Plus icon next to **Add the IP addresses or IP ranges to be scanned**. You can add more than one range of IP addresses if you need to.

Add hardware: Select hardware manufacturers to scan for

If you know the specific manufacturer of your hardware device(s), select these in the dropdown on this page. You can select as many manufacturers as you want to.

Note: By default, all manufacturers are selected. If you want to reduce the scanning time or know the specific manufacturers of your cameras, only select the checkboxes that represents these manufacturers.

Hardware detection and verification

Scanning for hardware devices that match your selected manufacturers begins. A status bar indicates how far in the scan process you are. Once scanning for cameras and devices is complete, you may need to provide user name and password for your selected devices or cameras. When you have typed in the relevant credentials, click the **Verify** button to add the device to your system.

Note: Not all devices and cameras need a user name and password. You can add such devices to your system without any need to type in credentials.

Once you have added the number of devices and cameras you want to add, your system sets up storage for you. Storage is the location to which your system saves recordings. By default, your system chooses the location with most available disk space.

Manual

The **Manually specify the hardware to add** method lets you specify details about each hardware device separately. This options is a good choice if you only want to add a few hardware devices, and you know their IP addresses, user names and passwords and so on. Similarly, automated searches on the local network using the **Scan for hardware** option might not work for all cameras, for example cameras using the system's **Universal Driver**. For such cameras, you must add these to the system manually.

Alternatively, choose **Import CSV file...**. This option lets you import data about hardware devices and cameras as comma-separated values (CSV) (see "Add hardware: Import from CSV file - CSV file format and requirements" on page 51) from a file. This is a highly effective method if you set up several similar systems.

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

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

Overview and names

Information, driver selection and verification

Specify information about each hardware device you want to add:

Name	Description
IP Address	IP address or host name of the hardware device.
Port	Port number on which to scan. The default is port 80. If a hardware device is located behind a NAT-enabled router or a firewall, you may need to specify a different port number. When this is the case, also remember to configure the router/firewall so it maps the port and IP address used by the hardware device.
User Name	User name for the hardware device's administrator account. Many organizations use the hardware device manufacturer's default user names for their hardware devices. If that is the case in your organization, select <default> (do not type a manufacturer's default user name as this can be a source of error—trust that your system knows the manufacturer's default user name). You can also select other typical user names, such as admin or root, from the list. Type a new user name if you want a user name which is not on the list.
Password	Password required to access the administrator account. Some hardware devices do not require user name/password for access.
Driver	The driver to scan for for your hardware device. By default, the wizard shows the Autodetect option. The Autodetect option finds the relevant driver automatically. Select a manufacturer if you know the specific manufacturer to reduce scanning time.

Once you have added the number of devices and cameras you want to add, your system sets up storage for you. Storage is the location to which your system saves recordings. By default, your system chooses the location with most available disk space.

Import from CSV file

Import data about hardware devices and cameras as comma-separated values (CSV) from a file. This is a highly effective method if you set up several similar systems.

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

The following is an example of a CSV file for use when cameras and server are online. It includes the parameters **HardwareAddress, HardwarePort, HardwareUsername, HardwarePassword** and **HardwareDriverID.** Note that HardwareUserName and HardwareDriverID are optional parameters.

You can leave out the HardwareUsername if you have not changed the default HardwareUsername for the device. HardwareDriverID is an optional field. If empty, it is automatically set to autodetect.

```
HardwareAddress;HardwarePort;HardwareUsername;HardwarePassword;HardwareDriverID;
192.168.200.220;80;root;pass;128;
192.168.200.221;80;user;password;165;
192.168.200.222;80;r00t;pass;172;
192.168.200.223;80;;p4ss;
192.168.200.224;80;usEr;pASs;
```

Add hardware: Import from CSV file - CSV file format and requirements

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

Name	Description
HardwareAddress	IP address of the hardware device.
HardwareUsername	User name for hardware device's administrator account.
HardwarePassword	Password for hardware device's administrator account.
HardwareDeviceName	Name of the hardware device. Name must unique, and must not contain any of the following special characters: **< > & ' " ¥ / : * ? | [ ]**
HardwareDriverID	If cameras and server are offline—specify a **HardwareDriverID** for each hardware device you want to add. Example: **ACTi ACD-2100 105** indicates that you should use **105** as the ID if adding an ACTi ACD-2100 hardware device.

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

The following applies for the information present in CSV files:

- The first line of the CSV file must contain the headers, and following 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.

Configure storage wizard

The **Video storage** step helps you quickly configure your cameras' video and recording properties.

Steps in this wizard:

Configure storage: Video settings and preview

Video settings let you control bandwidth, brightness, compression, contrast, resolution, rotation, and more. Use the list on 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. Video settings are to a large extent camera-specific, so you must configure these settings individually for each camera.

Click **Open Settings Dialog** to configure the camera's settings in a separate dialog. When you change video settings, they are applied immediately. This means that—for most cameras—you can immediately 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 can typically 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 are included in the video. Note, however, that cameras are separate units which may have separate timing devices, power supplies, etc. Camera time and XProtect system time may therefore not correspond fully, and this may occasionally lead to confusion. As your system time-stamps all frames upon reception, and exact date and time information for each image is already known, Milestone recommends that you set it to **No**.

Tip: For consistent time synchronization, you may automatically synchronize camera and system time through a time server if your camera supports this.

Configure storage: Online schedule

Specify when each camera should be online. An online camera is a camera that transfers video to the server for live viewing and further processing. The fact that a camera is online does not in itself mean that your system records video from the camera (configure recording settings on one of the following pages). By default, cameras you add to your system are automatically online (**Always on**), and you only need to modify their online schedules if you require cameras to be online only at specific times or

events. Note, however, that you can change this default as part of the scheduling options (on page 140).

For each camera, you can initially select between two online schedules:

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

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

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

Name	Description
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
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	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.

Select **pre- and post-recording**, which allows you to store recordings from the time before and after detected motion and/or specified events. Also specify which frame rates to use for each camera.

Name	Description
Pre-recording	You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.
Seconds [of pre-recording]	Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving (see "About archiving" on page 133) times. That can be problematic since pre-recording does not work well during archiving.

Name	Description
Post-recording	You can store recordings from periods following detected motion and/or stop events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.
Seconds [of post-recording]	Specify the number of seconds for which you want to record video from after recording stop conditions (that is motion or stop event) are met. Usually, only some seconds of post-recording is required, but you can specify up to 65535 seconds of post-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long post-recording time, you can potentially run into a scenario where your post-recording time spans scheduled or unscheduled archiving times. That can be problematic since post-recording does not work well during archiving.
Frame Rate	Required average frame rate for video from the camera. Select number of frames, then select the time unit interval (second, minute or hour).
Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

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

Name	Description
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
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	Apply the value from the template to selected cameras.

Live and recording settings MPEG cameras

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

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

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

Name	Description
Live Frame Rate	Required average frame rate for live video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). If the camera supports dual stream and dual stream is enabled, the **Live Frame Rate** column will be read-only with the value **Dual streaming—**which cannot be altered.
Record on	Select under which conditions video from the camera should be recorded: • **Always:** Record whenever the camera is enabled (see "General" on page 93) and scheduled to be online (see "Online period" on page 142) (the latter allows for time-based recording). • **Never**: Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera. • **Motion Detection**: Select this to record video in which motion (see "Motion detection & exclude regions" on page 102) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected. • **Event**: Select this to record video when an event occurs and until another event occurs. Use of recording on event requires that events have been defined, and that you select start and stop events. **Tip:** If you have not yet defined any suitable events, you can quickly do it: use the **Configure events** list, located below the other fields. • **Motion Detection and Event**: Select this to record video in which motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.
Pre-recording	You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.

Name	Description
Seconds [of pre-recording]	Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving (see "About archiving" on page 133) times. That can be problematic since pre-recording does not work well during archiving.
Post-recording	You can store recordings from periods following detected motion and/or stop events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.
Seconds [of post-recording]	Specify the number of seconds for which you want to record video from after recording stop conditions (that is motion or stop event) are met. Usually, only some seconds of post-recording is required, but you can specify up to 65535 seconds of post-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long post-recording time, you can potentially run into a scenario where your post-recording time spans scheduled or unscheduled archiving times. That can be problematic since post-recording does not work well during archiving.
Keyframe Only	If you want motion detection to take place only on keyframes of the video stream to reduce the system resources used on motion detection, select **Keyframe only**.

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

Name	Description
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
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	Apply the value from the template to selected cameras.

Drive selection

Specify which drives you want to store cameras' recordings on. You can specify separate drives/paths for recording and archiving (see "About archiving" on page 133).

Name	Description
Drive	Letter representing the drive in question, for example C:.
Purpose	Select what you want to use the drive for: **Not in use:** Do not use the drive. **Recording:** Only available if the drive is a local drive on the Milestone Husky server. Network drives cannot be used for recording. Use the drive for storing recordings in the regular database for Milestone Husky. **Archiving:** Use the drive for archiving. For archiving, it is generally a good idea to use a drive which has plenty of space. With dynamic path selection for archives (see description in the following), you do not have to worry about drive space. **Rec. & Archiving:** Only available if the drive is a local drive on the Milestone Husky server. Network drives cannot be used for recording. Use the drive for storing recordings in the regular database for Milestone Husky as well as for archiving.
Recording Path	Path to the folder in which the camera's database should be stored. Default is C:¥MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to a folder on a **local** drive. You cannot specify a path to a network drive. If you use a network drive, it is not be possible to save recordings if the network drive becomes unavailable. If you change the recording path, and you have existing recordings at the old location, you are asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them. **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.
Archiving Path	Only editable if not using dynamic paths for archiving (see "About archiving" on page 133). 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 relevant cell. If you change the archiving path, and there are existing archived recordings at the old location, you are asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if you move archived recordings, Milestone Husky will also archive what is currently in the camera database. In case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.
Total Size	Total size of the drive.
Free Space	Amount of unused space left on the drive.

Name	Description
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 Milestone Husky database is on one of the drives you have selected for archiving, Milestone Husky will always try to archive to that drive first. If not, Milestone Husky 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 Times	Specify when you want Milestone Husky to automatically move recordings to your archiving path(s). You can specify up to 24 archiving times per day, with minimum one hour between each one. Select the hour, minute and second values and click the **up** and **down** buttons to increase or decrease values, or simply overwrite the selected value, and then click **Add**. The more you expect to record, the more often you should archive.
Network Drive	Lets you add a network drive to the list of drives. First specify the network drive, then click **Add** (the button becomes available when you specify a network drive) . Note that network drives cannot be used for recording, only for archiving.

Recording and archiving settings

Select recording and archiving (see "About archiving" on page 133) paths for each individual camera.

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

Name	Description
Recording Path	Path to the folder in which the camera's database should be stored. Default is C:¥MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to a folder on a **local** drive. You cannot specify a path to a network drive. If you use a network drive, it is not be possible to save recordings if the network drive becomes unavailable. If you change the recording path, and you have existing recordings at the old location, you are asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them. **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.

Name	Description
Archiving Path	Only editable if not using dynamic paths for archiving (see "About archiving" on page 133). 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 relevant cell. If you change the archiving path, and there are existing archived recordings at the old location, you are asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if you move archived recordings, Milestone Husky will also archive what is currently in the camera database. In case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.
Retention time	Total amount of time for which you want to keep recordings from the camera (that is, recordings in the camera's database as well as any archived recordings). Default is 7 days. Retention time covers the **total** amount of time you want to keep recordings for.

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

Name	Description
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
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	Apply the value from the template to selected cameras.

Adjust motion detection wizard

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

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, Milestone recommends that you stop (see "Start and stop services" on page 178) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 206).

Steps in this wizard:

Exclude regions

Exclude regions lets 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 cannot connect to the surveillance server and the Management Application at the same time. Milestone recommends that you stop (see "Start and stop services" on page 178) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 206).

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

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

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

Motion Detection

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

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

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Milestone recommends that you stop (see "Start and stop services" on page 178) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 206).

You can configure motion detection settings for each camera, or for several cameras at once. Use the list in the left pane of the wizard window to select cameras. To select several cameras at a time, press

CTRL or SHIFT while you select. When you select a camera, you see a preview from that camera. If you select several cameras, you see a preview from the last camera you select. A green area in the preview indicates motion.

Name	Description
Sensitivity	Adjust the **Sensitivity** slider so that irrelevant background noise is filtered out, and only real motion is shown in green. Alternatively, specify a value between 0 and 256 in the field next to the slider to control the sensitivity setting. The slider determines how much each pixel must change before it is regarded as motion. With a high sensitivity, very little change in a pixel is required before it is regarded as motion. The more you drag the slider to the left, the more of the preview becomes green. This is because with high sensitivity, even the slightest pixel change is regarded as motion.
Motion	Adjust the **Motion** slider so that motion detection is only triggered by the required level of motion. The selected motion level is indicated by the black vertical line in the **Level** bar above the sliders. The black vertical line serves as a threshold. When motion is above (to the right of) the selected level, the bar changes color from green to red, indicating a positive motion detection. Alternatively, specify a value between 0 and 10000 in the field on the left to control the motion setting. The more you drag the slider to the left, the more positive motion detections you see because less change will be needed to trigger a positive motion detection. The number of positive motion detections may also affect the amount of video you record, the amount of notifications you receive, etc.
Detection interval	Specify how often motion detection analysis is carried out on video from the camera. The default is every 240 milliseconds (close to once a quarter of a second). The interval is applied regardless of your cameras' frame rate settings. Adjusting this setting can help lower the amount of system resources used on motion detection.
Detection resolution	Specify whether the full image or a selected percentage of the image should be analyzed. For example, by specifying 25%, every fourth pixel is analyzed instead of all pixels, reducing the system resources used but also offering less accurate motion detection.

Name	Description
Keyframe Only	If you want motion detection to take place only on keyframes of the video stream to reduce the system resources used on motion detection, select **Keyframe only**.

Manage user access wizard

Use the **Manage user access step** to add individual users so they can access the system and its clients. The access summary at the end of the wizard lists the cameras your users have access to.

Important: When you use the wizard, all users you add get access to all cameras, including any new cameras added at a later stage. You can, however, specify access settings, users and user rights (see "Configure user and group rights" on page 173) separately, see Configure server access (on page 166). You cannot add users to groups (see "Add user groups" on page 173).

Steps in this wizard:

Basic and Windows users

You can add client users in two ways. You can combine these if you need to.

Name	Description
Basic user	Create a dedicated surveillance system user account with basic user name and password authentication for each individual user.
Windows user	Import users defined locally on the server, or users from Active Directory, and authenticate them based on their Windows login.

Note: You must define users as local PC users on the server and disable simple file sharing on the server.

Add Basic users

1. Specify a user name and password, and click the **Add Basic User** button. Repeat as required.

Add Windows users

1. Click **Add Windows User...** to open the **Select Users or Groups** dialog. You can only make selections from the local computer, even if you click the **Locations...** button.
2. In **Enter the object names to select,** enter the user name(s), then use the **Check Names** feature to verify the user name. If you enter several user names, separate each name with a semicolon. Example: **Brian; Hannah; Karen; Wayne.**
3. When done, click **OK**.

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

Access summary

The access summary lists which cameras your users have access to. When you use the wizard, all users you have added have access all to cameras, including any new cameras added at a later stage. You can, however, limit individual users' access to cameras by changing their individual rights (see "Configure user and group rights" on page 173).

Advanced configuration

Hardware devices

About hardware devices

You add cameras and other hardware devices, such as video encoders, to your Milestone Husky system through the **Add Hardware Devices...** wizard (see "Add hardware wizard" on page 47). If microphones or speakers are attached to a hardware device, they are automatically added as well (if your XProtect version supports this).

About microphones

In your system, **Microphones** are typically attached to hardware devices, and therefore physically located next to cameras. Operators, with the necessary rights, can then listen to recordings through the XProtect Smart Client (provided the computer running the XProtect Smart Client has speakers attached). You manage microphones in Milestone Husky, meaning you can always manage the microphones attached to cameras, **not** microphones attached to XProtect Smart Client operators' computers.

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

About speakers

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

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

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

About recording audio

Available functionality depends on your product version.

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

- Your system only records incoming audio (from microphones). The system does not record outgoing audio (from speakers).
- Audio recording affects video storage capacity. The system records audio to the associated camera's database. Therefore, it is important to bear in mind that the database is likely to become full earlier if you record audio and video than if you only record video. The fact that the database becomes full is not in itself a problem since Milestone Husky automatically archives (see "About archiving" on page 133) data if the database becomes full. However, you may need additional archiving space if you record audio.
    - Example: If you use MPEG4, each one-second video GOP (Group Of Pictures) are stored in one record in the database. Each second of audio is stored in one record in the database. This reduces the database's video storage capacity to half its capacity, because half of the database's records is used for storing audio. Consequently, the database runs full sooner, and automatic archiving takes place more often than if you were only recording video.
    - Example: If you use MJPEG, audio is stored in one record for every JPEG for as long as the audio block size does not exceed the time between the JPEGs. In extreme cases, this reduces the database's video storage capacity to half its capacity, because half of the database's records is used for storing audio. If you use very high frame rates, which means less time between each JPEG, a smaller portion of the database is used for storing audio records, and consequently a larger portion is available for storing video. The result is that the database runs full sooner, and automatic archiving takes place more often than if you were only recording video.

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

About dedicated input/output devices

You can add a number of dedicated input/output (I/O) hardware devices to your system. For information about which I/O hardware devices your system supports, see the release notes.

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

With certain I/O hardware devices, the surveillance system must regularly check the state of the hardware devices' input ports to detect whether input has been received. Such state checking at regular intervals is called **polling**. The interval between state checks, called a **polling frequency**, is specified as part of the general ports and polling properties (see "Ports and polling" on page 123). 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.

Show or hide microphones or speakers

Available functionality depends on your product version.

If you have added more microphones or speakers to your system than you need, you can hide the ones you do not need by right-clicking the relevant microphone or speaker and select **Hide**. If you

need the hidden microphone/speaker again, you can right-click the overall microphone or speaker icon and select **Show Hidden Items**.

Configure hardware devices

Once you have added hardware devices (see "Add hardware wizard" on page 47), you can specify/edit device-specific properties, such as the IP address, which video channels to use, which COM ports to use for controlling attached PTZ (pan-tilt-zoom) cameras, whether to use 360° lens technology, etc.

1. In the Management Application's navigation pane, expand **Advanced Configuration**, expand **Hardware Devices**, right-click the relevant hardware device, and select **Properties**.
2. Specify Name and video channels, Network, device type and license (see "Network, device type, and license" on page 70), PTZ device (on page 71), and 360° lens (see "Fisheye" on page 105) properties as required.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Delete hardware devices

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

1. In the Management Application's navigation pane, expand **Advanced Configuration**, expand **Hardware Devices**, right-click the hardware device you want to delete, and select **Delete Hardware device**.
2. Confirm that you want to delete the hardware device and all its recordings.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.
4. Restart (see "Start and stop services" on page 178) the Recording Server service.

Alternately, you can also consider disabling the individual cameras, speakers or microphones connected to the hardware device:

1. In the Management Application's navigation pane, expand **Advanced Configuration**, expand **Hardware Devices**, and expand the relevant hardware device.
2. Right-click the camera, microphone or speaker that you want to disable, and select **Disable**.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.
4. Restart (see "Start and stop services" on page 178) the Recording Server service.

About replacing hardware devices

If you need to, you can replace a hardware device that you have added and configured on your system with a new one, for example to replace a physical camera on your network.

Open the Replace Hardware Device wizard (on page 67), which helps you through the entire replacement process on the surveillance system server, including:

- Detecting the new hardware device
- Specifying license for the new hardware device
- Deciding what to do with existing recordings from the old hardware device

Replace Hardware Device wizard

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

The wizard is divided into these pages:

- New hardware device information (on page 67)
- Database action (see "Camera and database action" on page 68)

New hardware device information

Specify details about the new hardware device:

Name	Description
IP Address	IP address or host name of the hardware device.
Port	Port number on which to scan. The default is port 80. If a hardware device is located behind a NAT-enabled router or a firewall, you may need to specify a different port number. When this is the case, also remember to configure the router/firewall so it maps the port and IP address used by the hardware device.
User Name	User name for the hardware device's administrator account. Many organizations use the hardware device manufacturer's default user names for their hardware devices. If that is the case in your organization, select <default> (do not type a manufacturer's default user name as this can be a source of error—trust that your system knows the manufacturer's default user name). You can also select other typical user names, such as admin or root, from the list. Type a new user name if you want a user name which is not on the list.
Password	Password required to access the administrator account. Some hardware devices do not require user name/password for access.

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

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

  - or -

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

When the right driver is found, the **Serial number (MAC address)** field displays the MAC address of the new hardware device. When done, click **Next**.

Camera and database action

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

The table in the left side of the wizard page lists available video channels on the new hardware device. For a regular single-camera hardware device, there are only one video channel. For video encoders, there are typically 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 inherit camera names, recordings databases as well as any archives from the old hardware device. Databases and archives (see "About archiving" on page 133) are renamed to reflect the new hardware device's MAC address and video channels. The rights (see "Configure user and group rights" on page 173) of users with access to the inherited cameras are automatically updated so they can view both old and new recordings. Users do not notice the hardware device replacement since camera names remain the same.

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

3. If the new hardware device has fewer video channels than the old hardware device, it is not possible for the new hardware device to inherit all cameras from the old hardware device. When that is the case, you are 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 are deleted. It is not

possible to view recordings from before the hardware replacement. New databases are, of course, 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 are not deleted. Even though the old databases still exist on the Milestone Husky server, it is not possible to view recordings from before the hardware replacement. Should you later want to delete the old databases, you must delete this manually. New databases will, of course, be created for future recordings by the new hardware devices.

4. Click **Finish**.

   When you are ready, restart (see "Start and stop services" on page 178) the Recording Server service. The hardware replacement are not evident in clients until you restart the Recording Server service.

Speaker properties

When you configure video and recording (see "About video and recording configuration" on page 71) for specific cameras, you can determine when to record audio. Your choice applies for all cameras on your Milestone Husky system.

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

Hardware properties

Hardware name and video channels

When you configure hardware devices (on page 66), specify the following properties:

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

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

Network, device type, and license

When you configure hardware devices (on page 66), specify the following properties:

Name	Description
IP 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 port is port 21. To use the default port, select **Use default FTP port**.
User name	Only relevant when you have selected **Server requires login**. Specify the user name required for using the SMTP server.
User Name	User name for the hardware device's administrator account. Many organizations use the hardware device manufacturer's default user names for their hardware devices. If that is the case in your organization, select <default> (do not type a manufacturer's default user name as this can be a source of error—trust that your system knows the manufacturer's default user name). You can also select other typical user names, such as admin or root, from the list. Type a new user name if you want a user name which is not on the list.
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 "Replace Hardware Device wizard" on page 67), with which you can replace the selected hardware device with another one if you need to. This can be relevant if you replace a physical camera on your network. The wizard helps you take all relevant issues into account: for example, deciding what to do with recordings from cameras attached to the old hardware device, etc.

PTZ device

The PTZ Device tab is only available if you configure (see "Configure hardware devices" on page 66) video encoder hardware devices on which the use of PTZ (pan-tilt-zoom) cameras is possible:

Name	Description
Connected cameras have Pan-tilt-zoom capabilities	Select the checkbox 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 a COM port, select the relevant option. Options are device-specific, depending on which PTZ protocols the device uses. Select None if you have no PTZ cameras controlled through COM ports.

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

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

Cameras and storage information

About video and recording configuration

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

Name	Description
Wizard-driven	Guided configuration where you can specify video, recording and archiving settings for all your cameras.

General	Specify video, recording and shared settings (such as dynamic archiving paths and whether to record audio or not) for all your cameras.
Camera-specific	Specify video, recording and camera-specific settings (such as event notification, PTZ preset positions and fisheye view areas) for each individual camera.

About database resizing

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

- If archives (see "About archiving" on page 133) are present on the same drive as the camera's database, the oldest archive for all cameras archived on that drive is moved to another drive (moving archives is only possible if you use dynamic archiving (see "Dynamic path selection" on page 79), 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 is reduced by deleting a percentage of their oldest recordings, temporarily limiting the size of all databases.

When the Recording Server service (see "About services" on page 177) is restarted upon such database resizing, the original database sizes are used. Therefore, you should make sure to solve the drive size problem. Should the database resizing procedure take place, you are informed on-screen in XProtect Smart Client, in log files, and, if set up, through notifications.

About motion detection settings

Motion detection settings are linked to the Recording properties (see "Recording" on page 97) settings for the camera. Motion detection is enabled as default. Disabling it will improve CPU and RAM performance of your Milestone Husky system, but will—depending on your system settings—also affect your motion detection, event and alarm management. In the following two tables, you can see the differences between enabling (table 1) and disabling (table 2) built-in motion detection for a camera.

Enabled motion detection

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

Disabled motion detection

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

About motion detection and PTZ cameras

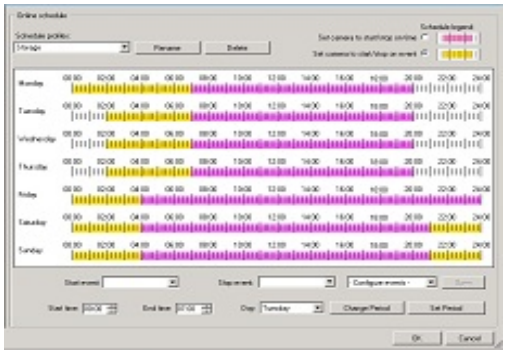
Motion detection generally works the same way for PTZ (pan-tilt-zoom) cameras as it does for regular cameras. However, you cannot configure motion detection separately for each of a PTZ camera's preset positions.

- In order to activate unwanted recordings, notifications and more, the system automatically disables motion detection while a PTZ camera moves between two preset positions. After a number of seconds, the transition time, specified as part of the PTZ camera's PTZ patrolling properties (see "PTZ patrolling" on page 109), the system automatically enables motion detection again.

Configure camera-specific schedules

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

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



The fact that a camera transfers video to Milestone Husky does not necessarily mean that video from the camera is recorded. Recording is configured separately, see Configure video and recording (see "About video and recording configuration" on page 71).

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

Online periods

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

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

Speedup

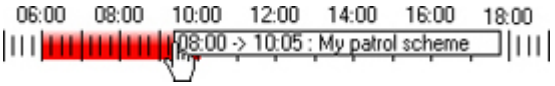
- Periods of time (example: Mondays from 08.30 until 17.45), shown in olive green:

E-mail notification

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

PTZ patrolling

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



SMS notification

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

Set up a profile

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

   Tip: You can combine the two, so you may return to this step in order to toggle between the two options.
4. In the calendar section, place your mouse pointer at a required start point, then hold down the left mouse button, drag the mouse pointer and release at the required end point.
   - You specify each day separately.

- You specify time in increments of five minutes. Milestone Husky helps you by showing the time over which your mouse pointer is positioned.

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

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

Configure when cameras should do what

Available functionality depends on your product version.

Use the scheduling feature to configure when:

- Cameras should be online (that is transfer video to Milestone Husky)
- Cameras should use speedup (that is use a higher than normal frame rate)
- You want to receive email and/or SMS notifications regarding cameras
- PTZ cameras should patrol, and according to which patrolling profile
- Archiving should take place

See Configure general scheduling and archiving (on page 138) and Configure camera-specific schedules (on page 73).

Configure motion detection

To configure motion detection, do the following:

1. In the Management Application navigation pane, expand **Advanced Configuration**, expand **Cameras and Storage Information**, right-click the relevant camera, and select **Properties**.
2. In the **Camera Properties** window, select the **Recording Properties** tab, and select the relevant settings (see "About motion detection settings" on page 72).
3. Select the **Motion Detection** tab. If there are any areas to exclude from motion detection (for example, if the camera covers an area where a tree is swaying in the wind), you can exclude that area (see "Exclude regions" on page 60) by selecting it with your mouse.

4. Fill in the relevant properties (see "Motion detection & exclude regions" on page 102). Note that there are some differences in motion-detection behavior for PTZ cameras (see "About motion detection and PTZ cameras" on page 73).

Disable or delete cameras

All cameras are enabled by default. This means that video from the cameras can be transferred to your system if the cameras are scheduled to be online (see "Online period" on page 142).

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 **Save** in the yellow notification bar in the upper-right corner of the Management Application.

To **delete** a camera, you have to delete the hardware device (see "Delete hardware devices" on page 66). If you delete the hardware device, you also delete any attached microphones or speakers. If you do not want this, consider disabling the camera instead.

Move PTZ type 1 and 3 to required positions

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

1. Click the required position in the camera preview (if supported by the camera).

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

3. Use the navigation buttons:


Moves the PTZ camera up and to the left


Moves the PTZ camera up


Moves the PTZ camera up and to the right


Moves the PTZ camera to the left


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

 Moves the PTZ camera to the right

 Moves the PTZ camera down and to the left

 Moves the PTZ camera down

 Moves the PTZ camera down and to the right

 Zooms out (one zoom level per click)

 Zooms in (one zoom level per click)

Recording and storage properties

Recording and archiving paths

When you configure video and recording (see "About video and recording configuration" on page 71), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

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

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

Name	Description
Shortcut	Users of the Smart Client can take advantage of keyboard shortcuts, some of which let the users toggle between viewing different cameras. Such shortcuts include numbers which are used to identify each camera. Shortcut numbers must be unique for each camera. A camera shortcut number must not contain any letters or special characters, and must not be longer than eight digits. Examples of correct camera shortcut numbers: 3, 12345678. Examples of incorrect camera shortcut numbers: Cam#3, 123456789. More information about using the keyboard shortcuts is available in the separate documentation for the Smart Client.
Recording Path	Path to the folder in which the camera's database should be stored. Default is C:¥MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to a folder on a **local** drive. You cannot specify a path to a network drive. If you use a network drive, it is not be possible to save recordings if the network drive becomes unavailable. If you change the recording path, and you have existing recordings at the old location, you are asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them. **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.
Archiving Path	Only editable if not using dynamic paths for archiving (see "About archiving" on page 133). 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 relevant cell. If you change the archiving path, and there are existing archived recordings at the old location, you are asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if you move archived recordings, Milestone Husky will also archive what is currently in the camera database. In case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.
Retention time	Total amount of time for which you want to keep recordings from the camera (that is, recordings in the camera's database as well as any archived recordings). Default is 7 days. Retention time covers the **total** amount of time you want to keep recordings for.

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

Dynamic path selection

When you configure video and recording (see "About video and recording configuration" on page 71), you can specify certain properties for many cameras in one go. In the case of Dynamic Path Selection, this is because the properties are shared by all cameras.

With dynamic archiving (see "About archiving" on page 133) paths, you specify a number of different archiving paths, usually across several drives. If the path containing the Milestone Husky database is on one of the drives you have selected for archiving, Milestone Husky always tries to archive to that drive first. If not, Milestone Husky automatically archives to the archiving drive with the most available space at any time, provided there is not a camera database using that drive. Which drive has the most available space may change during the archiving process, and archiving may therefore happen to several archiving drives during the same process. This fact will have no impact on how users find and view archived recordings.

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

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

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

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

Video recording

When you configure video and recording (see "About video and recording configuration" on page 71), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

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

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the Video Recording properties can also be specified individually for each camera (see "Recording" on page 97).

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

Name	Description
Record on	Select under which conditions video from the camera should be recorded: • **Always:** Record whenever the camera is enabled (see "General" on page 93) and scheduled to be online (see "Online period" on page 142) (the latter allows for time-based recording). • **Never**: Never record. Live video will be displayed, but—since no video is kept in the database—users will not be able to play back video from the camera. • **Motion Detection**: Select this to record video in which motion (see "Motion detection & exclude regions" on page 102) is detected. Unless post-recording (see the following) is used, recording will stop immediately after the last motion is detected. • **Event**: Select this to record video when an event occurs and until another event occurs. Use of recording on event requires that events have been defined, and that you select start and stop events. **Tip:** If you have not yet defined any suitable events, you can quickly do it: use the **Configure events** list, located below the other fields. • **Motion Detection and Event**: Select this to record video in which motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.
Start Event	Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).
Stop Event	Select required stop event. Recording will end when the stop event occurs (or later if using post-recording; see the following).
Pre-recording	You can store recordings from periods preceding detected motion and/or start events. Select check box to enable this feature. Specify the required number of seconds in the neighboring column.
Seconds [of pre-recording]	Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met. Usually, only some seconds of pre-recording is required, but you can specify up to 65535 seconds of pre-recording, corresponding to 18 hours, 12 minutes and 15 seconds. However, if specifying a very long pre-recording time, you can potentially run into a scenario where your pre-recording time spans scheduled or unscheduled archiving (see "About archiving" on page 133) times. That can be problematic since pre-recording does not work well during archiving.

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

If the camera uses the MJPEG video format

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

Note that there are three places where you can set frame rate:

- Live Frame Rate - used for the regular recording stream
- Live Frame Rate - used when speeding up recordings in connection with motion detection or similar functionality.
- FPS (Frames per second) - used for the additional stream used for live viewing.

Regular frame rate mode:

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

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

Speedup frame rate mode:

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

Name	Description
Recording Frame Rate	Required average frame rate for recorded video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

Tip: Speedup does not necessarily have to be based on motion- or events, you can also use scheduling (see "Speedup" on page 142) to configure speedup based on particular periods of time. If you prefer such time-based speedup, you should still enable the use of speedup by selecting the **Enable speedup** check box.

Dual stream:

This feature is only available on cameras supporting dual stream.

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

If the camera uses the MPEG video format

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

Name	Description
Frame rate per second	Frame rate for viewing live and recorded video from the camera. Select number of frames per second.
Record keyframes only	Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change. This helps greatly reducing the size of MPEG files. Select the check box if you only want to record keyframes. Note that you can specify exceptions if motion is detected or events occur.
Record all frames on motion	Allows you to make exceptions if you have selected to record keyframes only. Select this check box to record all frames when motion is detected. Two seconds after the last motion **is detected**, the camera will return to recording keyframes only**.**

Name	Description
Record all frames on event	Allows you to make exceptions if you have selected to record keyframes only. Select this check box to record all frames when an event occurs and until another event occurs. Use of this feature requires that events have been defined, and that you select start and stop events in the neighboring lists. **Tip:** If you have not yet defined any suitable events, you can quickly do it: use the **Configure events** list, located below the other fields.
Start Event	**Use when recording on Event or Motion Detection & Event.** Select required start event. The camera will begin recording all frames when the start event occurs.
Stop Event	Select required stop event. The camera will again only recording keyframes when the stop event occurs.

Dual stream:

This feature is only available on cameras supporting dual stream.

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

Manual recording

When you configure video and recording (see "About video and recording configuration" on page 71), you can specify certain properties for many cameras in one go. In the case of Manual recording, it is because the properties are shared by all cameras.

When manual recording is enabled, Smart Client users with the necessary rights (see "Configure user and group rights" on page 173) can manually start recording if they see something of interest while viewing live video from a camera which is not already recording.

If enabled, manual recording can take place even if recording for individual cameras (see "Recording" on page 97) is set to **Never** or **Conditionally**.

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

Name	Description
Enable manual recording	Select check box to enable manual recording and specify further details.
Default duration of manual recording	Period of time (in seconds) during which user-driven recording 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 Milestone Husky through an API or similar, and in such cases specifying a maximum duration may be relevant. If you are simply using manual recording in connection with the Smart Client, disregard this property.

Frame rate - MJPEG

When you configure video and recording (see "About video and recording configuration" on page 71), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

All properties on a white background are editable, properties on a light blue background cannot be edited. Note that all of the Frame rate - MJPEG properties can also be specified individually for each camera (see "Recording" on page 97) using MJPEG.

Template and common properties

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras. **Tip:** To select more than one value press CTRL while selecting.
Set all template values on selected cameras	Apply all values from the template to selected cameras.

Name	Description
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " ¥ / : * ? | [ ]**

Regular frame rate properties

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

Speedup frame rate properties

Name	Description
Enable Speedup	The speedup feature lets you use a higher than normal frame rate if motion is detected and/or an event occurs. When you enable speedup, further columns for specifying speedup details become available.
Frame Rate	Speedup frame rate for viewing video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

Name	Description
Time Unit	Select required unit for live and recording frame rates (per second, minute, or hour). Note that you can only select time bases that let you speed up frame rates. Example: If you have specified 15 frames per **second** in normal mode, you cannot specify 16 frames per **minute** or **hour** in speedup mode.
Speedup On	• **Motion Detection**: Select this to speed up when motion (see "Motion detection & exclude regions" on page 102) is detected. Normal frame rates will be resumed immediately after the last motion **is detected.** • **Event:** Select this to speed up when an event occurs and until another event occurs. Use of speedup on event requires that events have been defined, and that you select start and stop events in the neighboring columns. **Tip:** If you have not yet defined any suitable events, you can quickly do it: use the **Configure events** list, located below the other fields. • **Motion Detection & Event:** Select this to speed up when motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns.
Schedule Only	Select this to speed up according to the camera's speedup schedule (see "Speedup" on page 142) 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.

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

Frame Rate - MPEG

When you configure video and recording (see "About video and recording configuration" on page 71), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

Note that you can also specify all of the Frame Rate - MPEG properties individually for each camera (see "Recording" on page 97) using MPEG.

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " ¥ / : * ? | [ ]**
Dual Stream	Allows you to check if dual streaming is enabled on the camera(s). Note that the information is read-only. For cameras that support dual streaming, this can be enabled/disabled as part of individual cameras' Video (on page 94) properties.
Live FPS	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.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.

Name	Description
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras. **Tip:** To select more than one value press CTRL while selecting.
Set all template values on selected cameras	Apply all values from the template to selected cameras.
Record Keyframe Only	Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change; this helps greatly reduce the size of MPEG files. Select the check box if you only want to record keyframes.
Record All Frames on	Allows you to make exceptions if you have selected to record keyframes only. • **Motion Detection**: Select this to record all frames when motion is detected. Two seconds after the last motion (see "Motion detection & exclude regions" on page 102) is detected, the camera will return to recording keyframes only**.** • **Event**: Select this to record all frames when an event occurs and until another event occurs. Requires that events have been defined, and that you select start and stop events in the neighboring columns. **Tip:** If you have not yet defined any suitable events, you can quickly do it: use the **Configure events** list, located below the other fields. • **Motion Detection & Event**: Select this to record all frames when motion is detected, or when an event occurs and until another event occurs. Remember to select start and stop events in the neighboring columns. • **Schedule only**: Select this to record all frames according to the camera's speedup schedule (see "Speedup" on page 142) only.
Start Event	**Use when recording on Event or Motion Detection & Event.** Select required start event. The camera will begin recording all frames when the start event occurs.
Stop Event	Select required stop event. The camera will again only recording keyframes when the stop event occurs.

Audio recording

When you configure video and recording (see "About video and recording configuration" on page 71) for specific cameras, you can determine whether audio should be recorded or not. Your choice applies for all cameras on your Milestone Husky system.

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

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

- Audio recording affects video storage capacity: Audio is recorded to the associated camera's database. Therefore, it is important to bear in mind that the database is likely to become full earlier if you record audio and video than if you only record video. The fact that the database becomes full is not in itself a problem since Milestone Husky automatically archives (see "About archiving" on page 133) data if the database becomes full. However, you may need additional archiving space if you record audio.
    - Example: If you use MPEG4, each one-second video GOP (Group Of Pictures) are stored in one record in the database. Each second of audio will also be stored in one record in the database. This reduces the database's video storage capacity to half its capacity, because half of the database's records is used for storing audio. Consequently, the database runs full sooner, and automatic archiving takes place more often than if you were only recording video.
    - Example: If you use MJPEG, audio is stored in one record for every JPEG for as long as the audio block size does not exceed the time between the JPEGs. In extreme cases, this reduces the database's video storage capacity to half its capacity, because half of the database's records is used for storing audio. If you use very high frame rates, which means less time between each JPEG, a smaller portion of the database is used for storing audio records, and consequently a larger portion is available for storing video. The result is that the database runs full sooner, and automatic archiving takes place more often than if you were only recording video.

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

Audio selection

When you configure video and recording (see "About video and recording configuration" on page 71), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras. With a default microphone and/or speaker selected for a camera, audio from the microphone and/or speaker is automatically used when you view video from the camera. Note that all of the properties can also be specified individually for each camera.

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

Name	Description
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " ¥ / : * ? | [ ]**
Default Microphone	Select a default microphone. **Tip:** Note that you can select microphones attached to another hardware device than the selected camera.
Camera	Click the **Open** button to configure detailed and/or camera-specific settings (such as event notification, PTZ preset positions, and fisheye view areas) for the selected camera.
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras. **Tip:** To select more than one value press CTRL while selecting.
Set all template values on selected cameras	Apply all values from the template to selected cameras.
Default Speaker	Select a default speaker.

Storage information

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

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

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

Camera properties

General

When you configure video and recording (see "About video and recording configuration" on page 71) for specific cameras, properties include:

Name	Description
Enabled	Cameras are by default enabled, meaning that provided they are scheduled to be online (see "Online period" on page 142) and that they can to transfer video to Milestone Husky. You can disable an individual camera, in which case no video/audio is transferred from the camera source to your system.
Preview	Select this check box to show a preview of your camera's video. If you clear the check box, your system does not show a preview for your camera.
Camera Name	The name as it appears in the Management Application as well as in clients. You can overwrite the existing name with a new one. Names must be unique, and must not contain any of these special characters: **< > & ' " ¥ / : * ? | [ ]**
Camera shortcut number	Users of XProtect 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 XProtect Smart Client.

Note: 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 you can access the selected camera, 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, and more by overwriting existing values of selecting new ones. When you adjust video settings, you can—for most cameras—preview the effect of your settings in an image below the fields.

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

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

Video

When you configure video and recording (see "About video and recording configuration" on page 71) for specific cameras, properties include:

If the camera uses MJPEG video format

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

Note that there are three places where you can set frame rate:

- Live Frame Rate - used for the regular recording stream
- Live Frame Rate - used when speeding up recordings in connection with motion detection or similar functionality.
- FPS (Frames per second) - used for the additional stream used for live viewing.

Regular frame rate mode:

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

Speedup frame rate mode:

Name	Description
Enable speedup frame rate	The speedup feature lets you use a higher than normal frame rate if motion is detected and/or an event occurs. When you enable speedup, further columns for specifying speedup details become available.
Frame Rate	Speedup frame rate for viewing video from the camera. Select number of frames, then select the time unit interval (second, minute or hour). The frame rate must be higher than the frame rate specified under normal mode.

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

Tip: Speedup does not necessarily have to be based on motion- or events, you can also use scheduling (see "Speedup" on page 142) to configure speedup based on particular periods of time. If you prefer such time-based speedup, you should still enable the use of speedup by selecting the **Enable speedup** check box.

Dual stream:

This feature is only available on cameras supporting dual stream.

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

If the camera uses MPEG video format

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

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

Dual stream:

This feature is only available on cameras supporting dual stream.

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

Audio

When you configure video and recording (see "About video and recording configuration" on page 71) for specific cameras, properties include the possibility of selecting a default microphone and/or speaker for the camera. With a default microphone and/or speaker selected for a camera, audio from the microphone and/or speaker is automatically used when you view video from the camera. If a microphone and/or speaker is attached to the same hardware device as the camera, that particular microphone and/or speaker is the camera's default microphone and/or speaker if you do not select otherwise.

Available in all XProtect software versions:

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

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

Recording

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

When you configure video and recording (see "About video and recording configuration" on page 71) for specific cameras, recording properties include:

Name	Description
Always	Record whenever the camera is enabled (see "General" on page 93) and scheduled to be online (see "Online period" on page 142) (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.

Name	Description
Conditionally	Record when certain conditions are met. When you select this option, specify required conditions (see the following) which enables you to store recordings from periods preceding and following detected motion and/or specified events. Example: If you have defined that video should be stored when a door is opened, being able to see what happened immediately prior to the door being opened may also be important. Say you have specified that video should be stored conditionally on event, with a start event called **Door Opened** and a stop event called **Door Closed**. With three seconds of pre-recording, video is recorded from three seconds before **Door Opened** occurs and until **Door Closed** occurs.
Built-in motion detection	Select this check box to record video in which motion (see "Motion detection & exclude regions" on page 102) 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 have been defined, and that you select start and stop events in the neighboring lists. **Tip:** If you have not yet defined any suitable events, you can quickly do it: use the **Configure events** list, located below the other fields.
Start Event	Select required start event. Recording will begin when the start event occurs (or earlier if using pre-recording; see the following).
Stop Event	Select required stop event. Recording will end when the stop event occurs (or later if using post-recording; see the following).
Enable pre-recording	Available only when the option **Conditional** is selected. Specify the number of seconds for which you want to record video from before recording start conditions (that is motion or start event) are met.
Enable post-recording	Available only when the option **Conditional** is selected. Specify the number of seconds for which you want to record video after recording stop conditions (that is motion end or stop event) are met.

Note that manual recording (on page 85) may be enabled. With manual recording, users of XProtect Smart Client with the necessary rights (see "Configure user and group rights" on page 173) can manually start recording if they see something of interest while viewing live video from a camera which is not already recording. If enabled, manual recording can take place even if recording for individual cameras is set to **Never** or **Conditionally**.

Recording and archiving paths

When you configure video and recording (see "About video and recording configuration" on page 71) for specific cameras, properties include:

Component	Requirement
Recording Path	Path to the folder in which the camera's database should be stored. Default is C:¥MediaDatabase. To browse for another folder, click the browse icon next to the required cell. You can only specify a path to a folder on a **local** drive. You cannot specify a path to a network drive. If you use a network drive, it is not be possible to save recordings if the network drive becomes unavailable. If you change the recording path, and you have existing recordings at the old location, you are asked whether you want to move the recordings to the new location (recommended), leave them at the old location, or delete them. **Tip:** If you have several cameras, and several local drives are available, you can improve performance by distributing individual cameras' databases across several drives.
Delete Database	Click button to delete all recordings in the database for the camera. Archived recordings will not be affected. **IMPORTANT:** Use with caution. All recordings in the database for the camera will be permanently deleted. As a security measure, you are asked to confirm the deletion.
Archiving Path	Only editable if not using dynamic paths for archiving (see "About archiving" on page 133). 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 relevant cell. If you change the archiving path, and there are existing archived recordings at the old location, you are asked whether you want to move the archived recordings to the new location (recommended), leave them at the old location, or delete them. Note that if you move archived recordings, Milestone Husky will also archive what is currently in the camera database. In case you wonder why the camera database is empty just after you have moved archived recordings, this is the reason.
Delete Archives	Click button to delete all archived recordings for the camera. Recordings in the camera's regular database will not be affected. The ability to delete is available regardless of whether you use a single archiving path or dynamic archiving paths. **IMPORTANT:** Use with caution. All archived recordings for the camera are permanently deleted. As a security measure, you are 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 7 days. Retention time covers the **total** amount of time you want to keep recordings for.

Component	Requirement
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. XProtect Smart Client can often repair a corrupt database if it has been archived. When you open the corrupt database in XProtect Smart Client, XProtect Smart Client repairs the database automatically if at all possible. **Tip:** There are several things you can do to prevent (see "About protecting recording databases from corruption" on page 205) that your databases become corrupt in the first place.
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, Milestone Husky always tries to archive to that path first. If not, Milestone Husky 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 79).

Event notification

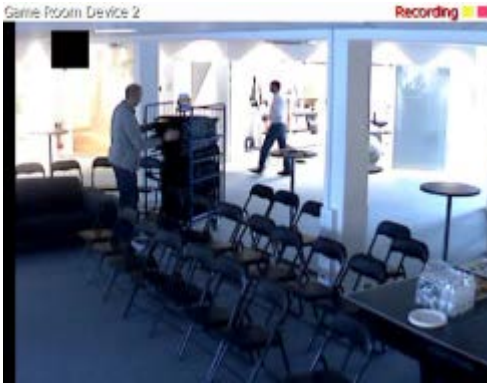
When you configure video and recording (see "About video and recording configuration" on page 71) for specific cameras, properties include event notification:

About event notifications

Event notifications inform XProtect Smart Client users that an event has occurred on your Milestone Husky system. Event notifications can be valuable for client users, as they can quickly detect that an event has occurred. Even though you configure event notifications separately for each camera, you can select between all events on your Milestone Husky system, regardless whether events are manual, generic or originate on another hardware device than the camera itself.

In the XProtect Smart Client, event notification is given by a yellow indicator which lights up when a relevant event has taken place. You can also add an optional sound on event notification in XProtect Smart Client itself.

Three indicators are available for each camera in the XProtect Smart Client:



- The yellow event indicator. Lights up when a relevant event has taken place.
- 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.

You can turn off the bar in which the indicators are displayed in the XProtect Smart Client. Do not turn off if XProtect Smart Client must rely on event notifications.

How to select required events

1. In the **Available events** list, select the relevant event. You can only 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, select the relevant event, and click the **<<** button.

Output

When you configure video and recording (see "About video and recording configuration" on page 71) for specific cameras, you can also associate a camera with particular hardware output (see "Add a hardware output" on page 118), for example the sounding of a siren or the switching on of lights.

Associated output can then be activated automatically when motion is detected in video from the camera, or manually when Smart Client users with the necessary rights (see "Configure user and group rights" on page 173) view live video from the camera.

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

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

   Tip: Even though output is configured separately for each camera, you can select between all output on your Milestone Husky 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 is available for manual activation in the Smart Client.

     - and/or -

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

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

3. Repeat for each required output.

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

Motion detection and exclude regions

When you configure video and recording (see "About video and recording configuration" on page 71) for specific cameras, adjusting motion detection is important because it may determine when video from the camera is recorded, when e-mail notifications are generated, when hardware output (such as lights or sirens) is activated, etc. Time spent on finding the best possible motion detection settings for each camera may help you later avoid unnecessary recordings, notifications, etc. Depending on the physical location of the camera, it may be a very good idea to test motion detection under different physical conditions (day/night, windy/calm weather, etc.).

Before you configure motion detection for a camera, you should configure the camera's video properties (see "General" on page 93), such as compression, resolution, etc.

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, Milestone recommends that you stop (see "Start and stop services" on page 178) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 206).

Name	Description
Enable	Lets you enable or disable (see "About motion detection settings" on page 72) the built-in motion detection.

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

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

Privacy masking

If you need to mask any areas of the camera image from viewing, set the following properties:

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

360° lens

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

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

Name	Description
Enable panomorph support	Select to enable panomorph support. Panomorph is an advanced technology can provide high resolution in zones of interest, while at the same time using fewer pixels than conventional fisheye solutions.
Immervision Enables® panomorph RPL number	When you enable the panomorph support functionality, you must also select a Registered Panomorph Lens (RPL) number from the **ImmerVision Enables® panomorph RPL number** list. This is to ensure that the lens is correctly identified and configured with the lens used with the camera. You can usually find the RPL number on the lens itself or on the box it came in. If you, at some point, want to add additional types of lenses, go to **File** and select **Import new lens types.** Locate the .xml file that contains information about the lens type and press **OK.** For details of ImmerVison, panomorph lenses, and RPLs, see http://www.immervision.com/en/home/index.php**.**
Camera position/orientation	Choose whether the camera is mounted in the ceiling, on a wall or on ground level.
Enable fisheye support	Select to enable fisheye support. Fisheye technology uses a wide-angle lens to capture a hemispherical image, which can then be de-warped through configured fisheye settings (see "Fisheye" on page 105) for the camera in question.
License key	If required, enter your special fisheye license key and click OK, after which you can configure fisheye settings for camera(s) attached to the hardware device.

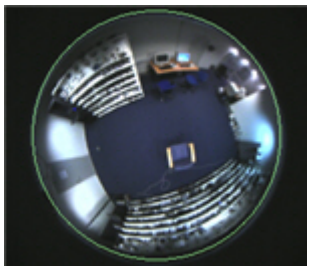
If you are unsure if you need a special fisheye license key, contact your system vendor for further information.

Fisheye

When you configure video and recording (see "About video and recording configuration" on page 71) for specific cameras, fisheye properties may be available. Fisheye is a technology that allows viewing of 360-degree panoramic video through an advanced lens.

You will not see the fisheye properties until certain conditions are met: The camera must be either a dedicated fisheye camera or be equipped with a special fisheye lens. A special fisheye license key is also required. You enter the key when you configure the hardware device (see "Configure hardware devices" on page 66) to which the fisheye camera is attached.

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



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

Button	Description
	Moves the flattened view up

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

PTZ preset positions

Available functionality depends on your product version.

PTZ-related properties are only available when you are dealing with a PTZ (pan-tilt-zoom) camera. You can use PTZ preset positions for making the PTZ camera automatically go to a particular position when particular events occur, and when setting up PTZ patrolling profiles. Preset positions can also be used in clients to allow users that have been given rights (see "Configure user and group rights" on page 173) to move the PTZ camera between preset positions. Names of preset positions must contain only the characters A-Z, a-z and the digits 0-9. If you import preset positions from cameras (see the following), verify that their names do not contain other characters. If they do, change the preset position names before you import them.

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, Milestone recommends that you stop (see "Start and stop services" on page 178) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 206).

Name	Description
PTZ type	Your configuration options depend on the type of PTZ camera in question: • Type 1 (stored on server): You define preset positions by moving the camera using the controls (see "Move PTZ type 1 and 3 to required positions" on page 76) in the upper half of the window, then storing each required position on the Milestone Husky server. You can define up to 260 preset positions this way. • Type 2 (imported from camera): You import preset positions which have previously been defined and stored on the PTZ camera itself through the camera's own configuration interface. The number of allowed preset positions depends on the PTZ camera and driver used. • Type 3 (stored on camera): You define preset positions by moving the camera with the controls (see "Move PTZ type 1 and 3 to required positions" on page 76) in the upper half of the window, then storing each required position in the camera's own memory. You can define up to 260 preset positions this way. If preset positions have already been defined for the camera, you can simply import them for use with Milestone Husky.
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 Milestone Husky. If you have already imported preset positions this way, and preset positions have since then been added or changed on the camera, you can use this button to refresh the imported preset positions.
Add New	Only available when you have selected PTZ type 1. When you have move the camera to a required position using the controls in the upper half of the window, type a name for the position in the blank field, then click the button to add the position to the list of defined preset positions. Remember that names of preset positions must contain only the characters A-Z, a-z and the digits 0-9.
Set New Position	Only available when you have selected PTZ type 1 or 3. Lets you change an already defined preset position. In the list, select the preset position you want to change. Then move the camera to the new required position using the controls in the upper half of the window. Then click the button to overwrite the old position with the new one.

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

PTZ patrolling

PTZ-related properties are only available when you are dealing with a PTZ (pan-tilt-zoom) camera. PTZ patrolling is the continuous movement of a PTZ camera between a number of preset positions (see "PTZ preset positions" on page 107). To use patrolling, you should normally have specified at least two preset positions for the relevant PTZ camera.

To configure PTZ patrolling, select a patrolling profile in the **Patrolling profiles** list and specify relevant properties to define the exact behavior of the patrolling profile. When you have defined your patrolling profiles, remember to schedule (see "PTZ patrolling" on page 143) the use of patrolling profiles. Note that if users manually operate PTZ cameras, this can override patrolling.

Tip: You can specify a patrolling profile with only one preset if needed. Such a patrolling profile can be useful in two cases: For moving a PTZ camera to a specific position at a specific time, and for moving a PTZ camera to a specific position upon manual control of the PTZ camera.

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, Milestone recommends that you stop (see "Start and stop services" on page 178) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 206).

Patrolling profiles

A PTZ camera may patrol according to several different patrolling profiles. For example, a PTZ camera in a supermarket may patrol according to one patrolling profile during opening hours, and according to another patrolling profile when the supermarket is closed.

From the **Patrolling profiles** list, select which patrolling profile to configure.

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

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

- **Delete:** Delete an existing patrolling profile. Note that the selected patrolling profile is removed from the list without further warning.

Note: You can reuse the names of patrolling profiles defined for other cameras. This allows you to use a single patrolling profile name across several PTZ cameras, and can make scheduling (see "PTZ patrolling" on page 143) of PTZ patrolling much easier. Even though several PTZ cameras share a patrolling profile name, the movement between preset positions is individual for each camera.

Preset positions to use in a patrolling profile

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

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

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

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

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

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

Wait and transition timing for a patrolling profile

ame	Description
Wait time (sec.)	Specify the number of seconds for which the PTZ camera should stay at each preset position before it moves on to the next preset position. The default is 10 seconds. The wait time applies to all presets in the patrolling profile. The PTZ camera stays at each preset position for the same number of seconds.

ame	Description
	Specify the number of seconds needed for the PTZ camera to move from one preset position to another. The default is five seconds. During this transition time, motion detection is automatically disabled, as irrelevant motion is otherwise likely to be detected while the camera moves between the preset positions. After the specified number of seconds, motion detection is automatically enabled again.
Transition time (sec.)	The transition time applies to all presets in the patrolling profile. It is important that the camera can switch between any of the patrolling profile's preset positions within the number of seconds you specify. If not, the system is likely to detect false motion. Note that it takes longer for the PTZ camera to move between positions that are located physically far apart (for example from an extreme left position to an extreme right position) than between positions that are located physically close together.

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

PTZ scanning

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

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

Note that PTZ scanning only works for PTZ type 1 cameras (where preset positions are configured and stored on the Milestone Husky server). If the camera is a PTZ type 2 camera, and you import preset positions which have previously been defined and stored on the PTZ camera itself through the camera's own configuration interface, PTZ scanning will stop working. For more information about PTZ types, see PTZ preset positions (on page 107).

Pause PTZ patrolling

PTZ patrolling pauses automatically when users operate the camera manually as well if your system is using PTZ on Event (on page 112). If the system detects motion, it may also pause PTZ patrolling.

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

Pause patrolling if motion is detected

To pause PTZ patrolling when the system detects motion, so that the PTZ camera remains at the position where the system detected motion for a specified period of time, do the following:

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

or

- After a certain number of seconds has passed without further detection of motion

3. Specify the number of seconds for the selected option (default is ten and five seconds respectively).
4. Unless the transition time is set to zero, the system automatically disables motion detection while the camera moves between preset positions, as the system is likely to detect irrelevant motion otherwise while the camera moves between the preset positions.

Resume PTZ patrolling

The system automatically pauses PTZ patrolling when users operate the camera manually as well as if PTZ on Event is in use. You can specify how many seconds should pass before the system resumes regular patrolling after a manual or event-based interruption. The default is 30 seconds.

Apart from manual control, users of XProtect Smart Client can also stop a selected PTZ camera's patrolling entirely. For XProtect Smart Client users, the number of seconds specified in the **Patrolling settings** section therefore only applies when users manually control a PTZ camera and not when users stop a PTZ camera's patrolling entirely. When XProtect Smart Client users stop a PTZ camera's patrolling entirely, the camera's patrolling resumes only when the XProtect Smart Client user selects to resume it.

PTZ on event

PTZ-related properties are only available when you are dealing with a PTZ (pan-tilt-zoom) camera. When a PTZ camera supports preset positions (see "PTZ preset positions" on page 107), you can make the PTZ camera automatically go to a particular preset position when a particular event occurs.

When associating events with preset positions on a PTZ camera, you can select between **all** events defined on your 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 relevant event.
2. In the **PTZ Preset Position** list in the right side of the window, select the relevant preset position. For this purpose, you can only use an event once per PTZ camera. However, use different events for making the PTZ camera go to the same preset position.

   Example:

   - Event 1 makes the PTZ camera go to preset position A
   - Event 2 makes the PTZ camera go to preset position B
   - Event 3 makes the PTZ camera go to preset position A

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

After you have made the PTZ setting changes, restart services (see "Start and stop services" on page 178).

Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, Milestone recommends that you stop (see "Start and stop services" on page 178) the Recording Server service when you configure

such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 206).

Microphones

About microphones

In your system, **Microphones** are typically attached to hardware devices, and therefore physically located next to cameras. Operators, with the necessary rights, can then listen to recordings through the XProtect Smart Client (provided the computer running the XProtect Smart Client has speakers attached). You manage microphones in Milestone Husky, meaning you can always manage the microphones attached to cameras, **not** microphones attached to XProtect Smart Client operators' computers.

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

Configure microphones or speakers

1. In the Management Application's navigation pane, expand **Advanced Configuration**, expand **Hardware Devices**, and expand the hardware device to which the relevant microphone or speaker is attached.
2. Right-click the relevant microphone or speaker, and select **Properties**.
3. Specify properties (see "Speaker properties" on page 69) as required.

Configuration of microphones and speakers in Milestone Husky is very basic. Settings such as volume, etc. are controlled on the microphone or speaker units themselves.

Show or hide microphones or speakers

Available functionality depends on your product version.

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

Microphone (properties)

When you configure video and recording (see "About video and recording configuration" on page 71) for specific cameras, you can determine when audio should be recorded or not. Your choice applies for all cameras on your Milestone Husky system.

Microphone properties

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

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

Recording settings

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

Events and output

About input and output

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

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

Before you specify use of hardware input and hardware output units on a hardware device, verify the hardware device recognized the sensor operatione. Most hardware devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the Milestone Husky release notes to verify that the hardware device and firmware used supports input and output-controlled operations.

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 Milestone Husky. The same goes for hardware output, but hardware output does require some simple configuration in Milestone Husky.

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 118) and Configure hardware output on event (on page 120).

About events and output

Events and output of various types can be used for automatically triggering actions in Milestone Husky. Examples of actions: starting or stopping recording on cameras, switching to a particular video frame rate, triggering notifications, making PTZ cameras move to specific preset positions, etc. Events can also be used for activating hardware output. You can also configure events and output to generate alarms.

Events can be divided in to:

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

Overview of events and output

Types of events:

Name	Description
Analytics events:	Analytics events can be used as alarms and integrated seamlessly with the Alarms feature. Analytics events (see "Overview of events and output" on page 115) are typically data received from external third-party video content analysis (VCA) (see "VCA" on page 214) providers. An example of a VCA-based system could be an access control system.

Name	Description
Hardware input events:	Hardware input, such as door sensors, can be attached to input ports on hardware devices. Input from such external hardware input units can be used for generating events in Milestone Husky. 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, Milestone Husky 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 Milestone Husky detecting motion in video from a camera, based on motion detection settings in Milestone Husky. This type of hardware input events is also called system motion detection events or VMD (Video Motion Detection) events. VMD events are considered a type of hardware input event.
Hardware output:	Hardware output units can be attached to output ports on many hardware devices, allowing you to activate lights, sirens, and more from Milestone Husky. Such hardware output can be activated automatically by events, or manually from clients.
Manual events:	Events may be generated manually by the users selecting them in their clients. These events are called manual events. Manual events can be of the type **Global events** or **Timer events:** Global events apply to all hardware whereas timer events are separate events, triggered by the hardware input event, manual event or generic event under which they are defined. Timer events occur a specified number of seconds or minutes after the event, under which they are defined, has occurred. Timer events may be used for a wide variety of purposes, typically for stopping previously triggered actions. **Example:** A camera starts recording based on a hardware input event, for example when a door is opened. A timer event stops the recording after 15 seconds.
Generic events:	Input may also be received in the form of TCP or UDP data packages, which can be analyzed by Milestone Husky, and—if they match specified criteria—used to generate events. Such events are called generic events.

Name	Description
Output control on event:	Hardware output can be activated automatically when events occur. For example, when a door is opened (hardware input event), lights are switched on (hardware output). When configuring the output control, you can select between all output and events defined in Milestone Husky. You are not limited to selecting output or events defined on particular hardware devices. You can use a single event for activating more than one output.

Before you configure events of any type, **configure general event handling**, such as which ports Milestone Husky should use for event data. Normally, you can just use the default values, but it is a good idea to verify that your organization is not already using the ports for other purposes. See Configure general event handling (on page 121).

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 Milestone Husky 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 Milestone Husky. The same goes for hardware output, but hardware output does require some simple configuration in Milestone Husky.

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 118) and Configure hardware output on event (on page 120).

When you are ready to **configure events**, see Add a hardware input event (on page 117), Add a generic event (on page 119), and Add a manual event (on page 119). If you want to use timer events with your other events, see Add a timer event (on page 120).

Add an analytics event

To add an analytics event, do the following:

1. In the Management Application's navigation pane, expand **Events and Output**, right-click **Analytics Events** and select **Create New**.
2. Specify required properties (see "Analytics event" on page 124).
3. Click **OK**.
4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Add a hardware input event

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

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

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

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

2. In the **Hardware Input Event Properties** window's list of hardware devices, expand the required hardware device to see a list of pre-defined hardware input.

3. Select the required types of input to use them as events. The types of input often vary from camera to camera. If motion detection (see "Motion detection & exclude regions" on page 102) is enabled in Milestone Husky 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.

   Note that some types of input are mutually exclusive. When you select one type of input, you may therefore note that other types of input become unavailable for selection.

4. For each selected type of input, select required properties (see "Hardware input event" on page 126). When ready, click **OK**, or click the **Add button** to add a timer event (on page 120) to the event you have just created.

5. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Add a hardware output

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

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

To add a hardware output event, do the following:

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

2. In the **Hardware Output Properties** window's list of hardware devices, select the required hardware device, and click the **Add** button below the list.

3. Specify required properties (see "Hardware input event" on page 126).

4. Click **OK**.

5. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

For information about how to configure automatic activation of hardware output when events occur, see Configure hardware output on event (on page 120). You configure output for manual activation in

clients as well as for automatic activation on detected motion individually for each camera (see "Output" on page 101).

Add a manual event

With manual events, your users with required rights (see "Configure user and group rights" on page 173) can trigger events manually from their clients. Manual events can be global (shared by all cameras) or tied to a particular camera (only available when the camera is selected). You can use manual events for a wide variety of purposes, for example:

- As start and stop events for use when scheduling cameras' online periods (see "Online period" on page 142). For example, you can make a camera start or stop transferring video to the surveillance system based on a manual event.
- As start and stop events for controlling other camera settings. For example, you can make a camera use a higher frame rate based on a manual event or you can use a manual event for triggering PTZ on event (on page 112).
- For triggering output. Particular output can be associated (see "Configure hardware output on event" on page 120) with manual events.
- For triggering event-based notifications (see "About notifications" on page 151).
- In combinations. For example, a manual event could make a camera start transferring video to the surveillance system while an output is triggered and an e-mail notification is sent to relevant people.

To add a manual event, do the following:

1. In the Management Application navigation pane, expand **Advanced Configuration,** then expand **Events and Output.** Right-click **Manual Events** and select **Add New Manual Event**
2. In the list in the left side of the **Manual Event Properties**, select global or a camera as required.
3. Click the **add** button and specify required properties (see "Hardware input event" on page 126). When ready, click **OK**, or click the **Add** button again to add a timer event (on page 120) to the event you have just created.
4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Add a generic event

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

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

2. In the Generic Event Properties window, click the **Add** button, and specify required properties (see "Generic event" on page 129). When ready, click **OK**, or click the **Add** button to add a timer event to the event you have just created.

3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Add a timer event

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

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

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

To add a timer event, select any event you have previously configured, click the **Add** button, and specify required properties (see "Timer event" on page 128). Your system comes with two simple schedule profiles, **Always on** and **Always off,** which you cannot edit or delete. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. You can reuse a customized schedule profile for more than one purpose if you want to. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

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

Configure hardware output on event

Once you have added hardware output (see "Add a hardware output" on page 118), such as lights, sirens, door openers, etc., you can associate the hardware output with events. This way, particular hardware output can be activated automatically when events occur. Example: When a door is opened (hardware input event), lights are switched on (hardware output).

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

1. In the Management Application's navigation pane, expand **Advanced Configuration,** then expand **Events and Output.** Right-click **Output Control on Event** and select **Properties**.

2. Fill in the relevant properties (see "Output control on event (Events and Output-specific properties)" on page 132).

3. Click **OK**.

4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

You can use a single event for activating more than one output. You cannot delete associations, but you can change your selections or select **None** in both columns as required.

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

Configure general event handling

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

1. In the Management Application's navigation pane, expand **Advanced Configuration**, right-click **Events and Output**, and select **Properties.**
2. Specify required properties (see "Ports and polling" on page 123). Your system comes with two simple schedule profiles, **Always on** and **Always off,** which you cannot edit or delete. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. You can reuse a customized schedule profile for more than one purpose if you want to.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Generate alarms based on analytics events

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

1. Enable the analytics events feature and set up its security. A list of allowed addresses can be used to control who can send event data to the system and on which port the server listens.
2. Create the analytics event, possibly with a description of the event, and test it.
3. Use the analytics event as the source of an alarm definition (see "Alarms definition" on page 190).

As indicated, to use VCA-based events (see "VCA" on page 214), most often a third-party VCA tool is required for supplying data to Milestone Husky. Which VCA tool to use is entirely up to you, as long as the data supplied by the tool adheres to the applied formatting rules described in the Milestone Analytics Events Developers Manual. Contact Milestone for more details.

Test a generic event

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

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

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

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

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

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

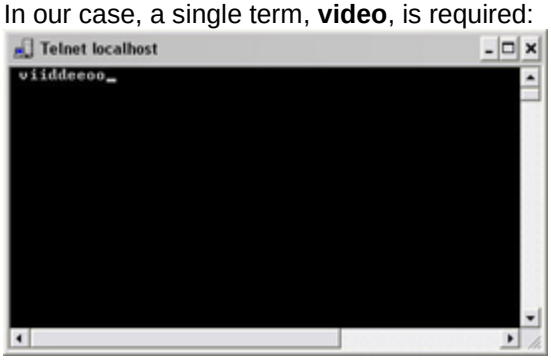
5. In Windows' **Start** menu, select **Run...**, and type the following in the **Open** field:

   - If you are performing the test on the Milestone Husky server itself: `telnet localhost 1234`
   - If you are performing the test from a remote computer: Substitute **localhost** with the IP address of your system's server. Example: If the IP address of the Milestone Husky server is 123.123.123.123, type: `telnet 123.123.123.123 1234`

   This opens a **Telnet** window.

   In the above examples, the number **1234** indicates the port on which the Milestone Husky server listens for generic events. Port 1234 is the default port for this purpose, but you can change this by specifying another port number as part of the general event handling configuration (see "Configure general event handling" on page 121). If you have changed the alert and generic event port number on your system, type your system's alert and generic event port number instead of **1234**.

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



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

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

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

General event properties

Ports and polling

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

Name	Description
Alert and generic event port	Specify port number to use for handling events. Default port is port 1234.
SMTP event port	Specify port number to use for sending event information from hardware devices to Milestone Husky via SMTP. Default port is port 25.
FTP event port	Port to use for FTP communication with the hardware device. Default port is port 21.
Polling interval [1/10] second	For a small number of hardware devices, primarily dedicated input/output devices (see "About dedicated input/output devices" on page 65), it is necessary for Milestone Husky to regularly check the state of the hardware devices' input ports in order to detect input. Such state checking at regular intervals is called polling. You can specify (in tenths of a second) the interval between state checks. Default value is 10 tenths of a second (that is one second). For dedicated input/output devices, it is highly recommended that the polling frequency is set to the lowest possible value (one tenth of a second between state checks). For information about which hardware devices require polling, see the release note.

Events and output properties

Analytics event

When you configure analytics events (see "Add an analytics event" on page 117), specify the following:

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

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

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

Remember to save any changes made during the test.

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

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

Conditions	Description	Error messages and solutions
Send analytics event	Did sending a test event to the Event Server succeed?	See table below.

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

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

Hardware input event

When you add hardware input events (see "Add a hardware input event" on page 117), some properties depend on the selected type of input:

Name	Description
Enable	Select check box to use selected type of input as an event in Milestone Husky, and specify further properties.
Event name	Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " ¥ / : * ? | [ ]** Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Images from camera	Only relevant if using pre- and post-alarm images, a feature available for selected cameras only; it enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. Pre- and post-alarm images should not be confused the pre- and post-recording feature (see "Recording" on page 97) particular to Milestone Husky. Lets you select which camera you want to receive pre- and/or post-alarm images from.
Number of pre-alarm images	Only relevant if using pre-alarm images, a feature available for selected cameras only. Specify required number of pre-alarm images. Allowed number may differ from camera to camera; allowed range is displayed to the right of the field.
Frames per second	Only relevant if using pre-alarm images, a feature available for selected cameras only. Specify required frame rate. Used in combination with the Number of pre-alarm images field, this field indirectly allows you to control how long before the event you want to receive pre-alarm images from.
Send e-mail if this event occurs	Only available if e-mail notification (see "Configure email notifications" on page 152) is enabled. Select if Milestone Husky 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.
Attach image from camera	Only available if e-mail notification (see "Configure email notifications" on page 152) is enabled. Select to include an image, recorded at the time the event is triggered, in the e-mail notification, then select the relevant camera in the list next to the check box.
Delete	Delete a selected event.
Add	When a specific hardware input event is selected, clicking Add adds a timer event (see "Add a timer event" on page 120) to the selected hardware input event.

Name	Description
Send SMS if this event occurs	Only available if SMS notification (see "Configure SMS notifications" on page 154) is enabled. Select if Milestone Husky should automatically send an SMS when the event occurs. Recipients are defined as part of the SMS notification configuration. When using SMS notifications, also bear in mind individual cameras' scheduling.

Hardware output

When you add hardware output (see "Add a hardware output" on page 118), specify the following properties:

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

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

Manual event

When you add manual events (see "Add a manual event" on page 119), specify the following properties:

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

Name	Description
Event name	Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " ¥ / : * ? | [ ]** Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Send e-mail if this event occurs	Only available if e-mail notification (see "Configure email notifications" on page 152) is enabled. Select if Milestone Husky 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.
Attach image from camera	Only available if e-mail notification (see "Configure email notifications" on page 152) is enabled. Select to include an image, recorded at the time the event is triggered, in the e-mail notification, then select the relevant camera in the list next to the check box.
Delete	Delete a selected event.
Add	Add a new event. When **Global** or a specific camera is selected, clicking **Add** adds a new manual event. When a specific manual event is selected, clicking **Add** adds a timer event (see "Add a timer event" on page 120) to the selected manual event.
Send SMS if this event occurs	Only available if SMS notification (see "Configure SMS notifications" on page 154) is enabled. Select if Milestone Husky should automatically send an SMS when the event occurs. Recipients are defined as part of the SMS notification configuration. When using SMS notifications, also bear in mind individual cameras' scheduling.

Timer event

When you add timer events (see "Add a timer event" on page 120), specify the following properties:

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

Generic event

When you add generic events (see "Test a generic event" on page 121), specify the following properties:

Name	Description
Event name	Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " ¥ / : * ? | [ ]** Some cameras only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Event port	Read-only field displaying the port number on which Milestone Husky listens for generic events (default is port 1234). The port number can be changed as part of the general event handling configuration (see "Configure general event handling" on page 121).
Event substring	Lets you specify the individual items for which Milestone Husky should look out for when analyzing data packages. Specify one or more terms, then click the Add button to add the specified term(s) to the Event message expression field, the content of which will be used for the actual analysis. Examples: • **Single term:** User001 (when added to the Event message expression field, the term will appear as "User001") • **Several terms as one item:** User001 Door053 Sunday (when added to the Event message expression field, the terms will appear as " User001 Door053 Sunday") When you add several terms as one item (appearing as, for example, " User001 Door053 Sunday" in the Event message expression field), everything between the quotation marks must appear together in the package, in the specified sequence, in order to match your criterion. If the terms must appear in the package, but not necessarily in any exact sequence, add the terms one by one (that is so they will appear as "User001" "Door053" "Sunday" in the Event message expression field). **Tip:** It is OK for TCP and UDP packages used for generic events to contain special characters, such as @, #, +, 嶽~, etc. within the text string to be analyzed.

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

Name	Description
Event priority	The same data package may be analyzed for different events. The ability to assign a priority to each event lets you manage which event should be triggered if a received package matches the criteria for several events. The priority must be specified as a number between 0 (lowest priority) and 1000 (highest priority). When Milestone Husky receives a TCP and/or UDP package, analysis of the packet will start with analysis for the event with the highest priority. This way, when a package matches the criteria for several events, only the event with the highest priority will be triggered. If a package matches the criteria for several events with an identical priority, for example two events with a priority of 999, all events with the priority in question will be triggered.
Event protocol	Select which protocol Milestone Husky should listen for in order to detect the event: • **Any:** Listen for, and analyze, packages using TCP as well as UDP protocol. • **TCP:** Listen for, and analyze, packages using TCP protocol only. • **UDP:** Listen for, and analyze, packages using UDP protocol only.
Event rule type	Select how particular Milestone Husky should be when analyzing received data packages: • **Search:** In order for the event to occur, the received package must contain the message specified in the Event message expression field, but may also have more content. Example: If you have specified that the received package should contain the terms "User001" and "Door053", the event will be triggered if the received package contains the terms "User001" and "Door053" and "Sunday" since your two required terms are contained in the received package. • **Match:** In order for the event to occur, the received package must contain exactly the message specified in the Event message expression field, and nothing else.
Send e-mail if this event occurs	Only available if e-mail notification (see "Configure email notifications" on page 152) is enabled. Select if Milestone Husky 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.
Attach image from camera	Only available if e-mail notification (see "Configure email notifications" on page 152) is enabled. Select to include an image, recorded at the time the event is triggered, in the e-mail notification, then select the relevant camera in the list next to the check box.

Name	Description
Send SMS if this event occurs	Only available if SMS notification (see "Configure SMS notifications" on page 154) is enabled. Select if Milestone Husky should automatically send an SMS when the event occurs. Recipients are defined as part of the SMS notification configuration. When using SMS notifications, also bear in mind individual cameras' scheduling.
Delete	Delete a selected event.
Add	Add a new event. When the **Generic Events** node is selected, clicking **Add** will add a new generic event. When a specific generic event is selected, clicking **Add** will add a timer event (on page 120) to the selected generic event.

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

When you add output controls on events (see "Configure hardware output on event" on page 120), specify the following properties:

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

Scheduling and archiving

About scheduling

The scheduling feature lets you specify:

- When you want to archive (see "About archiving" on page 133)
- That some cameras transfer video to Milestone Husky at all times
- That some cameras transfer video only within specific periods of time or when specific events occur
- When you want to receive notifications from the system

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

- One or more cameras should be online (that is transfer video to Milestone Husky)
- One of more cameras should use speedup (that is use a higher than normal frame rate)

- You want to receive any notifications (see "About notifications" on page 151) regarding one or more cameras.
- Archiving takes place.
- PTZ cameras should patrol, and according to which patrolling profile

About archiving

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

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

The default settings for Milestone Husky is to perform archiving once a day, or if your database becomes full. You can change the settings for when and how often archiving takes place in the Management Application. You can also schedule archiving (see "About archiving schedules" on page 136) up to 24 times a day, with a minimum of one hour between each one. This way, you can proactively archive recordings, so databases never become full. The more you expect to record, the more often you should archive.

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

Milestone Husky automatically archives recordings if a camera's database becomes full. You only specify **one** time limit (the retention time) as part of the general Recording and Archiving paths (on page 77) properties. Note that retention time determines when archiving takes place. Retention time is the **total** amount of time for which you want to keep recordings from a camera (that is recordings in the camera's database **as well as** any archived recordings).

Backup of archives

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

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

If archiving fails

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

About archiving locations

The default archiving folder (see "Default File Paths" on page 42) (C:¥MediaDatabase) is located on the Milestone Husky server. You can change the default archiving folder to any other location locally, or select a location on a network drive to use as the default archiving folder. In the archiving folder, separate subfolders for storing archives for each camera are automatically created. These subfolders are named after the MAC address of the hardware device to which the camera is connected.

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

The subfolders are named according to the following structure:

```
...¥Archives¥CameraMACAddress_VideoEncoderChannel¥DateAndTime
```

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

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

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

About archiving to other locations

When you archive to other locations than the default archiving directory, your system first temporarily stores the archive in the local default archiving directory, then immediately moves the archive to the archiving location you have specified. Archiving directly to a network drive can mean that archiving time varies depending on the available bandwidth on the network. First storing the archive locally, then moving it speeds up the archiving procedure, and reduces delays in case of network problems.

If you archive to a network drive, the regular camera database can only be stored on a local drive attached directly to your system's server.

About dynamic archive paths

With dynamic archiving paths, you specify a number of different archiving paths, usually across several drives. Milestone recommends using dynamic paths, which also is the default setting when you configure cameras through the Configure video & recording wizard (see "About video and recording configuration" on page 71).

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

The drive that has the most available space may change during the archiving process, and archiving may happen to several archiving drives during the same process. This does not have 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 "Default File Paths" on page 42) 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, Milestone Husky will always try to archive to that drive first. Archiving will take place quickly, but may also fill up the drive with data fairly quickly.

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

  Recordings and archives are on separate drives. Archiving takes place less quickly. Milestone Husky will first temporarily store the archive in the local default archiving directory on C:, then immediately move the archive to the archiving location on D:. Therefore, sufficient space to accommodate the temporary archive is required on C:.

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

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

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

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

About archiving audio

If you have enabled an audio source (for example, a microphone) on a hardware device, audio recordings are archived together with video recordings from the camera attached to the hardware device. If the hardware device is a video encoder with several channels, audio is archived with the camera on channel 1. When you have enabled an audio source, the system records audio to the associated camera’s database. This affects the database’s capacity for storing video. You may, therefore, want to use scheduled archiving more frequently if you record audio and video than if you only record video.

Storage capacity required for archiving

The storage capacity required for archiving depends entirely on the amount of recordings you plan to keep, and on how long you want to keep them (retention time). Some organizations want to keep archived recordings from a large number of cameras for several months or years. Other organizations may only want to archive recordings from one or two cameras, and they may want to keep their archives for much shorter periods of time.

You should always first consider the storage capacity of the **local** drive containing the default archiving directory to which archived recordings are always moved, even though they may immediately after be moved to an archiving location on another drive. Basically, the capacity of the local drive should be at least twice the size required for storing the databases of all cameras.

When you archive, Milestone Husky 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 is deleted until there is sufficient free space for the new data to be archived.

When you estimate storage capacity required for archiving, consider your organization's needs, then plan for worst case rather than best case scenarios.

Tip: The Storage Calculator in the Support section of the Milestone website can help you determine the storage capacity required for your surveillance system.

About archiving schedules

There are two ways in which to configure archiving schedules:

- While you configure your cameras through the Configure Video and Recording wizard (see "Configure storage wizard" on page 52), in which case you configure your archiving schedule on the wizard's **Drive selection** page.
- As part of the general Scheduling and Archiving properties: In the Management Application's navigation pane, expand **Advanced Configuration**, right-click **Scheduling and Archiving**, select **Properties**, select **Archiving** in the dialog, and specify relevant properties (see "Archiving" on page 141).

Automatic response if running out of disk space

If Milestone Husky runs of disk space while archiving, you can set up an automatic response. Two scenarios can occur, depending on whether the camera database drive is different from, or identical to, the archiving drive:

Different drives: Automatic archiving if database drive runs out of disk space

In case the Milestone Husky server is running out of disk space, and the archiving drive is **different from** the camera database drive, and archiving has not taken place within the last hour, archiving will automatically begin in an attempt to free up disk space. This will happen regardless of any archiving schedules. The server is considered to be running out of disk space if:

- there is less than 10% disk space left, and the available disk space goes below 30 GB plus 1.5 GB per camera
- the available disk space goes below 150 MB plus 20 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 350 MB (150 MB plus 20 MB for each of the ten cameras))

The difference ensures that very large disks are not necessarily considered to be running out of disk space just because they have less than 10% disk space left.

On the archiving drive, Milestone Husky 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 relevant camera is deleted until there is sufficient free space for the new data to be archived.

IMPORTANT: You will lose the archive data that is deleted.

Same drive: Automatic moving or deletion of archives if drive runs out of disk space

Available functionality depends on your product version.

If your system server is running out of disk space, and the archiving drive is identical to the camera database drive, your system automatically does the following in an attempt to free up disk space:

1. First, the program will attempt to move archives (moving archives is only possible if you use dynamic archiving, with which you can archive to several different drives). This happens 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 are not necessarily 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, your system attempts to delete the oldest archives. This happens 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 not necessarily are considered to be running out of disk space just because they have less than 10% disk space left.

   IMPORTANT: You lose data from the archives you delete.

3. Ultimately, if there are no archives to delete, your system attempts to resize camera databases by deleting their oldest recordings. This happens if:

   - there is less than 5% disk space left, and the available disk space goes below 20 GB plus 1 GB per camera

   - or -

   - the available disk space goes below 75 MB plus 10 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 175 MB (75 MB plus 10 MB for each of the ten cameras))

   The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 5% disk space left.

   IMPORTANT: You 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.

4. First, your system attempts to delete archives. This happens 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 150 MB plus 20 MB per camera

The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 10% disk space left.

IMPORTANT: You will lose data from the archives being deleted.

5. Ultimately, if there are no archives to delete, Milestone Husky will attempt to resize camera databases. This will happen if:

   - there is less than 5% disk space left, and the available disk space goes below 20 GB plus 1 GB per camera

   - or -

   - the available disk space goes below 75 MB plus 10 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 175 MB (75 MB plus 10 MB for each of the ten cameras))

   The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 5% disk space left.

   IMPORTANT: You lose the data deleted as part of the database resizing process.

When the recording server is restarted after database resizing, the original database sizes are used. Therefore, you should make sure that 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 are informed on-screen in XProtect Smart Client, in log files, and or in notifications (see "About notifications" on page 151) (if set up).

View archived recordings

You can view archived recordings via the Smart Client. Use, for example, all of the Smart Client's advanced features (video browsing, and export) for archived recordings.

Stored archives

Exported archives

Configure general scheduling and archiving

To configure general scheduling and archiving, do the following:

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

2. Specify properties as required for Scheduling all cameras (on page 139), Scheduling options (on page 140), and Archiving (on page 141).

3. Your system comes with two simple schedule profiles, **Always on** and **Always off,** which you cannot edit or delete. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. You can reuse a customized schedule profile for more than one purpose if you want to.

4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

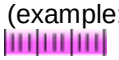
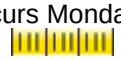
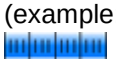
When archiving, disable any virus scanning (on page 24) of camera databases and archiving locations.

General scheduling properties

Scheduling all cameras

When you configure general scheduling and archiving (see "Configure general scheduling and archiving" on page 138), you can specify certain properties for many cameras in one go. Either in order to speed up things, or because the properties in question are shared by all cameras rather than being specific to individual cameras.

Note that you can specify the properties for **Online Period**, **Speedup**, **Notifications (Email and SMS)**, and **PTZ Patrolling** individually for each camera.

Name	Description
Template	The template can help you configure similar properties quickly. Say you have 20 cameras and you want to change the recording path, archiving path, and retention time for all of them. Instead of having to enter the same three pieces of information 20 times, you can simply enter them once in the template, and then apply the template to the 20 cameras with only two clicks.
Apply Template	Select which cameras you want to apply the template for. Use one of the two **Set** buttons to actually apply the template.
Camera	The name as it appears in the Management Application as well as in clients.
Online	Select the required profile (for example **Always on**) for the online schedule (see "Configure camera-specific schedules" on page 73) for the relevant camera(s). You specify a camera's online periods by creating schedule profiles based on: • Periods of time (example: Mondays from 08.30 until 17.45), shown in pink:  • Events within periods of time (example: from Event A occurs until Event B occurs Mondays from 08.30 until 17.45), shown in yellow:  The two options can be combined  , but they cannot overlap in time.
E-mail	Select the required profile for the e-mail notification schedule for the camera(s) in question. You specify a camera's e-mail notification periods by creating schedule profiles based on periods of time (example: Mondays from 08.30 until 17.45), shown in blue: 

Name	Description
Select All	Click button to select all cameras in the **Apply Template** column.
Clear All	Click button to clear all selections in the **Apply Template** column.
Set selected template value on selected cameras	Apply only a selected value from the template to selected cameras. **Tip:** To select more than one value press CTRL while selecting.
New schedule profile	Create a new schedule profile of any type by clicking the **Create...** button.
SMS	Select the required profile for the SMS notification schedule for the camera(s) in question. You specify a camera's SMS notification periods by creating schedule profiles based on periods of time (example: Mondays from 08.30 until 17.45), shown in green: 
PTZ Patrolling	Only available for PTZ (pan-tilt-zoom) cameras with patrolling, the continuous movement of a PTZ camera between a number of preset positions. Lets you select the required profile for the PTZ patrolling schedule (see "PTZ patrolling" on page 143) for the camera(s) in question. You specify a camera's patrolling schedule based on patrolling profiles within particular periods of time (example: Mondays from 08.30 until 17.45), shown in red: 

Scheduling options

When you configure general scheduling and archiving (see "Configure general scheduling and archiving" on page 138), you can specify certain properties for many cameras in one go. In the case of Scheduling Options, it is because the properties are shared by all cameras.

Name	Description
Start cameras on client requests	Cameras may be offline, for example because they have reached the end of an online recording schedule (see "Online period" on page 142), 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	Enable recording on the camera when **Start cameras on client requests** (see the previous) is also selected. If a user does not have access to manual recording (see "Camera access" on page 175), selecting **Enable recording when started on client request**, will **not** enable the user to do manual recording.

Name	Description
Schedule profile for new cameras	Select which online schedule profile to use as default for cameras you subsequently add to your Milestone Husky 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 Milestone Husky server for live viewing and further processing.
Maximum delay between reconnect attempts	Control the aggressiveness of reconnection attempts. If Milestone Husky loses the connection to a camera, it will by default attempt to re-establish the connection after ten seconds. In some environments, for example if using vehicle-mounted cameras through wireless connections, camera connections may frequently be lost, and you may want to change the aggressiveness of such reconnection attempts.

You can view live and even record video from a camera outside its online recording schedule. To do this, you select the **Start cameras on client requests** and, if needed, the **Enable recording when started on client request** options in the following when setting up your scheduling properties for the camera in question.

Archiving

Milestone Husky automatically archives (see "About archiving" on page 133) recordings if a camera's database becomes full.

Name	Description
Archiving Times	Specify when you want Milestone Husky to automatically move recordings to your archiving path(s). You can specify up to 24 archiving times per day, with minimum one hour between each one. Select the hour, minute and second values and click the **up** and **down** buttons to increase or decrease values, or simply overwrite the selected value, and then click **Add**. The more you expect to record, the more often you should archive.
Send e-mail on archiving failure	If selected, Milestone Husky will automatically send an e-mail to selected recipients if archiving fails. This requires that the e-mail notification feature is enabled. Recipients are defined as part of the e-mail notification properties (see "Email (Properties)" on page 152).
Send SMS on archiving failure	If selected, Milestone Husky will automatically send an SMS (mobile phone text message) to selected recipients if archiving fails. This requires that the SMS notification feature is enabled. Recipients are defined as part of the SMS notification properties (see "SMS properties" on page 155).

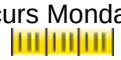
Camera-specific scheduling properties

Online period

When you configure scheduling (see "Configure camera-specific schedules" on page 73) for specific cameras, your **Online Period** settings are probably the most important, since they determine when each camera should transfer video to Milestone Husky.

By default, cameras added to Milestone Husky are automatically online, and you only need to modify the online period settings if you require cameras to be online only at specific times or events. Note, however, that this default may be changed as part of the general scheduling options (see "Scheduling options" on page 140), in which case cameras added at a later time are not automatically online.

The fact that a camera transfers video to Milestone Husky does not necessarily mean that video from the camera is recorded. Recording is configured separately, see Configure video and recording (see "About video and recording configuration" on page 71).

Name	Description
Online	Select the required profile (for example **Always on**) for the online schedule (see "Configure camera-specific schedules" on page 73) for the relevant camera(s). You specify a camera's online periods by creating schedule profiles based on: • Periods of time (example: Mondays from 08.30 until 17.45), shown in pink:  • Events within periods of time (example: from Event A occurs until Event B occurs Mondays from 08.30 until 17.45), shown in yellow:  The two options can be combined  , but they cannot overlap in time.

Tip: If you want to view live video as well as record video from a camera outside its online recording schedule, you can select the Start cameras on client requests (see "Scheduling options" on page 140) and, if needed, the Enable recording when started on client request **(see "Scheduling options" on page 140)** options to set up your scheduling properties for a relevant camera.

Speedup

Speedup may also take place based on events, but that is configured elsewhere. See Frame rate - MJPEG (General recording and storage properties) (see "Frame rate - MJPEG" on page 86) and Video (Camera-specific properties) (see "Video" on page 94).

Name	Description
Speedup	For specific MJPEG cameras, specify speedup periods. Before you can define this type of schedule, you must enable (see "Frame rate - MJPEG" on page 86) speedup. 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: 

PTZ patrolling

When you configure scheduling (see "Configure camera-specific schedules" on page 73) for PTZ (pan-tilt-zoom) cameras capable of patrolling (see "PTZ patrolling" on page 109), you can specify which patrolling profiles to use at specific times. Before you can define this type of schedule, you must configure patrolling for the relevant cameras.

Name	Description
PTZ Patrolling	Only available for PTZ (pan-tilt-zoom) cameras with patrolling, the continuous movement of a PTZ camera between a number of preset positions. Lets you select the required profile for the PTZ patrolling schedule (see "PTZ patrolling" on page 143) for the camera(s) in question. You specify a camera's patrolling schedule based on patrolling profiles within particular periods of time (example: Mondays from 08.30 until 17.45), shown in red: 

Use of one patrolling profile may be followed immediately by use of another (example: use the Daytime patrolling profile Mondays from 08.30 until 17.45, then the Evening patrolling profile Mondays from 17.45 until 23.00). Use of two patrolling profiles cannot overlap.

Unlike other types of scheduling, there are no ready-made **Always on** and **Always off** schedule profiles for PTZ patrolling. You can create any number of customized schedule profiles for each camera. When you create a customized schedule profile (see "Configure camera-specific schedules" on page 73) for one camera, you can reuse it with other cameras if required.

Matrix

About Matrix video sharing

The Matrix feature allows distributed viewing of live video from any camera to any Matrix-recipient on a network operating with Milestone Husky. A computer on which Matrix-triggered video can be viewed is known as a Matrix recipient. In order to become a Matrix recipient, the computer must have the XProtect Smart Client installed.

For more information about Matrix video sharing, refer to the XProtect Smart Client User's Manual, available on the Milestone Husky software DVD as well as from www.milestonesys.com, or the XProtect Smart Client's own built-in help system.

There are two ways in which Matrix-triggered video can appear on a Matrix-recipient:

- **Manual triggering**: Another user wants to share important video, and sends it from XProtect Smart Client—or from a custom-made web page—to the required Matrix-recipient.
- **Automatic triggering**: Video is sent to the relevant Matrix-recipient automatically when a predefined event occurs, for example when a door sensor detects that a door is opened, or when the surveillance system detects motion in the video from a camera.

About Matrix-recipients

A computer on which Matrix-triggered video can be viewed is known as a Matrix-recipient. In order to become a Matrix-recipient, the computer must have the XProtect Smart Client installed.

There are two ways in which Matrix-triggered video can appear on a Matrix-recipient:

- **Manual triggering**: Another user wants to share important video, and sends it from an XProtect Smart Client—or from a custom-made web page—to the required Matrix-recipient.
- **Automatic triggering**: Video is sent to the relevant Matrix-recipient automatically when a predefined event occurs, for example when a door sensor detects that a door is opened, or when the surveillance system detects motion in the video from a camera.
- For more information about Matrix-recipients, refer to the XProtect Smart Client User's Manual, available on the Milestone Husky software DVD as well as from www.milestonesys.com, or the XProtect Smart Client's own built-in help system.

Configure Matrix

1. In the Management Application's Navigation pane, expand **Advanced Configuration**, right-click **Matrix** and select **Properties**.
2. Enable the use of Matrix by selecting the **Enable Matrix** check box.
3. Specify required properties (see "Matrix recipients" on page 144), or, for automatically triggered video sharing, select **Matrix Event Control** and configure Matrix Event Control properties (see "Matrix event control" on page 145). When ready, click **OK.**
4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Matrix properties

Matrix recipients

The **Matrix Recipients** tab is used to enable Matrix functionality and to define which computers to display Matrix-triggered live video. A computer on which Matrix-triggered video can be displayed is known as a Matrix-recipient. Being able to view Matrix-triggered video requires that you have installed XProtect Smart Client on the user's computer.

Name	Description
Enable Matrix	Select check box to enable Matrix functionality.

Name	Description
[List of Defined Matrix recipients]	Lists any already defined Matrix recipients, that is computers on which Matrix-triggered video can be displayed. To change the properties of an already defined Matrix recipient, select the required Matrix recipient, make the changes in the fields below the list, then click the Update button. To remove a Matrix recipient from the list, select the unwanted Matrix recipient, then click the **Delete** button.
Name	Name of the Matrix-recipient. Used when you add a new Matrix-recipient or edit the properties of an existing one. The name appears in various day-to-day usage situations. Therefore, is a good idea to use a descriptive and unambiguous name. Names must be unique, and must not contain any of these special characters: **< > & ' " ¥ / : * ? | [ ]**
Address	IP address of the Matrix recipient, used when adding a new Matrix recipient or editing the properties of an existing one.
Port	Specify the port number to be used when sending commands to the Matrix recipient. Used when adding a new Matrix recipient or editing the properties of an existing one. The Matrix recipient will listen for commands on this port. By default, port 12345 is used; you can of course specify another port number.
Password	Specify the password to be used when communicating with the Matrix recipient. Used when adding a new Matrix recipient or editing the properties of an existing one
Matrix-recipient is an XProtect Smart Client	Select if the relevant Matrix-recipient is an XProtect Smart Client. If you use XProtect Smart Client, distribution of Matrix-triggered live video takes place slightly differently.
Clear	Removes any content in the **Name**, **Address,** and **Password** fields.
Update	Updates the properties of the selected Matrix recipient with the changes made during editing. Available only if you have edited the properties of an existing Matrix recipient.
Add	Adds the new Matrix-recipient to the list. Available only if you have added properties of a new Matrix-recipient in the **Name**, **Address**, **Port**, **Password**, and possibly XProtect Smart Client fields.

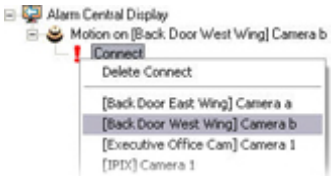
Matrix event control

The **Matrix Event Control** tab is used to configure the automatic sending of live video based on predefined events. You can define exactly which events and cameras to use on a per-Matrix recipient basis. The **Matrix Event Control** tab displays the list of Matrix recipients defined on the **Matrix Recipients** tab.

Right-clicking a Matrix recipient brings up a list of devices with belonging events. When you select an event, it will initially be highlighted by a red exclamation mark, indicating that there is additional configuration to be done. Right-clicking an event brings up a list of options for the selected event:

Component	Requirement
Delete [selected event]	Deletes selected event on the selected device.
Connect	Connects to the camera (actual camera is specified after selecting action to be taken).
Disconnect, then connect	Disconnect any existing connections, then connect again. With this option the live video will appear in the Matrix recipient on a first-in-first-out basis. Each time a new event occurs, video from the latest event is displayed prominently in a specific position on the Matrix recipient, while at the same time video from the older events is shifted to less prominent positions and eventually ”pushed out” of the Matrix recipient in order to make space for the latest event's video. With the **Connect** option, you may experience that if video triggered by one event on a camera is already shown on the Matrix recipient, videos triggered by another event on the same camera will not be displayed prominently as coming from the latest event – simply because the Matrix recipient is already showing video from the camera in a less prominent position. By selecting **Disconnect, then connect** you can avoid this issue, and ensure that video from the latest event is always displayed prominently.
Disconnect	Disconnects any existing connection. Use if a particular event should cause video to stop being displayed in the Matrix-recipient, even if they are not yet old enough to be “pushed out” of the Matrix-recipient.

If you selected **Connect**, another red exclamation mark will indicate that there is still some configuration to be done. Right-click an action to select which camera to apply the action on.



In this example, we have specified that when motion is detected on Camera b, the selected Matrix-recipient should connect to Camera b:

Logs

About logs

Your system can generate various logs:

Log types

Name	Description
Management Application log files	Shows Management Application activity. For every day you use the Management Application, a new log file is created. 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	Shows Recording Server service activity. A new log file is created for each day this 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	Shows Image Server service activity. 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	Shows Image Import service activity, when this service is used for fetching pre-alarm images, and storing the fetched images in camera databases. Pre-alarm images is a feature available for selected cameras only. It enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail. A new log file is created for each day the service is used. You cannot disable this type of logging. Image Import service log files are named according to the structure ImageImportLog_YYYMMDD.log, for example ImageImportLog20091231.log.
Event log files	Shows registered events' activity. 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 XProtect Smart Client (use the **Playback** tab's **Alerts** section).

Name	Description
Audit log files	Shows XProtect Smart Client user activity (if audit logging is enabled). A new log file is created for each day with audit logging enabled and client user activity. Audit log files are named according to the structure is_auditYYYMMDD.log, for example is_audit20091231.log. The _is prefix is due to the fact that the audit log files are generated by the Image Server service.

Log locations

All log files are by default placed in the appropriate **All Users** folder for the operating system you are using. By default, they are stored there for seven days. Note that you can change log file locations as well as the number of days to store the logs when you configure logging.

Log structures

Most log files generated by your system use a shared structure complying with the W3C Extended Log File Format. Each log file consists of a header and a number of log lines:

- The header outlines the information contained in the log lines.
- The log lines consist of two main parts: the log information itself as well as an encrypted part. The encrypted part makes it possible, through decryption and comparison, to assert that a log file has not been tampered with.

Log integrity checks

All log files, except Management Application log files, are subjected to an integrity check once every 24 hours. The integrity check is performed by your system'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 you are using.

Any inconsistencies are reported in the form of error messages written in the log check file. Possible error messages:

Name	Description
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. 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.

Name	Description
Last line changed/removed in [log file name]	The last line of the log file did not match the validation criteria.
Encrypted data missing in [log file name] near line [#]	The encrypted part of the relevant log line 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.

Note: Other messages that are not error-related may also appear in the log check file.

Configure system, event and audit logging

Milestone Husky can generate various logs.

To configure logging, do the following:

1. In the Management Application's Navigation pane, expand **Advanced Configuration**, right-click **Logs** and select **Properties**.
2. Specify properties (see "Log properties" on page 149) for your system logs, including the event log and the audit log. Administrators can only disable/enable audit logging. All other logs are compulsory.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Log properties

Milestone Husky can generate various types of logs. When you configure logs, you can define the following:

Logs (Management Application log, Recording Server service log, Image Server service log, and Image Import service log)

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

Name	Description
Days to log	A new log file is created each day the Management Application and/or the services are used. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day's activity is always logged, even with a value of 0 in the field. Therefore, if you specify 0, you will log current day's activity; if you specify 1, you will keep one day plus the current day's activity, and so on.

Event Log

Name	Description
Path	These log files are by default placed in the appropriate **All Users** folder for the operating system you are using. To specify another location for your log files, type the path to the required folder in the **Path** field, or click the browse button next to the field to browse to the required folder.
Days to log	A new log file is created for each day on which events occur. A log file older than the number of days specified in the field is automatically deleted. By default, the log file will be stored for seven days. To specify another number of days (max. 9999), simply overwrite the value in the field. The current day's activity is always logged, even with a value of 0 in the field. Therefore, if you specify 0, you will log current day's activity; if you specify 1, you will keep one day plus the current day's activity, and so on.

Audit Log

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

Name	Description
Days to log	A new log file is created for each day with audit logging enabled and client user activity. A log file older than the number of days specified in the field is automatically deleted. By default, the log file is stored for seven days. To specify another number of days (max. 9999), 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 keep one day plus the current day's activity. Note that if you specify 0 (zero), audit log files are 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	The 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 reduce the size of the audit log. The default is ten seconds.

Notifications

About notifications

In case of problems with hardware, activation of motion detection on your camera or similar incidents, you can set up your system to send notifications through SMS and/or email.

Email

About email

With email notifications, you can instantly get notified when your surveillance system requires attention. Milestone Husky can automatically send e-mail notifications to one or more recipients when:

- Motion (see "Motion detection & exclude regions" on page 102) is detected
- Events occur. You can select individually for each event whether you want to receive an email notification or not.
- Archiving (see "About archiving" on page 133) fails (if email notification has been selected as part of the archiving properties (see "Archiving" on page 141))

Configure email notifications

To set up email notifications, do the following:

In the Management Application's Navigation pane, expand **Advanced Configuration**, expand **Notifications**, right-click **Email** and select **Properties**.

1. Enable the use of email by selecting the **Enable email** check box.
2. Specify required properties (see "Message Settings (email)" on page 152).
3. Choose a schedule profile to associate with your email notifications. Your system comes with two simple schedule profiles, **Always on** and **Always off,** which you cannot edit or delete. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. You can reuse a customized schedule profile for more than one purpose if you want to.

Email (Properties)

Message Settings (email)

Specify the following message settings for email:

Name	Description
Enable	Select to enable the use of email notifications, allowing you to specify further properties.
Recipient(s)	Specify the email addresses to which the system should send email notifications. To specify more than one e-mail address, separate the e-mail addresses with semicolons (example: aa@aa.aa; bb@bb.bb; cc@cc.cc).
Subject text	Enter a subject text for email notifications.
Message text	Enter a message text for email notifications. Note that camera information as well as date and time information is automatically included in email notifications.
Variables	Click a link to include a variable to the notification. The options are: • Name of triggering event • Camera name • Trigger time (the time when the notification was registered) • Error text (for example, camera failure)
Ignore similar messages for:	Specify the number of seconds to ignore sending similar notifications. This function is to ensure that you do not receive too many notifications before you have solved the relevant problem.

Name	Description
Use schedule profile	Select the schedule profile you want to use. By default, you can choose between **Always On**, **Always Off** or choose **Add new...** to set up a custom schedule (see "Notification Scheduling properties" on page 156).

Attachment Settings (email)

Specify the following attachment settings:

Component	Requirement
Include images	Select the check box to include still images in email notifications. When selected, each email notification includes one or more attached still JPEG images. Attached images includes images of before the incident, after the incident and the actual incident, with the incident that triggered the notification in the middle. **Important:** If your device does not record any images while the sending of notifications are turned on, no images are included in the email notification you receive.
Number of images	The number of images you want to include in the email. You can include between 1 and 20 images.
Time between images (ms)	Minimum time (in milliseconds) to be between each image. You can set any time range between 0 and 300 seconds (5 minutes).
Embed images in email	Select the check box to embed images directly in the email.

Server Settings (email)

Specify the following server settings for email:

Component	Requirement
Sender e-mail address	Enter the email address you wish to use as the sender of the email notification.

Component	Requirement
Outgoing mail server address (SMTP)	Type the name of the SMTP (Simple Mail Transfer Protocol) server which you want to use to send the email notifications. Compared with other mail transfer methods, SMTP has the advantage that you avoid automatically triggered warnings from your email client. Such warnings may otherwise inform you that your email client is trying to automatically send email messages on your behalf. TLS (Transport Layer Security) and its predecessor, SSL (Secure Socket Layer), are supported.
Outgoing mail server port (SMTP)	Type the port for your mail server. The default port number is 25.
Server requires login	Select the check box if you must use a user name and password to use the SMTP server.
Security type	Choose the type of security you want to use.
User name	Only relevant when you have selected **Server requires login**. Specify the user name required for using the SMTP server.
Password	Only relevant if you have selected **Server requires login**. Specify the password required for using the SMTP server.
Max attachment size (MB)	Specify a maximum size of attached images.

SMS

About SMS

With SMS notifications, you can instantly get notified on your mobile device when your surveillance system requires attention. To use the SMS notification feature, you must connect a 3G/USB modem to the server on which you have installed your system.

Your system can automatically send SMS notifications when:

- Motion (see "Motion detection & exclude regions" on page 102) is detected
- Events occur. You can select individually for each event whether you want to receive an SMS notification or not.
- Archiving (see "About archiving" on page 133) fails (if an SMS notification has been selected as part of the archiving properties (see "Archiving" on page 141)).

Configure SMS notifications

To configure SMS notifications, do the following:

1. In the Management Application's Navigation pane, expand **Advanced Configuration**, expand **Notifications**, right-click **SMS** and select **Properties**.

2. Enable the use of SMS by selecting the **Enable SMS** check box.
3. Specify required properties (see "SMS properties" on page 155).
4. Choose a schedule profile to associate with your SMS notifications.

Note: Your system comes with two simple schedule profiles, **Always on** and **Always off,** which you cannot edit or delete. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. You can reuse a customized schedule profile for more than one purpose if you want to.

SMS properties

Message Settings (SMS)

Specify the following message settings for SMS:

Component	Requirement
Enable SMS	Enables the use of SMS notifications, allowing you to specify further properties.
Recipient(s)	Indicate the telephone number of the recipient. To send SMS to more than one recipient, separate the phone numbers with a semicolon.
Message text	Specify required message text for the SMS notification. Message text must only contain the following characters: a-z, A-Z, 0-9 as well as commas (,) and full stops (.). Note that camera information, date and time information are all automatically included in SMS notifications.
Variables	Click a link to include a variable to the notification. The options are: • Name of triggering event • Camera name • Trigger time (the time when the notification was registered) • Error text (for example, camera failure)
Ignore similar messages for:	Specify the number of seconds to ignore sending similar notifications. This function is to ensure that you do not receive too many notifications before you have solved the relevant problem.
Use schedule profile	Select the schedule profile you want to use. By default, you can choose between **Always On**, **Always Off** or choose **Add new...** to set up a custom schedule (see "Notification Scheduling properties" on page 156).

Server Settings (SMS)

Specify the following server settings for SMS:

Component	Requirement
Serial port	Select the serial port to use for your USB/3G modem. The list from which you can choose ports shows open serial ports on the computer running your system.
Speed	The baud speed of your USB modem device. The default value is 9600 baud. Although you can set any custom value for the baud rate, Milestone does not recommend that you change the baud rate unless you are a highly advanced user.
SIM card PIN code	Specify PIN code for the SIM card inserted in the USB/3G modem.
SMS encoding	Different types of SMS encodings exist to accommodate various language needs in the world. Milestone Husky gives you the following options: • 7-bit • 8-bit (default) • 16-bit 7-bit encryption allows you to use up to 160 characters per SMS, however it also limits the type of characters you can use. 8-bit encryption is the standard form of encryption with more special characters allowed. It allows you to use up to 140 characters per SMS. 16-bit encryption is necessary for non-Latin alphabeat languages. Characters from, for example, Arabic, Chinese, Korean, Japanese or Cyrillic alphabet languages require 16-bit SMS encoding. If you use any of these languages in your organization, you must set your Milestone Husky to use 16-bit encoding. 16-bit has a limit of 70 characters per SMS.

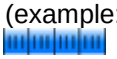
Scheduling

About scheduling of notifications

Scheduling of notifications allows you to set up schedule profiles which you can use with Email (see "Message Settings (email)" on page 152) and SMS (see "Message Settings (SMS)" on page 155) notifications.

Notification Scheduling properties

When you set up schedules to use with email or SMS notifications, specify the following:

Component	Requirement
Notification profile	Select the relevant profile (for example **Always on**) for your notification schedule profile. You specify a notification schedule profile by creating schedule profiles based on: • Periods of time (example: Mondays from 08.30 until 17.45), shown in blue: 

Central

About Central

Central Settings lets you specify the login settings required for an XProtect Central server to access the surveillance system in order to retrieve status information and alarms. If you are a user of the Milestone Integration Platform, this is also the dialog that lets you specify the login settings for the Milestone Integration Platform to access the surveillance system.

Enable XProtect Central

1. In the Management Application's Navigation pane, expand **Advanced Configuration**, right-click Central and then select **Properties**.
2. Enable the use of Central connections by selecting the **Enable Milestone XProtect Central** check box.
3. Specify required properties (see "Central properties" on page 157).
4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Central properties

Name	Description
Enable Milestone XProtect Central connections	Enables the use of Central connections, allowing you to specify further properties.
Login Name	Type the name used for the connection between the Milestone Husky and Central servers or the Milestone Integration Platform. The name must match the name specified on the Central server or in the Milestone Integration Platform.
Password	Type the password used for the connection between Milestone Husky and Central servers or the Milestone Integration Platform. The password must match the password specified on the Central server or in the Milestone Integration Platform.

Name	Description
Port	Type the port number to which the XProtect Central server or the Milestone Integration Platform should connect when accessing the Milestone Husky server. The port number must match the port number specified on the XProtect Central server or in the Milestone Integration Platform. Default port is 1237.

Access control

About access control integration

The use of XProtect Access Control Module 2014 requires that you have purchased a license that allows you to access this feature.

You can use XProtect Access Control Module 2014 with access control systems from vendors that have a vendor-specific plug-in for XProtect Access Control Module 2014.

The access control integration feature introduces new functionality that makes it simple to integrate customers' access control systems with XProtect. You get:

- A common operator user interface for multiple access control systems in the XProtect Smart Client
- Faster and more powerful integration of access control systems
- More functionality (see below)

In the XProtect Smart Client, the operator gets:

- Live monitoring of access control events
- Operator aided passage for access requests
- Map integration
- Alarm definitions for access control events
- Investigation of access control events
- Centralized door state overview and control
- Cardholder information

Apart from a license, you need a vendor-specific integration plug-in installed on the event server before you can start an integration.

Wizard for access control system integration

The **Access control system integration** wizard is for step-by-step configuration of the initial integration with an access control system. Use the wizard to get through the most basic configuration tasks. You can do more detailed configuration afterwards from **Properties**.

Before you start the access control integration wizard make sure you have the integration plug-in installed on the event server.

Some of the fields to fill out and their default values are inherited from the integration plug-in. Therefore the appearance of the wizard may differ depending on the access control system you integrate with.

To start the wizard, select **Access Control** in the node tree, right-click, and click **Create new**.

Steps in this wizard:

Access control system integration

Specify the connection details for the access control system you want to add. The parameters that you must specify depend on the type of system, but are typically the network address of the access control system server and an access control administrator user name and password.

The video management system uses the specified user name and password when you log into the access control system for retrieving configuration.

The integration plug-in may also define secondary parameters which are not listed in the wizard, but you can change these in **General Settings** after setting up the integration. The default values for the parameters are supplied by the plug-in or XProtect.

Connecting to the access control system

When the plug-in has been successfully integrated, a summary of the retrieved access control system configuration appears. Review the list to ensure that all items have been integrated before you continue to the next step of the wizard.

Associate cameras with doors

Configure mappings between access points in the access control system and the cameras in the XProtect system, to show related video for events from the doors.

You can map several cameras to one access point. The primary camera is the camera defined at the top of the list, but the XProtect Smart Client user is able to switch between all cameras when investigating events, for example.

The XProtect Smart Client user is also able to add each of the cameras when configuring **Access Monitor** view items, for example.

Final summary

Your system has been successfully integrated with default settings inherited from the integration plug-in. The access control feature is immediately available for use by operators of the XProtect Smart Client. You can refine the configuration in **Properties**. Press **F1** to launch the help system.

Access control properties

General Settings

Name	Description
Enable	Systems are by default enabled, meaning that they are visible in the XProtect Smart Client and XProtect receives access control events. You can disable a system, for example during maintenance, to avoid creating unnecessary alarms.
Name	The name of the integrated access control system as it appears in the Management Application as well as in XProtect Smart Client. You can overwrite the existing name with a new one.
Integration plug-in	Shows the type of access control system selected during the initial integration.
Last configuration refresh	Shows the date and time of the last time the configuration was imported from the access control system.
Refresh configuration	Click the button when you need to reflect configuration changes made in the access control system in XProtect, for example you have added or deleted a door. A summary of the configuration changes from the access control system appears. Review the list to ensure that your access control system is reflected correctly before you apply the new configuration.

The naming and content of the following fields are imported from the integration plug-in. Below are examples of some typical fields:

Name	Description
Address	Type the address of the server that hosts the integrated access control system.
Port	Specify the port number on the server to which the access control system is connected.
User name	Type the name of the user, as defined in the access control system, who should be administrator of the integrated system in XProtect.
Password	Specify the password for the user.

Associated Cameras

Provides mappings between door access points and cameras, microphones or speakers. Mappings to microphones and speakers are implicit through the related microphone or speaker on the camera. You associate cameras as part of the integration wizard, but you can change the setup at any time.

Name	Description
Doors	Lists the available door access points defined in the access control system, grouped by door. It also shows whether or not a door is licensed and if it has associated cameras.
Cameras	Lists the cameras configured in the XProtect system. Select a camera from the list, and drag and drop it at the relevant access point to associate the access point with the camera. The primary camera is the camera defined at the top of the list.

Access Control Events

Event categories allow you to group events. The configuration of event categories affects the behavior of access control in the XProtect Smart Client and allows you to, for example, define an alarm to handle multiple event types in a single alarm definition.

Name	Description
Access Control Event	Lists the access control events imported from the access control system. The integration plug-in controls default enabling and disabling of events. You can disable or enable events any time after the integration. When an event is enabled, it is stored in the XProtect event database and is, for example, available for filtering in the XProtect Smart Client.
Source Type	Shows the access control unit, for example access point or a server, that an event is sourced from in the access control system.

Event Category	Assign none, one or more event categories to the access control events. The system automatically maps relevant event categories to the events during integration. This enables a default setup in XProtect Smart Client. You can change the mapping at any time. Built-in event categories are: • Access request • Access granted • Access denied • Error Events and event categories defined by the integration plug-in also appear. See also **Edit User-defined Categories** about creating additional event categories.
Edit User-defined Categories	Allows you to create, modify or delete user-defined event categories. You can create event categories when the built-in categories do not meet your requirements, for example, in connection with defining triggering events for access control actions. The categories are global for all integration systems added to the XProtect system. They allow setting up cross-system handling, for example on alarm definitions. If you delete a user-defined event category, you receive a warning if it is used by any integration. If you delete it anyway, all configurations made with this category, for example access control actions, do not work anymore.

Access Control Actions

Actions specify the behavior of the access control system in the XProtect Smart Client, based on the configuration of the triggering events.

You can specify one or more actions related to:

- An event category
- Events from the access control system
- Events from the XProtect system

Triggering events are from a specific access control unit or from a group of access control units.

Name	Description
Trigger Event	Select from the list an event category that should trigger an action. The list includes built-in, plug-in and user-defined event categories. Select **Access control event**, to create a trigger based on specific access control events instead of an event category. Select **External event**, to create a trigger based on an input event in the XProtect system. Specify the input source in the **Source** field for each trigger.
Source	Select the source which the action affects. The options depend on the setting of the **Trigger Event** field. For event categories and access control events, select: • All doors • Individual doors • Other... Click **Other** to select multiple doors, door access points or other units in the access control system. For external event: Select the source from a list of events and input devices in the XProtect system.
Time Profile	Select the time profile in which you want the action to be performed if triggered. Configure time profiles as part of **Advanced Configuration**.
Action	Select the type of action: • Display access request notification • Go to PTZ preset • Start recording • System action For each action, specify action details. To set up multiple actions, click **Add access control action**. You can do this, for example, if you want different actions triggered by the same event depending on weekend vs. office hours.
Add access control action	Click to add and define actions as required.

Action details	Configure the parameters for an action: Display access request notification: o Specify which cameras, microphones or speakers the XProtect Smart Client user connects to via the notification user interface when a given event occurs. Also specify the sound to alert the user when the notification pops up. To enable more commands in the notification, see **Add Command**. Go to PTZ preset: o Specify the camera and select from the pre-configured presets a pattern for the camera and the time of return to preset when a given event occurs. Start recording: o Specify the cameras that should start recording and the duration when a given event occurs. System action: o Specify an action predefined in the XProtect system.
Add command	Select which commands that should be available as buttons in the access request notifications in the XProtect Smart Client. Related access request commands: o Enables all commands related to access request operations available on the source unit. For example **Open door**. All related commands: o Enables all commands on the source unit. Access control command: o Enables a selected access control command. System command: o Enables a command predefined in the XProtect system.

o

Cardholders

If your access control system does not include pictures of the cardholders, you can add and delete pictures in the XProtect system.

If your access control system does not support adding/deleting pictures in the XProtect system, you can use the **Cardholder** pane to review information retrieved from the access control system.

Name	Description
Search cardholder	Type the first few characters of the name of the cardholder, that you look for and it appears in the list, if it exists.
Name	Lists the names of the cardholders retrieved from the access control system.
Type	Lists the type of cardholder, for example: • Employee • Guard • Guest
Select picture	Specify the path to a file with a picture of the cardholder. This button is not visible if the access control system manages the pictures. Allowed file-formats are .bmp, .png, and .jpg. Pictures are resized to maximize the view.
Delete picture	Click to delete the picture.

Server access

About server access

You can configure clients' access to your system's server in two ways:

- **Wizard-driven:** Guided configuration which lets you specify how clients access the server and which users can use clients. See Configure User Access wizard (see "Manage user access wizard" on page 62). When you use the wizard, all users that you add have access to all cameras, including new cameras added at a later stage. If this is not what you want, specify access settings, users and user rights separately.
- **Through advanced configuration:** In previous versions of Milestone Husky, this was known as Image Server administration, since technically it is the Image Server service (see "About services" on page 177) which handles clients' access to the surveillance system.

About registered services

Registered services displays the services installed and running on your Milestone Husky system. It displays the following information about the individual services:

Name	Description
Enabled	Indicates if the relevant service is enabled.

Name	Description
Name	The name of the service.
Description	A description of the service.
Addresses	The inside and outside addresses used by the service.

You can change the inside and outside addresses for a service. To do this, click the **Edit** button and enter the relevant inside and/or outside addresses. Note that you cannot edit all services. You can delete a service registration from the system by clicking the **Delete** button. You are prompted for confirmation before the service is deleted.

Configure server access

1. In the Management Application's navigation pane, expand **Advanced Configuration,** right-click **Server Access** and select **Properties**.
2. Specify required properties for Server Access (on page 166), Local IP Ranges (on page 167), and Language Support and XML Encoding (on page 168). Your system comes with two simple schedule profiles, **Always on** and **Always off,** which you cannot edit or delete. If these do not meet your needs, you can create any number of customized schedule profiles for each camera. You can reuse a customized schedule profile for more than one purpose if you want to.
3. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

When you use this option, you configure client users separately from clients' access. See Add individual users (see "Add basic users" on page 171), Add user groups (on page 173), and Configure user and group rights (on page 173).

Server access properties

Server access

When you configure server access (on page 166) (that is clients' access to the Milestone Husky server), specify the following:

Name	Description
Server name	Name of the Milestone Husky 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.

Name	Description
Enable internet access	Select the check box if the server should be accessible from the internet through a router or firewall. If you select this option, also specify the public (“outside”) IP address and port number in the following fields. When using public access, the router or firewall used must be configured so requests sent to the public IP address and port are forwarded to the local (“inside”) IP address and port of the Milestone Husky server.
Internet address	Lets you specify a public IP address or hostname for use when the Milestone Husky server should be available from the internet.
Internet port	Specify a port number for use when the Milestone Husky should be available from the Internet. The default port number is 80. You can change the port number if needed.
Max. number of clients	You can limit the number of clients allowed to connect at the same time. Depending on your Milestone Husky configuration and the performance of the hardware and network used, limiting the number of simultaneously connected clients may help reduce server load. If more than the allowed number of simultaneously connected clients attempt to log in, only the allowed number of clients will be allowed access. Any clients in excess of the allowed number will receive an error message when attempting to log in. By default, a maximum of ten simultaneously connected clients are allowed. To specify a different maximum number, simply overwrite the value. **Tip:** To allow an unlimited number of simultaneously connected access clients, type **0** (zero) in the **Max. number of clients** field. A four-minute session timeout period applies for client sessions on Milestone Husky. In many cases, client users may not notice this at all. However, the session timeout period will be very evident if you set the Max. number of clients value to 1. When that is the case, and the single allowed client user logs out, four minutes must pass before it will be possible to log in again.

Local IP ranges

You can specify IP address ranges which Milestone Husky 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 range.
3. In the **End Address** column, specify the last IP address in the range.
4. Repeat if you want to add other local IP address ranges.

Tip: If required, an IP address range can include only one IP address (example: 192.168.10.1-192.168.10.1).

Language support and XML encoding

You can select the language/character set that should be used by your system's server and clients.

Component	Requirement
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. If you are using a master/slave setup, remember to specify the same language/character set on all relevant servers.

Master/Slave

About master and slave

You can create a master/slave setup of your system servers. A master/slave setup allows remote users to transparently connect to more than one server at the same time. When remote users connect to the master server, they instantly get access to the slave servers as well.

You can designate an unlimited number of servers per SLC (Software License Code) as master servers. If you need to, for example if your organization is very large and spread over many geographical locations, or in case your organization wants to create a redundancy solution, you can use several master servers in a master/slave setup. You can use up to four servers as slave servers under a designated master server that uses the same SLC.

Configure master and slave servers

Configure a master/slave setup

In the Management Application 's Navigation pane, expand **Advanced Configuration**, right-click **Master/Slave** and select **Properties**.

1. Select the **Enable as master server** check box.
2. Click **Add** to add a slave server.
3. Specify slave server properties. When ready, click **OK.**
4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Add a slave server

To add a slave server, expand **Advanced Configuration** in the Management Application, right-click **Master/Slave** and select **Add New Slave Server**, then specify slave server properties. You can also add slave servers from the **Master/Slave Properties** window by clicking **Add.**

Tip: Instead of specifying a host name when adding a slave server, you can specify the IP address of the slave server. Type in the IP address in the **Address** field when you add the slave server. Remember you must use the local IP address of the slave server if you are on a local network.

Before you start using your master/slave setup, remember to verify that:

- Required users have be defined on the master server as well as on each of the slave servers.
- Public Access (see "Configure server access" on page 166) has been enabled on all involved servers, and ports mapped accordingly in the routers or firewalls used, if the slave servers are to be accessed from the internet.

When you use a master/slave setup, remote users and their rights must be defined in the Management Application's **Users** section on the master server as well as on each of the slave servers. Only cameras to which a remote user has been given access will be visible to the user, regardless of whether the cameras are connected to the master server or to one of the slave servers. If they are to be accessed from the internet, you must enable **Public Access** on all involved servers, and map ports accordingly in the routers and/or firewalls used.

Frequently asked questions about using master/slave

- **How many master servers can I use in a master/slave setup?**

  You can designate an unlimited number of servers per SLC (Software License Code, specified during installation) as master servers. If required—for example if your organization is very large and spread over many geographical locations, or in case your organization wants to create a redundancy solution—this allows you to use several master servers in a master/slave setup.

- **How many slave servers can I use in a master/slave setup?**

  You can define Up to four servers as slave servers under a designated master server using the same Software License Code.

- **How do I switch around which server is master and which server is slave?**

  If you want a slave server to become a master server, simply clear **Enable as master server** on the original master server and click OK. In the Management Application's navigation pane, right-click the slave server which you want to become master server, and select **Properties**. Then select **Enable as master server**. Next, click **Add to add slave servers** to the new master server.

- **How do I ensure that I am actually connected to my slaves?**

  You can verify the connection to your slaves by clicking Update Status and let the system report the number of connected slaves back to you.

Event Server installation in a master/slave setup

To run a master/slave setup, choose a **Typical** installation on the master server and **Custom** installation, where you do not install the Event Server service, on the slave server(s). This is because there can only be one Event Server service in a master/slave setup. If you install more than one Event Server service, the master server may experience problems with accessing cameras on slave servers.

However, if you have an Event Server installed on the master server and no Event Server installed on slave servers, you can create alarms that triggers when events occur on the slave. If you cannot see

an event from the slave server when you create an alarm and enter the source in the Management Application, this may be because you need to be a user on the slave server with administrator access before you can see the events on the slave server.

The slave server does not recognize a locally defined Windows user created on the Windows server, and an event from the slave server is not be available for creating alarms. You must add domain users to both the master server and the slave server with administrator access. This allows you to see the events on the slave server and create alarms. If you are set up as a basic user on both the master server and slave server, with administrator rights on both, you can see events on the slave server and create alarms when you log in to the master server with this user ID.

By default, the Management Application does not prompt you for a login, but does log you in with the Windows user ID with which you have logged in to Windows. If you want to log in to the Management Application as a basic user, you must therefore do the following: Start the Management Application and go to **File** > **Log Out**. This opens a login dialog where you can use your basic user ID to log in.

Master/slave properties

If you have several Milestone Husky servers, you can create a master/slave setup. A master/slave setup allows users to connect to more than one server at the same time. When users connect to the master server, they instantly get access to the slave servers as well.

Master server properties

Name	Description
Enable as master server	Select to enable as master server.
Timeout	Set timeout of slave update. See **Update Status on Slaves** further below.
Add	Lets you add slave servers. Select **Master Server** in the list and click the **Add** button.

When you select **Master Server**, the **Delete** button is disabled and the **Add** button is enabled (provided you have selected **Enabled as master server**). This allows you to add slave servers to the master server, but prevents your from deleting the master server.

Slave server properties

Name	Description
Address	IP address of the slave server.
Port	Port number of the slave server.
Delete	Remove a slave server from the list of slave servers. Select the slave server in the list and click the **Delete** button.

If you want a slave server to become a master server, clear **Enable as master server** on the original master server and click **OK**. In the Management Application's navigation pane, right-click the slave

server which you want to become master server and select **Properties**. Then select **Enable as master server.** Next click **Add** to add slave servers to the new master server.

Update status on slaves

In the **Master Settings Summary** and **Slave Settings Summary** table area, you can verify/update added slaves by clicking **Update Status**. A status dialog runs and afterwards informs you of the status of your slave server(s).

If you select **Pre version 8.0 slaves**, it is not possible to update slave status on any slaves and **Update Status** is therefore disabled. In the **Slave Settings Summary** table, slave status on all slaves is **Not applicable**.
If you do **not** select **Pre version 8.0 slaves**, slave status for pre version 8.0 slaves is **Unreachable.** Slave status for 8.0 slaves and beyond reflects the actual status.

Users

About users

The term **users** primarily refers to users who connect to the surveillance system through their clients. You can configure such users in two ways:

- As **basic users**, authenticated by a user name/password combination.
- As **Windows users**, authenticated based on their Windows login

You can add both types of users through the Configure User Access wizard (see "Manage user access wizard" on page 62) or individually (see Add basic users (on page 171) and Add Windows users (on page 172)).

By grouping users, you can specify rights (see "Configure user and group rights" on page 173) for all users within a group in one go. If you have many users performing similar tasks, this can save you significant amounts of work. User groups are logical groups created and used for practical purposes in the Management Application only. They are not in any way connected with user groups from central directory services. If you want to use groups, make sure you add groups (see "Add user groups" on page 173) before you add users: you cannot add existing users to groups.

Finally, the Administrators group is also listed under Users. This is a default Windows user group for administration purpose which automatically has access to the Management Application.

Add basic users

When you add a basic user, you create a dedicated surveillance system user account with basic user name and password authentication for the individual user. Note that creating Windows users provides better security. If you want to include users in groups, make sure you add required groups (see "Add user groups" on page 173) before you add users: you cannot add existing users to groups.

You can add basic users in two ways: One is through the Configure User Access wizard (see "Manage user access wizard" on page 62). Alternatively, add Windows users this way:

1. In the Management Application's navigation pane, expand **Advanced Configuration**, right-click **Users**, and select **Add New Basic User**.
2. Specify a user name. Names must be unique, and must not contain any of these special characters: **< > & ' " ¥ / : * ? | [ ]**

   Specify a password, and repeat it to be sure you have specified it correctly.
3. Click **OK**.
4. Specify General Access (on page 174) and Camera Access (on page 175) properties. These properties determine the rights of the user.
5. Click **OK**.
6. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Add Windows users

When you add Windows users, you import users defined locally on the server and authenticate them based on their Windows login. This generally provides better security than the basic user concept, and it is the method Milestone recommends. If you want to include users in groups, make sure you add required groups (see "Add user groups" on page 173) before you add users. You cannot add existing users to groups.

Add Windows users in two ways: One is through the Manage user access wizard (on page 62). Alternatively, add Windows users this way:

1. In the Management Application's navigation pane, expand **Advanced Configuration**, right-click **Users**, and select **Add New Windows User**. This opens the **Select Users or Groups** dialog.

   Note that you can only make selections from the local computer, even if you click the Locations... button.
2. In the **Enter the object names to select** box, type the relevant user name(s), then use the **Check Names** feature to verify it. If you type several user names, separate each name with a semicolon. Example: **Brian; Hannah; Karen; Wayne.**
3. When done, click **OK**.
4. Specify General Access (on page 174) and Camera Access (on page 175) properties. These properties will determine the rights of the user.
5. Click **OK**.
6. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Users added from a **local database** logging in with a client should not specify any server name, PC name, or IP address as part of the user name. Example of a correctly specified user name: USER001. Example of an incorrectly specified user name: PC001/USER001. The user should still specify a password and any required server information.

Add user groups

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

By grouping users, you can specify rights (see "Configure user and group rights" on page 173) for all users within a group in one go. If you have many users performing similar tasks, this can save you significant amounts of work.

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

1. In the Management Application's navigation pane, expand **Advanced Configuration**, right-click **Users**, and select **Add New User Group**.
2. Specify a name. Names must be unique, and must not contain any of these special characters: **< > & ' " ¥ / : * ? | [ ]**
3. Click **OK**.
4. Specify General access (on page 174) and Camera access (on page 175) properties. These properties will determine the rights of the group's future members.
5. Click **OK**.
6. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.
7. Now you can add users to the group: in the navigation pane, right-click the group you just created, and Add basic users **(on page 171) or** Add Windows users (on page 172) as required.

Configure user and group rights

User/group rights are configured during the process of adding users/groups, see Add basic Users (on page 171), Add Windows users (on page 172) and Add user groups (on page 173). Note that you can also add basic and Windows users through the Manage user access wizard (on page 62). However, when using the wizard all users you add will have access all to cameras, including any new cameras added at a later stage.

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

1. In the Management Application's navigation pane, expand **Advanced Configuration**, expand **Users**, right-click the required user or group, and select **Properties**.
2. Edit General Access (on page 174) and Camera Access (on page 175) properties. These properties determine the rights of the user/group.
3. Click **OK**.
4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

User properties

User information

Name	Description
User name	Edit the user name. You can only edit this if the selected user is a Basic user. Names must be unique, and must not contain any of these special characters: **< > & ' " ¥ / : * ? | [ ]**
Password	Only editable if the selected user is of the type basic user. Edit the password. Remember to repeat the password to be sure you have specified it correctly.
User type	Non-editable field, displaying whether the selected user is of the type basic user or Windows user group.

Group information

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

General access

When you add or edit basic users (see "Add basic users" on page 171), Windows users (see "Add Windows users" on page 172) or groups (see "Add user groups" on page 173), specify general access settings:

Name	Description
Live	Ability to access the **Live** tab in XProtect Smart Client.
Playback	Ability to access the **Playback** tab in XProtect Smart Client.
Setup	Ability to access setup mode in XProtect Smart Client. **Tip:** By clearing the **Live**, **Playback** and **Setup** check boxes you can effectively disable the user's/group's ability to use XProtect Smart Client. You can use this as a temporary alternative to deleting the user/group, for example while a user is on vacation.
Edit shared views	Ability to create and edit views in shared groups in XProtect Smart Client. Every user can access views placed in shared groups. If a user/group does not have this right, shared groups are protected, indicated by a padlock icon in XProtect Smart Client.

Name	Description
Edit private views	Ability to create and edit views in private groups in XProtect Smart Client. Views placed in private groups can only be accessed by the user who created them. If a user/group does not have this right, private groups will be protected, indicated by a padlock icon in XProtect Smart Client. Denying users the right to create their own views may make sense in some cases, for example, to limit bandwidth use. For more information about shared and private views, see the separate XProtect Smart Client documentation.
Administrator Access	Select the checkbox to allow users to access and work with the Management Application. If you have more than one Administrator member, you can clear the checkbox to ensure that other administrators cannot access the Management Application.

Camera access

When you add or edit basic users (see "Add basic users" on page 171), Windows users (see "Add Windows users" on page 172) or groups (see "Add user groups" on page 173), you can specify camera access settings.

In the list of cameras, select the camera(s) you want to work with. Note the last item in the list, **Rights for new cameras when added to the system**, with which you can allow the user/group access to any future cameras.

Tip: If the same features should be available for access for several cameras, you can select multiple cameras by pressing SHIFT or CTRL on your keyboard while you select.

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 you work with the selected camera(s). The sub-features are listed in two columns in the lower part of the window: the left column lists features related to live viewing, the right column lists features related to playback.

The **Camera access settings** check boxes work like a hierarchy of rights. If the **Access** check box is cleared, everything else is cleared and disabled. If the **Access** check box is selected, but, for example, the **Live** check box is cleared, everything under the **Live** check box is cleared and disabled.

Depending on the selected column, the following default features for live or playback from the selected camera(s) give you the ability to:

Live	Features
PTZ	Use navigation features for PTZ (Pan-tilt-zoom) cameras. A user/group can only use this right if the user has access to one or more PTZ cameras.

Live	Features
PTZ preset positions	Use navigation features for moving a PTZ camera to particular preset positions. A user/group can only use this right if the user/group has access to one or more PTZ cameras with defined preset positions.
Manage PTZ presets	Manage PTZ positions in XProtect Smart Client.
Output	Activate output (lights, sirens, door openers, etc.) related to the selected camera(s).
Events	Use manually triggered events related to the selected camera(s). This feature is available in XProtect Smart Client only.
Incoming audio	Listen to incoming audio from microphones related to the selected camera(s). This feature is available in XProtect Smart Client only.
Manual recording	Manually start recording for a fixed time (defined (see "Manual recording" on page 85) by the surveillance system administrator).
Outgoing audio	Talk to audiences through speakers related to the selected camera(s). This feature is available in XProtect Smart Client only.

Playback	Features
AVI/JPEG export	Export evidence as movie clips in AVI format and as still images in JPEG format.
Database export	Export evidence in database format. This feature is available in XProtect Smart Client only.
Sequences	Use the **Sequences** feature when playing back video from the selected camera.
Smart search	Search for motion in one or more selected areas of images from the selected camera. This feature is available in XProtect Smart Client only.
Recorded audio	Listen to recorded audio from microphones related to the selected camera(s).

You cannot select a feature, if the selected camera does not support the relevant feature. For example, PTZ-related rights are only available if the relevant camera is a PTZ camera. Some features depend on the user's/group's General Access (on page 174) properties.

Square-filled check boxes can appear in the lower part of the window if you have selected several cameras and a feature applies for some but not all of the cameras. Example: For camera A, you have selected that use of the Events is allowed, for camera B, you have not allowed this. If you select both camera A and camera B in the list, the Events check box in the lower part of the window is square-filled. Another example: Camera C is a PTZ camera for which you have allowed the PTZ preset positions feature whereas camera D is not a PTZ camera. If you select both camera C and camera D in the list, the PTZ preset positions check box is square-filled.

Alarm management

When you add or edit basic users (see "Add basic users" on page 171), Windows users (see "Add Windows users" on page 172) or groups (see "Add user groups" on page 173), specify their XProtect Smart Client alarm management rights:

Name	Description
Manage	Allows users of the XProtect Smart Client to: • Manage alarms (for example, change priorities of alarms and re-delegate alarms to other users) • Acknowledge alarms—in the XProtect Smart Client's alarm list and maps. • Change state (for example from **New** to **Assigned**) of several alarms simultaneously (otherwise state must be changed on a per-alarm basis).
View	Allows users of the XProtect Smart Client to: • View alarms • Print alarms reports.
Disable	Allows users of the XProtect Smart Client to disable alarms.

Access control management

When you add or edit basic users (see "Add basic users" on page 171), Windows users (see "Add Windows users" on page 172) or groups (see "Add user groups" on page 173), specify access control settings:

Name	Description
Use Access Control	Allows the relevant user to use any access control-related features in XProtect Smart Client.

Services

About services

The following services are all automatically installed on the Milestone Husky server if you run a **Typical** installation. By default, services run transparently in the background on the Milestone Husky server. If you need to, you can start and stop services separately from the Management Application, see Start and stop services (on page 178).

Service	Description
Milestone Recording Server service	A vital part of the surveillance system. Video streams are only transferred to your Milestone Husky system while the Recording Server service is running.
Milestone Image Server service	Provides access to the surveillance system for users who log in with XProtect Smart Client. Note: If the Image Server service is configured in Windows Services to log in with another account than the Local System account, for example as a domain user, installed instances of XProtect Smart Client on other computers than the surveillance server itself are not 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 that enables sending of images from immediately before and after an event took place from the camera to the surveillance system via e-mail. Pre- and post-alarm images should not be confused with the Milestone Husky pre- and post-recording feature (see "Recording" on page 97).
Milestone Log Check service	Performs integrity checks on Milestone Husky log files. For more information, see Overview of Logs.
Milestone Event Server service	Manages all alarms and map-related communication. It stores events, image files and map configurations, and makes status information about the surveillance system available.
Milestone Mobile service	Manages the communication between the Recording Server and mobile devices (such as smartphones and tablets) and between the Recording Server and web browsers.

If you run a Custom installation, you can choose not to install the Mobile server and/or the Event Server. If you do so, the Mobile service and/or the Event Server service will not be seen in your Services overview.

Start and stop services

On a Milestone Husky server, several services (see "About services" on page 177) by default run in the background. If you need to, you can start and stop each service separately:

1. In the Management Application's Navigation pane, expand **Advanced Configuration** and select **Services**. This displays the status of each service.
2. You can now stop each service by clicking the **Stop** button. When a service is stopped, the button changes to **Start**, allowing you to start the service again when required.

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

Servers

Mobile server

About Mobile server

A Mobile server handles log-ins to the system from Milestone Mobile client (see "About Milestone Mobile client" on page 15) from a mobile device or XProtect Web Client (see "About XProtect Web Client" on page 16).

Upon correct login, the Mobile server distributes video streams from relevant recording servers to Milestone Mobile client. This offers an extremely secure setup, where recording servers are never connected to the Internet. When a Mobile server receives video streams from recording servers, it also handles the complex conversion of codecs and formats allowing streaming of video on the mobile device.

Important: Before you begin the installation of the Mobile server, make sure you are logged in with an account that has administrator rights. Installation cannot be successful if you use a standard user account.

About Video push

Video push is feature in your Milestone Mobile client that allows you to use your mobile device's camera to, for example, collect evidence when you investigate an alarm or event. You do this by sending a video stream from your mobile device to your system. In the Mobile server settings, you can set up how many users should be able to use the Video push feature in the system.

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

If you are logged into the Milestone Mobile client and are watching one or more cameras views while at the same time changing configuration in the Management Application, the live video from the camera may freeze in the Milestone Mobile client if you click **File > Save** in the Management Application**.**

To avoid this scenario, you must restart the Milestone Mobile service manually. See the Windows Help for information about how to do this. If you are using newer versions of XProtect, the Milestone Mobile service restarts with the other services and no user action is required.

Add/edit a Mobile server

1. Go to **Servers** > **Mobile Servers.** From the menu that appears, select **Create New**. Fill in/edit the needed properties.

IMPORTANT: If you edit settings for **Login method, All cameras view** and **Outputs and events**, while you are connected to the Milestone Mobile client, you must restart the Milestone Mobile client for the new settings to take effect.

Add a Video push channel

Each Video push channel requires a separate camera license.

To add a Video push channel (see "About Video push" on page 179), do the following:

1. On the **Video Push** tab, select the **Video push** checkbox to enable the functionality.
2. In the bottom right corner, click **Add** to add a video push channel to the **Channels** mapping.
3. Channels are mapped to devices through user names. Select a user name from a user account already set up in your system to associate with the relevant Video push channel. If you do not associate the Video push channel with an already created user, you cannot use Video push in your Milestone Mobile client when you log in.
4. Add the Video push driver as a hardware device (see "Add a Video push driver as a hardware device" on page 180) to the system. You must choose the **Manual** hardware device detection method as the Video push driver does not show up in automatic hardware searches.
5. On the **Video Push** tab, click **Find Cameras**. If successful, the newly added Video push driver appears in this list. Save your configuration to make the Video push driver ready for use.

You can remove video push channels you do not require. To do so, select the relevant channel and click **Remove** in the bottom right corner.

Add a Video push driver as a hardware device

If you add a Video push channel, you must add the Video push driver to your Management Application/Management Client. To do so:

1. Open the **Add New Hardware Wizard** in your Management Application/Management Client.
2. Choose the **Manual** option. The Video push driver will not be detected in automatic hardware searches.
3. Specify hardware device settings (see "Add hardware devices settings" on page 180) and select the hardware driver manually.
4. Once finished, your Video push driver must be associated with your Video push channel. To do so, return to your Mobile server > **Video Push** tab and click **Find Cameras**.

Add hardware devices settings

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

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

Name	Description
Port:	Type in the port number for your Video push driver. The default port is 80. The port is for communication between the Milestone Mobile server and your XProtect server. **Important:** The port number you set must be identical with the port number you set when you specify your Video push settings (see "Video Push" on page 182). If the port numbers are not identical, your Video push channel will not work.
User name:	Select the same user name as associated with the Video push channel when you added (see "Add a Video push channel" on page 180) this.
Password:	Type in the password for the Video push driver. The password for your Video push driver is **Milestone** (this cannot be changed).
Hardware Driver:	Select the **Video push driver**.
Verified:	Select if the Video push driver runs on a secured HTTPS connection.

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

Mobile server settings

General

Fill in and specify general settings for the Mobile server:

Name	Description
Server name	Name of the Mobile server.
Description	Description of the Mobile server.
Mobile server	Choose between all Mobile servers currently installed to the specific XProtect system. Only Milestone Mobile servers that are running are shown in the list.
Connection type	Possible methods are: **HTTP only**, **HTTP and HTTPS** or **HTTPS Only**.
Client timeout (HTTP)	Default time frame (30 sec.) for how often the Mobile server client must indicate to the Mobile server server that it is up and running. Milestone recommends that you do **not** increase the time frame.
Login method	Select how you want to log in to the Mobile server server should take place. Possible methods are: **Automatic, Windows Only** or **Basic Only.**
XProtect Web Client	Enable the use of XProtect Web Client.
Enable all cameras view	Enable/disable viewing of **All Cameras** view. This view contains all cameras on a recording server (user rights permitting).

Name	Description
Enable actions	Enable/disable actions in Milestone Mobile clients.
Enable keyframes	Enable/disable video stream to stream key frames only. Enabling key frames only reduces bandwidth usage.
Configuration backup	Import or export your Milestone Mobile server configuration. Your system stores the configuration in an XML file.

Server Status

See the status details for your Mobile server. The details are read-only:

Name	Description
Server active since	Shows how long the Mobile server has been running since it was last stopped.
CPU usage	Shows current CPU usage on the Mobile server.
Internal bandwidth	Shows the current bandwidth in use between the Mobile server and the relevant recording server.
External bandwidth	Shows the current bandwidth in use between the mobile device and Mobile server.
User Name column	Shows user name(s) of the Mobile server user(s) connected to the Mobile server.
State column	Shows the current relation between the Mobile server and the Milestone Mobile client user in question. Is the user connected (a state preliminary to servers exchanging keys and encrypting credentials) or is he/she actually logged in? Possible states are: **Connected** and **Logged** In XProtect.
Bandwidth Usage column	Shows the level of bandwidth used by the Mobile server client user in question.
Live Streams column	Shows the number of live video streams currently open for the Milestone Mobile client user in question.
Playback Streams column	Shows the number of playback video streams currently open for the Mobile client user in question.

Video Push

If you enable Video push, specify the following settings:

Name	Description
Video push	Enable Video push on the Mobile server.
Number of channels	Specify the number of enabled Video push channels in your XProtect system.
Channel column	Shows the channel number for the relevant channel. Non-editable.

Name	Description
Port	Port number for the relevant Video push channel.
MAC	MAC address for the relevant Video push channel.
User Name	Enter the user name associated with the relevant video push channel.
Camera Name	Shows the name of the camera if the camera has been identified.

Once you have completed all necessary steps (see "Add a Video push channel" on page 180), click **Find Cameras** to search for the relevant camera.

Export

Specify the following settings for exported recordings:

Name	Description
Export	Select to enable export in clients.
Include timestamps	Select to add timestamps to exported video.
Used codec for AVI files	Choose a codec to use to encode your exported AVI video files.
Export to	Specify the location to which recordings should be exported.
Delete exported recordings older than	Enter the number of days to pass before recordings are deleted. Note that if the value is set to 1 day, exported files are deleted up to 10 minutes from the applied change, not immediately. Users can restart the Mobile server manually to make the changes take effect immediately.
Limit size of exports folder to	Enter a number to set a maximum limit for the folder to which the recordings are exported.
View exports of other users	Select this check box to enable users to be able to view exports made by other users.

Automatic exports

If you want to set up your system to automatically export video when a certain event occurs, you must set up rules to instruct the system about when to carry out automatic exports:

Enabled	Select this check box to enable automatic exports.

In the columns below the **Enabled** check box is a list of all automatically exported video. See the following details for individual automatic exports:

Name column	Name of the rule.
Item column	Item that triggers the automatic export.
Event column	Shows event that triggers the automatic export.
Camera column	Camera from which the video is recorded.

Duration column	Length of the exported video file.
Export type column	Indicates whether the export file format is database format or AVI format.

Exported recordings

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

Name column	Name of the exported recording.
State column	State of the exported recording.
Camera column	The camera that provided the exported recording.
Timestamp column	The point of time when the export took place.
Duration column	The length of the exported recording.
User column	The name of the user who provided the exported recording.
MB column	The size of the exported recording.

Tip: Click **Refresh** to update the list of exported recordings shown.

Mobile Server Manager

About Mobile Server Manager

The Mobile Server Manager is a tray-controlled feature connected to Mobile server. Right-clicking the Mobile Server Manager icon in the system tray opens a menu from which you can easily access Mobile server functionality. You can:

- Open XProtect Web Client (see "Access XProtect Web Client" on page 16)
- Start, stop and restart the Mobile service (see "Start, stop and restart Mobile service" on page 186)
- Fill in or change surveillance server credentials (see "Fill in/edit surveillance server credentials" on page 186)
- Show/edit port numbers (on page 186)
- Edit certificate (on page 185)
- Open today's log file (see "About accessing logs and exports" on page 185)
- Open log folder (see "About accessing logs and exports" on page 185)
- Open export folder (see "About accessing logs and exports" on page 185)
- Show Mobile server status (see "About show status" on page 185)
- Access the Milestone Mobile Help website (where you find manuals, frequently asked questions (FAQs) and product demonstration videos.)

About show status

If you right-click the Mobile Server Manager and select **Show Status...** (or double-click the Mobile Server Manager icon), a window opens, showing the status of the Mobile server. You can see the following:

Name	Description
Server running since:	Time and date of the time when the Mobile server was last started.
Connected users:	Number of users currently connected to the Mobile server.
CPU usage:	How many % of the CPU is currently being used by the Mobile server.
CPU usage history:	A graph detailing the history of CPU usage by the Mobile server.

About accessing logs and exports

The Mobile Server Manager lets you quickly access the log file of the day, open the folder to which logs files are saved, and open the folder to which exports are saved.

To open any one of these, right-click the Mobile Server Manager and select **Open Today's Log File**, **Open Log Folder** or **Open Export Folder** respectively**.**

Important: If you uninstall Milestone Mobile from your system, its log files are not deleted. Administrators with proper rights can access these log files at a later timer, or decide to delete them if they are not needed any longer. The default location of the log files is in the ProgramData folder. If you change the default location of log files, existing logs are not copied to the new location nor are they deleted.

Edit certificate

If you want to use a secure HTTPS protocol to establish connection between your mobile device or the XProtect Web Client and the Mobile server, you must have a valid certificate for the device or web browser to accept it without warning. The certificate confirms that the certificate holder is authorized to establish the connection.

When you install the Mobile server, you generate a self-signed certificate if you run a **Typical** installation. If you run a **Custom** installation, you get the choice between generating a self-signed certificate or loading a file containing a certificate issued by another trusted site. If you, at a later point, want change the certificate you use, you can do this from the Mobile Server Manager.

1. Right-click the Mobile Server Manager and select **Edit Certificate...**
2. Choose whether you want to either:
   - Generate a self-signed certificate or
   - Load a certificate file.

Generate a self-signed certificate

1. Choose the **Generate a self-signed certificate** option and click **OK**.
2. Wait for a few seconds while the system installs the certificate.
3. Once finished, a window opens and informs you that the certificate was installed successfully. The Mobile service is restarted for the changes to take effect.

Locate a certificate file

1. Choose the **Load a certificate file** option.
2. Fill in the path for the certificate file or click the ... box to open a window where you can browse for the file.
3. Fill in the password connected to the certificate file.
4. When finished, click **OK**.

Note that HTTPS is not supported on Windows XP and Windows 2003 operating systems and works on Windows Vista or newer Windows OS only.

Fill in/edit surveillance server credentials

1. Right-click the Mobile Server Manager and select **Surveillance Server Credentials...**
2. Fill in the **Server URL**
3. Select what user you want to log in as:
   - Local system administrator (no credentials needed) or
   - A specified user account (credentials needed)
4. If you have chosen a specified user account, fill in **User Name** and **Password**.
5. When finished, click **OK**.

Show/edit port numbers

1. Right-click the Mobile Server Manager and select **Show/Edit Port Numbers...**
2. To edit the port numbers, fill in the relevant port number. You can indicate a standard port number (for HTTP connections) and/or a secured port number (for HTTPS connections).
3. When finished, click **OK**.

Start, stop and restart Mobile service

If needed, you can start, stop and restart the Mobile service from the Mobile Server Manager.

To perform any of these tasks, right-click the Mobile Server Manager and select **Start Mobile service**, **Stop Mobile service** or **Restart Mobile service** respectively**.**

Alarms

About alarms

The Alarms feature is a Milestone Integration Platform (MIP) (see "About MIP plug-ins" on page 194)-based feature that uses functionality handled by the Event server. It provides central overview and control of alarms in any number of system installations throughout your organization.

You can configure alarms to be generated based on either:

- **Internal events (system-related):** for example motion, server responding/not responding, archiving problems, lack of disk space, and so on.
- **External events (integrated):** for example events from access control systems or license plate recognition.

The Alarms feature also handles general alarms settings and alarm logging.

About configuring alarms

Alarm configuration includes among other things:

- Dynamic setup of alarm handling (see "Add an alarm" on page 189) based on users access rights
- Central overview of all components: servers, cameras, and external units
- Setup of central logging of all incoming alarms and system information
- Handling of plug-ins, allowing customized integration of other systems, for example external access control or VCA-based systems.

About viewing alarms

The following can play a role with regards to alarms and who can view/control/manage them and to what degree. This is because alarms are controlled by the visibility of the object causing the alarm.

- Source/device visibility: if the device causing the alarm is not set to be visible to the user, the user cannot see the alarm in the alarm list in the XProtect Smart Client. See Configure User Access wizard (see "Manage user access wizard" on page 62).
- Right to trigger manually defined events: if manually defined events (see "Add a manual event" on page 119) are available in your Milestone Husky system, these can determine if the user can trigger selected manually defined events in the XProtect Smart Client. See Configure User Access wizard (see "Manage user access wizard" on page 62).
- External plug-ins: if any external plug-ins are set up in your system, these might control user's rights to handle alarms.
- General access rights: can determine whether the user is allowed to (only) view or also to manage alarms. See Configure User Access wizard (see "Manage user access wizard" on page 62).

About time profiles for alarms

Alarms can also be based on time profiles (for alarms) (see "Add a time profile (for alarms)" on page 190).

Time profiles for Alarms are periods of time to use when youcreate alarm definitions. You can, for example, create a time profile for alarms covering the period from 2.30 PM till 3.30 PM on Mondays, and then use the time profile to make sure that certain alarm definitions are only enabled within this period of time.

About alarms and XProtect Central/XProtect Analytics Generic VA

To a large extent, the Alarms feature covers the same functionality as XProtect Central.

However, configuration of former XProtect Central functionality is now included in the Alarms feature. XProtect Central was an independent product consisting of two parts: a dedicated server and a number of dedicated clients. Alarms, on the other hand, is an integrated part of your Milestone Husky system. This means that much configuration needed in XProtect Central has become redundant with the introduction of Alarms. Client-wise, the Alarms feature uses the XProtect Smart Client. However, you must still configure the features Alarms, Time Profiles (for Alarms) and General Settings in the Management Application. These features are very similar to XProtect Central. You cannot reuse old alarm and map definitions from XProtect Central. You must redefine your alarms and maps definitions in the Alarms feature.

Similarly, the Alarms feature also covers the same functionality as XProtect Analytics Generic VA. What was before before a plug-in to XProtect Analytics is now an integrated part of the Alarms feature and covers the same functionality.

About alarms in the XProtect Smart Client

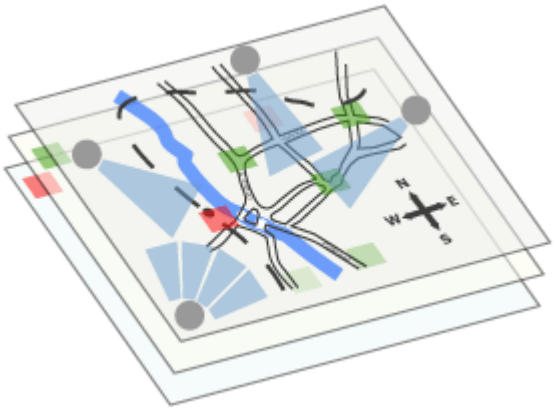
To ease overview, delegation and handling of alarms, these appear in the XProtect Smart Client alarm list where you can view and manage these (reassign, change status, comment, and similar). They can, if relevant, be integrated with the map functionality (see "About maps" on page 189). The Alarms feature is a powerful monitoring tool, providing instant overview of alarms and possible technical problems.

IMPORTANT: You can only view alarms based on the Alarms feature in XProtect Smart Client 6.0 if you run XProtect Smart Client 6.0 in a 32-bit version—not in a 64-bit version.

Tip: You can use manual events for triggering alarms and, if required, use the same event to trigger several different alarms.

About maps

With maps as an integrated part of alarms, you get a physical overview of your surveillance system: with the possibility to assign cameras to a map, you can always tell where alarms originate, which cameras are placed where, and in what direction are they pointing. Also, you can use maps to navigate from large perspectives to detailed perspectives, and vice versa: for example, a state map can have hot zones (small icons on the map) that point to more detailed maps of cities, neighborhoods, streets, floor plans, and so on.



Example: Hierarchy of maps

All user-interaction with maps, including adding and maintaining maps, takes place in XProtect Smart Client. For detailed information, see the XProtect Smart Client documentation.

Example: Map in XProtect Smart Client

In order to use maps, the Event Server service must be running. The Event Server service is automatically included if you run a **Typical** installation of your surveillance server installation (see "Install your surveillance server software" on page 25).

Add an alarm

For a detailed overview of Alarms and how the feature works, see About alarms (on page 187).

To add/configure an alarm, do the following:

1. In the Management Application's navigation pane, expand **Alarms**, right-click **Alarm Definition** and select **Create New**.
2. Specify required properties (see "Alarms definition" on page 190).
3. Click **OK**.

4. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

Add a time profile (for alarms)

Time profiles are periods of time used for the Alarms feature only.

To add a time profile for an alarm, do the following:

1. In the Management Application's navigation pane, expand **Alarms**, right-click **Time Profiles**, and select **Create New**. The small month overview in the top right corner of the **Time Profile Properties** window can help you get a quick overview of the time periods covered by the time profile, as dates containing specified times are highlighted in bold.
2. In the calendar, select the **Day View, Week View, or Month View** tab, then right-click inside the calendar and select either **Add Single Time...** or **Add Recurring Time...**.
3. If you select **Add Single Time...**, specify **Start time** and **End time**. If the time is to cover whole days, select the **All-day event** box.
   —or—
   If you select **Add Recurring Time...**, specify time range, recurrence pattern, and range of recurrence.
4. Click **OK**.
5. Save your configuration changes by clicking **Save** in the yellow notification bar in the upper-right corner of the Management Application.

When you edit an existing time profile, remember that a time profile may contain more than one time period, and that time periods may be recurring.

Analytics events (see "Overview of events and output" on page 115) are typically data received from external third-party video content analysis (VCA) (see "VCA" on page 214) providers. An example of a VCA-based system could be an access control system.

Alarms properties

Alarms definition

When you configure Alarm definitions (see "Add an alarm" on page 189), specify the following:

Name	Description
Enable	Enables the Alarms feature.
Name	Enter a name. The alarm's name appears whenever the alarm is listed. Alarm names do not have to be unique.
Description	Enter a description (optional).

Name	Description
Triggering event	This first list shows both system-related events and events from plug-ins (for example access control systems or similar). From the second list, select the event message to use when the alarm is triggered.
Sources	Select which cameras and/or other devices the event should originate from in order to trigger the alarm. Plug-in defined sources, for example license plate recognition, access control systems and MIP-plugins appear in the list if installed. Your options depend upon which type of event you have selected.
Time profile	If you select **Time profile**, you must select when the alarm should be enabled for triggering. If you have not defined alarm time profiles (see "Add a time profile (for alarms)" on page 190), you will only be able to select **Always**. If you have defined one or more time profiles, they will be selectable from this list.
Event based	If you select **Event based,** you must select which events should start and stop the alarm. Events available for selection are hardware events defined on cameras, video servers and input. You can also use global/manual event definitions (see "Add a manual event" on page 119). Note that when you select **Event based**, you cannot define alarms based on outputs—only on inputs.
Time Limit	Select the time-limit within which the operator must respond to the alarm.
Events triggered	Select the event to be triggered if the operator does not react withing the time limit specified in **Time limit**. This could be, for example, sending an email, SMS or similar.
Related cameras	Select (a maximum of 15) cameras for inclusion in the alarm definition even though they are not themselves triggering the alarm. This can be relevant, for example, if you have selected an external event message (such as a door being opened) as the source of your alarm. By defining one or more cameras near the door, you could attach the cameras' recordings of the incident to the alarm.
Related map	Select a map to associate with the alarm definition. The selected map is automatically be shown in XProtect Smart Client whenever the alarm is listed. This might help you to quicker identify the physical location of the alarm.
Initial alarm owner	Select a default user responsible for the alarm. You can only select from users allowed to view **all** cameras and/or other devices selected as source(s) for the event causing the alarm.
Initial alarm priority	Select a priority (**High**, **Medium** or **Low)** for the alarm. Priorities can be used for sorting purposes and workflow control in the Smart Client.

Name	Description
Initial alarm category	Select a category to which the alarm should initially be assigned. This could be, for example, **Building01**, **Burglary**, **ElevatorEast** or similar, depending on which categories have been defined.
Event triggered by alarm	Define an event to be triggered by the alarm in the Smart Client (if needed).
Auto-close alarm	Select if the alarm should automatically be closed upon a particular event. This is possible for alarms triggered by some (but not all) events.

See also Alarm data settings (on page 192) and Alarm sound settings (see "Sound settings" on page 193) for further information on how to configure alarm settings.

Alarm data settings

When you configure alarm data settings, specify the following:

Alarm Data Levels **tab,** Priorities

Name	Description
Level	Add new priorities with level numbers of your choosing or use/edit the default priority levels (numbers **1**, **2** or **3)**. These priority levels are used to configure the **Initial alarm priority** setting (see "Alarms definition" on page 190).
Name	Type a name for the entity. You can create as many as you like.
Sound	Select the sound to be associated with the alarm. Use one if the default sounds or add more in Sound Settings (on page 193).

Alarm Data Levels tab, States

Level	In addition to the default state levels (numbers **1**, **4**, **9** and **11,** which can not be edited or reused), add new states with level numbers of your choosing. These state levels are only visible in the Smart Client's **Alarm List**.
Name	Type a name for the entity. You can create as many as you like.

Alarm Data Levels tab, Categories

Level	Add new categories with level numbers of your choosing. These category levels are used to configure the **Initial alarm category** setting (see "Alarms definition" on page 190).
Name	Type a name for the entity. You can create as many as you like.

Alarm List Configuration tab

In **Available columns,** use **>** to select which columns should be available in the XProtect Smart Client **Alarm List**. Use **<** to clear selection. When done, **Selected columns** should contain the items to be included.

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

Sound settings

When you configure Sound Settings, specify the following:

Name	Description
Sounds	Select the sound to be associated with the alarm. The list of sounds contain a number of default Windows sounds. These cannot be edited. However, you can add new sounds of the file type .wav, but only if these are encoded in Pulse Code Modulation (PCM). Although the default sounds are standard Windows sound-files, local Windows settings might cause these to sound different on different machines. Some users might also have deleted one or more of these sound-files and will therefore be unable to play them. To ensure an identical sound all over, you should import and use your own .wav files encoded in PCM.
Add	Lets you add sounds. Browse to the sound to upload one or several .wav files.
Remove	Remove a selected sound from the list of manually added sounds. Default sounds cannot be removed.
Test	Lets you test the sound. In the list, select the sound. The sound will be played once.

Time profile

When you configure Time profiles (see "Add a time profile (for alarms)" on page 190), specify the following:

Component	Requirement
Name	Type a name for the time profile.
Description	Enter a description (optional).

Component	Requirement
Add Single Time	Right-click the calendar and select **Add Single Time**. Specify **Start time** and **End time**. If the time covers whole days, select **All-day event**.
Add Recurring Time	Right-click the calendar and select **Add Recurring Time**. Specify the time range, recurrence pattern, and range of recurrence.
Edit Time	Right-click the calendar and select **Edit Time**. Specify **Start time** and **End time**. If the time covers whole days, select **All-day event**. When you edit an existing time profile, remember that a time profile may contain more than one time period, and that time periods may be recurring. If you want your time profile to contain additional periods of time, add more single times or recurring times.

MIP plug-ins

About MIP plug-ins

If you install MIP (Milestone Integration Partner) plug-ins to your Milestone Husky system, the plug-ins can be found in the Management Application's navigation pane, expand **Advanced Configuration**, under **MIP Plug-ins**.

You can assign MIP-related user rights to users and user groups. You do this from the Management Application's navigation pane, expand **Advanced Configuration**, expand **Users**, right-click the relevant user and select **Properties**. Under the **Alarm Management** tab, a tab that allows access to MIP settings for the selected user is located.

You can also use online activation (see "About activating licenses" on page 33) in connection with licensing schemes of MIP-related plug-ins.

Backup and restore configuration

About backup and restore of configurations

Milestone recommends that you make regular backups of your Milestone Husky configuration (cameras, schedules, views, and so on) as a disaster recovery measure. While it is rare to lose your configuration, it can happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration.

Back up system configuration

The backup described here is a backup of your entire surveillance system setup (including, among other things, log files, event and Matrix configuration, restore points, view groups as well as Management Application and XProtect Smart Client configuration). Alternatively, you can export your configuration as a backup (see "Export and import management application configuration" on page 199), which is limited to the Management Application configuration.

To back up:

1. 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 exists if you have configured video properties (see "General" on page 93) 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 server, so that they are not affected if the server is damaged, stolen or otherwise affected.

Remember that a backup is a snapshot of your system configuration at the time of backing up. If you later change your configuration, your backup does not reflect the most recent changes. Therefore, back up your system configuration regularly.

Tip: When you back up your configuration as described, the backup includes restore points (see "Restore system configuration from a restore point" on page 201). This allows you to not only restore the backed-up configuration, but also to revert to an earlier point in that configuration if you need to.

Restore system configuration

1. If Milestone Husky is used on a server running any supported operating system, copy the content of the backed-up **Milestone Surveillance** folder into **C:¥Program Data¥Milestone¥Milestone Surveillance.**
2. If you backed up the file **devices.ini**, copy the file into **C:¥Program Files¥Milestone¥Milestone Surveillance¥devices.**

Back up and restore alarm and map configuration

Available functionality depends on your product version.

It is important that you regularly back up your alarm and map configurations. You do this by backing up the event server, which handles your alarm and map configuration as well as the Microsoft® SQL Server Express database, which stores your alarm data. This enables you to restore your alarm and map configuration in a possible disaster recovery scenario.

Tip: Backing up also has the added benefit that it flushes the SQL Server Express database's transaction log.

When you back up and restore alarm and/or map configuration, you must do it in the following order:

Prerequisites

- **You must have administrator rights on the SQL Server Express database** when you back up or restore your alarm configuration database on the SQL Server Express. Once you are done backing up or restoring, you only need to be a database owner of the SQL Server Express database.
- **Microsoft® SQL Server Management Studio Express**, a tool you can download for free from www.microsoft.com/downloads. Among its many features for managing SQL Server Express databases are some easy-to-use backup and restoration features. Download and install the tool on your existing surveillance system server and on a possible future surveillance system server (you will need it for backup as well as restoration).

Step 1: Stop the Event Server service

Stop the event server service to prevent configuration changes from being made:

1. On your surveillance system server, click **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Right-click the Event Server, click **Stop**.

This is important since any changes made to alarm configurations—between the time you create a backup and the time you restore it—will be lost. If you make changes after the backup, you must make a new backup.

Note that alarms are not generated while the Event Server service is stopped. It is important that you remember to start the service again once you have finished backing up the SQL database.

Step 2: Back up alarms data in SQL Server Express database

1. Open Microsoft SQL Server Management Studio Express from Windows' **Start** menu by selecting **All Programs** > **Microsoft SQL Server 2008 > SQL Server Management Studio Express**.
2. When you open the tool, you are prompted to connect to a server. Specify the name of the required SQL Server and connect with administrator user credentials. You do not have to type the name of the SQL server: if you click inside the Server name field and select **<Browse for more...>**, you can select the SQL Server from a list instead.

3. Once connected, you see a tree structure in the **Object Explorer** in the left part of the window. Expand the SQL Server item, then the **Databases** item, which contains your entire alarm configuration.
4. Right-click the **VIDEOOSDB** database, and select **Tasks** > **Back Up...**
5. On the **Back Up Database** dialog's **General** page, do the following:
   - Under **Source**: Verify that the selected database is **VIDEOOSDB** and that the backup type is **Full**.
   - Under **Destination**: A destination path for the backup is automatically suggested. Verify that the path is satisfactory. If not, remove the suggested path, and add another path of your choice.
6. On the **Back Up Database** dialog's **Options** page, under **Reliability**, select **Verify backup when finished** and **Perform checksum** before writing to media.
7. Click **OK** to begin the backup. When backup is finished, you will see a confirmation.
8. Exit Microsoft SQL Server Management Studio Express.

Tip: If you do not have **SQL Server Management Studio Express**, you can download it for free from www.microsoft.com/downloads.

Tip: VIDEOOSDB is the default name of the database containing the system configuration. If you can find the database, but it is not called **VIDEOOSDB**, it could be because you gave the database another name during the installation. In this procedure, we assume that the database uses the default name.

Step 3: Reinstall Milestone Husky (if needed).

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

Before you start: Shut down any existing surveillance software.

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

You can now begin to configure your Milestone Husky through its Management Application. For more information, see Get your system up and running (on page 28).

Step 4: Restore alarms data in SQL Server Express database

Luckily, most users never need to restore their backed-up alarm data, but if you ever need to, do the following:

1. In the Windows Start menu, open Microsoft SQL Server Management Studio Express.
2. Connect to a server. Specify the name of the required SQL Server, and connect using the user account the database was created with.
3. In the **Object Explorer** on the left, expand **SQL Server** < **Databases**, right-click the **VIDEOOSDB** database, and then select **Tasks** > **Restore** > Database...
4. In the **Restore Database** dialog, on the **General** page, under **Source for restore,** select **From device** and click <Browse for more...>, to the right of the field. In the Specify Backup dialog, make sure that **File** is selected in the **Backup media** list**.** Click **Add.**
5. In the **Locate Backup File** dialog, locate and select your backup file **VIDEOOSDB.bak**. Then click **OK.** The path to your backup file is now listed in the **Specify Backup** dialog.
6. Back on the **Restore Database** dialog's **General** page, your backup is now listed under **Select the backup sets to restore**. Make sure you select the backup by selecting the check box in the **Restore** column.
7. Now go to the **Restore Database** dialog's **Options** page, and select **Overwrite the existing database**. Leave the other options as they are, and then click **OK** to begin the restoration. When the restore is finished, you see a confirmation.
8. Exit Microsoft SQL Server Management Studio Express.

Tip: If you do not have **SQL Server Management Studio Express**, you can download it for free from www.microsoft.com/downloads.

Tip: You do not have to type the name of the SQL server: If you click inside the **Server name** field and select **<Browse for more...>**, you can select the required SQL Server from a list instead.

Tip: If you get an error message telling you that the database is in use, try exiting Microsoft SQL Server Management Studio Express completely, then repeat steps 1-8.

Tip: VIDEOOSDB is the default name of the database containing the system configuration. If you can find the database, but it is not called **VIDEOOSDB**, it could be because you gave the database another name during installation. In the following, we assume that the database uses the default name.

Step 5: Restart the Event Server service

During the restore process, the Event Server service is stopped to prevent configuration changes being made until you are done. Remember to start the service again:

1. On your surveillance system server, click **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Right-click the Event Server, click **Start**.

About the SQL Server Express transaction log and reasons for flushing it

Each time a change in the Milestone Husky alarm data take place, the SQL Server logs the change in its transaction log. The transaction log is essentially a security feature that makes it possible to roll back and undo changes to the SQL Server Express database. The SQL Server by default stores its transaction log indefinitely, and, therefore, the transaction log builds up more and more entries over time.

The SQL Server's transaction log is by default located on the system drive, and if the transaction log just keeps growing, it may in the end prevent Windows from running properly. Flushing the SQL Server's transaction log from time to time is therefore a good idea, however flushing it does not in itself make the transaction log file smaller, rather it prevents it from growing out of control. Milestone Husky does not, however, automatically flush the SQL Server's transaction log at specific intervals. This is because users have different needs. Some want to be able to undo changes for a very long time, others do not care.

You can do several things on the SQL Server itself to keep the size of the transaction log down, including truncating and/or shrinking the transaction log (for numerous articles on this topic, go to support.microsoft.com (see http://support.microsoft.com - http://support.microsoft.com) and search for SQL Server transaction log). However, backing up the Milestone Husky database is generally a better option since it flushes the SQL Server's transaction log and gives you the security of being able to restore your Milestone Husky alarm data in case something unexpected happens.

Export and import management application configuration

You can export the current configuration of your Milestone Husky Management Application, either as a safety measure in order to have a backup file of your configuration, or as a clone allowing you to use a similar Management Application configuration elsewhere. You can, at a later time, import previously exported Management Application configurations.

Export Management Application configuration as backup

With this option, all relevant Milestone Husky Management Application configuration files are combined into one single .xml file, which you can specify a location for. Note that if there are unsaved changes to your configuration, these are automatically 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 are not using the exact same physical cameras, etc. even though your new system may otherwise be identical to your existing one.

Note that there is a difference between this Management Application configuration backup and the system configuration backup done from the Milestone Surveillance folder because these are two different things. The backup described here is limited to a backup of the Management Application configuration. The type of system configuration backup done from the Milestone Surveillance folder is

a backup of your entire surveillance system setup (including, among other things, log files, event configuration, restore points, view groups as well as the Management Application and XProtect Smart Client configuration).

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

Export Management Application configuration as clone

With this option, all relevant Milestone Husky Management Application configuration files are collected, and GUIDs (Globally Unique IDentifiers, unique 128-bit numbers used for identifying individual system components, such as cameras) are marked for later 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 does not use the exact same physical cameras as the cloned system. When you use the cloned configuration later in a new system, the GUIDs are replaced with GUIDs representing the specific components of the new system.

After you have marked GUIDs for replacement, the configuration files are combined into one single .xml file, which you can then save at a location specified by you. Note that if there are unsaved changes to your configuration, they are automatically 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 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 relevant 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 are asked whether you want to delete or keep recordings from affected devices. If you want to keep the recordings, note that they are not accessible until you add the affected devices to Milestone Husky again. Select the option you need, 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. Restarting the two services applies the imported Management Application configuration.

Import changes to configuration

It is possible to imported changes to a configuration. This can be relevant if installing many similar Milestone Husky systems, for example in a chain of shops where the same types of server, hardware devices, and cameras are used in each shop. In such cases, you can use an existing configuration—typically a cloned configuration (see "Export and import management application configuration" on page 199)—as a template for the other installations. However, since the shops' installations are not exactly the same (the hardware devices and cameras are of the same type, but they are not physically the same, and therefore they have different MAC addresses), there needs to be an easy way of importing changes to the template configuration.

This is why Milestone Husky lets you import changes about hardware devices and cameras as comma-separated values (CSV) from a file (see "Add hardware: Import from CSV file - CSV file format and requirements" on page 51):

1. From the menu bar, select **File** > **Import Changes to Configuration...**
2. Select **Online verification** if the new hardware devices and cameras listed in your CSV file are connected to the server and you want to verify that they can be reached.
3. Point to the CSV file, and click the **Import Configuration from File** button.

Restore system configuration from a restore point

Restore points allow you to return to a previous configuration state. Each time you apply a configuration change 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 you start the Management Application 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 you select to restore a configuration from a restore point, the configuration from the selected restore point is applied and used once the services are restarted (see Start and stop services (on page 178)).

If you have added new cameras or other devices to Milestone Husky after the restore point was created, they are missing if you load the restore point. This is because they were not in the system when the restore point was created. In such cases, you are 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.
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 are asked whether you want to delete or keep recordings from affected devices. If you keep the recordings, note that they are not be accessible until you add the affected devices to Milestone Husky again. Select the relevant 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.

Tip: When you select a restore point, you can see information about the configuration state at the selected point in time in the right part of the dialog. This can help you select the best possible restore point.

Misc concepts and tasks

About handling daylight saving time

Daylight saving time (DST, also known as summer time) is the practice of advancing clocks in order for evenings to have more daylight and mornings to have less. Typically, you move clocks forward one hour during the spring season and adjust them backward during the fall season. Note that use of DST varies between countries/regions.

When you work with a surveillance system, which is inherently time-sensitive, it is important that you 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 has 23 hours. In that case, there is no data between 02:00 and 03:00 in the morning since that hour, for that day, did not exist.

Fall: Switch from DST to Standard Time

When you switch from DST to standard time in the fall, you jump one hour back. Typically, the clock jumps backward from 02:00 DST to 01:00 standard time, repeating that hour, and the day 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, Milestone Husky 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 XProtect Smart Client by opening the archived database directly.

Improve stability with 3 GB virtual memory

Microsoft Windows 32-bit operating systems can address 4 GB of virtual memory. The operating system kernel reserves 2 GB for itself, and each individual running process is allowed to address another 2 GB. This is a default setting in Windows, and for the vast majority of Milestone Husky installations it works fine.

As from Milestone Husky, the main components of the server—the Recording Server service and the Image Server service—have been compiled with the LARGEADDRESSAWARE flag. This means you can optimize the memory usage of the Recording Server and Image Server services by configuring your 32-bit Windows operating system so that it restricts the kernel to 1 GB of memory, leaving 3 GB of address space for processes compiled with the LARGEADDRESSAWARE flag.

This should improve the stability of especially the Recording Server service by allowing it to exceed the previous 2 GB virtual memory limit, making it possible for it to use up to 3 GB of memory. The change in Windows configuration is known as 3 GB switching.

When is 3 GB switching relevant?

For very large system installations and/or for installations with many megapixel cameras, it can be relevant to change Windows settings so that only 1 GB of virtual memory is reserved for the operating system kernel, leaving 3 GB for running processes.

If you use the Windows default setting, with only 2 GB virtual memory reserved for running processes, the Recording Server service in very large installations of your system may:

- Behave erratically when it gets close to the 2 GB virtual memory limit. Symptoms can include database corruption, and client-server or camera-server communication errors.
- Become unstable and crash if it exceeds the 2 GB virtual memory limit. During such crashes, the code managing the surveillance system databases is not closed properly, and databases will become corrupt. In case of a crash, Windows will normally restart the Recording Server service. However, when the Recording Server service is restarted, one of its first tasks will be to repair the databases. The database repair process can in some cases take several hours, depending on the amount of data in the corrupted databases.

If you experience problems, making Windows use 3 GB for running processes is likely to solve the problems. If you have not experienced problems, but your Milestone Husky installation is very large and/or features many megapixel cameras, 3 GB switching can help prevent the problems from occurring.

The way to configure 32-bit Windows to be LARGEADDRESSAWARE depends on your type of Windows operating system. In the following, see a method that outlines Microsoft's recommended procedure for increasing the per-process memory limit to 3 GB if running Windows 2008 Server, Windows Vista Business, Windows Vista Enterprise or Windows Vista Ultimate.

3 GB switch on Windows 2008 Server or Windows Vista

1. Select **Start** > **All Programs** > **Accessories**, right-click **Command Prompt**, and select **Run as administrator**, then click **Continue**.
2. Enter the following command to add the 3 GB switch to the current operating system boot entry:

   ```
   BCDEDIT /SET INCREASEUSERVA 3072
   ```

   Where:

   - **USERVA** specifies an alternate amount of user-mode virtual address space for operating systems.
   - **3072** Specifies 3 GB (3072 MB).
3. Reboot after editing for the changes to take effect.

Remove the /3GB switch

1. Select **Start** > **All Programs** > **Accessories**, right-click **Command Prompt**, and select **Run as administrator**, then click **Continue**.
2. Enter the following command to remove the 3 GB switch from the current operating system boot entry:

   ```
   BCDEDIT /DELETEVALUE INCREASEUSERVA
   ```

3. Reboot after editing for the changes to take effect.

About protecting recording databases from corruption

In the Management Application, you can select which action to take if a camera database becomes corrupted. The actions include several database repair options. While being able to select such actions is highly valuable, it is of course even better to take steps to ensure that your camera databases do not become corrupted.

Power outages: use a UPS

The single-most common reason for corrupt databases is the recording server being shut down abruptly, without files being saved and without the operating system being closed down properly. This may happen due to power outages, due to somebody accidentally pulling out the server's power cable, or similar.

The best way of protecting your recording servers from being shut down abruptly is to equip each of your recording servers with a UPS (Uninterruptible Power Supply).

The UPS works as a battery-driven secondary power source, providing the necessary power for saving open files and safely powering down your system in the event of power irregularities. UPSs vary in sophistication, but many UPSs include software for automatically saving open files, for alerting system administrators, etc.

Selecting the right type of UPS for your organization's environment is an individual process. When you assess your needs, however, bear in mind the amount of runtime you 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 you end processes

When you work 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 is not be given the chance to save its state or data before it is terminated. This may lead to corrupt camera databases.

Windows Task Manager will typically display a warning if you attempt to end a process. Unless you are absolutely sure that ending the process is not going to affect the surveillance system, click **No** when the warning message asks you if you really want to terminate the process.

Hard disk failure: protect your drives

Hard disk drives are mechanical devices and 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 (on page 213))

- Static electricity (make sure you ground yourself if you are going to handle a hard disk drive).
- Fire, water, etc. (avoid)

Monitor storage space usage

To view how much storage space you have on your system—and not least how much of it is free—do the following:

1. In the Management Application's navigation pane, expand **Advanced Configuration**, and select **Cameras and Storage Information**.
2. View the **Storage Usage Summary** for information about, which drives are available, what drives are used for, the size of each drive, as well as how much video data, other data, and free space there is in each drive.

View video from cameras in Management Application

You can view live video from single cameras directly in the Management Application:

1. In the Management Application navigation pane, expand **Advanced Configuration**, and expand **Cameras and Storage Information**.
2. Select the relevant camera to view live video from that camera. Above the live video, you find a summary of the most important properties for the selected camera. Below the live video, you find information about the camera's resolution and average image file size. For cameras using MPEG or H.264, you 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 relevant camera. Especially three scenarios are important to consider:

- Some cameras supporting multistreaming may halve their frame rate or respond with other negative effects if you open a second stream.

- 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.

- Cameras that do not support multiple simultaneous video streams cannot connect to the surveillance server and the Management Application at the same time. Therefore, Milestone recommends that you stop (see "Start and stop services" on page 178) the Recording Server service when you configure such devices for motion detection and PTZ. See also View video from cameras in Management Application (on page 206).

Glossary of Terms

Symbols & Numeric

360 degrees panomorph support

Cameras with 360 degrees panomorph support offer—as the name indicates—360 degree coverage and can survey an entire area without blind spots or distorted images.

A

Analytics Events

Analytics events are data received from an external third-party video content analysis (VCA) provider. An example of a VCA-based system is an access control system. Analytics events integrates seamlessly with the **Alarms** feature.

API

Application Program Interface—set of tools and building blocks for creating or customizing software applications.

Aspect ratio

The height/width relationship of an image.

ATM

Automatic teller machine—machine that dispenses money when a personal coded card is used.

AVI

A popular file format for video. Files in this format carry the .avi file extension.

B

Browser

A software application for finding and displaying web pages.

C

Carousel

A feature for displaying video from several cameras, one after the other, in a single camera position. The required cameras and the intervals between changes are specified by the Milestone Husky administrator. The carousel feature is available, if configured, in the Smart Client.

Central

A product available as an add-on to Milestone Husky. XProtect Central provides a complete overview of status and alarms from any number of Milestone Husky servers, regardless of location.

Codec

A technology for compressing and decompressing audio and video data, for example, in an exported AVI file. MPEG and Indeo are examples of frequently used codecs.

CSV

Comma-separated values data format that stores tabular data, where the lines represent rows in a table and commas define the columns, in a simple file. For example, data about cameras may appear as comma-separated values in a .csv file, which can then be imported into Milestone Husky. A simple but effective method if setting up several similar systems.

D

Device

In Milestone Husky : a camera, video encoder, input device, or output device connected to a recording server.

DirectX

A Windows extension providing advanced multimedia capabilities.

DNS

Domain Name System—system allowing translation between alphabetic host names (for example, mycomputer) or domain names (for example, www.mydomain.com) and numeric IP addresses (for example, 192.168.212.2). Many people find alphabetic names easier to remember than numeric IP addresses.

Driver

A program used for controlling/communicating with a device.

DST

Daylight saving time: temporarily advancing of clocks during the summer so that afternoons have more daylight and mornings have less.

Dual stream

Some cameras support two independent streams (which can be sent to the recording server): one for live viewing and another for playback purposes. Each stream has its own resolution, encoding, and frame rate.

DVR

Digital video recorder—device that records video in a digital format to a hard disk drive embedded in the DVR itself.

E

Event Server

A server that stores and handles incoming alarm data and events from all Milestone Husky servers. The Event Server enables powerful monitoring and provides an instant overview of alarms and possible technical problems within your systems.

F

Fisheye

A type of lens that allows the creation and viewing of 360-degree images.

FPS

Frames per second—measurement indicating the amount of information contained in a motion video. Each frame represents a still image, but when frames are displayed in succession, the illusion of motion is created. The higher the FPS, the smoother the motion appears. Note, however, that a high FPS may also lead to a large file size when video is saved.

Frame rate

A measurement indicating the amount of information contained in motion video—typically measured in FPS.

FTP

File Transfer Protocol—standard for exchanging files across the internet. FTP uses the TCP/IP standards for data transfer and is often used for uploading or downloading files to and from servers.

G

Generic events

Milestone Husky can receive and analyze input in the form of TCP or UDP data packages which, if they match specified criteria, can be used to generate events. Such events are called generic events.

GOP

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

Grace period

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

GUID

Globally unique identifier—unique 128-bit number used to identify components on a Windows system.

H

H.264

A standard for compressing and decompressing video data (a codec). H.264 is a codec that compresses video more effectively than older codecs, and it provides more flexibility for use in a variety of network environments.

Hardware device

Technically speaking, cameras are not added to Milestone Husky, rather to hardware devices. This is because hardware devices have their own IP addresses or host names. Being IP-based, Milestone Husky primarily identifies units based on their IP addresses or host names. Even though each hardware device has its own IP address or host name, several cameras, microphones, and so on, can be attached to a single hardware device and share the same IP address or host name. This is typically the case with cameras attached to video encoder devices. Each camera, microphone, and so on, can be configured individually, even when several of them are attached to a single hardware device.

Host

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

Hotspot

Particular position for viewing enlarged and/or high quality video in the Smart Client.

HTTP

HyperText Transfer Protocol—standard for exchanging files across the internet. HTTP is the standard used for formatting and transmission of data on the World Wide Web.

I

I/O

Input/Output: refers to the communication between a computer and a person. Inputs are the signals or data received by the system and outputs are the signals or data sent from it.

I-frame

Short name for intra-frame. Used in the MPEG standard for digital video compression. An I-frame is a single frame stored at specified intervals. The I-frame records the entire view of the camera, whereas the frames that follow (P-frames) record only the pixels that change. This helps greatly reduce the size of MPEG files. An I-frame is similar to a keyframe.

Image Server

A service that handles access to Milestone Husky for remote users logging in with Smart Client The Image Server service does not require separate hardware as it runs in the background on the Milestone Husky server. The Image Server service is not configured separately as it is configured through Milestone Husky 's Management Application.

IP

Internet Protocol—protocol (or standard) specifying the format and addressing scheme

used for sending data packets across networks. IP is often combined with another protocol, TCP. The combination, known as TCP/IP, allows data packets to be sent back and forth between two points on a network for longer periods of time and is used when connecting computers and other devices on the internet.

IP address

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

IPIX

A technology that allows the creation and viewing of 360-degree panomorph (fisheye) images.

J

JPEG

(Also JPG) Joint Photographic Experts Group—widely used lossy compression technique for images.

K

Keyframe

Used in the MPEG standard for digital video compression, a keyframe is a single frame stored at specified intervals. The keyframe records the entire view of the camera, whereas the frames between the keyframes record only the pixels that change. This helps greatly reduce the size of MPEG files.

M

MAC address

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

Manual events

You can generate an event manually from the client. These events are called manual events.

Master/Slave

A setup of servers where one server (the master server) is of higher importance than the remaining servers (the slave servers). With a master/slave setup in Milestone Husky, it is possible to combine several Milestone Husky servers and extend the number of cameras you can use beyond the maximum allowed number of cameras for a single server. In such a setup, clients will still have a single point of contact: they connect to the master server but also get access, transparently, to cameras and recordings on the slave servers.

Matrix

A feature that enables the control of live camera views on remote computers for distributed viewing. Once configured, you can view Matrix-triggered live video in XProtect Smart Client.

Matrix recipient

A computer equipped with XProtect Smart Client software and therefore capable of displaying Matrix-triggered live video.

MJPEG

Motion JPEG—compressed video format where each frame is a separately compressed JPEG image. The method used is quite similar to the I-frame method used for MPEG, but no interframe prediction is used. This allows for somewhat easier editing, and makes compression independent of the amount of motion.

MPEG

Compression standards and file formats for digital video developed by the Moving Pictures Experts Group. MPEG standards use so-called lossy compression as they store only the changes between frames, removing often considerable amounts of redundant information. Keyframes stored at specified intervals record the entire view of the camera, whereas the frames that follow record only pixels that change. This helps greatly reduce the size of MPEG files.

N

NTLM

In a Windows network, NT LAN Manager is a network authentication protocol.

P

Panomorph

A type of lens that allows the creation and viewing of 360-degree images.

P-frame

Predictive frame—the MPEG standard for digital video compression uses P-frames together with I-frames. An I-frame, also known as a keyframe, is a single frame stored at specified intervals. The I-frame records the entire view of the camera, whereas the frames that follow (the P-frames) record only the pixels that change. This helps greatly reduce the size of MPEG files.

PIN

Personal identification number (or personal identity number)—number used to identify and authenticate users.

Ping

A computer network administration utility used to determine whether an IP address is available, by sending a small amount of data to see if it responds. The word ping was chosen because it mirrors the sound of a sonar. You send the ping command using a Windows command prompt.

Polling

Regularly checking the state of something, for example, whether input has been received on a particular input port of a device. The defined interval between such state checks is often called a polling frequency.

Port

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

POS

(Also PoS) Point of sale: the physical place where a sale is made, for example, at the cash register.

Post-recording

The ability to store recordings from periods following motion and/or specified events. Based on incoming video being buffered on the Milestone Husky server in case it is going to be needed for a motion- or event-triggered recording. Using post-recording can be highly advantageous: if, for example, you have defined that video should be recorded while a gate is open, being able to see what happens immediately after the gate is closed may also be important.

Pre-alarm

Pre-alarm images is a feature available for selected cameras only. It enables the sending of images from immediately before an event

took place from the camera to Milestone Husky via e-mail.

Pre-buffer

See the description of Pre-recording.

Pre-recording

The ability to store recordings from periods preceding detected motion and/or specified events. Based on incoming video being buffered on the Milestone Husky server in case it is going to be needed for a motion- or event-triggered recording. Using pre-recording can be highly advantageous: if, for example, you have defined that video should be recorded when a door is opened, being able to see what happened immediately prior to the door being opened may also be important.

Privacy masking

The ability to define if and how selected areas of a camera's view should be masked before distribution. For example, if a Milestone Husky camera films a street, you can mask certain areas of a building (for example, windows and doors) with privacy masking in order to protect residents' privacy.

PTZ

Pan-tilt-zoom. A highly movable and flexible type of camera.

PUK

Personal Unblocking Key or PIN Unlock Key—number used as an extra security measure for SIM cards.

R

Recording

On IP video surveillance systems, recording means **saving video and, if applicable, audio from a camera in the cameraâ€™s database on the surveillance system**. In many IP surveillance systems, all the video/audio received from cameras is not necessarily saved. Saving of video and audio in a cameraâ€™s database is in many cases started only when there is a reason to do so, for example, when motion is detected, when an event occurs, or when a specific period of time begins. Recording is then stopped after a specified amount of time, for example, when motion is no longer detected, when an event occurs, or when a time period ends. The term **recording** originates from the analog video era, when images were taped only when the record button was pressed.

Recording Server service

Windows service (without any user interface) used by Milestone Husky for recording and displaying video. Video is only transferred to the surveillance system while the Recording Server service is running.

Restore point

Restore points allow you to return to a previous configuration state. When a configuration change is applied in Milestone Husky, a restore point is created. If something goes wrong in your configuration, you can browse through restore points, and return to a suitable one.

S

SCS

A file extension (.scs) for a script type targeted at controlling clients.

SDK

Software Development Kit—programming package enabling software developers to create applications for use with a specific platform.

SIM

Subscriber identity module—circuit stored on a small card inserted into a mobile phone or computer, or other mobile device. The SIM

card is used to identify and authenticate the user.

SLC

Software license code—product registration code required for using the Milestone Husky software. If you do not have system administration responsibilities, you do not have to deal with SLCs. System administrators use SLCs when installing and registering the software.

SMS

Short Message Service or Systems Management Server.

1) Short Message Service, a system for sending text messages to mobile phones.

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

SMTP

Simple Mail Transfer Protocol—standard for sending e-mail messages between mail servers.

Subnet

A part of a network. Dividing a network into subnets can be advantageous for management and security reasons, and may in some cases also help improve performance. On TCP/IP-based networks, a subnet is basically a part of a network on which all devices share the same prefix in their IP addresses, for example 123.123.123.xxx, where the first three numbers (123.123.123) are the shared prefix. Network administrators use subnet masks to divide networks into subnets.

T

TCP

Transmission Control Protocol—protocol (or standard) used for sending data packets across networks. TCP is often combined with another protocol, IP (Internet Protocol). The combination, known as TCP/IP, allows data packets to be sent back and forth between two points on a network for longer periods of time, and is used when connecting computers and other devices on the internet.

TCP/IP

Transmission Control Protocol/Internet Protocol—combination of protocols (or standards) used when connecting computers and other devices on networks, including the internet.

Telnet

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

Transact

An add-on to Milestone Husky. XProtect Transact can help you prevent loss and shrinkage through video evidence combined with time-linked POS or ATM transaction data.

U

UDP

User Datagram Protocol—connectionless protocol for sending data packets across networks. Primarily used for broadcasting messages. UDP is a fairly simple protocol, with less error recovery features than, for example, the TCP protocol.

UPS

A UPS (Uninterruptible Power Supply) works as a battery-driven secondary power source, providing the necessary power for saving open

files and safely powering down your system in the event of power irregularities. UPSs vary in sophistication, but many UPSs include software for automatically saving open files, for alerting system administrators, etc.

URL

Uniform Resource Locator; an address of a resource on the World Wide Web. The first part of a URL specifies which protocol (or data communication standard) to use when accessing the resource, whereas the second part of the URL specifies the domain or IP address at which the resource is located. For example, www.milestonesys.com.

V

VCA

Video content analysis (VCA) is a system that detects various types of previously specified behavior, both of humans and vehicles. A VCA-based system provides third-party video content analysis, spanning from face recognition, over advanced motion detection, to complex behavioral analysis. VCA systems and their output can seamlessly be integrated with the **Alarms** feature and used for, for example, triggering alarms. Here, the events resulting from VCA systems are called analytics events.

Third-party VCA tools are developed by independent partners delivering solutions based on an a Milestone open platform. These solutions can impact performance on Milestone Husky.

Video encoder

A device, typically a standalone device, that can stream video from a number of connected client cameras. Video encoders contain image digitizers, making it possible to connect analog cameras to a network.

Video server

Another name for a video encoder.

View

In Milestone Husky, a collection of video from one or more cameras, presented together in the Smart Client. A view may include other content, such as HTML pages and static images, in addition to video from cameras.

VMD

Video motion detection. A way of defining activity in a scene by analyzing image data and the differences in a series of images.

W

Wizard

A utility to help perform a particular task quickly, while also ensuring coverage of all relevant parameters. For example, the **Adjust Motion Detection** wizard quickly helps you configure motion detection on each of Milestone Husky's cameras without the risk of forgetting to set any key parameters.

Index

Copyright, trademarks and disclaimer

Trademarks

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

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

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

Disclaimer

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

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

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

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

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

About Milestone Systems

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

www.milestonesys.com.